IKSP
Institut pro kriminologii
a sociální prevenci

Kateřina Kudrlová
Viktorie Paloušová
Jiří Vlach

Kyberkriminalita z pohledu justiční praxe a každodenních uživatelů

Praha 2023

Ediční řada Studie

Institut pro kriminologii a sociální prevenci Praha 2023

Kyberkriminalita z pohledu justiční praxe a každodenních uživatelů

Kateřina Kudrlová
Viktorie Paloušová
Jiří Vlach

Autorský kolektiv:
Mgr. Kateřina Kudrlová, Ph.D. (kapitoly I.1., I.2., I.4., I.5., III., IV., V., VII.5., VIII., Resumé)
Mgr. Viktorie Paloušová (kapitoly II.2., VII.1., VII.2., VII.3., VII.4., VII.6.)
Mgr. Jiří Vlach (kapitoly I.3., I.5., II.1., III.1., VI.)

Recenzenti:
prof. JUDr. Bc. Tomáš Gřivna, Ph.D. (Právnická fakulta UK, Katedra trestního práva)
prof. Ing. Vladimír Smejkal, CSc. (Fakulta podnikatelská VUT, Ústav informatiky)

Technická spolupráce:
Lucie Černá

Poděkování:
Autoři děkují v první řadě oběma recenzentům za cenné připomínky k rukopisu monografie. Zvláštní poděkování patří také pracovníkům soudů, které poskytly požadovaný spisový materiál, a to za jejich vstřícný přístup a ochotu ke spolupráci.

ISBN 978-80-7338-204-9

www.iksp.cz
www.kriminologie.cz

Obsah

I.

Úvodní část

I.1 Úvod

Lze si představit současnou moderní společnost bez digitálních technologií? Těžko. Prostupují každodenním životem stejně jako výjimečnými událostmi. Zajišťují komunikaci, usnadňují běžné činnosti, umožňují pokrok ve vědě atd. A také nabízí prostor pro zneužití a s nimi spojenou kyberkriminalitu, ať už si pod ní představíme cokoliv.

Nabízí se řada definic, více či méně přiléhavých. Jde o oblast velice širokou, která může při troše fantazie zahrnout většinu myslitelných oblastí, od intimity mezilidského vztahu po mezistátní konflikty. Přikláníme se proto k široké definici kyberkriminality jako kriminality zahrnující využití informačních technologií.[1] Pro jakýkoliv úspěšný pokus porozumět kyberkriminalitě je ovšem nezbytné vymezit si určitou její výseč a zaměřit se na dílčí oblasti. Jen tak lze proniknout hlouběji a hledat vhodné cesty prevence i mitigace.

Institut pro kriminologii a sociální prevenci (dále jen „IKSP") se věnoval kyberkriminalitě (resp. její výseči) v rámci samostatného výzkumného úkolu poprvé v letech 2016–2019.[2] Původní projekt se zaměřil na analýzu trestních spisů, v nichž byla podána obžaloba pro některý z počítačových trestných činů (§ 230–232 TZ) a trestní řízení pravomocně skončilo v roce 2015.[3] Na to navazuje současný výzkumný úkol, projekt Posouzení trendů kyberkriminality, řešený v letech 2020–2023.

Zjištěné poznatky z předchozího projektu sloužily jako hlavní zdroj inspirace připravovaného dotazníkového šetření zaměřeného na zkušenosti české internetové populace, jehož výsledky zde předkládáme. Neméně důležitým zdrojem byla rozsáhlá rešerše dostupných statistických údajů relevantních pro kyberkriminalitu s cílem zamezit zdvojení dostupných informací a zároveň prohloubit stávající poznání. Po schválení znění dotazníku vědeckou radou IKSP a výběrovém řízení na realizátora sběru dat proběhl tento v listopadu roku 2020.

Druhou část stávajícího projektu představuje pokračování analýzy trestních spisů, tentokrát již úžeji ohraničené na trestní věci pachatelů, kteří byli v roce 2019 pravomocně odsouzeni pro spáchání počítačového trestného činu.

Publikace se na úvod zamýšlí nad právní kvalifikací kriminality vůbec, poté nastiňuje projekt jako takový a použitou metodologii. Samotný obsah se pak věnuje nejprve poznatkům z analýzy trestních spisů, do jisté míry srovnatelným s poznatky z předchozího projektu. Následuje stěžejní část zaměřená na výsledky dotazníkového šetření, rozdělená do několika tematických oblastí. Nejprve jde o „vybavenost" – jaká zařízení se používají k přístupu na internet a jak jsou chráněna, jak a kde se uživatelé prezentují online a jestli se orientují i v méně běžné oblasti darkwebu. Pokračujeme malwarovou částí se zaměřením na ransomware a phishing. Poté se věnujeme podrobně nejběžnějším online účtům – e-mailům, profilům na sociálních sítích, e-bankingu a herním účtům. Tím ovšem výčet

1 Blíže k definicím kyberkriminality viz např. publikaci vydanou v souvislosti s předchozím výzkumným úkolem IKSP (Vlach et al., 2020, str. 12).

2 Do té doby šlo pouze o dílčí publikace v rámci jiných projektů.

3 Projekt zahrnul např. i několik rozhovorů s experty. Informace o jeho průběhu i zjištěné poznatky jsou dostupné online (Vlach et al., 2020).

nekončí, publikace pokračuje zkušenostmi respondentů s obchodováním online (nákup i prodej), porušováním autorských práv a specifickou oblastí zaměstnanců coby rizikového faktoru pro zaměstnavatele. Závěrečné kapitoly obsahují poznatky o pachatelích vůbec, o obětech, rozlišení virtuálního násilí a majetkového zájmu v námi sledovaných oblastech a o tom, jakým způsobem respondenti reagovali na nastalé incidenty včetně toho, do jaké míry se obracejí na policii, potažmo do jaké míry můžeme hovořit o latentní kriminalitě. Některé z kapitol zakončuje závěrečná podkapitola shrnující určitý celek.

Na projektu pracoval kolektiv řešitelů vedený odpovědnou řešitelkou Mgr. Kateřinou Kudrlovou, Ph.D. Jako řešitelé se podíleli Mgr. Viktorie Paloušová, Mgr. Jiří Vlach a po jistou dobu též Mgr. Lukáš Kutil. Většina z řešitelů je autorem několika kapitol, případně ve spoluautorství s jiným řešitelem. Z toho důvodu se některé kapitoly odlišují způsobem zpracování odpovídajícím zaměření (zejména právo a/nebo sociologie) a stylu svých autorů.

I.2 Několik slov k problematické právní kvalifikaci § 230 odst. 1 TZ[4]

Při právní kvalifikaci kyberkriminality přichází na mysl samozřejmě na prvním místě tzv. počítačové trestné činy, tedy § 230–232 TZ: neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací (§ 230 TZ), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ) a neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti (§ 232 TZ). Kromě počítačových trestných činů ovšem dopadá na kyberkriminalitu i řada dalších skutkových podstat (Kudrlová, 2019, s. 84), jejichž aplikaci v kyberprostředí zevrubně nastiňuje např. prof. Smejkal (Smejkal, 2022).

Zaměřme se ovšem na ony počítačové trestné činy, resp. § 230 TZ (neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací), neboť z hlediska používané právní kvalifikace přichází ke slovu zbývající dva počítačové trestné činy jen sporadicky. V článku publikovaném v časopise Kriminalistika jsme se pokusili ukázat, že stávající formulace skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 1 TZ neodpovídá přiměřeně současné sociální realitě (Kudrlová & Vlach, 2023). Následující text vychází z uvedeného článku.

Inspirací, resp. závazkem ke stávající formulaci počítačových trestných činů se stala Úmluva Rady Evropy o počítačové kriminalitě (dále jen Úmluva).[5] Právě na ni odkazuje i důvodová zpráva k návrhu nového TZ, která se k počítačovým trestným činům (tehdy § 228–230 namísto současných § 230–232 TZ) vyjadřuje poměrně stroze, neboť pouze poukazuje na závazky plynoucí z Úmluvy, zejména její články 2–11 (Vláda ČR, 2008).

Úmluva vymezuje patero jednání, které se signatářské státy zavázaly kriminalizovat: protiprávní přístup (§ 230 odst. 1 TZ), neoprávněný zásah do dat nebo počítačového sys-

4 Projekt zahrnul např. i několik rozhovorů s experty. Informace o jeho průběhu i zjištěné poznatky jsou dostupné online (Vlach et al., 2020). Obsah kapitoly vychází z publikovaného článku (Kudrlová & Vlach, 2023).

5 Convention on Cybercrime, ETS No. 185. Úmluva vznikla na půdě Rady Evropy v roce 2001 a vstoupila v účinnost 1. 7. 2004, ČR ji podepsala 9. února 2005 a ratifikovala 22. srpna 2013.

tému [§ 230 odst. 2 písm. a), b), d) TZ], falšování údajů související s počítači [§ 230 odst. 2 písm. c) TZ], podvod související s počítači [§ 230 odst. 3 písm. a) TZ] a neoprávněný zásah do systému [§ 230 odst. 3 písm. b) TZ] (Šámal et al., 2012; Smejkal, 2022; Gřivna & Polčák, 2008; Kudrlová, 2019). Pro znění § 230 odst. 1 TZ je v rámci Úmluvy klíčový požadavek kriminalizace neoprávněného přístupu do počítačového systému nebo jeho části dle čl. 2. Signatářské státy mohou přitom podmínit trestnost jednání např. překonáním bezpečnostních opatření, což ČR činí.

ČR zavazovalo k postihu protiprávního přístupu i Rámcové rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům, které požadovalo v čl. 2 kriminalizaci protiprávního přístupu k informačním systémům [čl. 1 písm. a), d) a čl. 2, odpovídajícím ustanovením je v českém právním řádu § 230 odst. 1 TZ]. Podobně jako v případě Úmluvy, signatářské státy mohly podmínit trestnost překonáním překážky (čl. 2 odst. 2). Toto rámcové rozhodnutí bylo s účinností od 3. září 2013 nahrazeno směrnicí Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (dále jen Směrnice). Závazek kriminalizace neoprávněného přístupu k informačním systémům obsahuje čl. 3, přičemž porušení bezpečnostního opatření je zde již výslovně uvedeno jako podmínka trestnosti. Úmluva, původní rámcové rozhodnutí i Směrnice hovoří i o pokusu a účastenství, nicméně systém trestního práva ČR v tomto směru nevyvolává potřebu další pozornosti v tomto směru.[6]

I.2.1 Nezákonnost neoprávněných přístupů de lege lata

Trestný čin neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací skrývá dvě skutkové podstaty (Šámal et al., 2016, s. 696), první z nich ve znění „*kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán (…).*“ Dopadá tedy na jakýkoliv neoprávněný přístup k počítačovému systému za předpokladu překonání bezpečnostního opatření, jehož smyslem je přístup omezit (Šámal et al., 2012, s. 2305). Není přitom třeba, aby pachatel učinil cokoliv dalšího (typicky manipuloval s daty).[7]

Objektivní stránku této skutkové podstaty pachatel nezřídka naplní v rámci přípravy k dalšímu jednání, a to především v podobě neoprávněné manipulace s daty, které již naplňuje objektivní stránku druhé základní skutkové podstaty neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 2 TZ. V takovém případě již samotná (ne)oprávněnost přístupu nehraje roli. Lze si představit kombinaci oprávněného přístupu s neoprávněnou manipulací s daty (např. administrátor spravující firemní síť v rámci pracovněprávních povinností, jenž záměrně a neoprávněně vloží do jím spravované databáze nesprávný obsah). Neoprávněná manipulace s daty ovšem může snadno následovat po neoprávněném přístupu (pachatel např. po překonání hesla smaže ze žárlivosti partnerce obsah e-mailové schránky). V této variantě však bude první základní skutková podstata (neoprávněný přístup) pravděpo-

6 Pro podrobnější informace k mezinárodněprávním dokumentům, zavazujícím ČR k postihu kyberkriminality, viz např. Jelínek et al. (2015, s. 285).

7 To potvrzuje i judikát Nejvyššího soudu z 29. 11. 2017 ve věci 7 Tdo 1469/2017.

dobně (nikoliv však nutně) fakticky konzumována (Kudrlová, 2019; Smejkal, 2022). Setkat se lze i se samotným neoprávněným přístupem bez navazujícího jednání (např. pachatel pronikne do školního informačního systému, kde si pouze prohlíží klasifikaci, aniž by s jejím obsahem jakkoli manipuloval).

Z hlediska subjektivní stránky vyžadují obě základní skutkové podstaty § 230 TZ úmyslné zavinění. U kvalifikovaných skutkových podstat se úmysl vyžaduje pro naplnění skutkové podstaty dle § 230 odst. 3 písm. a) i b) TZ, stejně tak dle § 230 odst. 4 písm. a) TZ (vyplývá z povahy věci), ve všech ostatních případech postačí nedbalostní zavinění okolnosti zvlášť přitěžující, zde vždy v podobě těžšího následku [srov. § 17 písm. a) TZ a § 230 odst. 4 písm. b), c), d) a e), odst. 5 TZ]. Všechny tři počítačové trestné činy jsou zařazeny v rámci hlavy páté TZ. Kromě kvalifikované skutkové podstaty dle § 230 odst. 1 a/nebo 2, odst. 5 TZ, kdy jde o zločin, se jedná o přečiny (srov. § 14 odst. 2 a 3 TZ).

Objektem počítačových trestných činů (§ 230–232 TZ) je „zájem na ochraně počítačových systémů a jejich částí, dále dat v nich uložených a dat uložených na nosičích informací a také na ochraně počítačů nebo jiných technických zařízení pro zpracování dat před neoprávněnými přístupy a zásahy" (Šámal et al., 2016, s. 695). Roli zde proto hraje na jedné straně bezpečnost samotných zařízení, na straně druhé bezpečnost informací a dat – jejich důvěrnost, integrita a dostupnost, jak říká zákon o kybernetické bezpečnosti [§ 2 písm. c) zák. č. 181/2014 Sb.]. Přidáme-li údaje dostupné prostřednictvím e-bankingu, může jít zároveň o finanční stránku (např. zneužitelnost informací o finančních transakcích uživatele)[8] i soukromí uživatele (osobnostní stránka). Ta vystupuje do popředí zvlášť palčivě v případě narušování soukromí prostřednictvím neoprávněných vstupů na profily na sociálních sítích, na něž bývá mnohdy navázána významná část sociálních kontaktů uživatele (Kudrlová, 2019).[9]

I.2.2 Překonání překážky a svolení poškozeného

Neoprávněného přístupu předpokládaného prvním odstavcem § 230 TZ se dopustí, „*kdo překoná **bezpečnostní opatření**, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části (…).*" Překonání bezpečnostního opatření je klíčové, úroveň zabezpečení však není rozhodující – stačí existence jakéhokoliv bezpečnostního opatření. Základním opatřením, majícím za úkol zabránit zejména malwarovým útokům na samotné fyzické zařízení (hardware) či jeho programové vybavení (software), je v současnosti firewall, obvykle též zároveň doplněný o antivirový ochranný software, případně antispyware.[10] Pachatel si ani nemusí být bezpečnostních opatření zcela vědom (např. má jen jakousi představu, že cílené zařízení používá nějaký antivirus). Druhým stupněm ochrany, tentokrát obsahu či přístupu, je především heslo, bez ohledu na jeho snadnou prolomitelnost (např. heslo „12345") či naopak sílu (např. kombinace nejméně osmi různých znaků atp.).[11]

8 Nemluvě o případných neoprávněných finančních transakcích a jiných aktivitách.

9 Blíže k tomu viz kapitola Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily.

10 Malware znamená škodlivý software, antivirus ochranný software sloužící k detekci a eliminaci malwaru. Antispyware se zaměřuje na sledovací malware a může i nemusí být součástí antiviru.

11 Nutno zdůraznit, že zde hovoříme o právním posouzení naplnění skutkové podstaty. Z hlediska reálné ochrany heslem nemají snadno uhodnutelná hesla prakticky žádný účinek (Smejkal, 2022, str. 667).

V judikátu z roku 2020 konstatuje Nejvyšší soud nevýznamnost způsobu překonání hesla či jiného bezpečnostního opatření: „*Facebook je v podstatě virtuální prostor a má podobnou povahu jako „obydlí", jehož „dveře" tvoří počítačový systém, či jiný nosič informací, přičemž „klíčem" k těmto „dveřím" je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí,* ***a to i za pomoci shodného klíče, aniž by pachatel musel dveře do domu prolamovat násilím****. Obdobně je tedy nutno postihovat případy, kdy pachatel prolomí* ***„dveře" do virtuálního prostoru například za pomoci hesla, které znal z dřívější doby****, či za pomoci telefonního čísla, na který jsou tyto soukromé účty navázány. Rozhodující je – obdobně jako u porušování domovní svobody – že* ***v okamžiku, kdy pachatel tohoto způsobu narušení soukromí využívá, ví, že do toho důvěrného prostoru vstupuje neoprávněně****, a je s tímto následkem přinejmenším srozuměn. Za překonání „bezpečnostního opatření" ve smyslu § 230 odst. 1 trestního zákoníku je proto možno považovat i využití duplikátu telefonní SIM karty, na kterou jsou tyto soukromé účty vázány, s jejímž využitím lze do důvěrného prostoru vstupovat přímo, nebo za pomoci nově vygenerovaných hesel.*"[12] Překonáním bezpečnostní překážky předpokládané § 230 odst. 1 TZ bude proto i využití např. hesla uloženého v zařízení, poznamenaného na papírku, sděleného obětí za jiným účelem atp.

Častá praxe zneužívání hesel, která pachatelům sdělily samy oběti, vzbuzuje pochybnosti ohledně protiprávnosti jednání s ohledem na institut svolení poškozeného (§ 30 TZ). Svolení musí být dáno osobou oprávněnou, dobrovolně, určitě, vážně a srozumitelně. Může být dáno i následně jako důvodně předpokládaný a následně udělený souhlas. K jeho aplikaci se ovšem váží jistá úskalí, v první řadě z hlediska dobrovolnosti, určitosti, vážnosti a srozumitelnosti svolení. V praxi by neměly vznikat větší pochybnosti, neboť dotčené osoby[13] zpravidla reagují na zjištěný neoprávněný přístup ke svému online účtu jednoznačně (změna přístupových údajů, podání trestního oznámení aj.), kdy je nesouhlas zřejmý. Anebo nereagují vůbec, což lze považovat za konkludentní, dostačující souhlas (Šámal et al., 2012, s. 424). Problém nastává, když se dotčená osoba o neoprávněném přístupu ke svému účtu nedozví (pachatel si např. pouze prohlédne obsah) – v takovém případě nelze o souhlasu poškozeného vůbec uvažovat (resp. o jeho následném udělení).

Jiná situace nastává při použití cizích přístupových údajů k e-bankingu, neboť banky zpravidla smluvně stanovují prostřednictvím všeobecných obchodních podmínek přístup ke svým službám pouze na základě smlouvy či písemného zmocnění. Přístup neoprávněné osoby, resp. poskytnutí přístupových údajů, se tak dotýká nejen majitele účtu, ale i provozující banky, která předpokládá přístup ke svým službám pouze ze strany daného klienta (či disponenta nebo zmocněnce). Zvlášť pak ve spojení s tzv. identitou občana,

12 Viz rozhodnutí Nejvyššího soudu ze 4. 11. 2020 ve věci 7 Tdo 1134/2020.

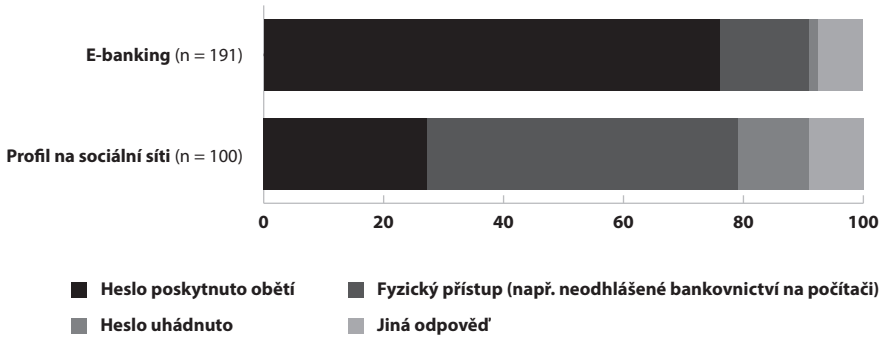
13 K problematickému označení dotčených osob za „poškozené" v případě uplatnění institutu svolení poškozeného viz např. (Klapal, 2005, s. 259).

tedy když banka potvrzuje tzv. bankovní identitu svého klienta pro účely komunikace se státními orgány.[14] Neoprávněně přistupující osoba by tak mohla jednat v omylu ohledně oprávněnosti majitele účtu udělit bez dalšího souhlas s jeho použitím.

I.2.3 De lege ferenda

Stávající právní úprava postihuje jakýkoliv neoprávněný přístup k online účtu, ať už půjde o e-banking, profil na sociální síti, e-mail či jiný účet. I v případě, že pachatel „má klíč" (typicky zná heslo), na neoprávněnosti přístupu po překonání překážky to nic nemění, a to zejména u soukromého prostoru či obsahu.[15]

Graf 1: Získání přístupu k napadenému účtu podle útočníků (%)



Každodenní praxe[16] však naznačuje relativně časté dobrovolné sdílení přihlašovacích údajů, včetně přístupu k e-bankingu Zároveň řada uživatelů sama neoprávněně používá cizí online účty (i kdyby šlo o „pouhé" prohlédnutí obsahu ze zvědavosti, tj. zásah do soukromí), přičemž část z nich si není vůbec vědoma protiprávnosti svého jednání.[17]

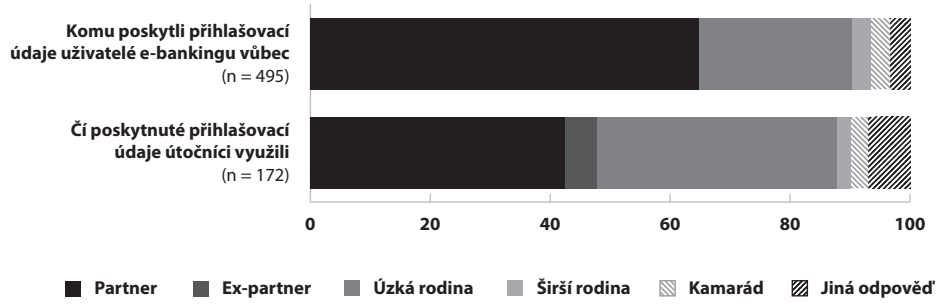
14 Vytrácí se tak společenská prospěšnost institutu svolení poškozeného spočívající v odpadnutí zájmu na stíhání odsouhlaseného jednání, viz např. Lukášová (2019, s. 60) – převažuje ji zájem na ochraně důvěrnosti a autenticitě komunikace mezi státem a obyvateli.

15 V případě soukromého profilu na sociální síti, e-mailu či e-bankingu bývá soukromý obsah zřejmý (i veřejně přístupný profil na sociální síti k sobě může mít např. navázané soukromé zprávy). Nelze však zároveň pominout, že samotná existence bezpečnostního opatření nemusí vyjadřovat soukromý charakter chráněného prostoru, ale pouze splňovat základní podmínky kladené na uživatele dané služby (není např. možné používat e-banking bez ochrany přístupu).

16 Blíže k tomu viz kapitoly E-mail a E-banking.

17 Domněnka vychází z analýzy trestních spisů, rozhovorů s experty i řady kurzů bezpečného chování online vedených autorkou.

Graf 2: Sdílení přihlašovacích údajů k e-bankingu (%)



Jeví se, že právní norma vtělená do § 230 odst. 1 TZ neodpovídá zcela sociální realitě. V řadě případů jde o jednání, které často z pozice aktérů na obou stranách, ale ani z pozice přihlížejících není vůbec chápáno jako protiprávní, natož trestné. Oběti si navíc ani nemusí přát trestněprávní postih útočníka, třeba z důvodu přetrvávajícího vztahu, absenci negativních dopadů atp.[18] Koneckonců latence neoprávněných přístupů je vysoká – na policii[19] se v roce 2020*[20] obrátilo kvůli neoprávněnému přístupu do jejich e-bankingu pouhých 15 % napadených respondentů, v případě účtů na sociálních sítích to bylo dokonce jen 5 %.[21]

Některé oblasti kyberkriminality vyžadují značné úsilí ze strany (všech) orgánů činných v trestním řízení k jejímu odhalení, vyšetření a odsouzení. Přitom „řešení" daného jednání samotným napadeným uživatelem může být výrazně rychlejší, efektivnější i preventivní. Sám zákonodárce navíc uvádí jako jediný důvod stávající právní úpravy mezinárodní závazky (Vláda ČR, 2008). Za zamyšlení proto stojí jiný přístup.

18 Ilustrací budiž nizozemský projekt zabývající se šířením intimních snímků mladých obětí bez jejich souhlasu. Mimo jiné se zde ukázalo, že oběti by daly před trestní sankcí pachatele přednost uložení mu povinnosti absolvovat osvětový kurz zaměřený na dopady daného jednání na oběti. Blíže k metodologii výzkumu a jeho výsledkům viz projekt @ntidote a program 3. dne (22. listopadu 2022) konference Human Factor in Cybercrime (2022), abstrakt vystoupení A., Gilen, C. Van de Heyning a M. Walrave – The non-consensual dissemination of intimate images (NCII): victims' rationales behind not reporting this crime and their perspective on how to legally conserve NCII. Viz BELSPO BRAIN-be 2.0 [cit. 2023-01-26]. @ntidote. Dostupné z <https://www.antidoteproject.be> a HFC conference (2022) [cit. 2023-01-08]. HFC conference. Dostupné z: < https://www.hfc-conference.com>.

19 Předpokládáme, že šlo o kontaktování Policie ČR, nicméně respondenti volili odpověď ve znění „Nahlásil/a jsem to policii," abychom se vyhnuli případnému zmatení respondentů při rozlišování Policie ČR či policejních orgánů dle trestního řádu a obecní/městské policie.

20 K přesnému vymezení sledovaného období viz kapitola Realizace dotazníkového šetření.

21 Blíže k tomu viz kapitola Latence a důvěra ve schopnosti policie a příslušné části jednotlivých kapitol. Několik dílčích poznatků ohledně latence různých typů online útoků je dostupných také prostřednictvím tiskové zprávy ze zasedání Republikového výboru pro prevenci kriminality z května roku 2021, příloha 1 – Kybernetická kriminalita v ČR z kriminologické perspektivy – IKSP, s. 5, viz MINISTERSTVO VNITRA ČESKÉ REPUBLIKY [cit. 2023-01-08]. Tisková zpráva ze zasedání Republikového výboru pro prevenci kriminality. Květen 2021. Dostupné z: <https://www.mvcr.cz/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci--kriminality-713175.aspx>.

I.2.4 Částečná dekriminalizace

Nabízí se legislativní úprava § 230 odst. 1 TZ – částečná dekriminalizace (ovšem pouze první, nikoliv druhé základní skutkové podstaty uvedené v odst. 2 § 230 TZ), byť v rámci úzkého prostoru vymezeného mezinárodními závazky.

Úmluva vyžaduje v článku 2 kriminalizaci úmyslného neoprávněného přístupu (k počítačovému systému nebo jeho části). Trestnost lze podmínit porušením bezpečnostních opatření, úmyslem získat počítačová data nebo jiným nečestným úmyslem, nebo jednáním ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.[22]

Úmluva – článek 2 – Nezákonný přístup

(…) aby (…) byl trestným činem, pokud je spáchán úmyslně, neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán porušením bezpečnostních opatření, s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.

Stávající právní úprava § 230 odst. 1 TZ zmiňuje toliko překonání bezpečnostních opatření. V úvahu proto připadá vložení dalšího znaku subjektivní a/nebo objektivní stránky. Tím by mohl být např. „úmysl získat počítačová data nebo jiný nečestný úmysl", tedy znění např. „*Kdo překoná bezpečnostní opatření* ***s úmyslem získat počítačová data nebo s jiným nečestným úmyslem****, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán (…).*" Zjevně by tak i samotný úmysl získat počítačová data musel být nečestný (srov. „nebo s jiným nečestným úmyslem"), což by vyloučilo řadu jednání se spornou (ne)oprávněností – např. sledování facebookového profilu rodiči.[23] V úvahu dále dle Úmluvy přichází i spojení napadeného počítačového systému nebo jeho části s jiným počítačovým systémem, které by ovšem kýženou míru dekriminalizace zřejmě nepřineslo.

Mírnější přístup oproti Úmluvě zastává směrnice, která jednak vyžaduje pro kriminalizaci neoprávněného přístupu kumulativní splnění podmínky úmyslu a porušení bezpečnostního opatření, jednak nepožaduje kriminalizaci méně závažných případů. V čl. 2 písm. d) uvádí definici „neoprávněného" jednání, včetně přístupu nepovoleného majitelem (či jiným držitelem práv k systému nebo k jeho části), a v čl. 3 upravuje regulaci neoprávněného přístupu.

Směrnice – článek 3 – Neoprávněný přístup k informačním systémům

(…) aby (…) je-li spáchán úmyslně, byl trestným činem, je-li tím porušeno bezpečnostní opatření, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

22 Úmluva výraz „neoprávněný přístup" blíže nespecifikuje.

23 Nutno ovšem podotknout, že v souladu s čl. 40 Úmluvy by musela být uvedená specifikace úmyslu písemně oznámena generálnímu tajemníkovi Rady Evropy již při podpisu nebo při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přístupu.

Při dodržení mezinárodních závazků by tak bylo možno upravit znění skutkové podstaty v § 230 odst. 1 TZ tak, aby nedopadalo na úmyslný neoprávněný přístup k počítačovému systému (či nosiči informací) či jeho části, při němž sice bylo porušeno bezpečnostní opatření, ale je méně závažný a chybí u něj nečestný úmysl (včetně získání počítačových dat s nečestným úmyslem). Zamyslet se lze ovšem i nad jazykovými konotacemi použitých výrazů, a to např. výkladem slova „**získat** počítačová data" nebo především nahrazení „**překonání** bezpečnostního opatření" jeho „**porušením**", které by mohlo alespoň částečně zmírnit dopad trestněprávní regulace.[24] Z procesního hlediska se pak nabízí na prvním místě zařazení § 230 odst. 1 TZ mezi trestné činy, pro které lze zahájit a v již zahájeném trestním stíhání pokračovat pouze se souhlasem poškozeného dle § 163 odst. 1 zák. č. 141/1961 Sb., trestní řád (dále jen TŘ).[25]

I.2.5 Závěr k několika slovům k problematické právní kvalifikaci § 230 odst. 1 TZ

Na kyberkriminalitu dopadá řada skutkových podstat, nicméně § 230 TZ patří nepochybně k těm významnějším. Formulace základní skutkové podstaty dle § 230 odst. 1 TZ nicméně není zcela přiléhavá sociální realitě. Mimo jiné proto, že z hlediska výkladu i judikatury se vztahuje také na neoprávněný přístup k online účtu chráněnému heslem, včetně případů, kdy pachatel heslo zná.

Některá jednání, zde konkrétně část neoprávněných přístupů k online účtům, by však bylo možné (a žádoucí) částečně dekriminalizovat, a to v souladu s mezinárodními závazky (Úmluvou a Směrnicí). Upravené znění § 230 odst. 1 TZ by mohlo být např. na „*Kdo **poruší** bezpečnostní opatření **s úmyslem získat počítačová data nebo s jiným nečestným úmyslem**, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán (…).*"

I.3 Vývoj registrované počítačové kriminality v ČR v letech 2015–2022

Resortní statistiky Ministerstva vnitra (policejní statistiky) a Ministerstva spravedlnosti (justiční statistiky) představují významný zdroj informací o stavu kybernetické kriminality v ČR.[26] Zatímco policejní statistiky sledují počítačové trestné činy pod společnou taktickou-statistickou klasifikací č. 865,[27] justiční statistiky jsou vedeny pro jednotlivé skutkové podstaty dle § 230–232 TZ samostatně.

24 Sluší se ovšem upozornit, že „porušení" by v takovém případě mohlo být vykládáno jako vyvolání trvalého následku oproti jednorázovému, překonání", a tedy představovat ve svém důsledku větší než žádoucí míru dekriminalizace.

25 K podrobnostem zejména ohledně dekriminalizace odkazujeme na původní článek (Kudrlová & Vlach, 2023).

26 Tyto statistiky vypovídají o stavu registrované kriminality, a je tak třeba mít na paměti předpokládanou vysokou míru latence u trestné činnosti páchané v kyberprostoru.

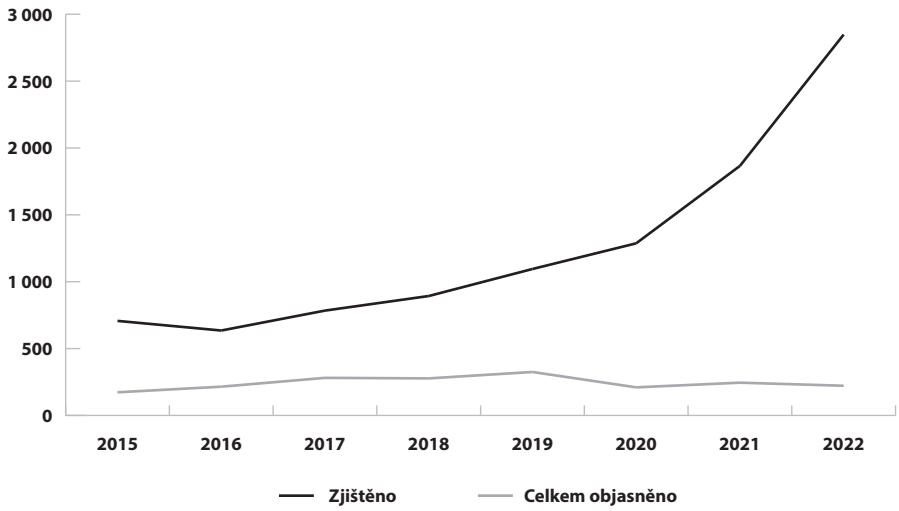
27 TSK č. 865 – poškození a zneužití záznamu na nosiči informací, respektive od r. 2021 neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla.

Tabulka 1: Přehled statistických údajů o skutcích dle § 230–232 TZ (§ 257a sTZ)[28]

Rok	Zjištěno	Objasněno	Míra objasněnosti (%)	Stíháno	Obžalováno	Odsouzeno
2015	707	144	20	167	113	51
2016	638	157	25	184	127	73
2017	784	206	26	176	116	111
2018	893	231	26	189	123	173
2019	1 096	208	19	185	139	146
2020	1 287	155	12	200	148	119
2021	1 866	158	8	221	153	148
2022	2 848	127	5	246	195	139

Na základě policejních statistik je zřejmé, že nárůst počtu registrovaných případů poškození a zneužití záznamu na nosiči informací v letech 2015–2022 vykazuje výrazněji vzrůstající trend oproti předchozímu období.[29] Výjimku v tomto trendu představuje pouze rok 2016, kdy byl naopak zaznamenán meziroční pokles o 72 případů (tj. o 10 %). Největší meziroční nárůst byl zaznamenán v roce 2022, kdy bylo oproti předchozímu roku registrováno o 982 případů více (tj. o 53 % více). V roce 2021 byl registrován 45% nárůst oproti roku 2020 (tj. o 579 případů více). Průměrná míra celkové objasněnosti činila ve zmíněném období 24 %, přičemž od roku 2017 (kdy činila 36 %) vykazuje setrvale klesající trend a v roce 2022 byla již jen 8 %. Vývoj počtu registrovaných skutků dle § 230–232 TZ a jejich objasněnosti je přehledně ilustrován následujícím grafem (Graf 3).

Graf 3: Vývoj počtu registrovaných skutků poškození a zneužití záznamu na nosiči informací v letech 2015–2022 dle statistik MV

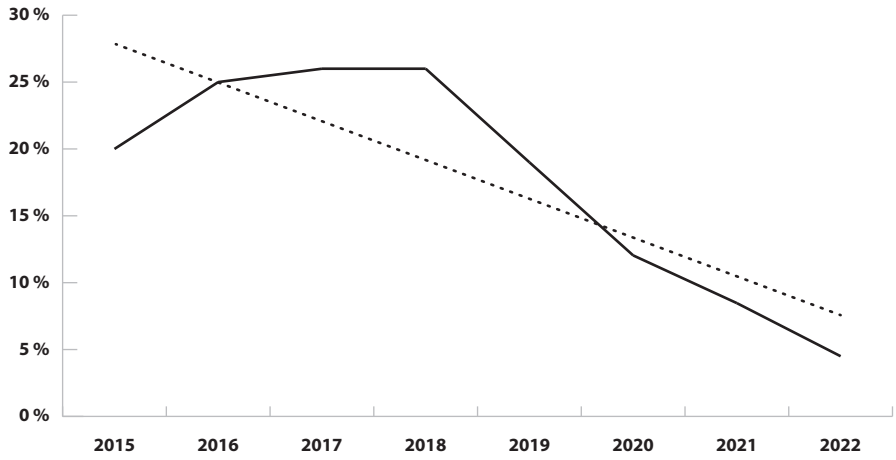


28 Údaje byly čerpány ze Statistických přehledů kriminality (Policie ČR) a přehledů vytvořených v systému CSLAV (Ministerstvo spravedlnosti). Zahrnují jednak stávající počítačové trestné činy, jednak trestný čin poškození a zneužití záznamu na nosiči informací dle zák. č. 140/1961 Sb., trestní zákon.

29 Srov. např. Vlach et al. (2020, s. 18).

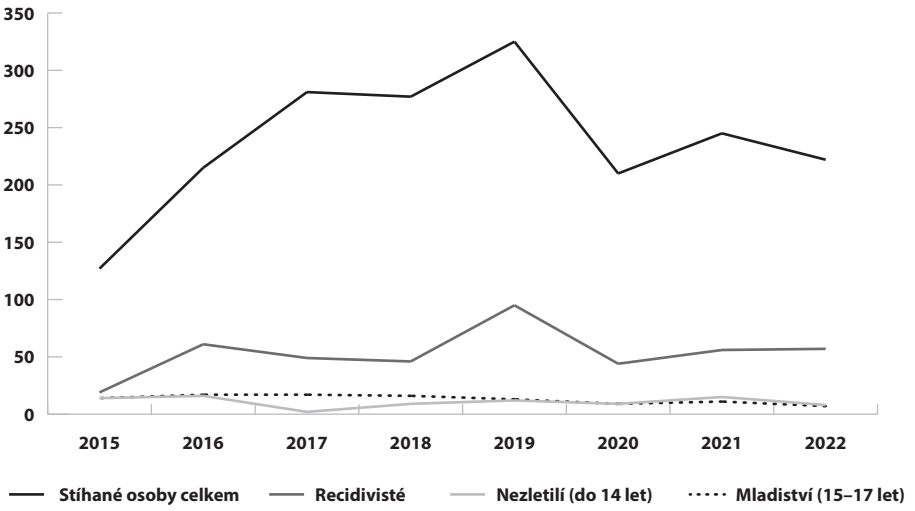
Naproti tomu míra objasněnosti těchto skutků vykazuje v období let 2015 až 2018 převážně stoupající trend. V následujícím období do roku 2022 však již dochází pouze k jejímu poklesu (Tabulka 1, Graf 4).

Graf 4: Míra objasněnosti skutků dle § 230-232 TZ v letech 2015–2022



Statistiky prezentované Ministerstvem vnitra (dále jen „MV“) též skýtají údaje o osobách, které spáchaly objasněné skutky dle § 230–232 TZ. V letech 2015–2022 vykazoval celkový počet osob stíhaných pro tyto skutky vzrůstající trend. Pouze v roce 2020 došlo oproti předchozímu roku k výraznému poklesu – tj. oproti 325 osobám v roce 2019 byl zaznamenán 35% pokles na 210 osob v roce následujícím. Recidivisté se na páchání zmíněných skutků podíleli ve sledovaném období v průměru 22 %, přičemž největšího podílu dosáhli v roce 2019, kdy činil 29 %. Nezletilí do 14 let se průměrně na páchání podíleli pouze 5 % a mladiství (od 15 do 17 let) 6 %. U obou věkových skupin mladších 18 let byl v letech 2015–2022 navíc zřejmý mírně klesající trend. Od roku 2017 již resortní statistiky MV nerozlišují pohlaví, nicméně v roce 2016 činil podíl žen na páchání uvedených skutků 28 % (Graf 5).

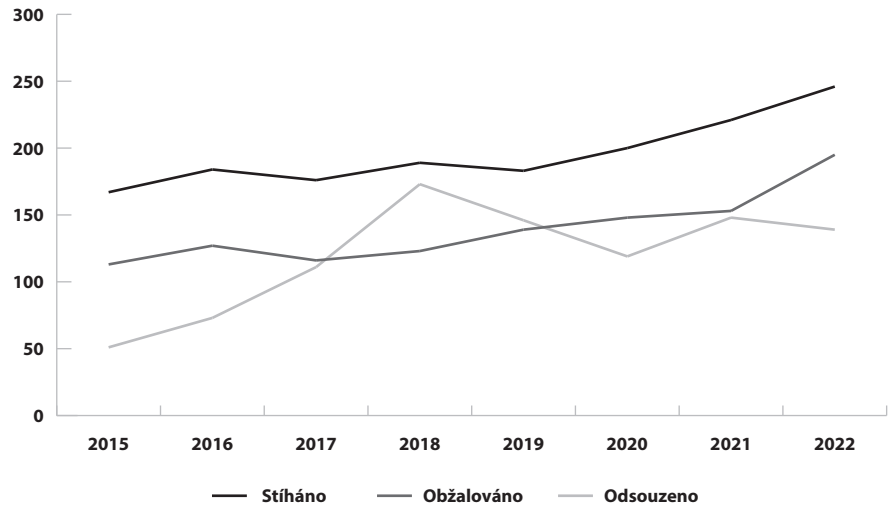
Graf 5: Vývoj počtu osob stíhaných pro poškození a zneužití záznamu na nosiči informací v letech 2015–2022 dle statistik MV



Neméně přínosné poznatky skýtají resortní statistické údaje Ministerstva spravedlnosti (dále jen „MSp"), dostupné především prostřednictvím systému CSLAV.[30] Jak je zřejmé z dat o stíhaných, obžalovaných a odsouzených osobách za počítačové trestné činy v letech 2015–2022, došlo v tomto období k víceméně plynulému nárůstu počtu stíhaných a obžalovaných. Naproti tomu vývoj počtu odsouzených nebyl ušetřen zásadního zvratu. Do roku 2018 počet odsouzených vykazoval vzrůstající trend, přičemž největšího meziročního nárůstu (o 56 %) bylo dosaženo právě v tomto roce. V následujících dvou letech naopak počet odsouzených klesal tak, že v roce 2020 činil meziroční pokles 19 %. Výše nastíněný vývoj je zobrazen v následujícím grafu (Graf 6).

30 Centrální statistické listy a výkaznictví.

Graf 6: Vývoj počtu osob stíhaných, obžalovaných a odsouzených za počítačové trestné činy v letech 2015–2022 podle statistik MSp



I.4 Předmět a cíl výzkumu

I.4.1 Předmět výzkumu

Předmětem výzkumného úkolu IKSP Posouzení trendů kyberkriminality jsou zkušenosti a praxe obyvatel ČR s vybranými jevy v online prostředí, indikované zejména údaji získanými z dotazníkového šetření, které proběhlo v roce 2020 (viz dále). Celkový obrázek doplňují údaje z trestních spisů o počítačových trestných činech, které poskytují konkrétní představu o registrované počítačové trestné činnosti ve vybraném období.

Výzkum zahrnuje několik relativně odlišných oblastí (jako e-banking, zneužívání e-mailových schránek, ransomware aj.), v jejichž rámci se vždy snažíme podat informace o „pachatelích“,[31] obětech, modu operandi a případně i bezpečnostních návycích uživatelů internetu.

U „pachatelů“ proto sledujeme jejich počet, sociodemografické charakteristiky včetně trestní minulosti a specifika v rámci dílčích tematických oblastí, kterými jsou obchodování online, e-banking, ransomware, phishing, zneužití herního účtu, napadení e-mailové schránky, zneužití skutečného a/nebo fiktivního účtu na sociální síti, zaměstnanci jako rizikový faktor, registrované počítačové trestné činy[32] (včetně případně uloženého trestu).

31 Za „pachatele“ zde označujeme i ty respondenty dotazníkového šetření, jejichž relevantní reportované jednání by mohlo naplnit znaky skutkové podstaty počítačového trestného činu.

32 Údaje o registrovaných počítačových trestných činech vychází především z analýzy trestních spisů, a jde tedy o pachatele, resp. osoby odsouzené pro spáchání některého z počítačových trestných činů, jejichž trestní řízení pravomocně skončilo v roce 2019 (případně 2015). Blíže k tomu viz kapitola Trestní spisy.

Z hlediska obětí se zajímáme o obdobné informace jako u „pachatelů“,[33] pouze chybí oblast zaměstnanců jako rizikového faktoru.[34] Co se týče modu operandi, rozlišujeme jednání charakterizovatelná jako virtuální násilí, sledování majetkového zájmu a ostatní. Přibližujeme některé podrobnosti vztahující se k sociálnímu inženýrství, znalostem informačních technologií a napadaným zařízením, potažmo používání různých zařízení k přístupu na internet vůbec (včetně jejich zabezpečení).

I.4.2 Cíl výzkumu

Hlavním cílem výzkumu je získat nové a prohloubit některé dosud nabyté poznatky ve vybraných oblastech kyberkriminality v českém prostředí. Má nastínit, „co se děje online“ (fenomenologie), pokusit se zjistit, zda spolu některé vybrané jevy souvisí (etiologie), shrnout tresty obvykle ukládané odsouzeným pachatelům (kontrola) a navrhnout, jak lze sledovaným jednáním zabránit či minimalizovat jejich škodlivý dopad (prevence).

Výzkum lze chápat jako reakci na obecně rostoucí míru kyberkriminality a její předpokládanou vysokou latenci a proměnlivost.[35] Předchozí projekt[36] zaměřený na počítačové trestné činy již naznačil, že viktimizace kyberkriminalitou (v rámci registrované kriminality) závisí z velké části na vlastním jednání uživatele (tehdy zejména v podobě slabých a/nebo nechráněných hesel). Proběhnuvší dotazníkové šetření poskytlo unikátní množství dosud nedostupných podrobných údajů, týkajících se např. motivace pachatelů. Nabízí tak vynikající příležitost osvětlit a porozumět kyberkriminalitě na úrovni běžných uživatelů internetu. Tato monografie tak mimo jiné naznačuje, kde vězí zranitelná místa na straně uživatelů, a zároveň také to, jaká jednání, aplikace či zařízení lze označit jako riziková, neboť často dochází k jejich zneužití.

Výzkum kombinující dotazníkové šetření spolu s analýzou vybraných trestních kauz umožnil důkladné zmapování vybraných oblastí kyberkriminality. Poskytl vhled do způsobů páchání tohoto druhu trestné činnosti, na charakteristiky jejích pachatelů i obětí, ale také do typických slabých stránek praxe kybernetické bezpečnosti v české populaci, a to v rámci registrované i latentní kriminality.

Uvedené poznatky mohou poskytnout dostatečně podložený základ pro činnost institucí věnujících se preventivnímu působení, a to zejména na úrovni primární a sekundární prevence. Poznatky o pachatelích a rizikovém jednání atp. mohou napomoci orgánům činným v trestním řízení při odhalování kyberkriminality.

Vedlejším cílem projektu je zjištění, zda a jak se odlišují pachatelé, oběti i modus operandi při jejich kategorizaci na virtuální násilí a majetkový zájem (a ostatní). Nezanedbatelné rozdíly umožňují načrtnout empiricky podložené teoretické východisko pro

33 U registrovaných počítačových trestných činů jde o poškozené.

34 Hlavní „obětí“ je v tomto případě zaměstnavatel.

35 Aktuálnost problematiky v českém prostředí dokládá i její opakované zařazování do Strategie prevence kriminality v České republice (na léta 2016 až 2020 i 2021 až 2026).

36 Poznatky získané v jeho rámci shrnuje publikace Kyberkriminalita v kriminologické perspektivě, dostupná na http://www.ok.cz/iksp/docs/463.pdf (2023-04-25) (Vlach et al., 2020).

rozlišování virtuálního násilí a majetkového zájmu v rámci páchání kyberkriminality vůbec, neboť taková kategorizace může do budoucna poskytnout vhodný interpretační i výzkumný nástroj.

Součástí výzkumu je analýza vybraných jevů za účelem zjištění vzájemného vztahu mezi nimi, včetně zahrnutí věku, pohlaví a vzdělání jako nezávislých proměnných.

I.5 Metodologie

I.5.1 Spisy

V rámci výzkumu byla provedena rozsáhlá analýza trestních spisů, neboť ty skýtají možnost seznámit se s jednotlivými případy počítačových trestných činů o poznání podrobněji, než jak nám to umožňují dostupné statistické údaje. Při přípravě a realizaci této analýzy byly využity poznatky získané předcházející analýzou relevantních trestních spisů, která proběhla jako stěžejní část výzkumného projektu IKSP zaměřeného na problematiku kyberkriminality (Vlach et al., 2020). Analýza se především zaměřuje na poznatky o právní kvalifikaci skutku a průběhu trestního řízení, osobě pachatele, oběti, způsobu páchání, jakož i o způsobené újmě v případech, kdy došlo k pravomocnému odsouzení pachatele za trestný čin neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 TZ. Celkem bylo vyžádáno 161 spisů, jejichž statistické listy byly do systému CSLAV odeslány v roce 2019. K analýze bylo soudy zapůjčeno 158 spisů (ve zbývajících třech případech nebylo možno požadovaný spis zapůjčit). S využitím záznamových listů bylo v anonymizované podobě sledováno celkem 95 položek, které byly strukturovány do následujících tematických okruhů:

- poznatky ke skutku dle obžaloby, zahrnující právní kvalifikaci skutku a jeho stručný popis,
- uložené sankce a jejich výměra,
- informace o průběhu trestního řízení, zahrnující délku řízení, případné využití opravných prostředků či využití služeb soudního znalce,
- poznatky k osobě pachatele, zejména jeho věku, pohlaví, socioprofesnímu statusu či případné předchozí kriminální kariéře,
- způsob spáchání skutku, včetně použité komunikační platformy,
- převažující charakter útoku, tj. zda se jednalo primárně o majetkový zájem či projev virtuálního násilí,
- informace o poškozeném subjektu či subjektech,
- způsobená škoda či případná nemajetková újma,
- informace o poměru pachatele k poškozenému subjektu.

I.5.2 Dotazník[37]

I.5.2.1 Realizace dotazníkového šetření

Inspirací pro formulaci dotazníkových otázek byla rozsáhlá rešerše zaměřená na dostupné statistické údaje a poznání relevantní pro kyberkriminalitu v rámci ČR. Dotazník,

37 Kapitola vychází z publikovaného článku (Kudrlová, 2022).

jehož znění schválila oponentní rada IKSP, se zabýval zejména těmi jevy online, kterým byla doposud věnována pozornost jen okrajově nebo téměř vůbec.[38] Předmětem šetření byla zejména sebeochrana uživatelů digitálních technologií a míra jejich viktimizace vybranými jevy v online prostředí. Významné množství dotazů směřovalo i na respondenty v pozici útočníka. Některé otázky směřovaly i na respondenty coby zaměstnance. Sledované období zahrnuje zhruba rok 2020, neboť výzkumné šetření proběhlo 3. až 25. listopadu roku 2020 a převážná většina dotazů se vztahovala k „uplynulým 12 měsícům", tedy přesněji k období od prosince roku 2019 do listopadu roku 2020. Dále proto hovoříme o roku „2020*".

Cílovou skupinou respondentů byli uživatelé internetu z řad obecné populace ČR ve věku 16–74 let. Sběr dat měl proběhnout metodou CAPI[39] s velikostí výzkumného souboru nejméně 3 000 osob. Vzhledem k nejisté situaci v souvislosti s vývojem pandemie a přidružených opatření přicházel ovšem v úvahu i sběr dat metodou CAWI[40] (s přiměřeným navýšením výzkumného souboru na nejméně 6 500 osob). Několik dní před zahájením terénního šetření pak vydala Vláda ČR vládní nařízení omezující volný pohyb osob,[41] a nezbylo proto, než se spolehnout výlučně na sběr dat metodou CAWI.

Na základě výběrového řízení realizovala sběr dat profesionální agentura, a to po převodu dotazníku do interaktivní webové podoby ve vzájemné spolupráci realizátora a řešitelů projektu. Testování zahrnulo funkčnost dotazníku, formulační a gramatickou správnost, funkčnost výsledné databáze a matice SPSS.

Respondenti byli vybíráni kvótní metodou na základě kvót předem zadaných dle údajů Českého statistického úřadu a informací SPIR,[42] přičemž se nejednalo o obecnou populaci ČR v určeném věku, ale o populaci internetovou.[43] Při výběru respondentů byly použity jako kvótní znaky pohlaví, věk, nejvyšší dosažené vzdělání, velikost místa bydliště a kraj, v němž se v době sběru dat nacházelo bydliště respondentů. Ve výsledném vzorku jsou mírně nadreprezentovány osoby s vyšším vzděláním[44] a z větších měst (tj. ze sídel s populací nad 20 tisíc obyvatel, přičemž k nejvyššímu nadhodnocení došlo u sídel od 100 do 500 tisíc obyvatel) oproti populaci se základním vzděláním a nejmenších sídel.[45] Soubor jako celek nicméně považujeme za dostatečně reprezentativní.

38 U jevů s již nějak dostupnými údaji se dotazník zaměřil na podrobnější informace – např. na sdílení přihlašovacích údajů k e-bankingu.

39 Osobní dotazování respondentů tazatelem (face-to-face), který zadává odpovědi přímo do počítače či tabletu (Computer Assisted Personal Interviewing).

40 Dotazování prostřednictvím interaktivního webového dotazníku (Computer Assisted Web Interviewing).

41 Usnesení Vlády ČR ze dne 26. října 2020 č. 1102 o přijetí krizového opatření.

42 Sdružení pro internetový rozvoj.

43 Klíčovým zdrojem k určení parametrů internetové populace byla publikace Českého statistického úřadu „Informační společnost v číslech – 2020" (Český statistický úřad, 2021a).

44 Respondenti se středoškolským vzděláním s maturitou a vysokoškoláci.

45 Pravděpodobně v důsledku využitých online panelů. Mimoto prvotní kontrola dat vyřadila některé respondenty, a tak bylo nutné některé kvóty doplnit dalšími respondenty, v důsledku čehož došlo k nadreprezentování.

Využité online panely[46] disponují kapacitou téměř 80 000 aktivních uživatelů internetu. Jsou profesionálně řízeny (eliminují fiktivní respondenty), respondenti jsou motivováni drobnými odměnami za vyplněné dotazníky. Respondenti v panelech se obměňují a sleduje se četnost dotazování (průměrně jednou měsíčně, opětovné dotazování ke stejnému tématu až po určité době). Výběr respondentů proběhl pomocí speciálního softwaru.

Sebraná data byla nahrána do matice statistického systému SPSS a vyčištěna. Některé otevřené otázky byly následně kódovány.[47] Poté proběhlo třídění prvního a druhého stupně a sledování případných korelací mezi vybranými proměnnými pomocí T-testů závislosti.

Analýza dat stále probíhá, nicméně zde prezentované dosud dostupné poznatky skýtají řadu zajímavých zjištění. A to především proto, že respondenti odpovídají jednak v pozici možných obětí, jednak i možných útočníků formou self-reportu. Zjištění tak poskytují ojedinělý obrázek zahrnujících do jisté míry obě strany.[48]

I.5.2.2 Tematické okruhy, formulace otázek a používaná terminologie

Tematické okruhy zhruba pokrývají oblast zařízení používaných k aktivitám online a jejich ochranu, vybrané uživatelské schopnosti (včetně zkušeností s darkwebem) a zkušenosti s neoprávněným jednáním: ransomwarem, phishingem, zneužíváním online účtů (e-maily, profily na sociálních sítích, e-banking, herní účty), podvody při obchodování online, zneužíváním přístupu zaměstnanců do neveřejného informačního systému, baitingem a porušováním autorských práv.

Dotazník zahrnoval několik samostatných částí, přičemž respondenti odpovídali pouze na otázky pro ně relevantní.[49] U self-reportových otázek, směřujících na neoprávněný přístup či neoprávněné použití jakéhokoliv online účtu, byla záměrně zvolena formulace „použití účtu bez výslovného svolení jeho majitele/ky". Důvodem je snaha vyhnout se použití výrazu „neoprávněný přístup", který je jednak do jisté míry částečně negativně zabarven, jednak by odpovědi byly zatíženy subjektivním hodnocením respondentů ohledně „neoprávněnosti" jejich jednání. Vycházeli jsme přitom z předchozí analýzy trestních spisů za rok 2015, ze kterých bylo patrné, že pachatelé si mnohdy nebyli vůbec vědomi, že by jejich přístup na cizí online účet nebo manipulace s daty mohly být neoprávněné, potažmo protiprávní až trestné. Také jsme předpokládali, že nastanou případy, kdy respondenti budou přistupovat na cizí účet na základě předchozí dohody s majitelem účtu (např. správa e-bankingu, občasná kontrola profilu na sociální síti potomka atp.). Věříme, že respondenti, přistupující na cizí účet v rámci takové dohody, nepovažují své jednání za „přístup bez výslovného svolení". A zároveň, že sami respondenti nejlépe vyhodnotí, zda při existenci takové předchozí dohody jejich jednání případně již vybočilo z vymezeného rámce, a tudíž šlo o „přístup bez výslovného svolení".

46 Jednalo se o panely Data Collect, s. r. o.

47 Vzhledem k prvovýzkumu byla řada otázek otevřená, aby se omezilo ovlivnění dat předpokladem výzkumníků.

48 Možnosti i omezení vyplývající z metody self-reportu přehledně shrnuje např. Tomášek (2013).

49 V textu proto na příslušných místech vždy uvádíme aktuální velikost výběrového souboru.

Části textu psané kurzívou a s uvozovkami vyjadřují doslovný přepis použitých otázek a odpovědí respondentů bez jakékoliv jazykové úpravy (tedy včetně případných chyb, hovorových výrazů atp.).

Pakliže používáme výraz „cizí účet", máme tím na mysli účet někoho jiného. Nejde tedy pouze o účet nějaké neznámé osoby. V rámci dotazníkových otázek byla použita vždy formulace „*účet někoho jiného*", abychom zamezili špatnému pochopení ze strany respondentů, kteří by např. účet svého partnera nepovažovali za „cizí" účet, protože ani onen partner vůči nim není „cizí".

Při používání výrazu „pachatel" jde v kapitolách věnovaných dotazníku pouze o zjednodušující zkratku. Někdy nelze neoprávněnost/protiprávnost dovodit s jistotou, jindy jde třeba o protiprávní jednání, ale nikoliv trestné. Podobně je tomu s výrazem „poškozený" či „oběť" – ne vždy se překrývají se svými legálními definicemi v TŘ a zákoně o obětech trestných činů (zák. č. 45/2013 Sb.). Používáme proto místy výrazy jako „útočník" nebo „napadený", které se mohou zdát příliš silné, leč jednoznačně určují, zda jde o osobu porušující určitá pravidla či jednající zlovolně, anebo o osobu, k jejíž tíži k takovému jednání dochází.

V otázkách směřujících na motivaci pachatelů mohli respondenti zpravidla volit mezi penězi, zvědavostí či napsat jinou motivaci dle vlastního uvážení. Důvodem takto zvolené formulace byla obava, že při výběru ostřejších, negativně zabarvených výrazů, spojených např. s virtuálním násilím (viz dále, např. stalking) by část respondentů raději neodpověděla vůbec.

V řadě případů mohli mít respondenti v roce 2020* zkušenost s více incidenty stejného druhu (např. zneužití jejich profilu na sociální síti). V takovém případě byli vždy požádáni, aby vybrali ten, který oni sami považují za nejzávažnější, a dále odpovídali již pouze ohledně tohoto jednoho incidentu.

Některé možnosti odpovědí byly kumulativní, typicky „soused/spolužák/známý". Je tomu tak zpravidla tam, kde shledáváme určitou společnou charakteristiku, kterou považujeme v dané oblasti za zásadní – např. v uvedeném případě je to skutečnost, že jde o osobu, se kterou je respondent pravděpodobně nějak v kontaktu, aniž by si to sám vybral.

Hovoříme-li o úzkém nebo užším rodinném kruhu, máme na mysli rodiče, prarodiče, děti, vnoučata a sourozence. V případě širšího rodinného kruhu jde o ostatní rodinné příslušníky. Žádná z těchto dvou skupin nezahrnuje partnery, kterým je vyhrazena samostatná kategorie.

Při dotazování ohledně reakce na incident měli respondenti možnost vybrat odpověď „*nahlásil/a jsem to policii*." Záměrně jsme se vyhnuli přesnějším výrazům jako Policie ČR, policejní orgány nebo obecní/městská policie, aby jejich rozlišování nebylo pro respondenty matoucí. Podobně jsme se následně takových respondentů tázali na jejich spokojenost s policií vůbec („*jak jste byl/a spokojen/a s policií*") – nechtěli jsme rozlišovat mezi spokojeností s přístupem policie, s výsledkem vyšetřování, s jednáním vůči oznamovateli atp., ale šlo nám o celkový výsledný dojem respondentů, kteří se na policii obrátili.

Několik otázek směřovalo na použití cizí paměťové karty či flashdisku. Dotazník ovšem používal pro jednoduchou srozumitelnost hovorový výraz „*paměťová karta nebo fleška*".

V rámci zjednodušení textu používáme zpravidla mužské verze výrazů, které mají i své protějšky v ženském rodě (typicky partner/ka). Jsme si vědomi genderové nevyváženosti, věříme však, že uvedené zjednodušení bude ku prospěchu celkové srozumitelnosti textu.

U některých otázek odpovídali respondenti výběrem na 5bodové škále, s hodnotami odpovídajícími obsahem zhruba „*ano – spíše ano – spíše ne – ne*", přičemž pátou možnou odpovědí byla varianta „*nemám jednoznačný názor.*" Při následné práci se škálou jsme odpovědi transformovali do 5bodové škály s neutrální odpovědí „*nemám jednoznačný názor*" uprostřed.

Procentuální hodnoty uvádíme zaokrouhlené na celá čísla, pouze v tabulkách zaokrouhlené na jedno desetinné místo. Na některých místech proto nedává výsledný součet přesně 100 %, ale drobně se liší. Jiná situace nastává tam, kde mohli respondenti vybrat více než jednu odpověď (pokud se vzájemně nevylučovaly) – v takových případech obvykle souhrn odpovědí převýšil 100 % výrazněji, zpravidla na to však upozorňujeme v poznámce pod čarou.

Závěrem této části ještě několik slov ke kategorii „virtuální násilí", kterou jsme začali používat již v souvislosti s předchozím výzkumným úkolem IKSP zaměřeným na kyberkriminalitu (Vlach, Kudrlová & Paloušová, 2020, str. 77). Zdánlivý oxymóron vyjadřuje specifickou formu násilí, která zjevně není srovnatelná s fyzickým násilím, ale zároveň zcela neodpovídá ani psychickému násilí, byť tomu se přibližuje nejvíce. Jde o takové jednání, jehož zraňující efekt zasahuje nějakým způsobem integritu člověka ve virtuálním prostředí. Zcela samozřejmě tak zahrnuje jednání, jako jsou kyberstalking, kyberšikana atp., které se velmi blíží již zmíněnému psychickému násilí. Za součást integrity člověka ve virtuálním prostředí však považujeme i jeho soukromí, neboť tak jako osobnost člověka emanuje do virtuálního prostoru, podobný přesah připisujeme i jeho soukromí. Zásah do soukromí (včetně osobních údajů) proto považujeme za zásah do této integrity. Z toho důvodu řadíme mezi tzv. virtuální násilí i jednání relativně nenásilného charakteru, jako jsou neoprávněná lustrace osobních údajů, neoprávněný přístup k profilu na sociální síti atp.

II.

Trestní spisy

II.1 Analýza trestních spisů

Analýza trestních spisů se již dříve ukázala být cenným zdrojem informací o případech počítačové trestné činnosti,[50] se kterou se soudy setkávají v rámci své činnosti. Celkem bylo za rok 2019 analyzováno 158 trestních spisů, týkajících se případů, kdy došlo k pravomocnému odsouzení pachatele.

Tabulka 2: Přehled počtu analyzovaných spisů dle soudů (n = 158)

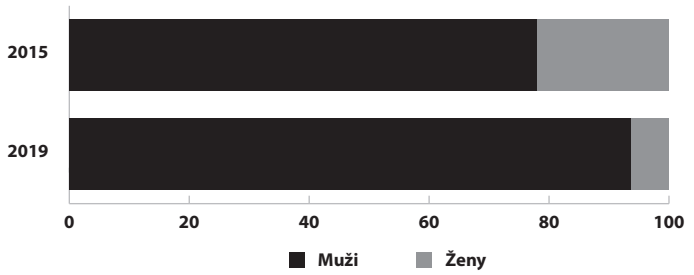
Soud	Počet	Soud	Počet
Krajský soud Hradec Králové	1	Okresní soud Karlovy Vary	2
Krajský soud Ústí nad Labem	1	Okresní soud Karviná	1
Městský soud Brno	8	Okresní soud Kladno	2
Městský soud Praha	1	Okresní soud Kolín	1
Obvodní soud Praha 1	2	Okresní soud Kroměříž	3
Obvodní soud Praha 10	3	Okresní soud Liberec	3
Obvodní soud Praha 4	2	Okresní soud Litoměřice	6
Obvodní soud Praha 5	1	Okresní soud Louny	1
Obvodní soud Praha 6	2	Okresní soud Mělník	1
Obvodní soud Praha 8	1	Okresní soud Most	3
Obvodní soud Praha 9	3	Okresní soud Náchod	1
Okresní soud Beroun	2	Okresní soud Nový Jičín	2
Okresní soud Brno-venkov	2	Okresní soud Olomouc	9
Okresní soud Bruntál	1	Okresní soud Opava	2
Okresní soud Břeclav	9	Okresní soud Ostrava	2
Okresní soud Česká Lípa	4	Okresní soud Písek	1
Okresní soud České Budějovice	13	Okresní soud Prachatice	2
Okresní soud Český Krumlov	1	Okresní soud Přerov	3
Okresní soud Domažlice	3	Okresní soud Rakovník	1
Okresní soud Frýdek-Místek	2	Okresní soud Semily	1
Okresní soud Havlíčkův Brod	2	Okresní soud Šumperk	4
Okresní soud Hodonín	2	Okresní soud Tábor	2
Okresní soud Hradec Králové	3	Okresní soud Teplice	3
Okresní soud Cheb	2	Okresní soud Trutnov	1
Okresní soud Chomutov	1	Okresní soud Třebíč	1
Okresní soud Jablonec nad Nisou	2	Okresní soud Uherské Hradiště	1
Okresní soud Jeseník	1	Okresní soud Ústí nad Labem	11
Okresní soud Jičín	3	Okresní soud Vsetín	1
Okresní soud Jihlava	3	Okresní soud Zlín	2
Okresní soud Jindřichův Hradec	3	Okresní soud Žďár nad Sázavou	1

50 Součástí předchozího výzkumného úkolu Kybernetická kriminalita v kriminologické perspektivě byla analýza trestních spisů, týkajících se případů počítačových trestných činů za rok 2015 (Vlach et al., 2020). U položek, kde byly zaznamenány zásadnější rozdíly mezi stavem z roku 2015 a 2019, bylo provedeno jejich porovnání.

II.1.1 Poznatky k osobě pachatele

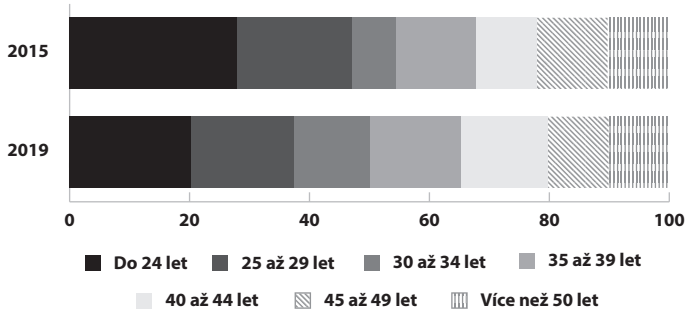
V analyzovaném vzorku 158 trestních spisů jako pachatelé výrazně převládají muži (148 mužů, tj. 94 %) oproti ženám (10 žen, tj. 6 %). I kdyby bylo odhlédnuto od poměrně početné specifické skupiny případů (50 případů, tj. 32 %), které spočívají v zásahu do funkce digitálního tachografu,[51] kde jsou pachateli výhradně muži, nedosáhl by podíl žen na zbývajících případech ani 10 %. Není jistě bez zajímavosti, že ve vzorku již dříve analyzovaných spisů za rok 2015 bylo zastoupení žen více než dvojnásobné (22 %). Porovnání struktury analyzovaného vzorku za roky 2015 a 2019 je ilustrováno následovně (Graf 7).

Graf 7: Struktura analyzovaného vzorku spisů dle pohlaví za roky 2015 (n = 68) a 2019 (n = 158) (%)



Věk pachatelů se pohyboval v rozmezí od 15 do 67 let, přičemž průměrný věk činil 35 let (medián 34 let).[52] Zatímco v roce 2015 tvořily osoby do 30 let téměř polovinu analyzovaného vzorku (47 %), v roce 2019 již tyto osoby představovaly jen o něco více než třetinu (37 %) (Graf 8 a Tabulka 3).

Graf 8: Porovnání věkové struktury pachatelů 2015 (n = 68) a 2019 (n = 158) (%)



51 Vzhledem k silnému zastoupení těchto případů jim je věnována samostatná podkapitola této publikace. U těch sledovaných položek, kde specifické charakteristiky případů, týkajících se digitálních tachografů, jakož i jejich pachatelů, výrazněji ovlivnily celkový obraz sledovaných položek, jsou uvedeny jak údaje za celý analyzovaný vzorek, tak také v komparaci s případy bez tachografů.

52 Pouze tři pachatelé (tj. 2 %) byli mladší 18 let.

Tabulka 3: Věková struktura pachatelů ve vzorku za rok 2019

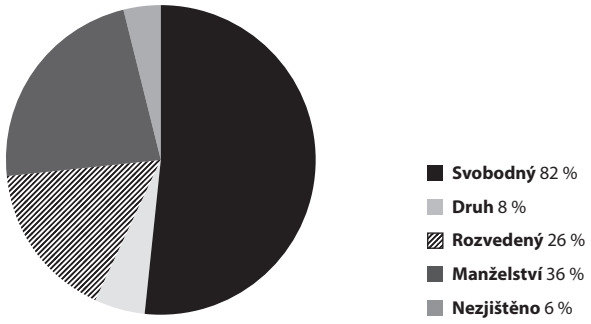
	Počet	%
Do 24 let	32	20,3
25 až 29 let	27	17,1
30 až 34 let	20	12,7
35 až 39 let	24	15,2
40 až 44 let	23	14,6
45 až 49 let	16	10,1
Více než 50 let	16	10,1
Celkem	158	100

Také věková struktura byla ovlivněna silně zastoupenými případy spočívajícími v zásahu do funkce digitálního tachografu. U případů, které se netýkaly tachografů (n = 108), figurovali pachatelé do 30 let v celé polovině těchto případů (51 %).

Nejsilněji byli v analyzovaném vzorku zastoupeni občané ČR (140 osob, tj. 89 %). Osm pachatelů (5 %) bylo slovenskými občany. Okrajově byli zastoupeni též občané dalších evropských zemí (6 %). Konkrétně se jednalo o dva občany Polska, dva občany Chorvatska a po jednom pak figurovali občané Irska, Itálie, Lotyšska, Rumunska, Srbska a Ukrajiny.

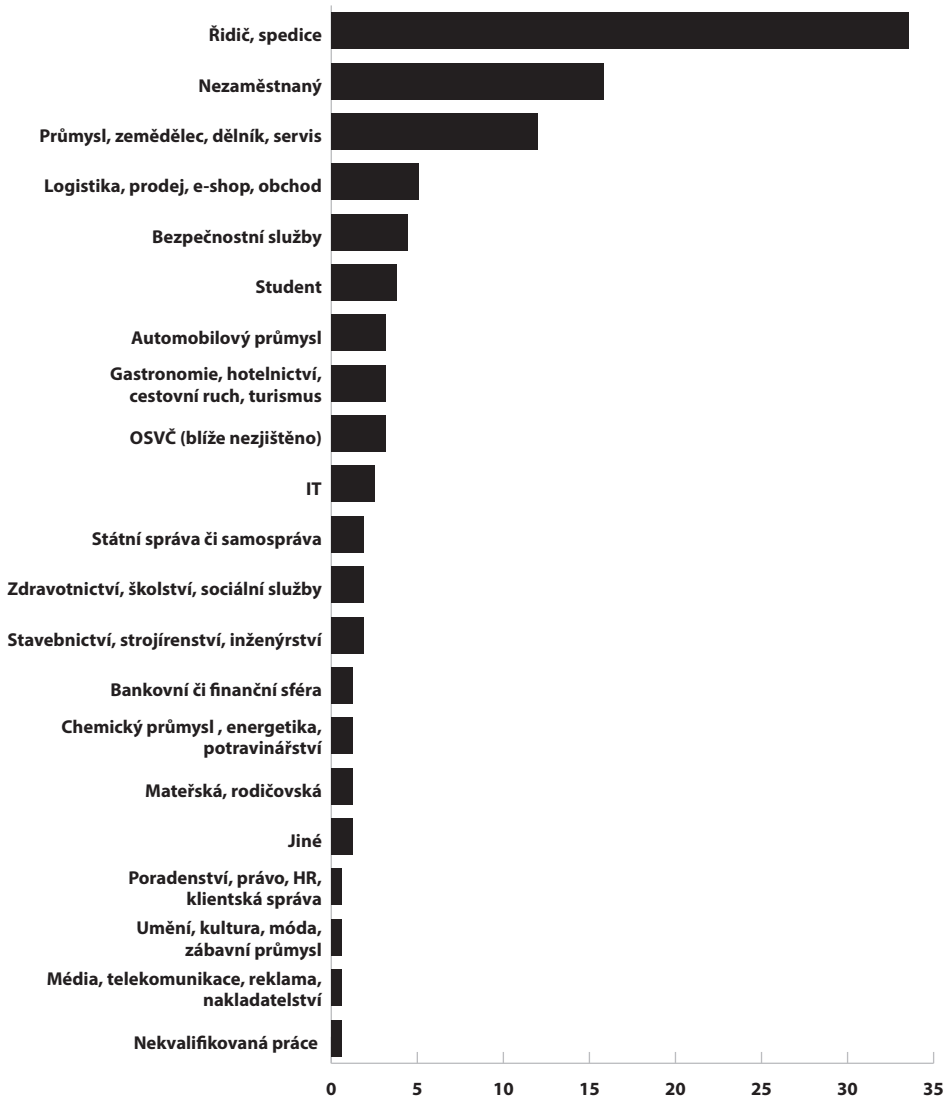
Celá polovina pachatelů byla svobodných (82 osob, 52 %). V manželském svazku žila necelá čtvrtina (36 osob, 23 %) a přibližně šestina (26 osob, tj. 17 %) pachatelů byla rozvedená (Graf 9).

Graf 9: Rodinný stav pachatelů (n = 158)



Sledován byl též socioprofesní status pachatelů. Již zmíněné výrazné zastoupení případů, vztahujících se k digitálním tachografům, se odrazilo zákonitě též ve struktuře zastávaných profesních pozic, kdy celá třetina pachatelů (53 osob, tj. 34 %) pracovala jako řidiči v oblasti spedice. Šestina pachatelů nebyla zaměstnána (25 osob, tj. 16 %) a přibližně osmina (19 osob, tj. 12 %) působila v dělnických profesích. Celkovou strukturu zastoupení profesních skupin v analyzovaném vzorku spisů ilustruje následující graf (Graf 10).

Graf 10: Socioprofesní status pachatelů (%, n = 158)



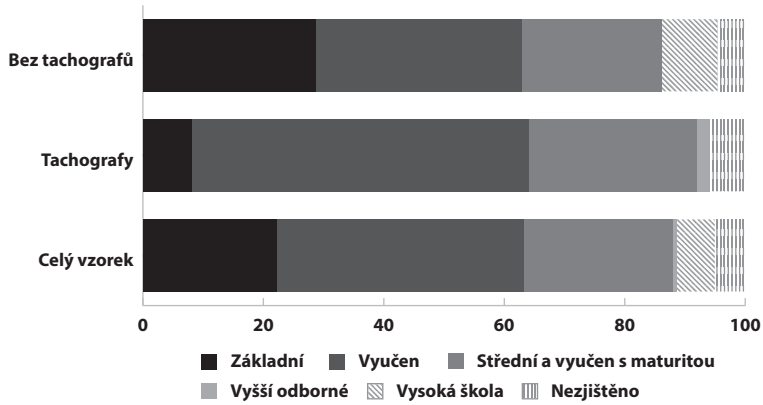
V sedmi případech[53] byl pachatel úřední osobou ve smyslu ustanovení § 127 TZ.

Trestní spisy též mimo jiné skýtají informace o nejvyšším dosaženém vzdělání. Nejhojněji byly zastoupeny osoby vyučené, které tvořily dvě pětiny vzorku (41 %, tj. 65 osob), a též osoby s úplným středoškolským vzděláním včetně osob vyučených s maturitou (25 %, tj. 39 osob), které představovaly čtvrtinu všech pachatelů. V řadách pachatelů, zasahujících do funkce tachografu, jsou, v porovnání se zbývajícími pachateli, dle očekávání výrazněji zastoupeny osoby vyučené, a naopak méně osoby se základním vzděláním. Pro názornost

53 U pěti mužů a dvou žen.

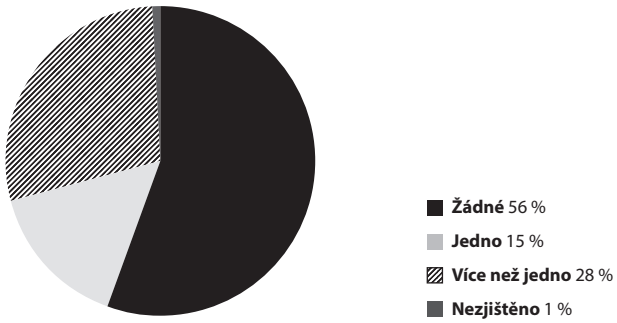
je porovnána celková vzdělanostní struktura (n = 158) se skupinou spojenou s tachografy (N = 50) a zbývajícími pachateli (n = 108) (Graf 11). Masivněji zastoupená skupina osob se základním vzděláním u pachatelů nemajících vztah k tachografům (31 osob) sestává převážně z nezaměstnaných (11 osob) a studentů (6 osob) a osob mladších 25 let.

Graf 11: Nejvyšší dosažené vzdělání (%)



Sledována byla též případná kriminální historie pachatelů, tedy zda již byli v minulosti pravomocně odsouzeni. Z následujícího grafu je zřejmé, že předchozí záznam v Rejstříku trestů měly více než dvě pětiny pachatelů (69 osob, 44 %), přičemž téměř třetina pachatelů (45 osob, tj. 29 %) měla dokonce více než jeden (Graf 12). Pomyslným rekordmanem co do počtu předchozích odsouzení byl 53letý muž s dvanácti předchozími záznamy.

Graf 12: Předchozí pravomocná odsouzení (n = 158)

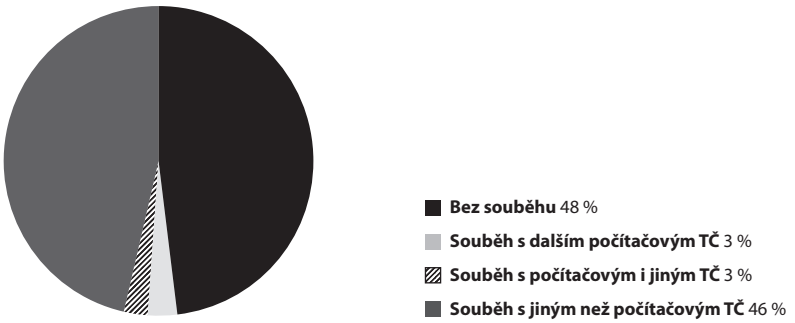


Jedním ze základních sledovaných znaků je přesná kvalifikace skutku, a to včetně odstavce a písmene zákonné úpravy počítačového trestného činu, který záznamový list sledoval. Téměř ve všech případech se jednalo o trestný čin neoprávněného přístupu k po-

čítačovému systému a nosiči informací dle § 230 TZ. Pouze v jednom případě šlo o přečin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ.[54]

V 76 případech (48 %) nebyl zaznamenán souběh s žádným dalším trestným činem. V pěti případech se jednalo o souběh s dalším počítačovým trestným činem a ve čtyřech případech o souběh s počítačovým trestným činem a dalším trestným činem. V 73 případech byl zaznamenán souběh pouze s jiným než počítačovým trestným činem (Graf 13).

Graf 13: Souběh s dalšími trestnými činy (n = 158)



Nejčastěji se v analyzovaném vzorku vyskytoval souběh některého z počítačových trestných činů s trestným činem podvodu dle § 209 TZ (v 21 případech), s trestným činem krádeže dle § 205 TZ (18 případů) a porušováním tajemství dopravovaných zpráv dle § 182 TZ (v 10 případech). Bylo též zaznamenáno devět případů souběhu s trestným činem neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 234 TZ, osm případů s neoprávněným přístupem k počítačovému systému a nosiči informací dle § 230 TZ, jakož i sedm případů souběhu s úvěrovým podvodem dle § 211 TZ a šest případů s vydíráním dle § 175 TZ.

II.1.2 Průběh trestního řízení

Celková délka trestního řízení od prvotního záznamu policie do pravomocného rozhodnutí soudu se pohybovala od jednoho do 3 177 dní – průměrně 414 dní. Pouze ve čtvrtině případů bylo pravomocně rozhodnuto do tří měsíců (38 případů, tj. 24 %), přičemž se jednalo téměř výhradně o případy týkající se tachografů.[55] Sledována byla též délka soudního řízení, tj. doba od doručení obžaloby, respektive návrhu na potrestání soudu do data nabytí právní moci konečného rozhodnutí ve věci. Ta se v rámci celého analyzovaného vzorku pohybovala od jednoho dne do 2 483 dní[56] – průměrně 161 dní (Tabulka 4).

54 V tomto případě v jednočinném souběhu s přečinem porušení tajemství dopravovaných zpráv dle § 182 TZ.

55 Blíže viz kapitola Digitální tachografy.

56 Enormní délka řízení byla zapříčiněna průtahy v rámci řízení před soudem a využitím opravných prostředků (odvolání i dovolání).

Tabulka 4: Celková délka řízení a délka řízení u soudu (n = 158)

	Celková délka řízení		Délka řízení u soudu	
	Počet	%	Počet	%
Do 1 měsíce	7	4,4	42	26,6
Od 1 do 2 měsíců	15	9,5	41	25,9
Od 2 do 3 měsíců	16	10,1	13	8,2
Od 3 do 4 měsíců	6	3,8	14	8,9
Od 4 do 5 měsíců	9	5,7	9	5,7
Od 5 do 6 měsíců	6	3,8	8	5,1
Od 6 do 7 měsíců	6	3,8	2	1,3
Od 7 do 8 měsíců	12	7,6	4	2,5
Od 8 do 9 měsíců	4	2,5	4	2,5
Od 9 měsíců do 1 roku	13	8,2	2	1,3
Od 1 do 2 let	38	24,1	15	9,5
Více než 2 roky	26	16,5	4	2,5

Délku řízení ovlivňuje mimo jiné využití opravných prostředků či vyžádání znaleckých posudků. Řádných opravných prostředků bylo využito ve 26 případech (17 % případů), kombinace řádného a mimořádného opravného prostředku byla využita v 9 případech (8 % případů). Znalecký posudek z oboru kybernetiky byl zpracován ve 13 případech (tj. 8 %), přičemž ve čtyřech případech byl zpracován i další znalecký posudek z jiného oboru – ve dvou případech z oboru zdravotnictví, odvětví psychiatrie, sexuologie, po jednom pak z odvětví psychiatrie, klinické psychologie, jakož i z oboru kriminalistika, odvětví analýza dat a zkoumání nosičů dat.

Ve třech čtvrtinách případů (120 případů, tj. 76 %) byla pachatelům uložena pouze jedna sankce. Ve 33 případech byl kromě hlavní sankce uložen také trest vedlejší. V jednom případě byla věc postoupena k projednání jako přestupek. Ukládán byl především podmíněný trest odnětí svobody dle § 81 a násl. TZ (v 90 případech samostatně či jako hlavní sankce), peněžitý trest dle § 67 a násl. TZ (ve 35 případech samostatně či jako hlavní sankce a v 11 případech spolu s dalším trestem – obvykle s podmíněným trestem odnětí svobody). Ve více než desetině případů (18 případů, tj. 11 %) byl pachatelům uložen nepodmíněný trest odnětí svobody. V osmi případech (tj. 5 %) byl pachatelům uložen samostatně či jako hlavní sankce trest obecně prospěšných prací dle § 62 a násl. TZ a v jednom případě jako vedlejší trest k trestu podmíněnému. Výměra uložených podmíněných trestů se pohybovala v rozmezí od jednoho měsíce do tří let se zkušební dobou od jednoho roku do pěti let. Peněžité tresty byly ukládány v částkách od 5 000 Kč do 10 800 Kč, přičemž jejich průměrná výše činila 30 840 Kč. Trest obecně prospěšných prací byl ukládán ve výměře od 100 do 800 hodin. V jednom případě bylo jako samostatný trest uloženo vyhoštění dle § 80 TZ ve výměře tří let a v dalším samostatný trest zákazu činnosti dle § 73 a násl. TZ

spočívající v zákazu řízení motorových vozidel ve výměře 12 měsíců. Trest zákazu činnosti spočívající v zákazu řízení motorových vozidel byl typicky vedle hlavní sankce ukládán pachatelům zasahujícím do funkce digitálních tachografů.[57]

II.1.3 Kazuistika

II.1.3.1 Lehkovážná babička

Třiadvacetiletý M. H. se v souvislosti se svým podnikáním dostal do finančních problémů, které se nelepšily ani poté, co nastoupil do zaměstnaneckého poměru jako automechanik. Situaci se snažil řešit prostřednictvím bankovních úvěrů, které opakovaně navyšoval až na částku 700 tis. Kč. V první polovině září 2017 byl telefonicky kontaktován pracovnicí banky s tím, že je v prodlení se splátkou ve výši 12 tis. Kč a pokud ji do tří dnů neuhradí, bude jeho dluh předán k vymáhání. Nakonec se s pracovnicí banky dohodl na prodloužení lhůty na 10 pracovních dnů, což mu banka potvrdila i písemně. Koncem měsíce potřeboval M. H. vytisknout několik dokumentů, ale neměl k dispozici počítač s tiskárnou. Rozhodl se proto navštívit své prarodiče a vytisknout si potřebné dokumenty u nich. Babička souhlasila s tiskem, nechala vnuka se svým počítačem o samotě. M. H. si povšiml na ploše ikony e-bankingu, neodolal a klikl na ni. Vzápětí se objevil na obrazovce přihlašovací formulář s předvyplněnými údaji. Po jejich odkliknutí byl vyzván k zadání bezpečnostního kódu, který byl zaslán SMS zprávou na babiččin mobilní telefon ležící na stole hned vedle počítače. V e-bankingu zjistil, že zůstatek na účtu činí přibližně 70 tis. Kč. Ihned ho napadlo, že by si mohl na svůj účet převést potřebnou splátku ve výši 12 tis. Kč, což také vzápětí udělal. Poté se z e-bankingu odhlásil, vytiskl si potřebné dokumenty a s babičkou se rozloučil, jako by se nic nestalo. Své prarodiče i nadále navštěvoval jako obvykle a přes výčitky svědomí nikomu nic neřekl. V polovině října se při další návštěvě od dědy dozvěděl, že jim někdo z účtu vybral peníze. Ani tehdy nenašel M. H. odvahu, aby se ke svému činu přiznal. Teprve poté, co věc začala vyšetřovat Policie ČR, se k činu doznal. Vzhledem k tomu, že svým prarodičům způsobenou škodu nahradil a doposud vedl řádný život, rozhodl státní zástupce o podmíněném odložení podání návrhu na potrestání dle § 179 g TŘ. Ve zkušební době se však M. H. neosvědčil, neboť se opakovaně dopustil řízení pod vlivem drog, za což mu kromě pokuty byl též uložen zákaz řízení motorových vozidel. Okresní soud v B. uznal v polovině února 2019 trestním příkazem M. H. vinným ze spáchání přečinů neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a), odst. 3 písm. a) TZ a neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 234 odst. 1 TZ. Za tyto činy mu byl uložen úhrnný peněžitý trest v celkové výši 6 tis. Kč.

Tento případ jasně ilustruje, že jistá míra opatrnosti při nakládání s přístupovými údaji je namístě i v rámci blízkých příbuzenských vztahů, ať již se jedná o e-banking, e-maily či profily na sociálních sítích.

57 Blíže viz kapitola Digitální tachografy.

II.1.3.2 Nenasytný křeček

Na přelomu let 2011 a 2012 vytvořil sedmadvacetiletý P. S. vystupující v online prostředí pod přezdívkou mr. křeček[58] sadu škodlivých zdrojových kódů s obecným názvem „tor" včetně aplikace umožňující vzdálené ovládání infikovaného počítače. Malware vytvořený pachatelem byl zaslán jako příloha e-mailu označeného jako elektronicky zasílaná faktura na e-mailovou adresu univerzity v O. Poté, co adresátka přílohu a v ní vložený odkaz otevřela, došlo k automatické instalaci sady škodlivých zdrojových kódů do jejího počítače, díky čemuž získal neomezený vzdálený přístup do univerzitní počítačové sítě. Zde sledoval komunikaci pracovníků univerzity s Českou národní bankou a zjistil tak, jakým způsobem je tato komunikace zabezpečena, jakož i kde se v počítačích zaměstnanců nachází bezpečnostní certifikát pro přístup do e-bankingu a pro platební styk. Následně vytvořil aplikaci, která vzhledem i funkcí věrně odpovídala stránkám e-bankingu ČNB ABO-K. S využitím bezpečnostního certifikátu provedl následně od dubna do srpna roku 2012 sérii šesti útoků typu „man-in-the-middle", při nichž převedl na svůj účet a následně vybral v bankomatech částky v celkové výši 642 452 Kč. V říjnu a listopadu roku 2012 provedl obdobným způsobem čtyři útoky, kdy z účtu Gymnázia v H. převedl částky v celkové výši 1 203 888 Kč. V únoru roku 2013 využil stejného postupu k získání částky 1 387 612 Kč z účtu organizace D. v Praze. Instalaci škodlivých kódů provedl také na několika počítačích univerzity v U., kde však bylo jejich infikování detekováno poté, co si jedna z pracovnic povšimla zpřeházeného pořadí položek na výpisu z účtu u ČNB. Univerzitě v U. tak naštěstí žádná škoda nevznikla. Na základě znaleckého zkoumání bylo zjištěno, že část škodlivého kódu, zachyceného v infikovaných počítačích, je identická s kódem uveřejněným autorem vystupujícím pod jménem „mr. křeček" na internetovém portálu zaměřeném na počítačovou bezpečnost, hacking, počítačové sítě a podobnou problematiku. Dalším pátráním bylo zjištěno, že pod zmíněnou přezdívkou vystupuje na sociálních sítích právě P. S. Okresním soudem byl následně P. S. uznán vinným ze spáchání trestných činů krádeže dle ustanovení § 205 odst. 1, 2 a 4 písm. c) TZ, neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1, 2 písm. a), d) a odst. 4 písm. d) TZ, jakož i neoprávněného opatření, padělání a pozměnění platebního prostředku podle ustanovení § 234 odst. 3 TZ. S přihlédnutím k jeho předchozí trestné činnosti mu byl uložen trest odnětí svobody ve výši čtyř let nepodmíněně spolu s trestem propadnutí věci.

II.1.4 Digitální tachografy

Poměrně velkou skupinu analyzovaných spisů tvořily případy zásahů do funkce digitálních tachografů. Jedná se o elektronická zařízení shromažďující celou řadu údajů, především pak informace o aktivitě řidiče, provozním režimu, době jízdy, rychlosti a ujeté vzdálenosti, jakož i informace o vkládání a vyjímání karty řidiče.[59] Zaznamenané údaje slouží primárně ke kontrole doby řízení a dodržování povinných přestávek a doby odpočinku.[60] Z celkového počtu námi analyzovaného vzorku 158 spisů připadala bezmála třetina (50 případů, tj. 32 %) na případy týkající se tachografů. Téměř ve všech případech se jednalo o jízdu, kdy byla do slotu tachografu vložena cizí čipová karta řidiče. Ve dvou

58 Přezdívka byla autory publikace změněna.

59 Blíže viz Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014.

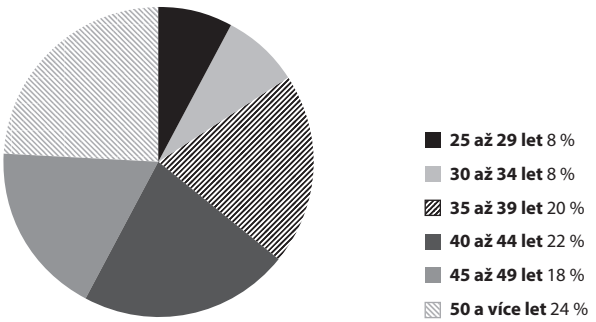
60 Blíže viz Sdělení Ministerstva zahraničních věcí č. 62/2010 Sb. m. s.

případech byla funkce tachografu ovlivněna důmyslně skrytým elektronickým zařízením a v posledním případě došlo k narušení funkce tachografu přiložením magnetů na příslušné snímače.

II.1.4.1 Poznatky k osobě pachatele

Co se týče pachatelů zasahujících do funkce tachografů, jednalo se výhradně o muže. Jejich věk se pohyboval od 25 do 67 let, s průměrným věkem 42 let, přičemž celé dvě třetiny tvořili pachatelé ve věku 40 a více let (Graf 14).

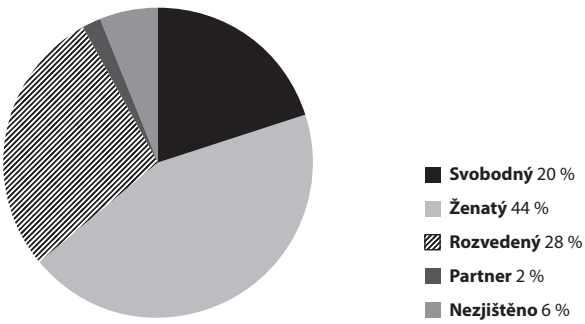
Graf 14: Věková struktura – tachografy (n = 50)



Z téměř tří čtvrtin se jednalo o občany ČR (36 osob, tj. 72 %). Slovenským občanstvím disponovalo 6 pachatelů (tj. 12 %). Dále byli mezi pachateli zastoupeni po dvou občané Polska a Chorvatska. Po jednom pak občané Irska, Lotyšska, Rumunska a Srbska.

Více než dvě pětiny pachatelů žily v manželství (22 osob, tj. 44 %), necelá třetina byla rozvedena (14 osob, tj. 28 %) a pětina pachatelů byla svobodných (10 osob, tj. 20 %). U třech pachatelů (z toho dva byli cizinci) se ze spisu nepodařilo poznatek o jejich rodinném stavu zjistit (Graf 15).

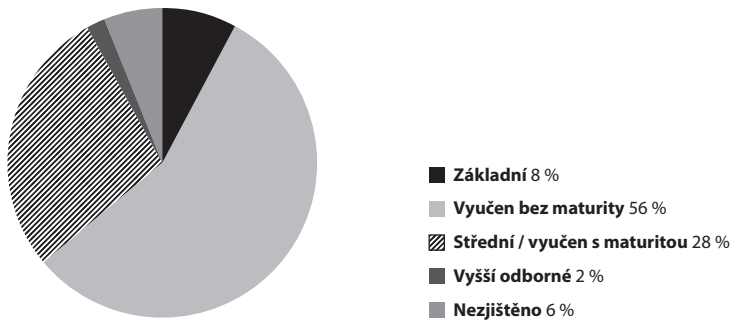
Graf 15: Rodinný stav – tachografy (n = 50)



Analýzou spisů byl dále sledován socioprofesní status pachatelů. S ohledem na specifika zásahu do funkce digitálního tachografu nebylo nijak překvapivé zjištění, že téměř všichni pachatelé byli zaměstnáni v oblasti spedice (46 osob, tj. 92 %). Ve dvou ze zbývajících případů šlo o zaměstnance v průmyslových oborech. Další z pachatelů uvedl, že je majitelem spediční firmy. Poslední z pachatelů uvedl, že je nezaměstnaný.

Spisy též obvykle poskytují informace o nejvyšším dosaženém vzdělání pachatelů. Více než polovina z nich byla vyučena bez maturity (28 osob, tj. 56 %) a téměř třetina měla úplné střední vzdělání či byla vyučena s maturitou (14 osob, tj. 28 %). Pouze jeden z pachatelů měl vyšší odborné vzdělání (Graf 16).

Graf 16: Nejvyšší dosažené vzdělání – tachografy (n = 50)



Nedílnou součástí analýzy trestních spisů v rámci kriminologického výzkumu je též sledování případné kriminální historie pachatelů. V téměř dvou třetinách případů (32 osob, tj. 64 %) se jednalo o osoby, které nebyly dosud pravomocně odsouzeny. Z těch, kteří již byli v minulosti odsouzeni (18 osob, tj. 36 %), byli pouze dva odsouzeni pro počítačové trestné činy.[61] Vícekrát než jednou bylo odsouzeno 13 osob, přičemž nejčastěji (v pěti případech) se jednalo o tři předchozí odsouzení. Jeden z pachatelů se mohl „pochlubit" dokonce osmi předchozími záznamy v opisu z Rejstříku trestů.

II.1.4.2 Průběh trestního řízení

Co se týče celkové délky trestního řízení od prvotního záznamu policie do pravomocného rozhodnutí soudu, ta se pohybovala od jednoho do 639 dní[62] – průměrně 144 dní. Ve dvou třetinách případů (31 případů, tj. 62 %) bylo pravomocně rozhodnuto do tří měsíců. Sledována byla též délka soudního řízení, tj. doba od doručení obžaloby, respektive návrhu na potrestání soudu do data nabytí právní moci konečného rozhodnutí ve věci. Ta se v rámci analyzovaného vzorku pohybovala od jednoho dne do 603 dní (Tabulka 5).

61 Konkrétně se jednalo v jednom případě o neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. d) TZ a v druhém o opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 1 písm. b) TZ.

62 Enormní délka řízení byla zapříčiněna průtahy v rámci řízení před soudem a využitím opravných prostředků (odvolání i dovolání).

Tabulka 5: Délka řízení – tachografy

	Celková délka řízení		Délka řízení u soudu	
	Počet	%	Počet	%
Do 1 měsíce	7	14	21	42
Od 1 do 2 měsíců	13	26	18	36
Od 2 do 3 měsíců	11	22	6	12
Od 3 do 4 měsíců	1	2	0	0
Od 4 do 5 měsíců	3	6	1	2
Od 5 do 6 měsíců	1	2	0	0
Od 6 měsíců do 1 roku	7	14	1	2
Od 1 do 2 let	7	14	3	6

Průběh trestního řízení a především jeho délka jsou mimo jiné ovlivněny využitím opravných prostředků a přibráním soudních znalců. Opravné prostředky byly využity pouze ve třech případech, z čehož pouze v jediném byl kromě řádných opravných prostředků využit též opravný prostředek mimořádný.[63] S ohledem na charakteristický způsob provedení zásahu do funkce digitálních tachografů nebyl ani k jednomu z případů zpracován znalecký posudek.

Ve více než dvou třetinách případů (35 případů, tj. 70 %) byla pachatelům uložena pouze jedna sankce. V jednom případě byla věc postoupena k projednání jako přestupek. Ve zbývajících případech (14 případů, tj. 28 %) byl kromě hlavní sankce uložen také trest vedlejší.

Ukládán byl především peněžitý trest dle § 67 a násl. TZ (ve 24 případech samostatně či jako hlavní sankce a ve čtyřech spolu s podmíněným trestem odnětí svobody) a podmíněný trest odnětí svobody dle § 81 a násl. TZ (ve 23 případech samostatně či jako hlavní sankce). Jednomu pachateli byl uložen samostatný trest zákazu činnosti dle § 73 a násl. TZ, spočívající v zákazu řízení všech motorových vozidel. Jednomu řidiči cizí státní příslušnosti byl uložen samostatný trest vyhoštění dle § 80 TZ. Vedle hlavní sankce byl čtrnácti pachatelům uložen též další trest. V osmi případech se jednalo o zákaz řízení motorových vozidel, ve čtyřech případech o peněžitý trest a ve dvou případech o propadnutí věci[64] dle § 70 TZ.

Výše uložených peněžitých trestů se pohybovala od 8 tis. Kč do 100 tis. Kč, kdy jejich průměrná výše činila 30 771 Kč. Podmíněný trest byl ukládán ve výměře od jednoho měsíce do 18 měsíců (průměrně 7 měsíců) se zkušební dobou v rozmezí od 12 do 30 měsíců (průměrně 17 měsíců). Trest zákazu činnosti byl uložen v délkách od 12 do 18 měsíců a jeho průměrná délka činila 13 měsíců.

63 Jednalo se o dovolání.

64 Konkrétně šlo o propadnutí elektronických zařízení použitých k zásahu do funkce tachografu a snímač pohybu KITAS s příslušnou kabeláží.

II.1.4.3 Kazuistika: zmatení tachografu

Koncem října 2018 zastavila hlídka Policie ČR nákladní vozidlo Volvo, které řídil 56letý polský státní příslušník J. S. Při kontrole údajů, zaznamenaných digitálním tachografem, bylo zjištěno, že v době, kdy bylo vozidlo zastaveno, měl řidič dle záznamů povinnou přestávku. Toto zjištění nasvědčovalo tomu, že by ve vozidle mohlo být nainstalováno zařízení, kterým řidič neoprávněně zasahuje do správného chodu digitálního tachografu. Řidič nejprve tvrdil, že muselo dojít k poruše záznamového zařízení, ale posléze doznal, že je vozidlo opravdu vybaveno zařízením ovlivňujícím chod digitálního tachografu. Následně vypověděl, že se zadrženým vozidlem jezdí asi tři roky a zhruba před měsícem si do něj nechal za 500 € nainstalovat zmíněné zařízení. S jeho pomocí chtěl ušetřit čas při popojíždění po lesních komunikacích v okolí místa nakládky dřeva ve V. Zde při vjezdu na lesní cestu aktivoval zařízení tím, že třikrát po sobě sešlápl plynový pedál a dvakrát brzdový pedál. Poté, co bylo dřevo naloženo, se J. S. vydal na cestu, přičemž zařízení ponechal nedopatřením zapnuté až do doby, kdy byl kontrolován policejní hlídkou. Následující den byla na základě příkazu Okresního soudu v B. provedena prohlídka nákladního vozu, k níž byl přizván konzultant zabývající se problematikou tachografů. Při prvotní prohlídce nebylo zařízení vzhledem k důmyslně skryté instalaci nalezeno, a tak došlo pouze k ověření toho, že způsobem, který řidič uvedl ve své výpovědi, lze skutečně ovlivnit funkci tachografu tak, že zaznamenával režim odpočinku. Na J. S. byla státním zástupcem Okresního státního zastupitelství v B. podána obžaloba pro spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. d), odst. 3 písm. a), b) TZ. Řidič byl následně samosoudcem Okresního soudu v B. uznán vinným z uvedeného přečinu a odsouzen k trestu odnětí svobody v trvání osmi měsíců, jehož výkon byl podmíněně odložen na zkušební dobu v trvání dvaceti měsíců. Dále mu byl uložen trest propadnutí věci, kdy se jednalo konkrétně o snímač pohybu vymontovaný z převodovky nákladního automobilu, plastovou krabičku se dvěma konektory vymontovanou ze zakrytovaného prostoru pod palubní deskou v místě spolujezdce a příslušnou napájecí kabeláž vymontovanou z prostoru šasi nákladního automobilu.

Tento případ ilustruje zásah do funkce digitálního tachografu prostřednictvím sofistikovaného technického zařízení. V rámci analyzovaných případů, týkajících se tachografů, nicméně docházelo spíše k případům jízdy s vloženou cizí kartou řidiče.

II.1.5 Závěr ke kapitolám Analýza trestních spisů a Digitální tachografy

Na základě poznatků získaných provedenou analýzou trestních spisů lze konstatovat, že v rámci celého zkoumaného vzorku převažují případy motivované majetkovým zájmem. Specifickou skupinu takto motivovaných skutků představují případy spočívající v zásahu do funkce digitálních tachografů. Tato skupina výrazněji ovlivnila složení vzorku co do pohlaví, věkové struktury a nejvyššího dosaženého vzdělání. Nejvýrazněji se projevila specifika této skupiny ve skladbě socioprofesního statusu pachatelů. Bez zajímavosti též není zjištění, že zatímco část vzorku, nemající vztah k tachografům, je ve více než polovině případů souzena v souběhu s dalšími trestnými činy, u tachografů se tak stalo jen v jediném případě. Skutková jednoduchost a s ní spojená absence důkazní nouze se odráží též v průběhu trestního řízení, neboť bylo ve dvou třetinách případů pravomocně rozhodnuto do tří měsíců od prvotního záznamu policie.

II.2 Virtuální násilí a majetkový zájem

Sledované případy bez věcí spojených s tachografy (n = 108) jsme rozdělili do dvou skupin dle motivace pachatele na majetkový zájem s motivací získání finančního obnosu (dále jen „MZ“) a na virtuální násilí, kdy bylo cílem poškodit oběť (dále jen „VN“). Tuto typologii jsme využili již v dřívější analýze spisů (Vlach, Kudrlová & Paloušová, 2020). Rozdíly mezi MZ a VN jsou podrobněji popsány v kapitole Tematické okruhy, formulace otázek a používaná terminologie. Téměř polovinu případů jsme identifikovali jako případy s MZ a více než dvě pětiny jako VN. Jeden v sobě nesl obě dvě dimenze a 10 případů nebylo možné zařadit ani do jedné skupiny (Tabulka 6).

Tabulka 6: Dělení případů dle jejich typu (n = 108)

	n	%
Majetkový zájem	52	48,1
Virtuální násilí	45	41,7
Kombinace obou typů	1	0,9
Nezařazeno	10	9,3

Mezi případy, které nebylo možné zařadit do ani jedné kategorie, se vyskytovaly např. kauzy, kde motivace nebyla zjištěna a ani ji nebylo možné odhadnout z kontextu. Nebo se jednalo o případy, které byly motivované zvědavostí pachatele, snahou někomu pomoci či touhou zvýšit si sebevědomí. Vyskytly se mezi nimi i pokusy o zajištění, nebo naopak smazání důkazů v souvislosti s jinou trestnou činností. V jediném případě, kde byla zjištěna kombinace VN a MZ, manžel sledoval prostřednictvím vzdáleného přístupu komunikaci své manželky a následně použil záznam této komunikace jako argumenty v rozvodovém řízení.

II.2.1 Majetkový zájem

MZ se v celém souboru vyskytl 52×, což tedy činilo téměř polovinu všech případů. Většina z nich byla řešena v souběhu s další trestnou činností (87 %), a to především v kombinaci s jinou než počítačovou trestnou činností – jmenovitě především s krádeží (§ 205), podvodem (§ 209) či neoprávněným opatřením, padělaním a pozměněním platebního prostředku (§ 234 TZ). Součinnost další osoby byla zaznamenána pouze v jednom případě.

Všechny tyto případy byly uzavřeny odsuzujícím rozsudkem. Většině pachatelů (60 %) byl uložen podmíněný trest na čtyři měsíce až tři léta (v průměru 15 měsíců, SD = 7,6) se zkušební dobou na jeden až tři roky (v průměru 34 měsíců, SD = 10,3). Čtvrtina pak dostala nepodmíněný trest na osm měsíců až pět let (v průměru 33 měsíců, SD = 16,6).

Nepodmíněný trest byl ukládán především v případech, kdy se pachatel dopustil trestného činu ve zkušební době předchozího trestu podmíněného, pachatel byl v minulosti již vícekrát trestán nebo svým jednáním způsobil větší či značnou škodu.

Ostatní pachatelé dostali pouze alternativní tresty, jako jsou obecně prospěšné práce (n = 2, na 250 a 800 dnů) či peněžitý trest (n = 6, s výší trestu od 5 do 108 tis. Kč). Další téměř čtvrtině pachatelů byl kromě hlavního uložen trest vedlejší. Jednalo se o další peněžité tresty (n = 6, od 3 do 60 tis. Kč) nebo propadnutí věci/í (n = 8), které však nemuselo nutně souviset s danou kyberkriminalitou, ale i jinou trestnou činností řešenou v souběhu.

Trestní řízení trvalo od 37 dnů po necelých sedm let, v průměru přibližně 20 měsíců. Řízení u soudu trvalo od 19 dnů po necelých šest let, v průměru přibližně sedm měsíců.

Nejdéle řešený případ se týkal neoprávněného vzdáleného přístupu k datům bývalého zaměstnavatele a jeho délka řízení se nejspíše odvíjela jak od zpracování několika znaleckých posudků (z oboru kybernetika, odvětví výpočetní technika), tak také využitím řádného i mimořádného opravného prostředku.

*O*pravný prostředek byl využit u více než čtvrtiny případů. U čtvrtiny byl také vytvořen znalecký posudek, z toho šest pouze z oblasti kybernetiky, pět pouze z jiné oblasti a dva jak z kybernetiky, tak i jiných oblastí.

V naprosté většině byli pachatelé (až na pět žen) muži ve věku od 17 do 45 let, v průměru 29 let (SD = 7,8). Mezi českými občany tvořili výjimku dva útočníci ze Slovenské republiky, jeden z Ukrajiny a jeden z Itálie. Především se jednalo o svobodné jedince (69 %). Většinou také měli nějaký příjem ze zaměstnání či podnikání (67 %), nicméně čtvrtina pachatelů byla nezaměstnaná. Necelá desetina měla vysokoškolské vzdělání, naopak třetina základní vzdělání včetně nedokončeného. V méně než polovině případů se jednalo o recidivisty (n = 25), z toho dvě třetiny byly trestány opakovaně.

Až na jeden případ byl vždy zjištěn způsob spáchání. U více než dvou třetin pachatel využil fyzického přístupu.

Jednalo se například o pachatele, který se zmocnil mobilního telefonu s aplikací pro e-banking, v níž jsou zadány přihlašovací údaje. Nebo zaměstnance, který z počítače na pracovišti přistupoval do firemních databází na firemní síti atp.

*K*romě dvou případů došlo ke zneužití hesla. Jednalo se především o využití zapamatovaného hesla v zařízení (např. na veřejném PC), nalezeného hesla či zneužití vlastního hesla k neoprávněnému jednání. Technický prostředek byl použit pouze v pěti případech. Třetina pachatelů zneužila přístupu v zaměstnání, a to především vlastního (pět pachatelů něčí jiný přístup). Cizí identitu využila necelá pětina, ale sociální inženýrství bylo identifikováno pouze ve třech případech.

Až na jeden případ byla zjištěna i použitá či napadená komunikační platforma. Ve třetině se jednalo o mobilní telefon, ve stejném množství o e-banking a v pětině případů o e-mail. Výskyt ostatních platforem byl minimální.

Co se týče poškozené strany, tak v necelé polovině (46 %) byla fyzickou osobou ve věkovém rozmezí 16–67 let v průměru 39 let (SD = 16,7),[65] více než třetina (38 %) právnickou osobou a zbytek případů poškodil různé kombinace obětí. Nikdy však nebyl poškozen stát. Ve většině případů (73 %) byl poškozen jeden subjekt. Byly však zaznamenány i případy, kdy došlo k poškození 31, 37 a 46 subjektů.

V *prvním a druhém případě se jednalo o podvodné nabídky zboží a služeb v prostředí sociálních sítí a inzertních portálů. Ve třetím případě pak šlo o aplikaci phishingu s následným neoprávněným přístupem k e-mailovým účtům a profilům na sociálních sítích, vydíráním, či nabídce hackerských služeb za úplatu.*

U necelé čtvrtiny případů nebyla zjištěna žádná způsobená škoda. Pokud však zjištěna byla, pak se pohybovala od 2 990 Kč do téměř šesti milionů korun, v průměru přibližně okolo 750 tis. Kč. Přičemž pět pachatelů způsobilo škodu za jeden milion korun. Průměrná zamýšlená škoda byla přibližně o 200 tis. Kč vyšší. Nemajetková újma byla zaznamenána pouze u šesti případů. Ve čtvrtině nebylo možné určit vztah pachatele a oběti. Pokud to ale určit šlo (n = 39), tak se jednalo především o kauzy z pracovního či rodinného prostředí.

II.2.2 Virtuální násilí

VN bylo zaznamenáno ve 45 případech, což tedy činí více než dvě pětiny. Oproti MZ bylo u VN řešeno signifikantně více případů bez souběhu s další trestnou činností (38 % oproti 14 %).[66] Nicméně většinou k souběhu stejně došlo. Skladba kvalifikací byla výrazně pestřejší než u MZ. Příkladem lze uvést paragrafy související s porušením tajemství (§ 182, 183 TZ) nebo z trestných činů proti pořádku ve věcech veřejných, jako je výtržnictví (§ 358) či stalking (§ 354). Součinnost byla zaznamenána pouze v jednom případě.

Tři případy skončily bez trestu z důvodu upuštění od potrestání pachatelů. Většina dostala trest podmíněný (69 %, což je o něco více než u MZ) na tři měsíce až dva a půl roku (v průměru 11 měsíců, SD = 5,8) se zkušební dobou od jednoho roku do čtyř let (v průměru 26 měsíců, SD = 10,6). Pěti pachatelům byl uložen trest nepodmíněný, a to ve čtyřech případech v rozmezí od jednoho roku do dvou a půl let. Nicméně jeden pachatel odešel s 12letým trestem. Dalších pět případů skončilo obecně prospěšnými pracemi (100–300 dní) a tři pachatelé dostali peněžitý trest (15, 16 a 36 tis. Kč). V rámci sedmi vedlejších trestů bylo čtyřikrát uloženo propadnutí věci a po jednom případě obecně prospěšné práce, peněžitý trest a zákaz činnosti (zaměstnání u Policie ČR aj. pořádkových služeb).

Trestní řízení trvalo 53 dnů po necelých devět let, v průměru přibližně 15 měsíců. Řízení u soudu trvalo od 15 dnů po necelých sedm let, v průměru přibližně sedm měsíců.

N*ejdéle řešený případ se týkal neoprávněné lustrace policistou v centrálním registru vozidel a jeho délka řízení se nejspíše odvíjela od plně využitých opravných prostředků, jak řádných, tak mimořádných.*

65 Pokud bylo v rámci jednoho případu vícero obětí, pak se nejprve spočítal průměr daného případu a až z něho celkový průměrný věk obětí.

66 Všechny uvedené rozdíly jsou signifikantní na hladině alfa menší 0,05.

Opravný prostředek byl využit o něco častěji (31 %), byť ne signifikantně, než u MZ (27 %). Znalecký posudek byl naopak vytvořen v menším množství – v jedné pětině oproti čtvrtině případů s MZ.

Až na čtyři ženy se jednalo o samé muže českého původu v rozmezí 15–53 let, v průměru 32 let. Podobně jako u MZ se jednalo především o svobodné jedince (62 %). Tři čtvrtiny měly nějaký příjem ze zaměstnání či podnikání (ve čtyřech případech se jednalo o úřední osobu), nicméně necelá pětina byla přímo nezaměstnaná. Oproti MZ byl u VN zaznamenán o něco vyšší podíl pachatelů se středoškolským vzděláním (69 % oproti 56 %) na úkor krajních kategorií (tento rozdíl však také není signifikantní). Podobně jako u MZ se z necelé poloviny jednalo o recidivisty (n = 20), z toho 70 % bylo trestaných opakovaně.

Stejně jako u MZ byl až na jeden případ zjištěn způsob spáchání. Oproti MZ pachatel výrazně méně častěji využil fyzický přístup (39 % oproti 67 %).

Šlo o fyzický přístup pachatele k napadenému/zneužitému systému. Např. policista, který měl přístup k služebnímu počítači a informačnímu systému při neoprávněných lustracích.

*K*e spáchání docházelo především prostřednictvím zneužití znalosti cizího hesla, případně zneužití hesla nalezeného nebo nahraného v zařízení. Technický prostředek nebyl použit v žádném z případů. A pouze ve třech případech došlo ke zneužití přístupu v zaměstnání. V těchto třech položkách se případy VN poměrně liší. Na druhou stranu cizí identitu zneužila podobně jako u MZ pětina pachatelů, stejně jako u sociálního inženýrství, které bylo identifikováno pouze ve třech případech.

U všech případů VN byla zjištěna komunikační platforma. Nejčastěji, a to téměř ve třech čtvrtinách, se odehrály přes sociální síť Facebook, více než polovina přes e-mail, třetina přes Messenger a pětina přes mobilní telefon. Ostatní platformy byly zastoupeny minimálně.

V naprosté většině se obětí stala fyzická osoba (respektive u dvou případů nebyla oběť známá a u jednoho došlo k poškození fyzické osoby a státu) ve věku od 12 do 62 let, v průměru 30 let (SD = 11,5), což je výrazně méně než u obětí MZ (39 let). Škoda byla způsobena pouze v jednom případě, a to v hodnotě 2 800 Kč. Zato nemajetková újma byla určena u více než poloviny případů, což je samozřejmě signifikantně více než u MZ (12 %). Především se jednalo o zamezení přístupu. Dále byla u pěti případů zaznamenána dehonestace, u čtyř fyzická újma, u tří psychická, u dalších tří manipulace s daty (poškození, úprava, smazání atp.) či jiné typy především související s narušením soukromí. Jako náhrada za nemajetkovou újmu byla oběti v jednom případě přiznána částka 200 tis. Kč. Pouze u pěti případů nebylo možné určit vztah mezi pachatelem a obětí. Pokud to šlo určit (n = 39), tak v naprosté většině případů (77 %) se jednalo o partnery, především ty současné.

II.2.3 Závěr k virtuálnímu násilí a majetkovému zájmu

Na aktuálních datech získaných ze spisů jsme opět mohli pozorovat rozdíly mezi námi vytvořenými kategoriemi případů s MZ a VN. V některých ohledech nesou obecná specifika kyberkriminality, ale v dílčích ohledech se samozřejmě liší, což upevňuje kvalitu této typologie.

Pokud bychom měli zmíněné rozdíly shrnout, tak VN je například v menší míře řešeno v souběhu s další trestnou činností než případy s MZ. Pokud k souběhu dojde, tak MZ je nepřekvapivě pojen především s majetkovými skutky. VN tak specifické není. Trestní řízení je v průměru u VN o něco kratší než u MZ, ale řízení u soudu už je srovnatelné. Paradoxně je však u VN o něco častěji využit opravný prostředek, ale naopak znaleckých posudků je realizováno méně (nejde však o signifikantní rozdíly).

Pachatelé spíše využívají fyzický přístup (mají přímý přístup k napadenému systému) u MZ a pět z nich dokonce využilo technický prostředek. V rámci VN je zase především využívána znalost hesla, protože se většinou jedná o případy, které se udály v kontextu (především stávajícího) vztahu. Z podstaty věci u MZ byla většinou zjištěna finanční škoda, která se naopak u VN téměř nevyskytovala – oběti VN byly totiž zasaženy především nemajetkovou újmou.

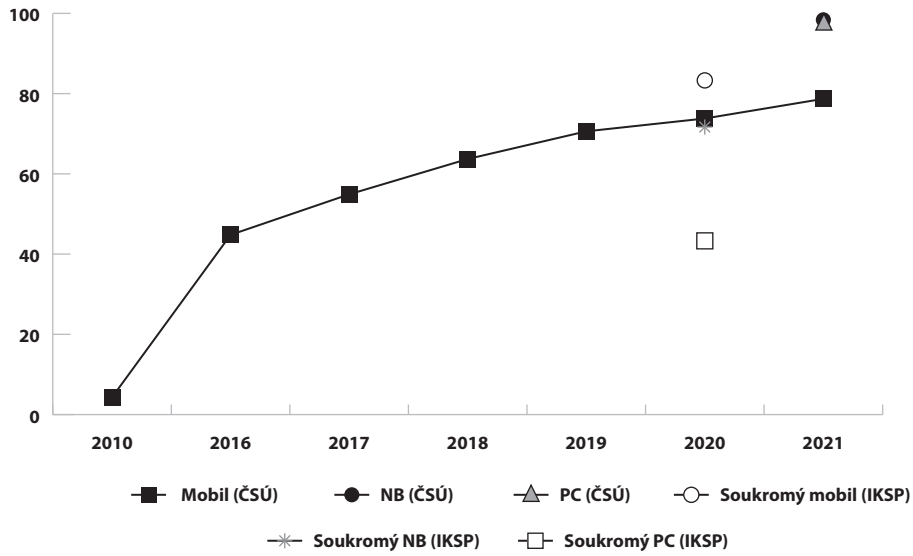
III.

Dotazník – vybavení

III.1 Fyzická vybavenost – používaná zařízení a jejich ochrana

Mezi nejpoužívanější digitální zařízení patří nepochybně počítač a mobilní telefon. Český statistický úřad (dále jen „ČSÚ“) eviduje počet uživatelů mobilního telefonu od roku 2010, přičemž z dat je patrný setrvalý nárůst (bez většího vlivu v souvislosti s pandemií covid-19). Ze stejného zdroje jsou dostupné údaje o používání počítačů při rozlišení stolního počítače (dále jen „PC“) a notebooku (dále jen „NB“), pouze však od roku 2021 (do té doby údaje o používání počítače zahrnovaly souhrnně PC i NB) (Graf 17).

Graf 17: Využívání různých zařízení k přístupu na internet (%)[67]



Z dotazníku vyplynulo, že čeští uživatelé internetu využívají k přístupu k němu zdaleka nejčastěji soukromý mobil, téměř stejně často pak soukromý NB a o poznání méně často soukromý PC. A protože drtivá většina osob patří mezi uživatele internetu,[68] v souvislosti s kyberkriminalitou rozhodně stojí za pozornost zabezpečení samotných zařízení používaných k přístupu na internet.

Pro lepší porozumění rozlišujeme údaje vztahující se k soukromým zařízením, zaměstnavatelským a k podnikatelským. Při používání více zařízení dané kategorie respondenti odpovídali vždy podle toho, které považovali za své hlavní.[69] Měli také k dispozici jednoduché definice: „*zaměstnanecká zařízení jsou poskytnutá zaměstnavatelem (např. počítač*

67 Zdrojem data dostupná na webu ČSÚ (czso.cz) pod kapitolou Využívání informačních a komunikačních technologií v domácnostech a mezi osobami, dále dotazníkové šetření IKSP.

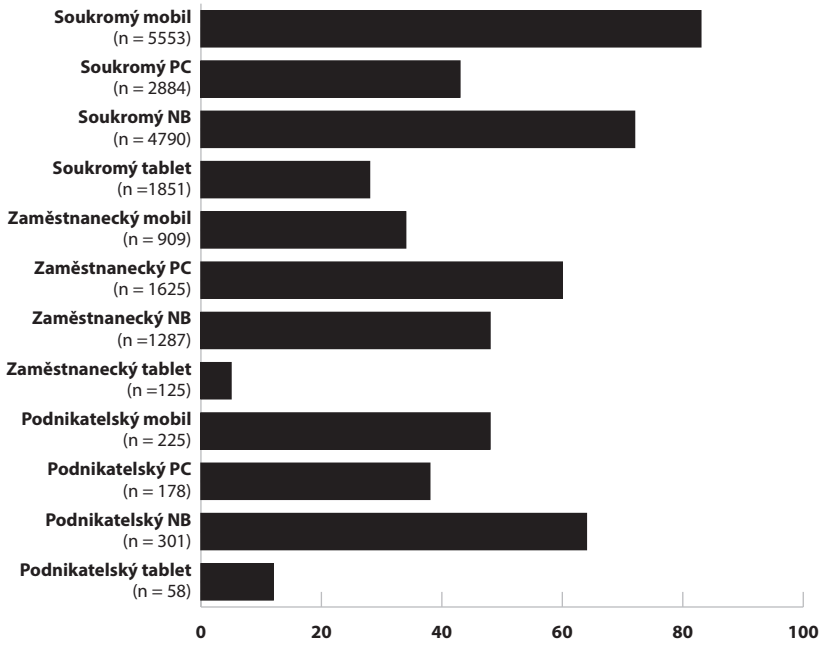
68 Podle ČSÚ v roce 2021 používalo 74 % osob starších 16 let internet denně nebo téměř denně, viz údaje dostupné na webu ČSÚ (czso.cz) pod kapitolou Využívání informačních a komunikačních technologií v domácnostech a mezi osobami – 2021.

69 Tzn. např. hlavní soukromý mobil spolu s hlavním zaměstnaneckým PC atp.

v kanceláři nebo služební mobil). Podnikatelská jsou Vaše vlastní, která však používáte výlučně pro pracovní aktivity. Soukromá zařízení jsou všechna ostatní, která jsou Vaše vlastní (např. Váš počítač, nikoliv partnerův/partnerčin)." Dotazy směrovaly na mobily, PC, NB a tablety.

Dle očekávání používalo nejvíce respondentů soukromá zařízení, a to mobilní: kromě předpokládaných mobilních telefonů převážily nad běžnými stolními počítači notebooky. Výjimku představují zaměstnanecká zařízení, mezi kterými stále převažuje PC (Graf 18).

Graf 18: Zařízení používaná k přístupu na internet (%)



Muži používají významně často soukromé PC a tablety a zaměstnanecká zařízení vyjma PC. Ženy naproti tomu preferují soukromé NB a zaměstnanecké PC. Osoby mladší 29 let soukromé mobily a NB, ve věku 30–44 let soukromé mobily a tablety spolu se zaměstnaneckými NB, starší osoby pak soukromé i zaměstnanecké PC. Z hlediska používaného operačního systému dle očekávání převažuje u mobilů a tabletů Android (78–81 % u mobilů a 45–63 % u tabletů) a u počítačů Windows (87–90 % u PC a 81–91 % u NB).[70]

III.1.1 Související bezpečnostní návyky

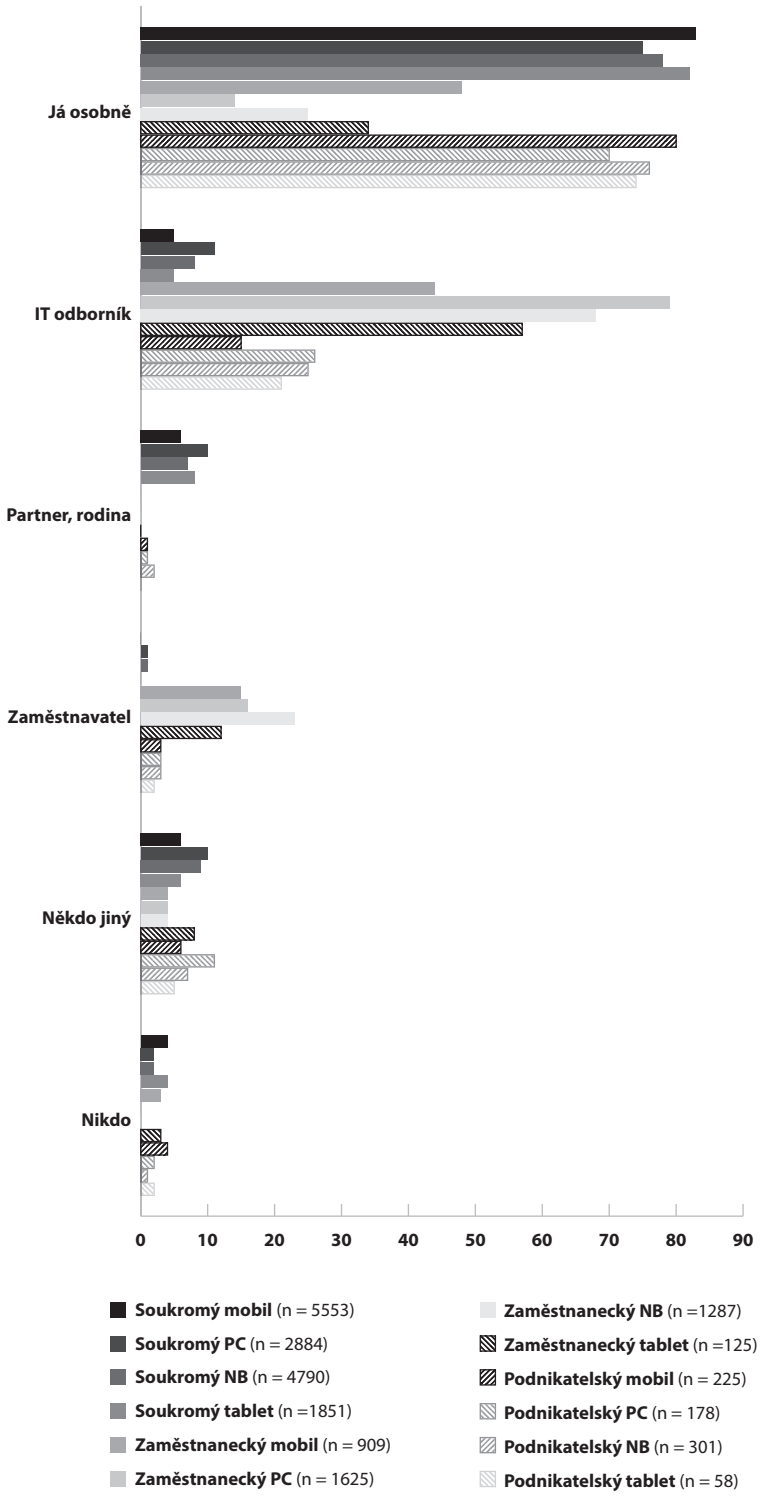
S používáním konkrétních zařízení a aplikací se pojí, resp. měly by být spojeny i základní bezpečnostní návyky, jako jsou zabezpečení zařízení, používání antiviru nebo (ne)ochota sdílet svá zařízení a hesla s dalšími osobami. Zařízení používaná k přístupu na internet jsou poměrně dobře zabezpečená (např. aktualizace, antivirus, nastavení hesla atp.), ať už

70 Jen několik desítek osob při výběru odpovědi nevědělo, co je to operační systém.

samotným uživatelem nebo někým jiným, nejčastěji IT odborníkem. Jen v minimálním počtu případů není soukromé zařízení zabezpečeno vůbec, žel nejčastěji právě u nejvíce používaných mobilních telefonů.

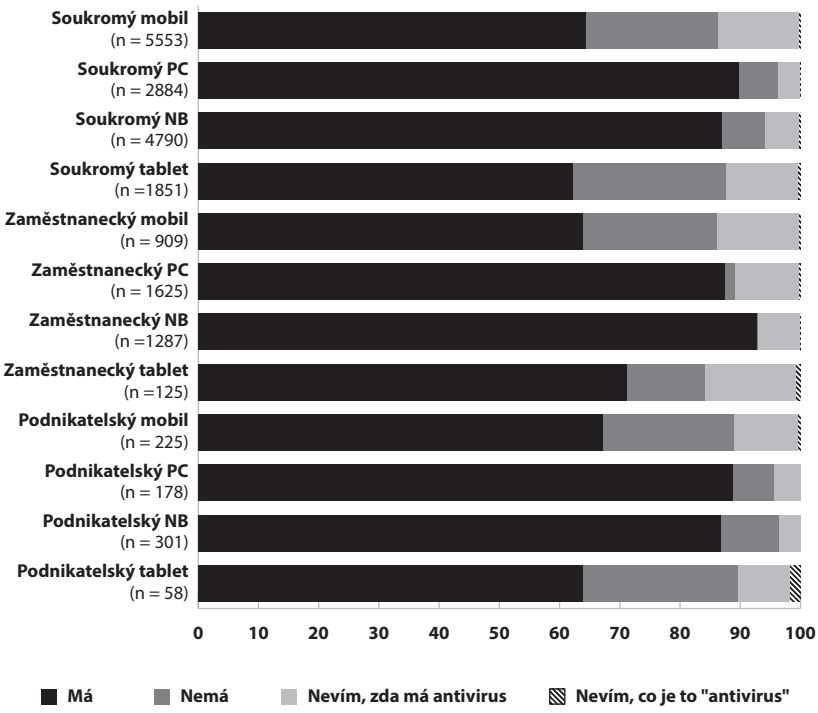
O zabezpečení zařízení se v převážné většině starají jejich uživatelé, ať už pouze sami nebo spolu s dalšími osobami. K těm se řadí především IT odborníci, kteří v některých případech dokonce péči o zařízení přebírají namísto uživatelů samotných, a to pochopitelně téměř výlučně v případě zaměstnaneckých zařízení (Graf 19). Respondenti se ovšem obraceli i na další osoby, ať už své nejbližší nebo kamarády, kolegy z práce, sousedy atp. Na kolegy zejména (nikoliv však výlučně) v případě zaměstnaneckých zařízení. Naopak na partnery a rodinné příslušníky výhradně při péči o vlastní soukromá zařízení, přičemž péče byla zhruba rozdělena napůl mezi partnery vs. (ostatní) rodinné příslušníky, pouze s drobnými rozdíly v závislosti na typu zařízení.

Graf 19: Kdo se stará o zabezpečení zařízení (%)



Bez ohledu na to, kdo se stará o zabezpečení zařízení, odpovídali respondenti i na otázku, zda má jejich zařízení antivirus. Pouze několik desítek jich nevědělo, co je to antivirus (řádově do 1 %).[71] Řada z nich ovšem nevěděla, zda jejich zařízení antivirus má, či nikoliv, a to zejména u mobilních telefonů, případně tabletů (Graf 20). Podotýkáme, že mobilní telefony v sobě zpravidla žádný antivirus nemají, pokud ho nenainstaluje sám uživatel, čímž se odlišují především od PC a NB, u kterých bývají alespoň minimální podoby antiviru součástí operačního softwaru. Kromě mobilních telefonů tak odpovědi respondentů ohledně antiviru v jejich zařízení spíše vyjadřují, zda mají vůbec povědomí o elementární formě ochrany svého zařízení.

Graf 20: Odpovědi na otázku: *„Má Vaše zařízení antivirus?“* (%)



Na první pohled je patrné, že ochrana mobilních telefonů a tabletů poněkud zaostává za PC a NB, a to jednak co do povědomí o jejich ochraně, tak co do absence antiviru vůbec. Signifikantně často nevěděly o přítomnosti antiviru ženy (všechna soukromá i zaměstnanecká zařízení a podnikatelský mobil) a osoby mladší 29 let (soukromá zařízení kromě NB, zaměstnanecké počítače).

Jistotu měli naopak muži a osoby ve středním věku, ať už šlo o používání či absenci antiviru. Antivirus používali významně často muži v soukromých NB a v zaměstnaneckých zařízeních kromě mobilů. Dále též osoby v produktivním věku 45–59 let – ty používaly

71 Některé podrobnější poznatky byly již publikovány (Kudrlová, 2022). Vliv na znalost antiviru má zřejmě pouze vzdělání.

antivir v soukromých mobilech a tabletech, ve všech zaměstnaneckých zařízeních a v podnikatelských mobilech. Pozadu nezůstávali ani respondenti starší 60 let, neboť používali antivirus ve všech soukromých zařízeních kromě NB a v zaměstnaneckých mobilech.[72] Za zmínku stojí též vysokoškoláci s antiviry v soukromých NB a zaměstnaneckých tabletech.

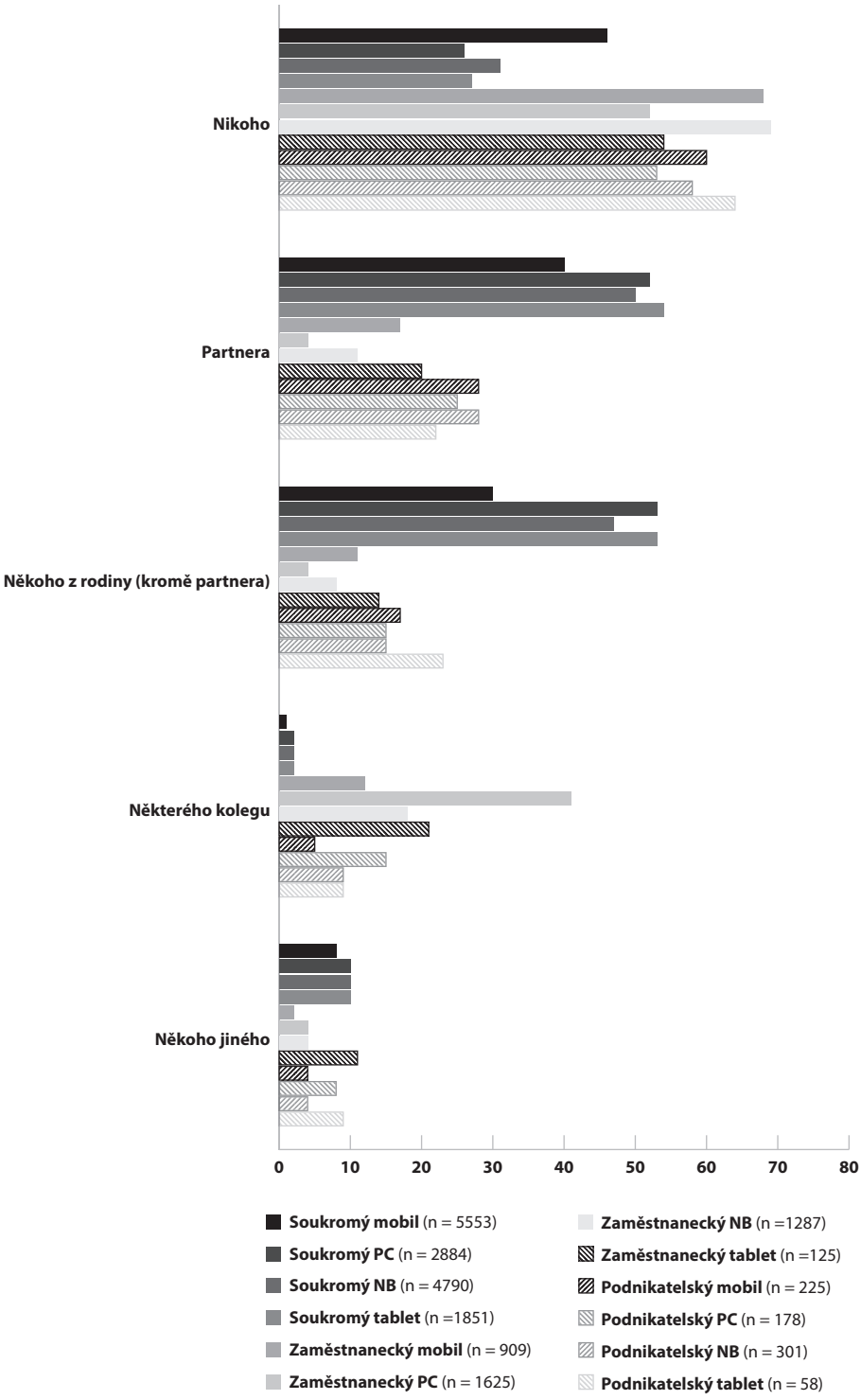
Muži ovšem zároveň významně často antivirus naopak nepoužívali (všechna soukromá zařízení a zaměstnanecké mobily a tablety), podobně jako osoby v mladším produktivním věku 30–44 let (soukromé mobily a tablety, zaměstnanecké mobily a PC a podnikatelské mobily a NB). Přidaly se k nim i osoby mladší 29 let (všechna soukromá zařízení) a vysokoškoláci (soukromé mobily a tablety, podnikatelské NB).

Používání ochranného softwaru má nepochybně svoji váhu, neméně důležitou roli však hraje (ne)ochota sdílet svá zařízení s jinými lidmi. Nemluvíme o vyzkoušení kamarádova mobilu, nahlédnutí do kolegova PC atp., ale o použití daného zařízení někým jiným bez vlastního dohledu.[73] Nejčastěji se dle očekávání sdílí zařízení s nejbližšími osobami, zaměstnanecká zařízení pak nezřídka i s kolegy (Graf 21). I sdílení s nejbližšími osobami však může mít svá úskalí, a to především v podobě zneužití k získání přístupu k online účtům, viz kapitola Dotazník – online účty.

72 Nutno podotknout, že u některých zařízení nelze určit případnou existenci vztahu s ohledem na nízký počet relevantních dat.

73 Podrobněji se zabýváme i sdílením přihlašovacích údajů k e-bankingu, viz kapitola E-banking.

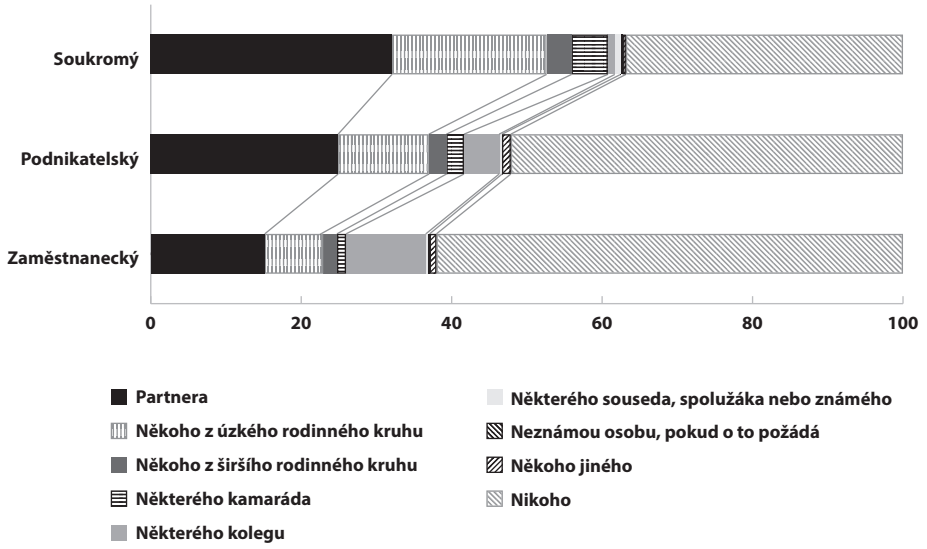
Graf 21: Odpovědi na otázku: *„Koho necháte použít Vaše soukromé zařízení bez dozoru?“* (%)



Obecně lze říci, že významně často nenechávají nikoho zacházet s vlastními zařízeními bez dozoru muži, osoby starší 45 let a vysokoškoláci. Partnerům a členům užšího rodinného kruhu v tomto směru důvěřují především ženy, osoby mladší 44 let a opět vysokoškoláci, osobám z širšího rodinného kruhu pak osoby mladší 29 let. Kamarádům ženy, osoby mladší 29 let a osoby s pouze základním vzděláním. Kolegům taktéž ženy a osoby mladší 29 let. Vše se ovšem vztahuje pouze na soukromá a/nebo zaměstnanecká zařízení, podnikatelská zařízení hrají v tomto směru jen mizivou roli.

Když se podíváme na jednotlivá zařízení podrobněji, zjistíme např., že ženy nechají významně často používat bez dozoru svůj soukromý mobil partnery, příslušníky užšího rodinného kruhu i kamarády, v případě zaměstnaneckého mobilu kolegy (muži naopak k soukromému mobilu nikoho bez dozoru nepouští). Osoby mladší 29 let nechají partnery, kamarády, kolegy i někoho ze skupiny soused/spolužák/známý, u zaměstnaneckého mobilu pak partnery a kolegy. Osoby ve věku 30–44 let opět partnery a členy užší rodiny, u zaměstnaneckého mobilu kamarády. Osoby starší 45 let k soukromému mobilu nikoho významně často nepouští, ve věku 44–59 let ani k zaměstnaneckému mobilu. Respondenti s pouze základním vzděláním umožňují přístup kamarádům. Vysokoškoláci partnerům a kolegům, v případě zaměstnaneckého mobilu ovšem významně často nikomu přístup bez dozoru nepovolí (Graf 22).

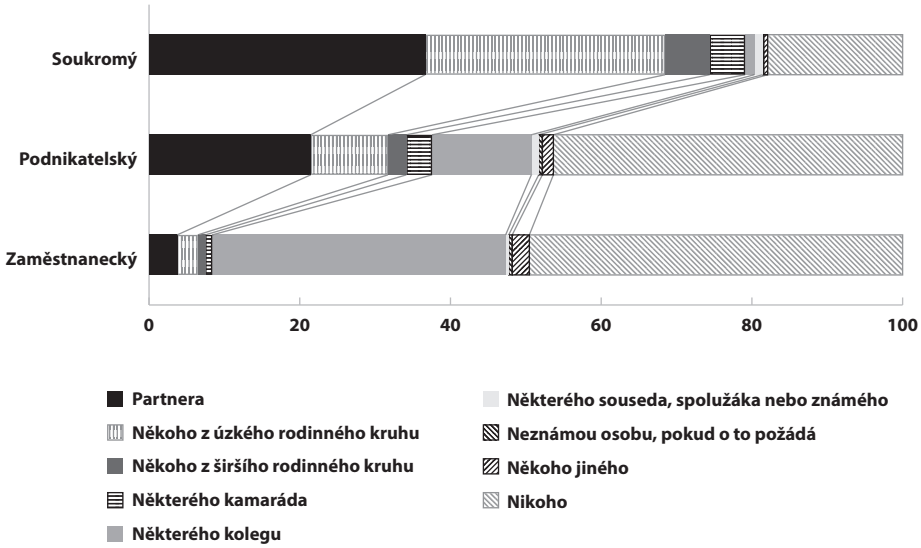
Graf 22: Odpovědi na otázku: *„Koho necháte použít svůj mobil bez dozoru?“* (%)



Z hlediska přístupu k PC (Graf 23) se ukázala podobná korelace u soukromých i zaměstnaneckých zařízení pouze u mužů, kteří nenechají se svým zařízením bez dozoru nikoho (s výjimkou umožnění dispozice se soukromým PC příslušníkům úzkého rodinného kruhu, vyjma partnerů). Ženy naproti tomu nechají používat svůj soukromý PC kamarády, sousedy/spolužáky/známé i někoho jiného, zaměstnanecký PC pak kolegy. Svá PC sdílejí ovšem převážně osoby mladší 29 let, a to soukromé (širší rodina, kamarád, soused/spolužák/známý) i zaměstnanecké (partner, úzká rodina, kolega). Osoby ve věku

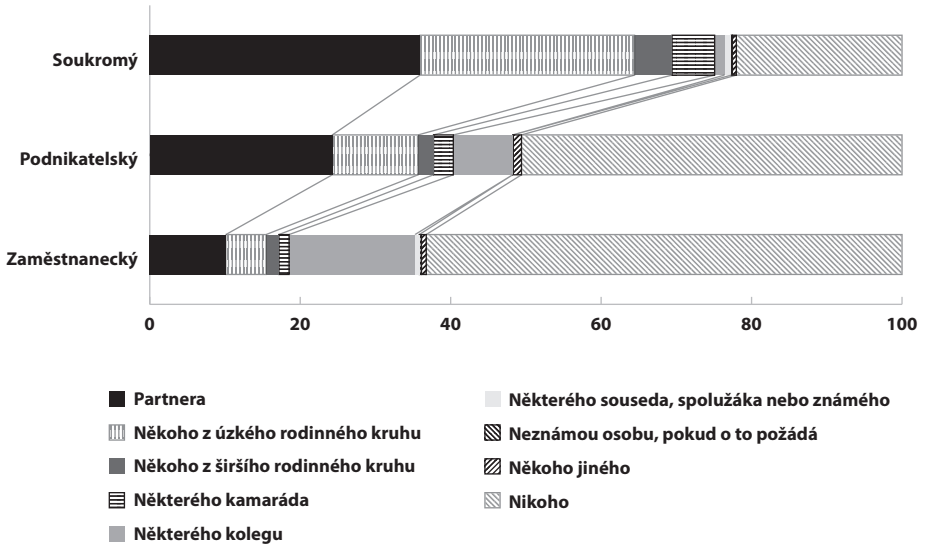
30–44 let sdílejí soukromé PC s partnery, kamarády, kolegy, ve věku 45–59 let už jen se členy úzké rodiny (zaměstnanecké PC pak s nikým), senioři starší 60 let už soukromé PC nesdílejí s nikým. Respondenti s pouze základním vzděláním by sdíleli své soukromé PC s kamarády a širší rodinou, vyučení bez maturity s někým jiným či nikým, kdežto zaměstnanecké PC s kolegy, podobně jako středoškolsky vzdělaní respondenti. Vysokoškoláci by naopak zaměstnanecké PC s nikým nesdíleli, kdežto soukromé by sdíleli s partnery, úzkou rodinou i kolegy.

Graf 23: Odpovědi na otázku: *„Koho necháte použít svůj PC bez dozoru?“* (%)



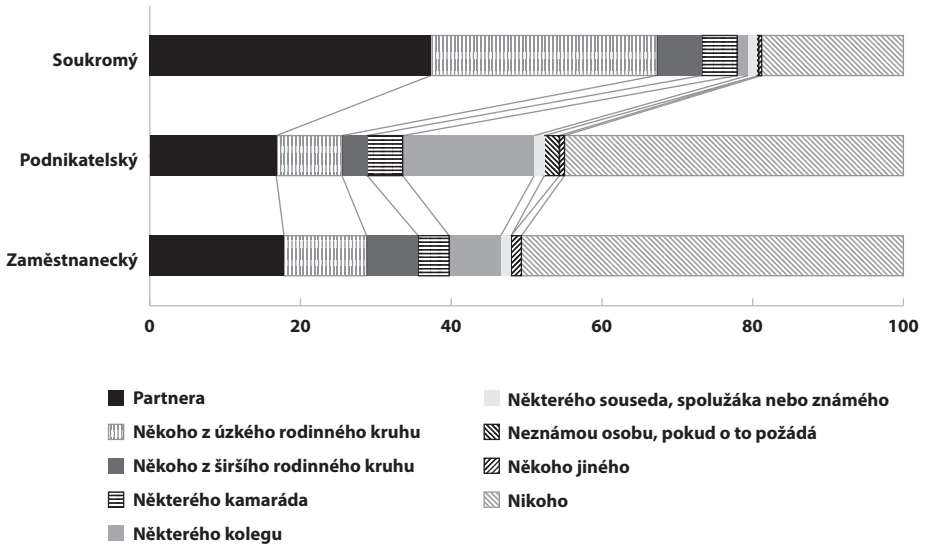
Sdílení NB se jeví v obecných rysech obdobně (Graf 24). Muži by soukromý ani zaměstnanecký NB nesdíleli, ženy naopak soukromý sdílely s partnery, úzkou rodinou, kamarádem i sousedem/spolužákem/známým a zaměstnanecký s kolegou. Ještě více sdílející se zdají osoby mladší 29 let, a to co do soukromého NB (partner, rodina, kamarád, kolega, soused/spolužák/známý) i zaměstnaneckého NB (partner, kolega). Ve věku 30–44 let by umožnili přístup k soukromému NB už jen partnerům, u zaměstnaneckého NB nikomu, podobně jako ve věku 45–59 let. Nad 60 let by neumožnili přístup k soukromému zařízení raději nikomu. Respondenti s pouze základním vzděláním by nechali použít svůj soukromý NB kamaráda, vyučení bez maturity zaměstnanecký NB kolegu. Při získání maturity by sdíleli soukromý NB s úzkou rodinou, s vyšším odborným vzděláním zaměstnanecký s kolegy. Vysokoškoláci jsou ochotni sdílet své soukromé NB s partnery a kolegy, zaměstnanecké naopak s nikým.

Graf 24: Odpovědi na otázku: *„Koho necháte použít svůj NB bez dozoru?“* (%)



U zaměstnaneckého tabletu (Graf 25) lze nalézt jen jediný vztah, a to seniory starší 60 let, kteří by ho nesdíleli s nikým. Muži mají tendenci nesdílet s nikým svůj soukromý tablet. Ženy jsou naopak ochotny soukromý tablet sdílet, a to s rodinou i kamarády. Osoby mladší 29 let s širší rodinou, kamarádem, kolegou i sousedem/spolužákem/známým. Ve věku 30–44 let pouze s partnerem a užší rodinou, po překročení 60 let pak již s nikým. Respondenti s pouze základním vzděláním by sdíleli soukromý tablet s kamarády, vysokoškoláci pouze s partnerem a užší rodinou (podobně jako osoby ve věku 30–44 let).

Graf 25: Odpovědi na otázku: *„Koho necháte použít svůj tablet bez dozoru?“* (%)



Zbývá ještě doplnit, že řada osob absolvovala někdy v životě nějaký kurz či školení spojené s používáním digitálních technologií, ať už v podobě práce s informačním systémem firmy, kancelářským softwarem či jiné. Nás zajímalo absolvování kurzu spojeného s bezpečným užíváním digitálních technologií, i když nelze vzhledem k jednorázovému dotazu bez časového ukotvení vyvodit spojení mezi absolvováním takového kurzu a případnou viktimizací, či naopak redukcí viktimizace (stejně jako používáním antiviru, sdílením hesel atp.). Kurz bezpečného užívání informačních technologií absolvovalo někdy v životě 17 % respondentů, 7 % si nevzpomnělo. Byli to významně často muži, osoby mladší 29 let a vysokoškoláci, na druhé straně stojí ženy a osoby starší 60 let. Vidíme zde určitý náznak opakující se v řadě dalších oblastí, kdy do popředí vystupuje na jedné straně skupina mužů a/nebo osob mladších 29 let, případně doplněná o vysokoškoláky, na straně druhé pak žen, případně doplněných seniory a/nebo osobami s nižším vzděláním. Signifikance se objevily i u jiných skupin osob (zde i jinde), nicméně tyto zmíněné se ukazují nejčastěji.

III.2 Mentální vybavenost – používané aplikace a sebeprezentace

III.2.1 Používané aplikace

Podobně jako používaná zařízení nás zajímaly i vybrané používané aplikace. Sociální sítě (dále jen „SNS“) od počátku své existence slouží jako významný komunikační prvek. Vznik prvních sice podnítila touha po sdílení obsahu,[74] komunikaci koneckonců relativně nově zajišťoval e-mail a chatovací aplikace jako ICQ, komunikační aspekt sociálních sítí však začal být záhy zřejmý.

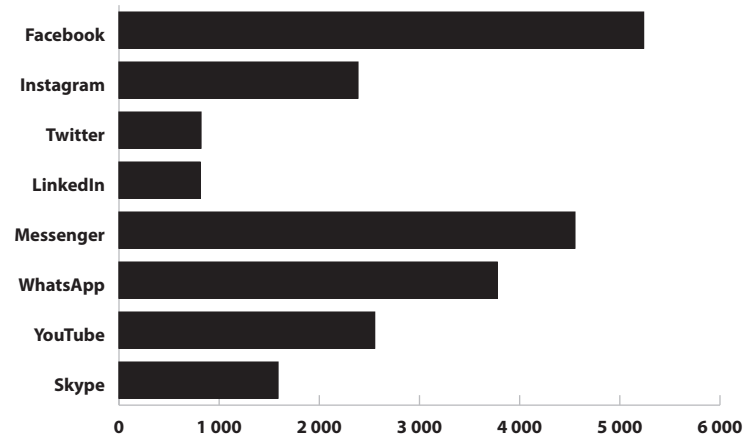
V roce 2020* používala soukromě sociální sítě většina respondentů (79 %), zdaleka nejčastěji šlo již tradičně o Facebook. Záměrně jsme se dotazovali také zvlášť na vybrané komunikační platformy, jako jsou WhatsApp, Messenger či Skype, které mohou sloužit jako sociální sítě i jako prostá alternativa SMS či telefonování. Specifický byl také dotaz na používání YouTube coby sociální sítě.[75] Zřejmá je drtivá převaha aplikací spojených s organizací Meta – zde Facebook, Messenger a WhatsApp (Graf 26).[76]

74 Zřejmě první sociální síť per se Myspace byla určena ke sdílení hudby.

75 Mělo by tedy jít nikoliv o pouhé pasivní konzumenty videí na YouTube, ale o aktivní uživatele komunikující s ostatními uživateli či svým publikem.

76 Společnost Meta Platforms, Inc., dříve Facebook, Inc., patří mezi největší giganty na poli informačních technologií. Dle svých prohlášení buduje postupně tzv. Metaversum – spojení různých virtuálních prostorů (sociální sítě, obchody, instituce atd.) v jeden celek, který budou moci uživatelé navštěvovat s pomocí zařízení pro virtuální realitu.

Graf 26: Počet uživatelů SNS v roce 2020*



K používání sociálních sítí v roce 2020* tíhly mezi respondenty spíše ženy, osoby pouze se základním, anebo naopak nejvyšším vzděláním,[77] respondenti ve věku do 44 let (naproti tomu signifikantní počet starších osob sociální sítě naopak nepoužíval).

Zhruba desetina z těchto uživatelů v roce 2020* nějakou sociální síť používat přestala. Činily tak zejména osoby mladší 29 let a osoby s pouze základním vzděláním. Nejvíce osob opustilo Facebook (zejména osoby vyučené bez maturity), Skype (respondenti ve věku 45–59 let) a WhatsApp (ženy). Za zmínku stojí také vysokoškoláci, kteří opouštěli LinkedIn, a mladí respondenti do 29 let spolu s respondenty s pouze základním vzděláním loučící se s aplikací Snapchat.[78]

Důvodů pro opuštění byla celá řada, mezi nejčastější patřil malý přínos dané sítě pro uživatele (typicky „*žrout času*“, „*nuda*“, „*nebaví mě*“, „*nepotřebuji ji*“, „*používám jinou*“, „*známí přešli jinam*“), nedostatečnost aplikace a jejího obsahu po technické stránce, zejména v porovnání s jinými aplikacemi (pomalost, příliš mnoho reklam, problémy s instalací atp.). V neposlední řadě to byly i otázky bezpečnosti či sebeochrany (např. „*ochrana soukromí*“, „*přerušení kontaktu s určitými osobami*“). Objevovaly se také odpovědi přímo odkazující na napadení nebo pochybnost o bezpečnosti účtu („*někdo mi napadl účet*,“ „*podvod s kryptoměnami*“, „*časté zneužívání, falešné profily*“ atp.). K méně častějším odpovědím pak patřily

77 Význam (nejen) vzdělání z hlediska používání sociálních sítí ukazují i jiné výzkumy, včetně českého prostředí (Pospíšilová, 2023).

78 Hlavní devizou aplikace Snapchat bylo sdílení fotografií jejich pouhým zobrazením na předem určený časový úsek (třeba i pouhých několik vteřin), po kterém aplikace fotografie automaticky smaže. Po počáteční euforii mnoha uživatelů ze zdánlivě bezpečného sdílení fotografií, které díky automatickému smazání nenesou riziko pozdějšího zneužití, přišlo vystřízlivění s poznáním, že zobrazené snímky lze přesto uchovat (aplikace sama to sice neumožňuje, ale na té nejjednodušší úrovni může kdokoliv s chytrým telefonem např. vyfotit zařízení zrovna zobrazující danou fotografii). Zdánlivá bezpečnost s sebou tak nese o to větší riziko zneužití, neboť může vést ke sdílení intimnějších fotografií než obvykle v důsledku dojmu bezpečnosti komunikace.

výroky jako „*digitální detox*“, „*nesouhlasím s tím, aby provozovatel sítě prováděl cenzuru*“ nebo také spojení soukromých účtů na sociálních sítích se zaměstnáním (např. „*užíval jsem v zaměstnání a to skončilo*,“ „*odevzdal jsem pracovní telefon*“ atp.).

III.2.2 Sebeprezentace

Sociální sítě nabízejí ohromný prostor pro sdílení nejen názorů, myšlenek či prostých údajů o životě toho či onoho, ale s rostoucí přenosovou rychlostí začalo nabývat na intenzitě sdílení fotografií a videí. A to do té míry, že vznikly a stále se používají aplikace určené prakticky výlučně ke sdílení vizuálního či audiovizuálního obsahu (typicky v tomto směru nejvyužívanější Instagram).

Nedílnou součástí používání sociálních sítí je proto vlastní sebeprezentace online. Řada uživatelů pečuje o vlastní digitální stopu velice důkladně (např. pořízení stovky fotografií za účelem zveřejnění jediného obrázku, mnoha hodin natáčení pro výsledné minutové video atp.).[79] Požádali jsme proto respondenty o stručné vyjádření ohledně jejich sebeprezentace (vybírali všechny přiléhající z nabídnutých odpovědí). Zhruba polovina respondentů používajících sociální sítě svůj účet na nich využívá aktivně (především ženy, mladší respondenti ve věku do 44 let a osoby s pouze základním vzděláním). Zhruba polovina také vystupuje pod vlastní identitou (zejména muži, respondenti do 29 let a vysokoškoláci), a zároveň téměř stejné množství se snaží minimalizovat svou digitální stopu (především senioři starší 60 let a vysokoškoláci). Zhruba pětina respondentů maže již neaktuální obsah (zvláště ženy, respondenti do 29 let a senioři).

K aktivním osobám patří pochopitelně především mladší generace (mladší 44 let), ale také osoby s pouze základním vzděláním. Na odpovídajících údajích si zakládají spíše ženy a osoby mladší 29 let (mažou již neaktuální údaje). U mužů je patrná určitá sebejistota,[80] vystupují především pod vlastní identitou (či méně často naopak nikoliv), dle svých slov aktivně pečují o svou sebeprezentaci a jsou youtubery. Naproti tomu vysokoškoláky lze označit za sebejisté, leč obezřetné, vzhledem k vystupování pod vlastní identitou a zároveň snahu o minimalizaci své digitální stopy. Specifickou skupinu již tradičně, jak se ostatně ukazuje i v jiných oblastech, tvoří senioři starší 60 let, kteří se zdají být opatrní spíše z neznalosti a podobně jako vysokoškoláci usilují o minimalizaci své digitální stopy, zároveň však mažou již neaktuální údaje.

79 V současnosti je však patrný určitý opačný trend, který začíná vyrovnávat usilování o dokonalost vlastní sebeprezentace online, a to snaha o naopak autentické zachycení běžných situací a osob v daném okamžiku. Na poli audiovizuální kultury jde např. o filmy zdánlivě či skutečně natočené obyčejným mobilním telefonem (byť ve skutečnosti nepochybně pečlivě upravené mimo jiné i s ohledem na to, aby výsledný dojem byl co nejautentičtější), příběhy „obyčejných“ lidí atp. Trend se nevyhýbá ani sociálním sítím, mezi nimiž se vymyká relativně nová aplikace BeReal. Usiluje o maximální autenticitu svých uživatelů tak, že každý den vydá v náhodném čase pokyn svým uživatelům, aby jejím prostřednictvím během následujících dvou minut pořídili fotografii sebe, své činnosti či případně svého okolí. Pakliže je fotografie pořízena opakovaně nebo mimo vyhrazený časový limit, informace o tom se zobrazí spolu s fotografií. Cílem je zachytit skutečnou realitu bez příkras. I zde má ovšem uživatel plnou kontrolu nad tím, zda a co zveřejní, či nikoliv.

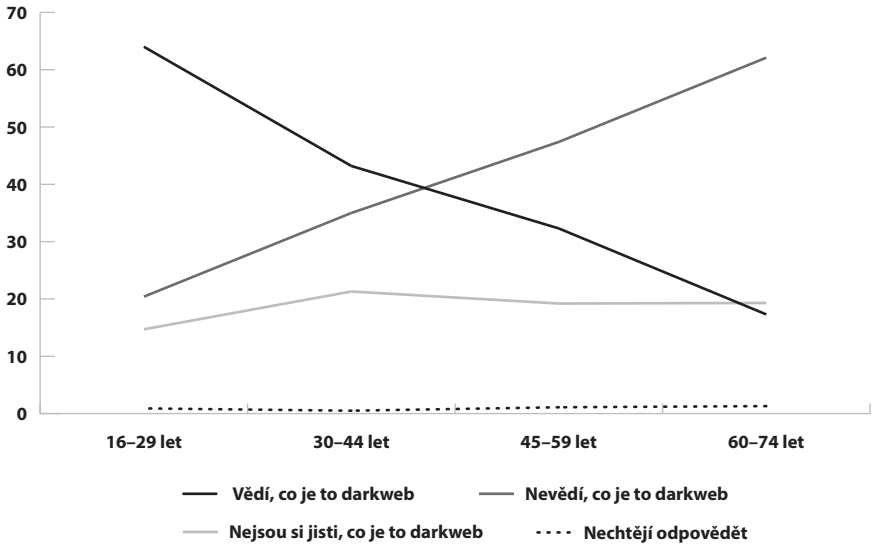
80 Odpovídá i datům zjištěným např. v souvislosti s phishingem a ransomwarem.

III.3 IT odbornost – darkweb

V předchozím výzkumu IKSP, zaměřeném na kyberkriminalitu prostřednictvím analýzy trestních spisů, se ukázalo, že většina aktérů přinejmenším počítačových trestných činů (§ 230–232 TZ) nedisponovala, resp. nevyužila žádné zvláštní IT dovednosti nad rámec běžných uživatelských znalostí. Zároveň se veřejně dostupné statistiky věnují v IT oblasti především počtům studentů či zaměstnanců v IT oborech. Kromě absolvování kurzu bezpečného užívání informačních technologií (viz kapitola Související bezpečnostní návyky) jsme proto také zjišťovali, zda a jaké mají zkušenosti s darkwebem, k jehož používání se uchylují obvykle jedinci uživatelsky již o něco zdatnější. Zajímalo nás, zda respondenti vůbec vědí, co si pod výrazem „darkweb" či „darknet" představit[81] a zda s ním mají vlastní zkušenost.

Překvapilo nás, že poměr respondentů znalých a neznalých darkwebu je prakticky stejný (40 a 41 %), 19 % si nebylo jisto, 1 % respondentů odpovědět nechtělo. Významně často měli povědomí o darkwebu muži (49 %), osoby mladší 44 let (64 % osob mladších 29 let a 43 % ve věku 30–44 let), se základním vzděláním, s maturitou nebo vysokoškolsky vzdělaní (50 %, 44 % a 50 %). O darkwebu nevěděly naopak významně často ženy (49 %), osoby starší 45 let (47 % osob ve věku 45–59 let a 62 % respondentů starších 60 let) a vyučené bez maturity (60 %). Určující pro povědomí o darkwebu se zdá být věk, když s rostoucím věkem klesá počet respondentů znalých darkwebu, a naopak stoupá počet těch neznalých (Graf 27).

Graf 27: Povědomí o darkwebu dle věku (%)

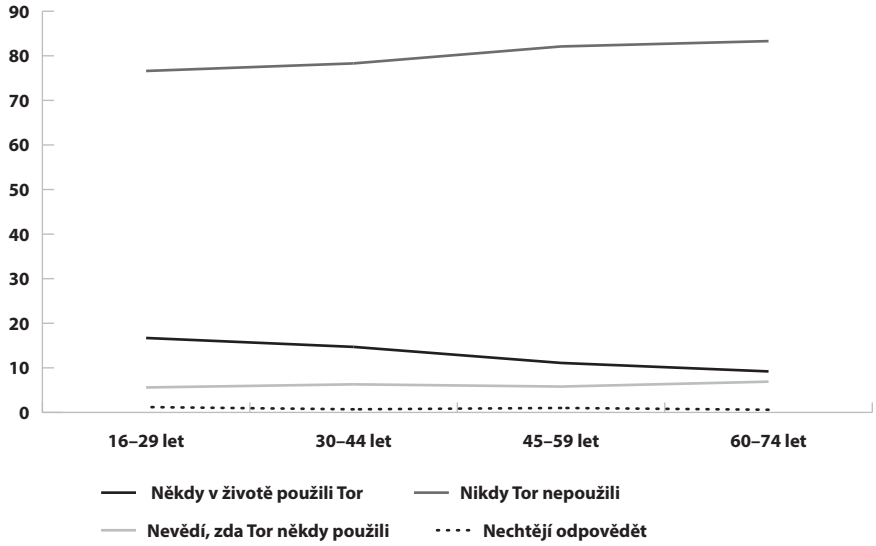


Bez ohledu na znalost či neznalost výrazu „darkweb" respondenti odpovídali i na otázku „*Použil/a jste někdy v životě prohlížeč Tor? Jde o prohlížeč internetu jako je Google*

81 Neposuzovali jsme, zda představa respondentů o darkwebu odpovídá skutečnosti, šlo nám o jejich vlastní posouzení svých vědomostí.

Chrome, Internet Explorer atp." Zkušenost s ním mělo 13 % ze všech respondentů (888 osob),[82] 6 % nevědělo a opět 1 % nechtělo odpovědět. I zde je patrné signifikantní spojení s pohlavím, vzděláním a věkem, když Tor použili především muži (16 % mužů Tor použilo oproti pouhým 10 % žen, 7 % žen si nebylo jisto) a osoby s pouze základním vzděláním (19 %), zatímco vysokoškoláci naopak použili Tor významně málo často. Význam věku je signifikantní ve všech věkových kategoriích, ať už jde o použití, či naopak nepoužití Toru (Graf 28).

Graf 28: Použití Toru dle věku (%)



Respondenti, kteří někdy v životě použili Tor, mohli vybrat v odpovědi na otázku po jejich motivaci k jeho použití zvědavost, snahu zakrýt svou identitu, nebo uvést jiný důvod. Čtvrtina jich nevěděla či si nevzpomněla (226 osob, 25 %, signifikantně často ženy a osoby starší 45 let), někteří odpovědět nechtěli (31 respondentů, 4 %, signifikantně často ženy).

Zdaleka nejvíce respondentů použilo Tor ze zvědavosti (495 osob, 56 %), signifikantně často muži a osoby mladší 29 let. Zvědavi byli především na samotný darkweb jako takový (356 osob, tj. 72 % zvědavých respondentů používších někdy Tor), významně často osoby mladší 29 let a respondenti jen se základním vzděláním. Jinou odpověď uvedlo pouze 51 respondentů (tj. 10 % zvědavých), přičemž i jejich odpovědi poukazovaly spíše na darkweb jako takový.[83] Ostatní již nevěděli nebo odpovědět nechtěli.

152 osoby (17 % respondentů, kteří někdy použili Tor) se snažily zakrýt svou identitu (signifikantně často muži a osoby ve věku 30–44 let). Převážná většina usilovala o anonymitu online vůbec, bez konkrétního důvodu (130 osob, tj. 86 % osob skrývajících identitu).

82 Z toho třetina respondentů (289 osob, tj. 33 %) použila Tor v roce 2020*.

83 Šlo o odpovědi jako *„anonymita"*, *„darkmarkety"*, *„jak funguje přístup k obsahu"* atp.

Další vycházely z politických důvodů (15 osob, tj. 10 %) nebo zakrývaly nelegální aktivitu (17 osob, tj. 11 %). Ostatní uvedli jiný důvod, nechtěli odpovědět nebo si nebyli jisti (5, 5 a 9 respondentů, tj. 3 % a 6 %).[84]

Jiný důvod použití Toru než zvědavost a/nebo snahu o zakrytí identity uvedlo 69 osob (8 % respondentů, kteří někdy použili Tor). Objevovaly se vlastní odpovědi jako „*bezpečnost*", „*drogy*", „*hledání informací*", „*kamarádi*", „*darkweb*", „*porno*", „*výzkum*" aj.

Dílčí aktivity na darkwebu zahrnovaly především brouzdání jen tak (583 osob, tj. 66 % respondentů používších někdy Tor), významně často v případě mužů a osob mladších 29 let. Osoby mladší 29 let se také významně často zajímaly o pornografii, kterou jinak uvedlo 56 osob (6 %). Téměř čtvrtina relevantních respondentů na rozdíl od brouzdání cíleně vyhledávala nějaký obsah (210 osob, 24 %). 71 osob (8 %) používalo Tor ke komunikaci s ostatními uživateli, pouhých 13 osob (2 %) k hazardní hře. 33 osob (4 %) navštívilo některé z darkwebových tržišť (významně často opět muži a osoby mladší 29 let), zajímaly se především o drogy a zbraně (15 a 13 osob, tj. 46 a 39 % návštěvníků), dále o software, pornografii a warez[85] (11, 10 a 9 osob, tj. 33, 30 a 27 % návštěvníků).[86] Jen několik málo respondentů uvedlo něco jiného, nevzpomnělo si či nechtělo odpovědět.

III.4 Závěr k dotazníkové sekci související s vybavením respondentů

Získaná data vypovídají o určité výseči fyzické a mentální vybavenosti i IT odbornosti respondentů. Potvrdila hojnost používání soukromých zařízení a mobilů vůbec, také prakticky absenci základní neznalosti „*co je to antivir*". Ukázala ovšem také slabiny v zabezpečení právě nejhojněji používaných mobilů. O zabezpečení se starají převážně uživatelé sami a/nebo s pomocí IT odborníků. Přesto, nebo možná právě proto, se najde i řada zařízení bez základní antivirové ochrany. Mimoto jsou mnohá zařízení sdílena s dalšími osobami, zejména ze strany žen a osob mladších 29 let, kdežto muži a senioři starší 60 let jsou v tomto směru opatrnější a svá zařízení by nesdíleli.

Bez ohledu na používaná zařízení a jejich případné sdílení používali v roce 2020* respondenti hojně sociální sítě, zejména Facebook (zvlášť ženy, osoby mladší 44 let a osoby s pouze základním vzděláním). Mezi aktivnější aktéry patří generace mladší 44 let, zejména osoby mladší 29 let. Sebejistě vystupují muži, sebejistě a obezřetně vysokoškoláci. Obezřetní se zdají být i senioři, nikoliv však výlučně k nelegálním aktivitám. Nějakou představu o něm má pravděpodobně téměř polovina internetové populace, přičemž zhruba osmina internetové populace s ním má osobní zkušenost (z toho třetina v roce 2020*,

84 Možné odpovědi zněly „*snaha zanechat o svém jednání online, co nejméně informací vůbec, bez konkrétního důvodu*", „*politické důvody*", „*nelegální činnost online*", „*z jiného důvodu, uveďte z jakého*", „*nevím, nevzpomínám si*" a „*nechci odpovědět*", přičemž bylo možné vybrat více odpovědí, pokud se vzájemně nevylučovaly. Posouzení případné „nelegálnosti" činnosti jsme opět záměrně ponechali na subjektivním zhodnocení samotných respondentů.

85 Zjednodušeně řečeno obsah porušující autorská práva (filmy, hudba atp.).

86 5 z 11 zájemců o software se zajímalo o malware, tj. škodlivý software (např. počítačový virus).

případně i z dřívějška). Z dat vystupuje do popředí specifická skupina respondentů-mužů a respondentů mladších 29 let. Zejména věk se zdá být předurčující pro povědomí, ale i pro používání darkwebu.

IV.

Dotazník – ransomware a phishing

IV.1 Ransomware

Mezi největší kyberstrašáky zejména organizací patří nepochybně ransomware.[87] Mezi aktuální hrozby ho pravidelně řadí ve svých zprávách český NÚKIB i evropská ENISA. Kritický dopad „úspěšného" ransomwaru na poškozený subjekt lze samozřejmě zmírnit pravidelnými zálohami systému i veškerých dat, ale jednak zálohy vyžadují ke své údržbě značné množství zdrojů, jednak samotná obnova vyžaduje čas i náklady (navíc není jisté, že obnovená data budou v pořádku nebo útok neproběhne opakovaně). S ransomwarem se ovšem setkávají i jednotlivci. Není jich sice tolik a většina z nich bude spíše náhodnou obětí plošného útoku než cíleným terčem, potíže spojené se zašifrováním dat a vydíráním s příslibem jejich obnovy se jich však také týkají.

Z našich respondentů se setkalo v roce 2020* s ransomwarem 290 osob (4 % ze všech respondentů), 415 osob (6 %) si nebylo jisto.[88] Významně často se osobně s ransomwarem setkali muži a naopak nesetkali ženy spolu s vysokoškoláky. 40 % napadených (117 respondentů) mělo v roce 2020* dokonce opakovanou zkušenost.

K našemu překvapení se našlo mezi respondenty 74 osob (1 %), které samy někdy v životě zablokovaly něčí zařízení a požadovaly za jejich zpřístupnění výkupné. Významně často tak odpovídali respondenti mladší 29 let.[89] 50 % z útočníků (37 osob) tak učinilo v roce 2020*, z toho 70 % (26 osob) v roce 2020* opakovaně. Následující informace vyjma motivace útočníků již čerpáme pouze od poškozených v roce 2020*.

Respondenti odpovídali ohledně toho incidentu, který oni sami považovali v roce 2020* za nejzávažnější,[90] uváděli nejčastěji napadání počítačů (PC i NB). Na jednu stranu bychom očekávali, že v ohrožení budou spíše mobilní telefony s ohledem na méně časté zabezpečení antivirem, nicméně zjištění jde na vrub pravděpodobně faktu, že řada uživatelů stahuje aplikace pouze z oficiálních obchodů Google Play a App Store, kde prochází automaticky kontrolou proti malwaru. Také je možné, že k napadení mobilních telefonů (nebo i jiných zařízení) docházelo častěji, dané incidenty však nebyly vyhodnoceny jako ty nejzávažnější.

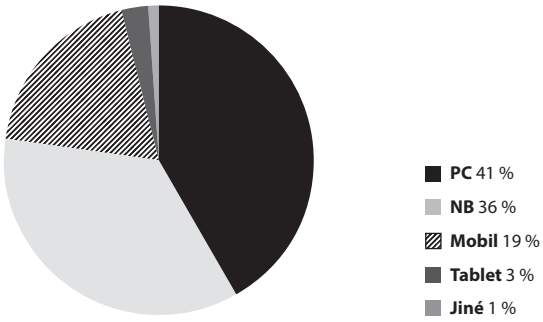
87 Zablokování (obvykle zašifrování) celého nebo části zařízení spojené zpravidla s požadavkem platby výměnou za jeho odblokování.

88 Předpokládáme, že v takovém případě o ransomware nešlo, neboť je těžko zaměnitelný s jiným škodlivým jednáním (např. pouhým zavirováním zařízení bez jakéhokoliv požadavku), a tudíž by si byli respondenti jisti. Jiným důvodem nejisté odpovědi může být pouze časová nejasnost, nicméně pro jistotu správnosti výsledků zde uvedené nejisté odpovědi nebereme v potaz.

89 47 respondentů odmítlo na otázku odpovědět, i zde významně často osoby mladší 29 let.

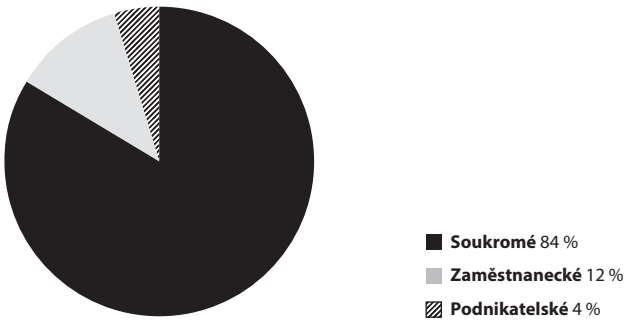
90 Tzn., že i když např. útočník zašifroval zároveň jejich mobilní telefon i NB, respondent měl možnost uvést pouze jeden z těchto incidentů.

Graf 29: Napadená zařízení



Zkušenost s napadením mobilního telefonu mělo 54 respondentů (19 %, významně často osoby mladší 29 let), s napadením PC ovšem 120 respondentů (41 %, významně často muži a osoby starší 60 let). Napadení NB zakusilo 103 respondentů (36 %, tj. dohromady s PC 77 % napadení počítačů), napadení tabletu 8 (3 %). Tři respondenti (1 %) uvedli „jiné" zařízení, konkrétně (různě označený) server (Graf 29).

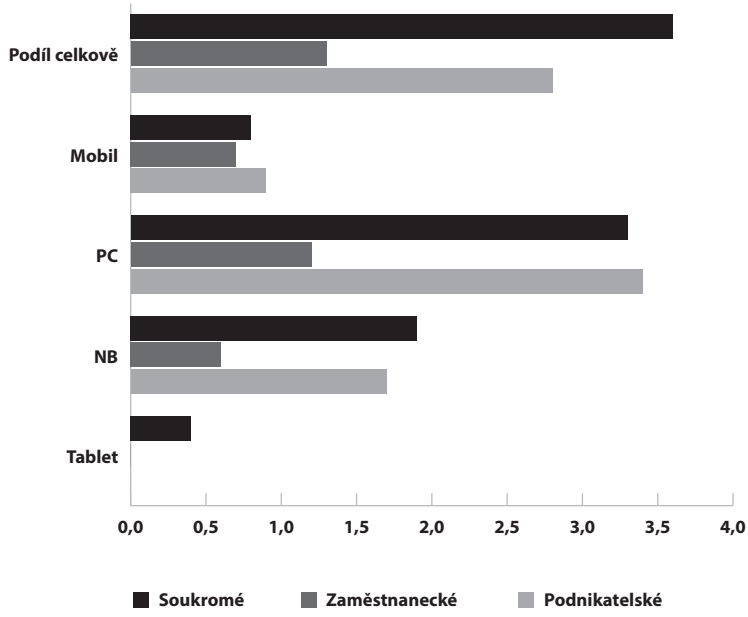
Graf 30: Určení napadeného zařízení



Mezi napadenými zařízeními převažují soukromá, která jsou využívána výrazně častěji než zaměstnanecká či snad podnikatelská (Graf 30). Podíl napadených zařízení v rámci celkového počtu používaných zařízení daného druhu ukazuje následující graf (Graf 31). I v tomto srovnání se ukazuje, že soukromá zařízení zaujímají ve své kategorii největší podíl, nicméně pohybujeme se pouze v desetinách až jednotkách procent. O incidentu se soukromým zařízením hovořili významně často respondenti s pouze základním vzděláním, kdežto o zaměstnaneckých zařízeních vysokoškoláci.[91]

91 Zřejmě je to ovlivněno tím, že vysokoškoláci pravděpodobně častěji zastávají pozice, ve kterých mají vůbec nějaká zaměstnanecká zařízení k dispozici.

Graf 31: Podíl napadených zařízení (%)



Z 290 respondentů, jejichž zařízení v roce 2020* někdo napadl ransomwarem, bylo zhruba ve třetině případů zablokováno celé zařízení (32 %, 93 zařízení), v 53 % pouze nějaký obsah (155 zařízení), část respondentů si nevzpomněla (42 zařízení). Při částečné blokaci šlo především o konkrétní aplikace a uložený obsah (46 % a 32 %), dále o uživatelské nastavení (např. fotografie na pozadí, 16 %) či něco jiného (14 %).

Více než dvěma třetinám respondentů (68 %, 63 osob) s celým zablokovaným zařízením se podařilo uvést zařízení do původního stavu, necelé čtvrtině alespoň částečně (24 %, 22 osob). Při pouze částečné obnově měli respondenti problémy zejména s uloženým obsahem či jeho částí (např. fotografie). Respondenti s pouze částečně zablokovaným zařízením měli výsledky obdobné, když se 90 osobám podařilo získat zpět celý zablokovaný obsah (58 %), 47 respondentům alespoň jeho část (30 %).

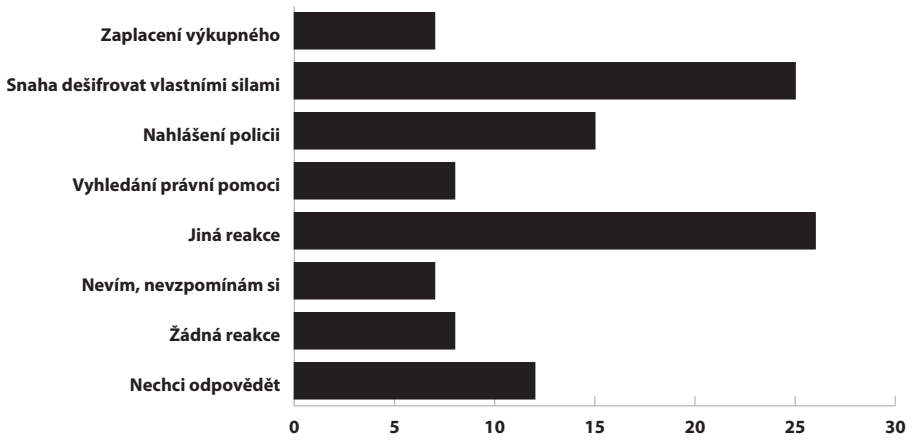
Jako primární motivaci uváděli samotní původci[92] ransomwaru především finanční prospěch (38 %). Objevila se ovšem i zvědavost (16 %) a jiná motivace (5 %), včetně např. „*aby se synovec učil*". Bohužel plných 27 % si již motivaci nevybavilo a 16 % odpovědět nechtělo.

92 Resp. část ze skupiny 37 respondentů, kteří sami nejméně jednou v roce 2020* zablokovali něčí zařízení či jeho obsah a požadovali výkupné výměnou za jeho opětovné zpřístupnění.

Po napadených respondentech požadovali útočníci finanční částky nejčastěji v českých korunách (32 %). Další v pořadí byly bitcoiny (22 %), eura (17 %) a americké dolary (11 %). Samotné výše požadovaných hodnot ovšem neuvádíme, neboť respondenti v řadě případů uváděli zjevně nesmyslné částky (např. 1 Kč nebo naopak 1 milion BTC atp.).[93]

Čtvrtina respondentů, jejichž zařízení bylo napadeno, se pokusila dešifrovat obsah sama, významně často tak činili muži. 21 respondentů zaplatilo výkupné, nicméně stojí za zmínku, že několika z nich se přesto nepodařilo získat ztracený obsah zpět nebo uvést zařízení zcela do původního stavu. „Jiná" reakce zahrnovala např. žádost o pomoc IT odborníka.

Graf 32: Reakce na ransomware (%)



Na policii se obracely významně často ženy, osoby mladší 29 let a vysokoškoláci, s jejím jednáním převládala spíše spokojenost (69 %). Celkově však důvěra ve schopnosti policie objasňovat ransomware není příliš velká, neboť se jí to spíše daří podle 15 % respondentů (významně často osoby mladší 29 let), kdežto 45 % si myslí opak (významně často muži a vysokoškoláci).

IV.1.1 Závěr k ransomwaru

Ransomware reálně postihuje jen relativně malou část používaných zařízení (nižší jednotky procent), přičemž část z nich se navíc daří uvést alespoň částečně do původního stavu. Přesto představuje závažné jednání s potenciálem způsobit výrazné škody. Jejich výši bohužel nedokážeme na základě referovaného výzkumného šetření hodnověrně posoudit, vzhledem k nesrovnalostem v odpovědích ohledně výše uvedených požadovaných částek.

93 Určitou pochybnost lze vyjádřit i ohledně překvapivě vysokého procenta respondentů, po nichž měli útočníci vyžadovat výkupné v českých korunách.

Zdá se, že ohroženy jsou především počítače, ať už stolní nebo notebooky, což může být do jisté míry vysvětleno vlivem oficiálních obchodů pro stahování aplikací do mobilních telefonů, které samy kontrolují přítomnost malwaru v nabízených aplikacích a z nichž řada uživatelů stahuje obsah výlučně.

Muži působí v reakcích na incidenty sebevědoměji, když se snaží uvádět svá zařízení do původního stavu vlastními silami, ženy a osoby mladší 29 let se zase častěji obracejí na policii. Přesto je latence ransomwaru značná.

IV.2 Phishing[94]

Troufáme si odhadnout, že s phishingem se v životě setkala drtivá většina uživatelů internetu, ať už ho odhalila jako phishing či nikoliv. Phishing může být součástí sofistikovaného sociálního inženýrství,[95] častěji však půjde o plošnou kampaň mířící na relativně náhodné cíle. Pro lepší porozumění a přidanou hodnotu poznatků rozlišujeme mezi phishingem osobních údajů a phishingem peněz. Cílem obou typů je zisk původce – u phishingu vyžadujícího peníze je cíl evidentní, u phishingu osobních údajů půjde zpravidla o snahu získat přihlašovací údaje k e-bankingu či jiné obdobné aplikaci nebo o osobní údaje za účelem jejich dalšího prodeje na černém trhu (např. údaje o platebních kartách). Respondenti měli při vyplňování dotazníku k dispozici jednoduché definice: phishingem jsou „*falešné e-maily, ve kterých se odesílatel vydává za někoho jiného a požaduje od Vás poslání peněz nebo sdělení osobních údajů. Příkladem může být falešný e-mail z banky požadující ověření přihlašovacích údajů nebo falešná výzva exekutora k zaplacení neexistujícího dluhu.*“ Zjišťovali jsme mimo jiné četnost útoků v roce 2020*, adresu odesílatele a reakci adresáta na incident.

IV.2.1 Aktéři phishingu

V roce 2020* se s phishingem osobních údajů setkalo 21 % respondentů používajících e-mail.[96] Významně často tak odpovídali muži, ženy si častěji nebyly jisty, zda šlo o podvodný e-mail, případně nevěděly, či si nevzpomínaly, zda jim takový e-mail v roce 2020* přišel. K nejistým odpovědím se přiklánějí i ohledně opakovanosti phishingových e-mailů požadujících osobní údaje, kdežto muži jsou si jistější. O opakované zkušenosti s phishingem osobních údajů v roce 2020* se vyjádřilo s jistotou 46 % adresátů, dalších 13 % mluvilo o pravděpodobně opakovaném phishingu. Významně často vypovídaly o phishingu vyžadujícím osobní údaje muži, osoby ve věku 30–44 let a vysokoškoláci, málo často naopak osoby starší 45 let a ženy, případně osoby s pouze základním vzděláním (liší se v závislosti na otázce po jakémkoliv nebo opakovaném útoku).

94 Kapitola vychází z publikovaného článku (Kudrlová, 2022), na kterém se autorsky podílel i tehdejší řešitel Mgr. Lukáš Kutil.

95 Např. v podobě tzv. spear phishingu (cílený phishing), mířícího na konkrétního zaměstnance za účelem proniknout jeho prostřednictvím do jinak uzavřené firemní sítě.

96 Další 4 % respondentů váhala, zda šlo o phishing.

Situace ohledně peněžního phishingu se velice podobá e-mailům vyžadujícím osobní údaje, je ovšem násobně častější. Setkalo se s ním 40 % respondentů používajících e-mail,[97] z toho 61 % opakovaně. Opět vidíme mezi jistějšími a častějšími adresáty muže a vysokoškoláky, na druhé straně pak ženy, nejmladší respondenty spolu s nejstarší generací (méně než 29 let a více než 60 let) a respondenty s nižším vzděláním.

Za nejčastějšího domnělého odesílatele phishingu požadujícího osobní údaje uváděli respondenti banku (18 %), významně často muži a osoby v produktivním věku 30–59 let. Ženy, nejmladší respondenti (méně než 29 let) a osoby s nižším vzděláním (základní či vyučen bez maturity) se dle svých vyjádření naopak setkávali s bankou coby domnělým odesílatelem méně často. Vzhledem k tomu, že velká část phishingových e-mailů necílí na konkrétní uživatele, uvedené hodnoty vypovídají zřejmě spíše o schopnosti phishing detekovat než o jeho cílení. Jiní domnělí odesílatelé se dostali spíše jen ojediněle do výběru incidentů (v nižších jednotkách procent), které respondenti považovali za nejzávažnější. Za zmínku stojí již jen sociální sítě nebo méně časté, leč zákeřné e-maily zdánlivě od exekutora či Policie ČR.

U peněžního phishingu stále figurovaly banky coby domnělí odesílatelé podvodných e-mailů nejčastěji (11 %), rozdíl oproti dalším v pořadí – exekutor, Česká pošta, Policie ČR či sociální síť – již nebyl tak patrný. Banky opět uváděli nejčastěji muži.

Jen mizivou část phishingových e-mailů oznámí respondenti na policii, častěji muži a osoby mladší 29 let. Nejméně podléhají phishingovým útokům, resp. zašlou své osobní údaje vysokoškoláci.

Požadované peníze pak odesílají častěji ženy než muži, následně ovšem také častěji vyhledávají právní pomoc. Častěji také v reakci na peněžní phishing mění své přihlašovací údaje.

Mezi respondenty se našlo i 1 % rozesílatelů phishingu (65 osob), významně často muži a osoby mladší 29 let.[98] Téměř polovina z nich (43 %) tak učinila v roce 2020*, z toho téměř tři čtvrtiny (71 %) opakovaně. Ať už šlo o peněžní phishing či osobní údaje (otázky směřovaly na phishing jako takový bez dalšího rozlišení), motivace převažovala finanční (57 %), nicméně zvědavost také hrála svou roli (39 %).

IV.2.2 Závěr k phishingu[99]

Některá zjištění v rámci České republiky potvrzují poznatky jiných obdobných studií provedených v zahraničí – např. informace o peněžním phishingu a poznatky R. Leukfeldta (2015), jiná je zpřesňují (např. odlišení peněžního phishingu od phishingu usilujícího o osobní údaje) a další jsou zcela ojedinělá (např. reakce na detekovaný phishing).

97 5 % si nebylo jisto, zda šlo o phishing. 12 % napadených respondentů si nebylo jisto, zda se s phishingem setkali v roce 2020* častěji.

98 42 respondentů odmítlo odpovědět.

99 Podrobnější údaje ohledně phishingu lze nalézt v již uvedeném článku (Kudrlová, 2022).

Zdá se, že muži a vysokoškoláci se z hlediska phishingu lépe orientují. Uvádějí sice vyšší incidenci (jednorázové i opakované zasažení), ale zároveň nižší viktimizaci. Pravděpodobně však nejde o samotné pohlaví a vzdělání jako takové, ale další okolnosti, taktéž ovlivněné věkem, pohlavím a vzděláním. Úvahy směřují k teorii rutinních aktivit, která jako vysvětlující faktory viktimizace phishingovými útoky identifikuje určité proměnné v oblasti aktivity a času stráveného na internetu, a nikoliv demografické charakteristiky obětí (Leukfeldt, 2014; Jansen & Leukfeldt, 2016).

Ženy sice častěji phishingu podléhají, častěji se však (spolu s osobami mladšími 29 let) obracejí na policii či jiné osoby, což může napomoci dopadení pachatele či alespoň zamezení dalšího šíření dané phishingové kampaně.

Osob rozesílajících phishing není mnoho, nicméně většina z nich tak činí opakovaně. Častěji se mezi původce řadí muži a osoby mladší 29 let.

v.

Dotazník – online účty

Online účty. Snad každý dnes disponuje hned několika, od sociálních sítí přes herní účty až po e-shopy a nepřeberné množství rozličných aplikací. Zcela běžně uživatelé využívají vícero účtů určitého typu, typicky několik e-mailových účtů, profily na sociálních sítích, herní účty i e-banking. Obvykle však některé z nich vynikají svým významem pro uživatele. Zaměřujeme se proto na e-mail coby pomyslnou bránu do virtuálního světa uživatele[100], sociální sítě jako významný prostředek sebeprezentace a komunikace,[101] e-banking jako samozřejmou součást správy financí a herní účty coby specifickou a rozšířenou formu trávení volného času.

Za spojující prvek uvedených účtů považujeme soukromí. V případě zneužití e-mailové schránky nebo profilu na sociální síti zřejmě není ohledně prvku soukromí pochyb. Koneckonců v případě sociálních sítí to dle judikátu Nejvyššího soudu ze 4. 11. 2020 ve věci 7 Tdo 1134/2020 trefně vyjádřil ve svém podání státní zástupce: „***Facebook je v podstatě virtuální prostor a má podobnou povahu jako „obydlí", jehož „dveře" tvoří počítačový systém, či jiný nosič informací,*** *přičemž „klíčem" k těmto „dveřím" je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně* ***ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí*** *(…).*"[102] U zneužívání profilů na sociálních sítích proto zařazujeme kapitolu věnovanou jak zkušenostem respondentů s převzetím jejich vlastního účtu/profilu jinou osobou (a zrcadlově přebíráním cizích profilů), tak kontaktem s falešnými profily a vlastním používáním falešných profilů.[103] Prvek soukromí ovšem zasahuje i do méně zřejmé oblasti správy financí. I z e-bankingu lze vyčíst kromě samotných finančních transakcí a stavů aktivitu majitele účtu, jeho zájmy i spojení s dalšími osobami.[104] Nakonec zde máme i herní účty, kde je prvek soukromí zřejmě nejslabší, přesto považujeme za vhodné se jimi alespoň okrajově zabývat, neboť hráčská komunita je značná a část uživatelů tráví hraním her významnou část svého času.[105]

Specifickou oblast tvoří také školní a pracovní účty. Při předchozí analýze trestních spisů (vedených o počítačových trestných činech a pravomocně skončených v roce 2015) se však neobjevil žádný případ zneužití školního účtu, do referovaného výzkumného šetření jsme je proto nezahrnuli.

100 Lze z něj vyčíst obsah komunikace, s kým je či byl uživatel v kontaktu, e-mailové adresy těchto osob, dobu aktivity (kdy je uživatel online) a v neposlední řadě také přihlašovací údaje k jiným aplikacím (pokud tyto e-maily uživatel aktivně nesmaže). Zároveň slouží e-mail obvykle také pro obnovu zapomenutých hesel pro jiné aplikace, a tak lze jeho prostřednictvím získat vstup dále. Několik kazuistik z předchozího projektu bylo již publikováno (Kudrlová, 2018; Vlach et al., 2020).

101 K sebeprezentaci vůbec a používání sociálních sítí obecně viz kapitola Mentální vybavenost – používané aplikace a sebeprezentace.

102 Podrobněji k judikátu viz kapitola Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily.

103 Vzhledem k tomu, že opakovaně již zmíněná předchozí analýza trestních spisů za rok 2015 potvrdila předpoklad používání falešných účtů k mámení peněz atp.

104 Prvek soukromí zde potvrzuje i nikoliv výjimečné zneužívání cizího e-bankingu motivované kupodivu zvědavostí, viz kapitola E-banking.

105 Mimoto se zdá, že vývoj ve světě digitálních technologií směřuje ke stále většímu propojení počítačových her s reálným prostředím, ať už jde o úvahy ohledně Metaversa nebo např. propojování her používajících virtuální realitu k fyzioterapii atp. Nemluvě o významném množství peněz pohybujících se v oblasti her (nejen vývoj a prodej, ale i celosvětové turnaje atp.).

V.1 E-mail

E-mail jako virtuální brána do světa uživatele. Lze z něj vyčíst obsah komunikace, s kým je či byl uživatel v kontaktu, e-mailové adresy těchto osob, dobu aktivity (kdy je uživatel online) a v neposlední řadě také přihlašovací údaje k jiným aplikacím (pokud tyto e-maily uživatel aktivně nesmaže). Zároveň slouží e-mail obvykle také pro obnovu zapomenutých hesel pro jiné aplikace, a tak lze jeho prostřednictvím získat vstup dále.[106]

Převážná většina respondentů (99 %, 6 737 osob) používala přinejmenším v době sběru dat, tj. v listopadu roku 2020, soukromý, zaměstnanecký a/nebo podnikatelský e-mail.[107] 98 % respondentů (6 584 osob) používalo soukromý mail (hlavní e-mail používaný k soukromým účelům), 39 % (2 650 osob) zaměstnanecký e-mail (poskytnutý zaměstnavatelem) a 7 % (475 osob) podnikatelský e-mail (vlastní, resp. soukromý, avšak používaný výlučně pro pracovní aktivity). Soukromý e-mail používali významně často respondenti starší 60 let, zaměstnanecký např. muži, osoby v produktivním věku 30–59 let a vysokoškoláci, podnikatelský taktéž muži a vysokoškoláci. Odpovědi se vztahují vždy k tomu e-mailu v dané kategorii (tj. soukromý, zaměstnanecký nebo podnikatelský), který považoval respondent za svůj hlavní, pokud jich používal více.[108]

Zajímala nás mimo jiné míra zabezpečení e-mailu a srovnání uvedených tří typů e-mailů, resp. charakteristiky hesla, které má chránit přístup do e-mailu coby klíči k dalším aplikacím, nemluvě o vlastním obsahu. Respondenti vybírali všechny přiléhavé z řady vlastností,[109] z nichž nejčastější zde uvádíme (Graf 33).[110]

106 Několik kazuistik z předchozího projektu bylo publikováno (Kudrlová, 2018; Vlach et al., 2020).

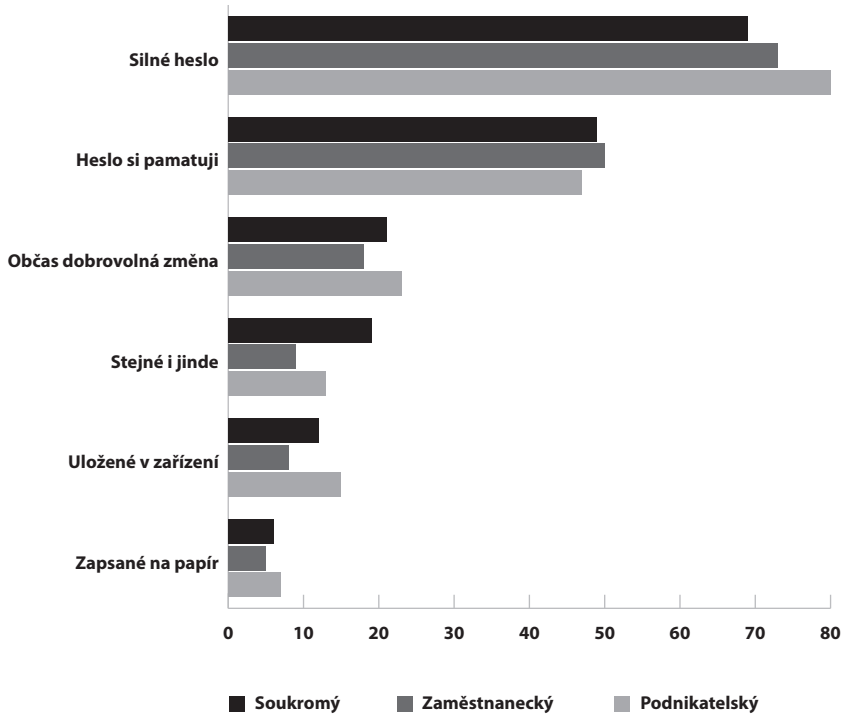
107 Zbývajících 44 respondentů buď nepoužívalo žádný, anebo používali pouze jiný – např. školní.

108 Tedy hlavní soukromý e-mail, hlavní zaměstnanecký a hlavní podnikatelský.

109 Otázka zněla *„Co byste řekl/a o svém hesle, kterým chráníte svůj přístup k… e-mailu?"*

110 Uvedená možnost „Silné heslo" je zkratkou, kterou zde používáme pro odpověď v dotazníku ve znění *„obsahuje alespoň 8 znaků kombinujících velká a malá písmena, číslice či jiné znaky"*.

Graf 33: Vlastnosti hesel k e-mailu (%)



Zdá se, že z hlediska zabezpečení přistupují respondenti ke všem třem typům e-mailů zhruba obdobně, snad jen s o trochu větší lehkovážností ve vztahu k vlastnímu soukromému e-mailu oproti zaměstnaneckému (méně často silné heslo, častěji opakující se heslo a uložení v zařízení[111]). Občasnou změnu hesla lze jedině doporučit, neboť k oblíbeným způsobům neoprávněného přístupu patří zkusmé použití hesla, které zná útočník od oběti z dřívějších dob (včetně použití hesla do jinak uzavřené firemní sítě bývalým zaměstnancem).

Méně obezřetní se zdají být především osoby mladší 29 let, které si u všech typů e-mailů významně často svá hesla pamatují a/nebo je používají i jinde. Používání stejného hesla na více místech přitom nelze doporučit, neboť „sebelepší heslo poskytuje jen takovou ochranu, jakou dává nejméně zabezpečená aplikace, ve které je používáno.[112] Není výjimkou, že případný útočník usilující o přístup nejprve vyzkouší heslo, která již zná z jiné aplikace oběti či z dřívějších dob (např. zná přihlašovací údaje oběti k jejímu profilu na sociální síti a vyzkouší je i pro přístup k e-mailu)“ (Kudrlová, 2022).

111 Samotné uložení hesla v zařízení nemusí znamenat bezpečnostní hrozbu samo o sobě – záleží na míře ochrany daného zařízení (včetně fyzického přístupu k němu).

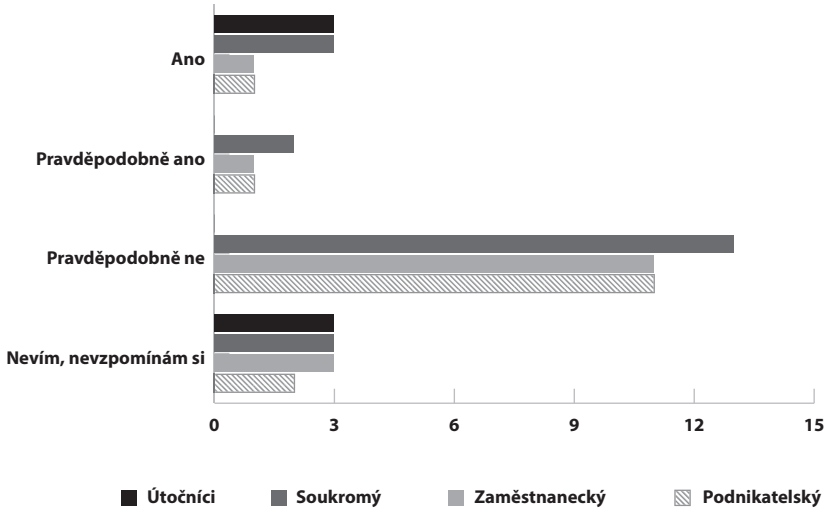
112 Typicky rizikovou aplikací je např. taková, která umožňuje přístup po zodpovězení snadné bezpečnostní otázky (třeba jméno za svobodna) a následné zobrazení stávajícího hesla.

Zodpovědněji přistupují k e-mailovému heslu muži, kteří významně často používají silná hesla k soukromému a zaměstnaneckému e-mailu. Podobně jako vysokoškoláci, ti však zároveň používají často na více místech stejná hesla, která si pamatují.

V.1.1 Zneužívání e-mailových schránek

Navzdory relativně silným heslům se respondenti potýkali v roce 2020* se zneužíváním svých e-mailů[113] a sami také cizí e-maily zneužívali. U napadených respondentů rozlišujeme nadále soukromý, zaměstnanecký a podnikatelský e-mail, respondenti-útočníci odpovídali souhrnně o zneužívání cizích e-mailů bez dalšího rozlišení. Žádnou zkušenost s napadením vlastního e-mailu neměla v roce 2020* většina respondentů, resp. 79 % u soukromého, 84 % u zaměstnaneckého a 86 % u podnikatelského e-mailu. Následující text se již věnuje těm méně šťastným (Graf 34).

Graf 34: Zneužití e-mailu v roce 2020* (%)



Pravděpodobné odpovědi spolu s „*nevím, nevzpomínám si*“, významně spojené se sledovanými charakteristikami respondentů, se objevovaly zejména u soukromého e-mailu, samotné „*nevím, nevzpomínám si*“ pak i u zaměstnaneckého. Předpokládáme, že respondenti, používající pravděpodobnostní výrazy, vychází z nějakého svého podezření, a tak je dále zařazujeme do jednotné skupiny „(pravděpodobně) napadených“ osob.

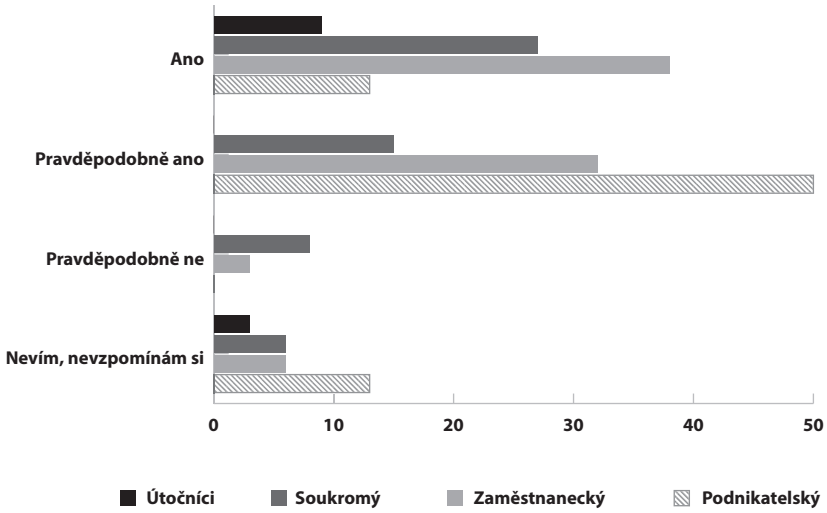
Zhruba 5 % respondentů (317 osob) „*použilo někdy v životě něčí e-mail bez výslovného svolení jeho majitele/ky*“.[114] V textu dále pracujeme již pouze se 169 respondenty (2,5 % ze všech respondentů), kteří tak učinili v roce 2020*. Naproti nim pak stojí 366 respondentů

113 V rámci zjednodušení zde hovoříme o zneužívání „e-mailů“, ačkoliv přesnější je zneužívání „e-mailových schránek“. V dotazníku bylo vždy důsledně uvedeno právě zneužívání „e-mailových schránek“, abychom vyloučili případy zneužití cizí e-mailové adresy samotné, kterým jsme se nezabývali.

114 Podrobněji k formulaci otázek viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

s (pravděpodobně) zneužitým soukromým e-mailem, 69 respondentů se zaměstnaneckým e-mailem a 8 respondentů s podnikatelským e-mailem, přičemž e-maily menší části z nich byly napadeny v roce 2020*opakovaně (Graf 35).

Graf 35: Opakované zneužití e-mailu (%)

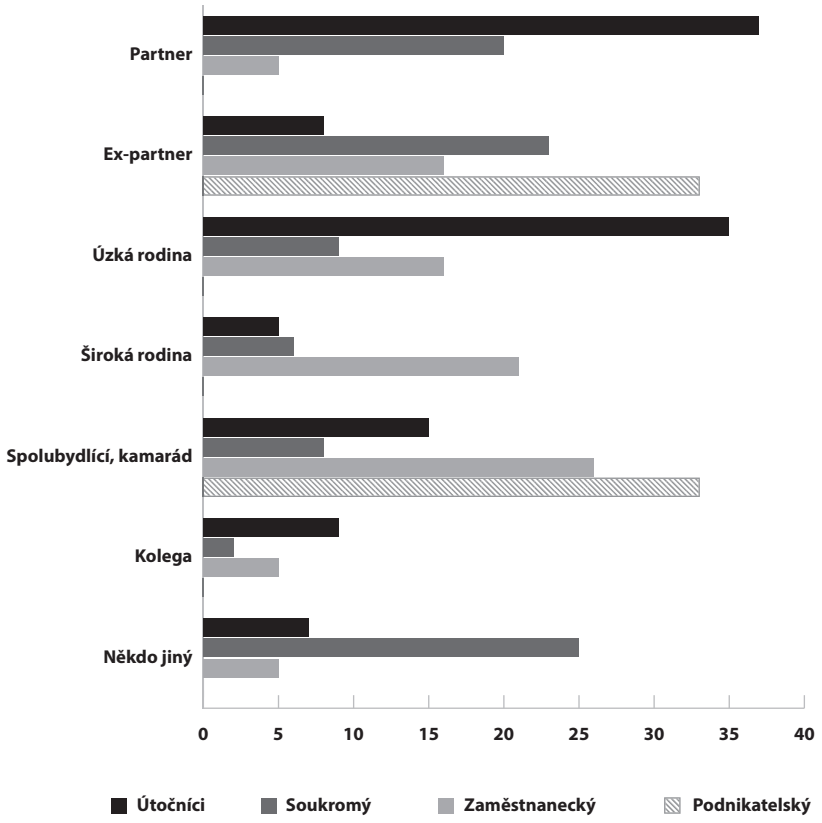


Pachatelé zneužívali převážně e-mail pouze jedné osoby, a činili tak v roce 2020* významně často ženy, osoby mladší 29 let a respondenti s pouze základním vzděláním, zneužití cizího e-mailu se z pachatelů v roce 2020* naopak vyhýbali vysokoškoláci.

V.1.2 Aktéři zneužívání e-mailů, získání přístupu a motivace

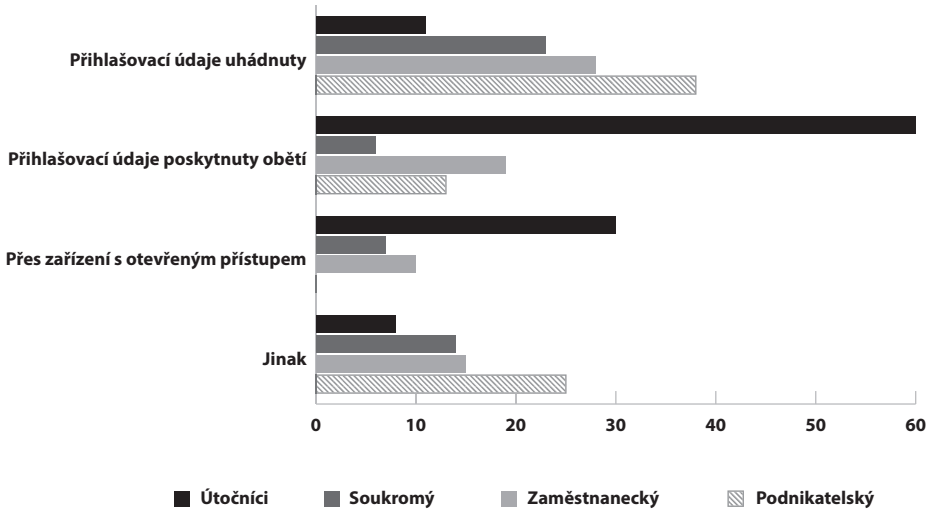
Někteří napadení vědí, kdo jejich e-mail zneužil. U soukromého e-mailu je to 18 % napadených (64 osob), u zaměstnaneckého 28 (19 osob) a u podnikatelského 38 % (3 osoby). Ze strany pachatelů pouze 3 adresáta neuvedli (2 si nevzpomněli, 1 nechtěl odpovědět). Jediné statisticky významné spojení aktérství a sledovaných charakteristik respondenta se ukázalo u pachatelů-mužů zneužívajících e-mail kamaráda a pachatelek-žen zneužívajících e-mail někoho z úzkého rodinného kruhu.

Graf 36: Oběti označené pachateli a domnělí útočníci podle obětí (%)



Je zde patrný výrazný rozdíl mezi odpověďmi útočníků a napadených, kdy napadení výrazně častěji podezírají své bývalé partnery a neznámé hackery (převážná většina odpovědí obětí spadajících do kategorie „někdo jiný"), kdežto zneuživatelé se obracejí více na své stávající partnery a osoby z úzkého rodinného kruhu (Graf 36). Patrně zde hraje určitou roli rodičovství a kontrola potomků, blíže k tomu viz následující kapitola Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily.

Graf 37: (Domnělé) získání přístupu (%)

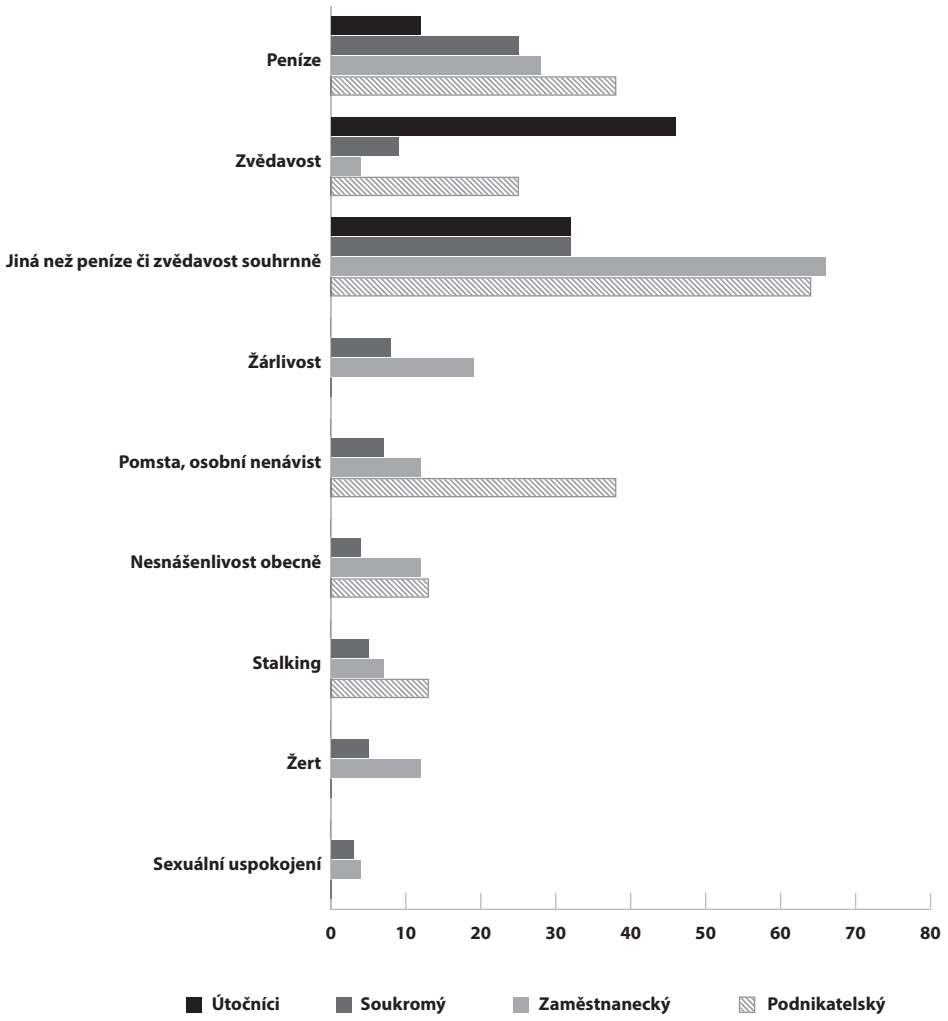


Ve způsobech získání přístupu je zcela evidentní rozdíl mezi tím, co předpokládají oběti, a tím, co vypovídají pachatelé (Graf 37). Zatímco oběti předpokládají především uhádnutí hesla (významně často u soukromého e-mailu osoby mladší 29 let),[115] pachatelé mnohem častěji použili zařízení s otevřeným přístupem k e-mailu (typicky zapůjčený NB nebo mobilní telefon se zapamatovanými přihlašovacími údaji) a/nebo využili své znalosti hesla z dřívějška. To jim majitelé napadených e-mailů poskytli většinou (68 %) v souvislosti s nějakou jednorázovou žádostí (např. prosba o kontrolu pošty při nedostatku signálu na telefonu) a/nebo vzhledem k trvalé správě e-mailu (typicky vnuk pomáhající s e-mailem babičce) – 32 %.[116]

115 To může naznačovat, že ačkoliv používají „silná" hesla, jsou si vědomi jejich slabin. Zároveň vyšší podíl v odpovědích „jinak" zřejmě reflektuje nikoliv výjimečný předpoklad, že e-mail napadl neznámý hacker, který heslo prolomil (odpovědi „jinak" uváděli u soukromého e-mailu významně často muži, vysokoškoláci a osoby starší 60 let).

116 Pro více informací ohledně sdílení přihlašovacích údajů viz kapitola E-banking.

Graf 38: (Domnělá) motivace (%)



I v (předpokládané) motivaci vidíme značné rozdíly mezi napadenými a zneužívajícími respondenty, a to zejména u zvědavosti ze strany útočníků, byť musíme vzít v potaz, že neměli k dispozici stejně širokou škálu odpovědí.[117] Častější předpoklad obětí, že útočníky vedla finanční motivace (významně často tak odpovídali muži v souvislosti s napadením jejich soukromého e-mailu),[118] zřejmě znovu reflektuje domněnku, že jejich e-mail mnohdy zneužívají neznámí hackeři. Osoby mladší 29 let významně často předpokládaly u soukromého e-mailu virtuální násilí ze strany domnělých pachatelů, a to žárlivost a/nebo pomstu.

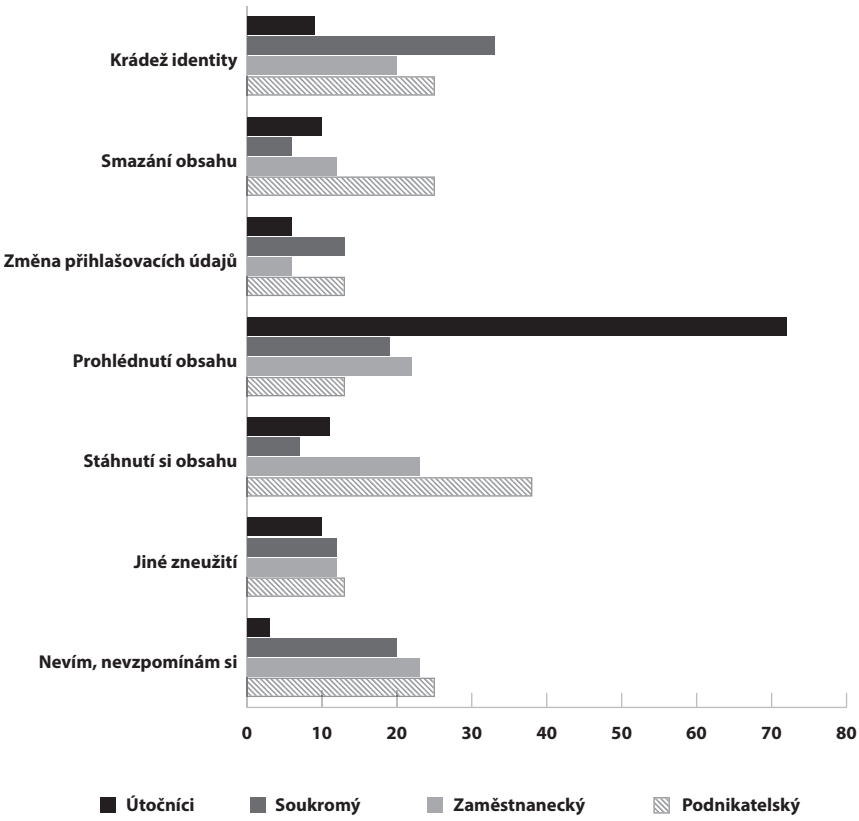
117 K formulaci otázek viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

118 Finanční motivace hraje v souvislosti s e-maily zřejmě u mužů obecně významnou roli, neboť signifikantně často ji uváděli i muži-pachatelé.

V.1.3 Způsob zneužití a následná reakce

Nejvýraznější rozdíl ve zkušenostech obětí a útočníků vidíme u způsobu zneužívání e-mailů (Graf 39). Převážná většina útočníků, resp. osob používajících cizí e-mail bez výslovného svolení jeho majitele, si „pouze" prohlíží obsah. Jde tedy o aktivitu, která zpravidla nezanechává v e-mailové schránce stopy patrné na první pohled.[119] Naproti tomu oběti mají častěji přehled o aktivitách, které zpravidla bývají patrné na první pohled, jako je změna přihlašovacích údajů nebo krádež identity[120] či smazání obsahu.

Graf 39: Způsob zneužití (%)



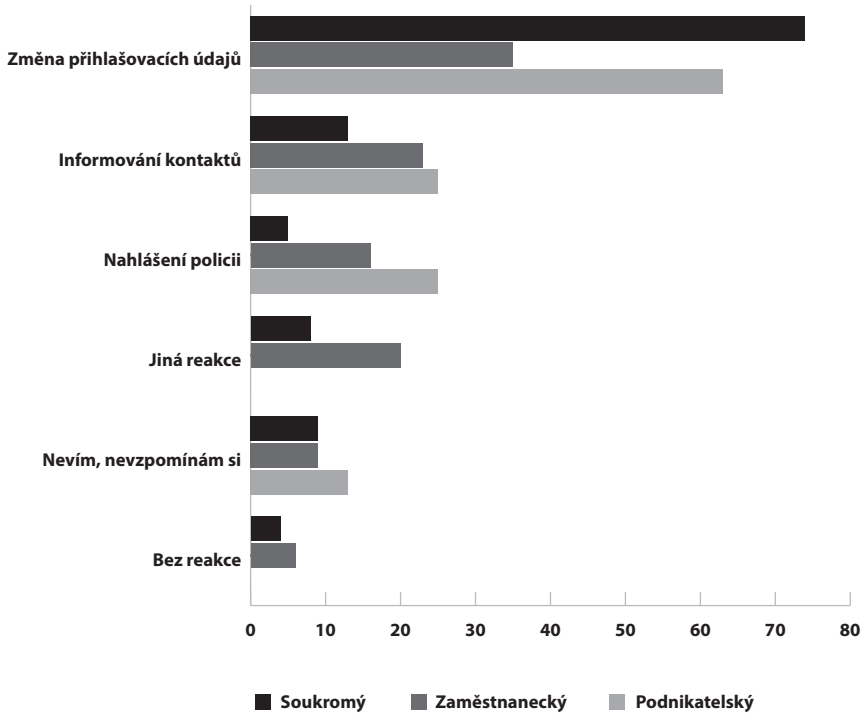
Se změnou přihlašovacích údajů se potýkaly u soukromého e-mailu významně často opět osoby mladší 29 let. Muži a osoby starší 60 let uváděli signifikantně často „jinou" odpověď, mezi ty častější patřilo rozesílání spamu, požadavek výkupného pod hrozbou

119 Pochopitelně za předpokladu, že dotyčný neotevírá dosud nepřečtené zprávy, případně je opětovně označí jako „nepřečtené".

120 Výraz „krádež identity" zde používáme pro případy, kdy se dotyčný vydává za majitele napadeného účtu (např. rozesílá jeho jménem e-maily).

zneužití zjištěného hesla nebo použití e-mailu k získání přístupu do jiných aplikací. Osoby ve věku 30–44 let významně často zakoušely neoprávněné prohlížení obsahu jejich zaměstnaneckého e-mailu.

Graf 40: Reakce na incident (%)



Většina osob v důsledku zneužití e-mailu změní své přihlašovací údaje, nicméně v případě zaměstnaneckého e-mailu je taková reakce výrazně méně častá. Zdánlivě překvapivé zjištění má jednoduché vysvětlení ve spojení s častější „jinou" reakcí, kterou bývá u zaměstnaneckých e-mailů spolupráce s firemním IT odborníkem či zaměstnavatelem. Jediný signifikantní vztah se ukázal u žen měnících své přihlašovací údaje k soukromému e-mailu.

Z několika málo osob, které se obrátily na policii (17 při napadení soukromého e-mailu, 11 u zaměstnaneckého e-mailu a 2 u podnikatelského e-mailu), s ní byla většina více či méně spokojena (v řádu 53–73 %, oba podnikatelé byli spokojeni zcela). Ovšem podobně jako v jiných oblastech, ani zde nepanuje celkově důvěra ve schopnosti policie objasňovat zneužití e-mailu vůbec – spíše se jí to daří pouze podle 16 % respondentů, kdežto částečně či zcela jejím schopnostem nedůvěřuje 46 % respondentů. Policii se spíše daří zneužívání e-mailu objasňovat zejména dle osob mladších 29 let a respondentů s pouze základním vzděláním, na druhé straně škály pak stojí osoby ve věku 30–44 let a vysokoškoláci. Ženy a respondenti starší 45 let významně často nemají na schopnosti policie v oblasti objasňování zneužití e-mailů jednoznačný názor.

V.1.4 Závěr ke zneužívání e-mailů

Nahlížení do cizí e-mailové schránky se někdy přirovnává k prohlížení došlé papírové pošty či poštovní schránky, avšak e-mail obsahuje mnohé informace nad rámec pouhého obsahu komunikace. Neoprávněný přístup proto představuje potenciálně výrazný zásah do soukromí uživatele.[121]

K hlavním aktérům neoprávněných přístupů patří stávající partneři a osoby z úzkého rodinného kruhu. Soudě dle srovnání odpovědí obětí i útočníků, pravděpodobně dochází k řadě neoprávněných přístupů umožněných znalostí přihlašovacích údajů z minulosti, o kterých majitele e-mailů neví, protože spočívají v aktivitách bez patrných stop (zejména prohlédnutí si obsahu). To je poznatek, který se objevuje napříč různými online účty, viz dále.

V.2 Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily

V.2.1 Viktimizace a neoprávnění uživatelé

Podle toho, do jaké míry uživatelé aktivně dbají o svou sebeprezentaci a jakou formou tak činí, lze jejich profily na sociálních sítích zahrnout do jejich osobnosti. Ať už se jedná o vystupování pod vlastní identitou nebo identitou smyšlenou.

Projekcí uživatele v online prostředí[122] bývá tzv. avatar – zpravidla nějaká forma zobrazení uživatele (od profilové fotografie či obrázku na sociální síti po kompletní postavu v počítačových hrách) spojená s vybraným jménem. Nabízí se jeho vnímání jako přesah osobnosti uživatele do virtuálního prostředí,[123] kde je jeho prostřednictvím „přítomen" a interaguje se svým okolím. Osobnost si lze představit jakou souhrn vlastností, vědomostí, zkušeností, sociálních vztahů atd., svázaných s konkrétní bytostí nadanou určitými přirozenými právy (čl. 5 Ústavy, čl. 19 odst. 1 a § 81 NOZ). „Podstatou osobnosti jsou její vztahy k vnímané skutečnosti, k druhým lidem (tzv. interpersonální vztahy) (…) apod. Tyto vztahy se projevují ve styku s lidmi, v jednání a chování člověka, jeho kulturními výtvory apod.," viz komentář P. Pavlíka k § 81 NOZ (Švestka, 2014, s. 268). Avatar tak představuje nejspíše specifický projev osobní povahy per se,[124] někdo ho vnímá dokonce jako pravdivější prezentaci osobnosti než vystupování v reálném světě (Wolfendale, 2007, s. 111).[125]

Při neoprávněném zásahu do avatara, zde rozumějme profilu na sociální síti, proto může nepochybně docházet k viktimizaci majitele účtu. Jednak tam, kde dojde ke znemožnění přístupu k profilu změnou přihlašovacích údajů. Pochybnosti ohledně viktimizace ovšem nevznikají ani při jakékoliv manipulaci s daty, od jejich úpravy přes smazání až po vložení

121 Nemluvě o snadnosti takového jednání oproti např. snaze rozlepit papírovou obálku a opětovně ji zalepit po přečtení obsahu.

122 Nejčastěji v počítačových hrách, ale v širším smyslu slova i v sociálních sítích, nemluvě o případném Metaversu.

123 Zejména u autorského díla lze do jisté míry hovořit o „emanaci osobnosti tvůrce" (Telec & Tůma, 2007, s. 26).

124 Nelze ho zredukovat na podobiznu, písemnost, soukromí, vztahy k okolí atp., nýbrž vytváří ho právě jejich souhrn.

125 Částečně převzato (Kudrlová, 2019).

jiných dat. Nelze však vynechat ani prosté prohlédnutí si obsahu profilu (v takovém případě ovšem nepřichází v úvahu profil, jehož obsah je zcela veřejný),[126] neboť představuje soukromý prostor, jak trefně uvádí státní zástupkyně ve svém vyjádření k dovolání v bodě 40 odůvodnění rozhodnutí Nejvyššího soudu ze 4. 11. 2020 ve věci 7 Tdo 1134/2020: „*Facebook je v podstatě virtuální prostor a má podobnou povahu jako „obydlí", jehož „dveře" tvoří počítačový systém, či jiný nosič informací, přičemž „klíčem" k těmto „dveřím" je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí,* ***a to i za pomoci shodného klíče, aniž by pachatel musel dveře do domu prolamovat násilím****. Obdobně je tedy nutno postihovat případy, kdy pachatel prolomí* ***„dveře" do virtuálního prostoru například za pomoci hesla, které znal z dřívější doby****, či za pomoci telefonního čísla, na který jsou tyto soukromé účty navázány. Rozhodující je – obdobně jako u porušování domovní svobody – že* ***v okamžiku, kdy pachatel tohoto způsobu narušení soukromí využívá, ví, že do toho důvěrného prostoru vstupuje neoprávněně****, a je s tímto následkem přinejmenším srozuměn*."

Mezi respondenty dotazníkového šetření používajícími sociální sítě mělo v roce 2020* 7 % (377 osob) zkušenost s (pravděpodobným) napadením jejich účtu v uvedeném období, z toho 36 % zřejmě opakovaně. Statisticky významně často měly zkušenost s napadením svého profilu na sociální síti ženy, osoby mladší 29 let a osoby s pouze základním vzděláním.

Na druhé straně stáli respondenti, kteří použili cizí účet na sociální síti bez výslovného svolení jeho majitele. Těch, kteří si takového jednání byli vědomi a zároveň byli ochotni nám to sdělit, bylo 256, k danému jednání tíhli respondenti mladší 29 let a s pouze základním vzděláním či středoškolským vzděláním s maturitou.

Více než třetina z nich (100 respondentů) tak učinila přinejmenším v roce 2020* a v převážné většině případů šlo v uvedeném období o účet jedné osoby na jedné sociální síti.[127] Na obou stranách vidíme zejména aktéry mladší 29 let a s pouze základním vzděláním.

Zdaleka nejčastěji docházelo ke zneužívání profilů na sociální síti Facebook a zakusili ho významně často senioři starší 60 let a respondenti vyučení bez maturity. 250 osob hovořilo o napadení jejich účtu na Facebooku, 19 osob o účtu v Messengeru.[128]

Z pohledu respondentů-útočníků byla převaha neoprávněného používání právě Facebooku a Messengeru ještě drtivější (75 % Facebook a 18 % Messenger).

Většina majitelů profilů, k nimž někdo (pravděpodobně) získal neoprávněně přístup, nevěděla, o koho se mohlo jednat. Častěji to věděli muži, zatímco ženy naopak nikoliv.

126 Za předpokladu, že vetřelec nenahlédne zároveň do jinak neveřejné soukromé komunikace vedené v rámci profilu.

127 Na rozdíl např. od phishingu, kde útočníci jednali naopak častěji opakovaně a vůči různým osobám, viz kapitola Phishing.

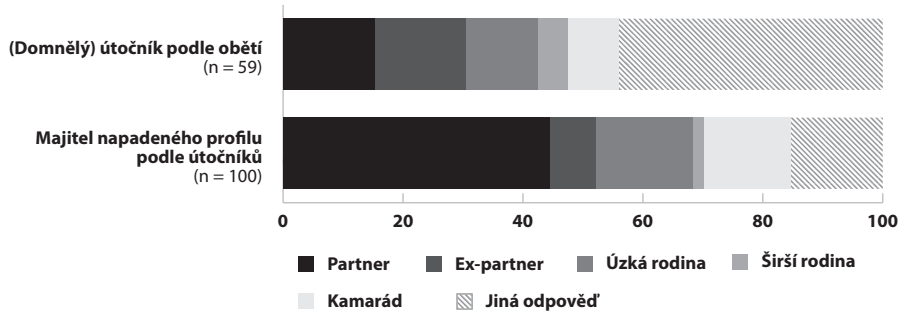
128 Účty na Facebooku a Messengeru mohou splývat, nicméně respondenti byli tázáni ohledně incidentu, který oni sami považují za nejzávažnější.

Respondenti označovali jako pravděpodobné především stávající i bývalé partnery a osoby z úzkého rodinného kruhu, v pozici (domnělého) útočníka se objevil i kamarád a v rámci odpovědi „*někdo jiný, uveďte kdo*“ dominoval „*neznámý hacker*“.

Naproti tomu neoprávněně vstupující osoby tak činily zejména vůči účtům tehdejších partnerů a osob z úzkého rodinného kruhu. Statisticky významně často tak odpovídaly ženy – ty mnohdy přistupovaly na profily svých potomků. V takových případech dost dobře nelze (ne)oprávněnost přístupů dovozovat bez dalšího – roli bude hrát např. věk dohlížené osoby (resp. její rozumová a volní vyspělost) nebo momentální situace (např. podezření na komunikaci s možným kybergroomerem nebo sdílení intimních fotografií nezletilých atp.) aj.[129] Téměř pětina respondentů zmínila účet kamaráda, zatímco pouhá desetina se zajímala o účet svého v tu dobu bývalého partnera.

Mezi aktéry na obou stranách hráli překvapivě poměrně velkou roli v té době stávající partneři (Graf 41). Za zmínku stojí, že z hlediska domnělých aktérů neoprávněných vstupů na účet na sociální síti napadení respondenti výrazně častěji přisuzovali neoprávněný vstup bývalým partnerům či neznámým hackerům. Naproti tomu respondenti neoprávněně vstupující na cizí účet tak jednali výrazně častěji vůči účtu svého stávajícího partnera. Nabízí se dvě vysvětlení. Zaprvé, majitelé napadených účtů neví, že na jejich účet neoprávněně vstoupil (či ho jinak zneužil) jejich partner. Zadruhé, majitelé účtů, na které přistoupil jejich partner, nemuseli takové jednání považovat za „zneužití“, i kdyby šlo o přístup bez jejich výslovného svolení.)

Graf 41: Aktéři neoprávněného vstupu do profilu na SNS (%)



V.2.2 Získání přístupu a aktivita na cizím profilu na sociální síti

Zhruba polovina majitelů napadených profilů měla určitou představu ohledně toho, jakým způsobem získal útočník přístup. Čtvrtina napadených předpokládala, že útočník jejich přihlašovací údaje uhádl,[130] necelá desetina měla podezření na zneužití jejich zaří-

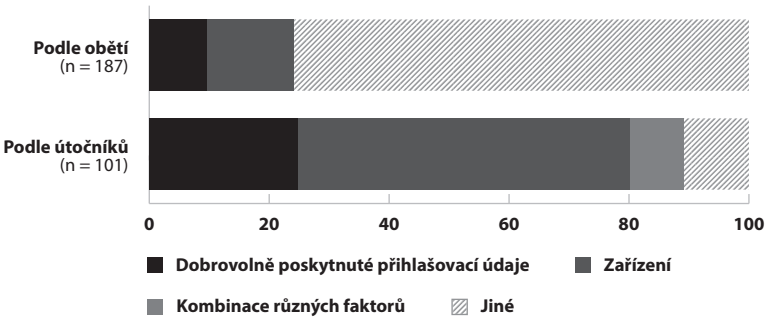
129 I z toho důvodu byla zvolena formulace, *přístupu bez výslovného svolení majitele účtu*“, podrobněji viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

130 Lze se domnívat, že používali jednoduchá hesla, která mohl útočník uhádnout, a byli si jejich uhádnutelnosti vědomi (přinejmenším po zjištění neoprávněného přístupu).

zení, ve kterém měli otevřený přístup k profilu, a dvacetina sama poskytnula přihlašovací údaje. Za zmínku stojí také téměř 15 % respondentů, kteří předpokládali napadení ze strany neznámého hackera.

Zatímco napadení respondenti předpokládali zejména uhádnutí hesla, mezi respondenty-pachateli jich heslo uhádlo dle svých výpovědí pouze 13 %. Alarmující je však více než poloviční podíl respondentů, kteří využili zařízení, na kterém byl daný profil či účet přihlášený (57 %). Rozdíl vynikne ještě výrazněji, když rozlišíme přístup s využitím pouze dobrovolně poskytnutých přihlašovacích údajů, díky použití konkrétního zařízení nebo kombinaci různých faktorů (typicky např. přístup k zařízení a zároveň znalost přihlašovacích údajů nebo uhádnutí hesla) (Graf 42).[131]

Graf 42: (Pravděpodobné) získání přístupu k profilu na SNS (%)



Za pozornost stojí také téměř třetina případů (30 %), kdy útočníci znali přihlašovací údaje přímo od samotné napadené osoby: 63 % z nich bylo požádáno o nějakou jednorázovou aktivitu (např. poslání zprávy), 40 % spravovalo daný profil trvale.[132]

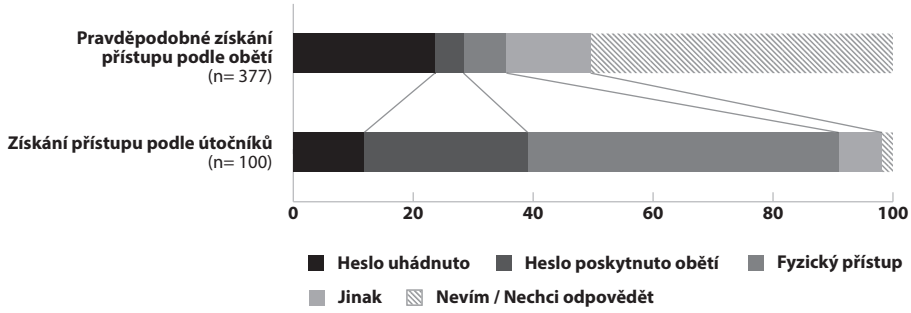
Je zde patrný výrazný rozdíl mezi domnělým a skutečným získáním přístupu k napadenému profilu na SNS, a to zejména u uhádnutí přihlašovacích údajů, fyzickém přístupu (využití zařízení s přihlášeným profilem) a „hacknutí" (Graf 43). Zřejmě souvisí s rozdílem mezi domnělými a skutečnými neoprávněně vstupujícími osobami (zejména hacker vs. partner). Dalším důvodem může být zapomenutí napadených respondentů, že heslo v minulosti někomu sdělili, nebo nevědomost, že někdo využil či mohl využít trvale přihlášený profil na nějakém zařízení.[133]

131 Respondenti měli v části věnované obětem možnost zvolit pouze jednu odpověď (tu, která nejvíce vystihovala daný incident), kdežto v self-reportové části mohli vybrat více odpovědí.

132 Všichni z uvedených odpovídali výlučně ohledně přístupu bez výslovného svolení majitele daného účtu, včetně osob spravujících daný profil trvale. Mohli vybrat více odpovědí (tedy i trvalou správu spolu s jednorázovou aktivitou), pouze 2 respondenti uvedli jiný důvod.

133 Může jít např. o zařízení napadeného respondenta půjčené někomu jinému. Anebo naopak o zařízení, které si napadený respondent půjčil od někoho jiného a přihlásil se z něj ke svému profilu, ale poté se před vrácením zařízení neodhlásil.

Graf 43: Domnělé vs. skutečné získání přístupu (%)



Podobně se odlišuje i neoprávněná[134] aktivita na cizím profilu na SNS. Napadení respondenti měli přehled pochopitelně především o jednání, která zanechávají viditelnou stopu. Více než třetina z nich zakusila vložení obsahu na jejich profil, stejné množství[135] převzetí jejich identity[136]. Téměř čtvrtině dokonce zamezili útočníci přístup změnou přihlašovacích údajů, necelé desetině smazali nějaký obsah. Téměř pětina napadených respondentů pak hovořila o prohlédnutí nějakého obsahu a několik o stažení obsahu. Nejjistější si byli ohledně formy zneužití jejich účtu respondenti mladší 29 let, a to zejména u prohlédnutí si obsahu, jeho smazání a změny přihlašovacích údajů.

Naproti tomu u respondentů-pachatelů drtivě převažovalo prohlédnutí obsahu (78 %), tedy činnost bez stop patrných na první pohled. 14 % si nějaký obsah stáhlo, ovšem žádná z ostatních aktivit (smazání nebo vložení obsahu, změna přihlašovacích údajů, převzetí identity) nedosáhla ani deseti procent. Významně často hovořili o prohlédnutí obsahu po neoprávněném vstupu na cizí profil respondenti ve věku 30–44 let, což by mohlo ukazovat opět na respondentky-matky kontrolující profily svých ratolestí.[137]

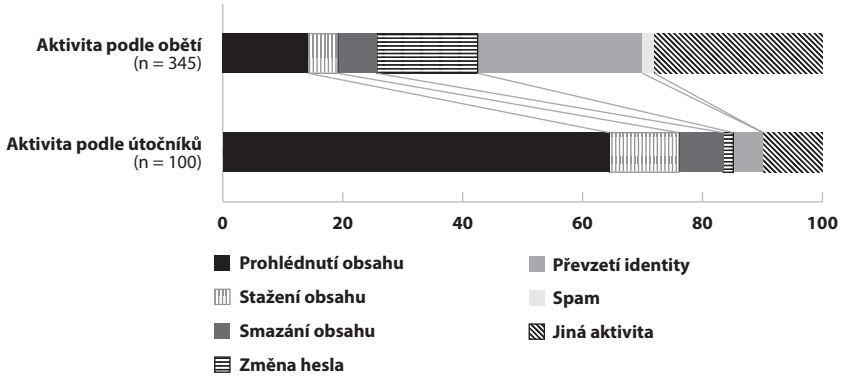
134 Po neoprávněném vstupu považujeme jakoukoliv aktivitu automaticky také za neoprávněnou.

135 Stejný počet případů, ne nutně však stejné osoby.

136 Typicky např. odeslání zprávy jménem majitele profilu.

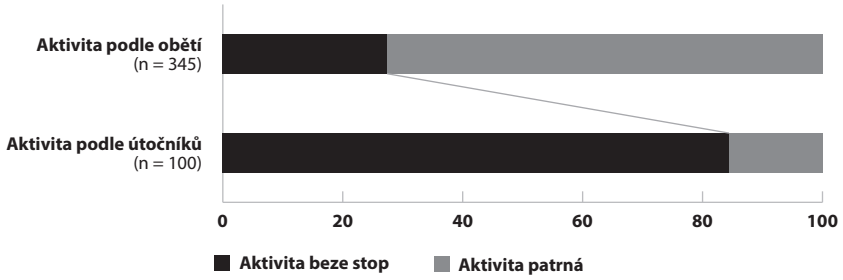
137 Stále se ovšem pohybujeme v rámci jednání *„bez výslovného souhlasu majitele účtu"*.

Graf 44: Aktivita po neoprávněném vstupu (%)



I zde stojí za zmínku podrobnější srovnání odpovědí napadených vs. neoprávněně vstupujících respondentů (Graf 44), zejména vzhledem k rozdílnému poměru patrných aktivit vs. těch „beze stop" (Graf 45). Respondenti s napadenými profily nemusí vědět o aktivitě útočníků v rámci jejich účtu, ale ani o samotném neoprávněném vstupu.

Graf 45: Aktivita beze stop vs. aktivita patrná (%)[138]



V.2.3 Motivace

Obrázek narušování soukromí v podobě neoprávněného vstupu na cizí profil na sociální síti dotváří (domnělá) motivace útočníků. Oproti předpokladu převažovala z pohledu napadených respondentů domnělá snaha majetkově se obohatit (14,6 %), zatímco jednání spadající do kategorie virtuálního násilí dosáhlo vyšších čísel až ve svém souhrnu kombinujícím nejčastější zvědavost (10,6 %), pomstu nebo osobní nenávist (9,3 %), stalking (8,2 %), žert a žárlivost (obojí shodně 6,4 %), nesnášenlivost obecně (5,6 %) a/nebo sexuální uspokojení (2,9 %).[139] Jiné, již jen sporadicky uvedené důvody, pak braly v potaz především

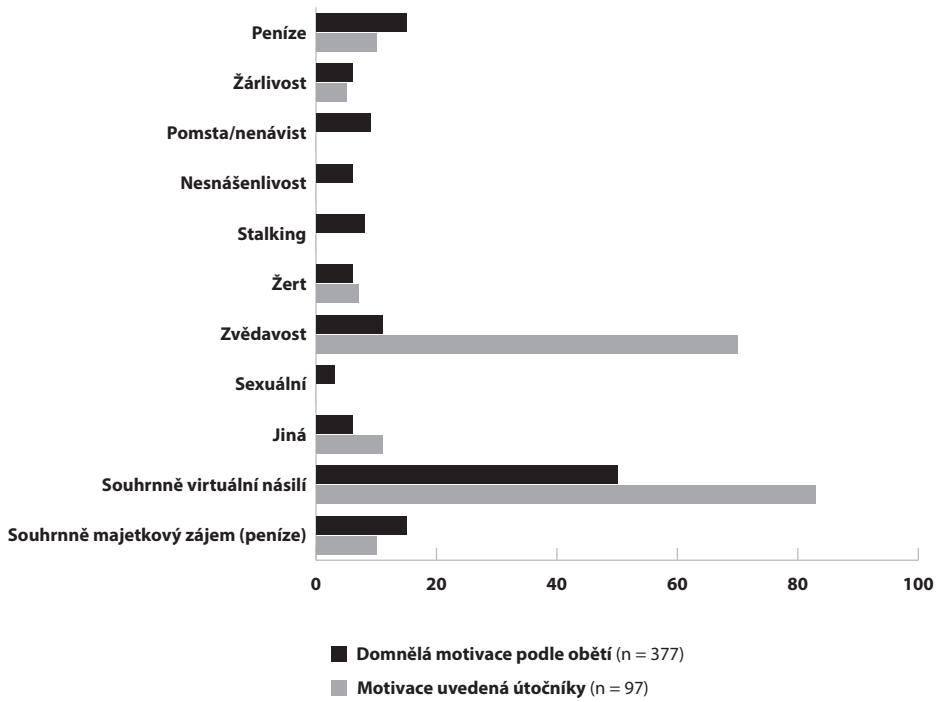
138 Aktivita „patrná" zahrnuje smazání obsahu, změnu hesla a/nebo převzetí identity, aktivita „beze stop" prohlédnutí a/nebo stažení obsahu.

139 Blíže k majetkovému zájmu vs. virtuálnímu násilí viz kapitola Rozlišování virtuálního násilí a majetkového zájmu.

„*klasický hack*“ účtu bez dalšího nebo spam. Majetkovou motivaci a obecnou nesnášenlivost předpokládali zejména muži[140] (nesnášenlivost i osoby mladší 29 let), ženy a osoby ve starším produktivním věku 45–59 let si naopak významně často nevzpomněly či nevěděly.

U respondentů vstupujících na cizí účet bez výslovného svolení jeho majitele se již převaha virtuálního násilí potvrdila, leč v méně očekávané podobě pouhé zvědavosti (68 %).[141] V rámci jiných odpovědí se objevil často v nějaké podobě žert či „*nuda*“, ale také různé formy žárlivosti (podezření na nevěru). Za zmínku stojí i odpověď naznačující tzv. FOMO:[142] „*Přítel nestíhá, nebo usne a tak mu zkontroluji zprávy na fb, aby nepřišel třeba o něco důležitého.*“ Nakonec pochopitelně také několikero odpovědí vyjadřujících obavy o bezpečnost potomků. Finanční motivaci („*peníze*“) uvedlo pouze 10 % respondentů neoprávněně vstupujících na cizí účet (Graf 46).

Graf 46: (Domnělá) motivace (%)



140 V případě zkušenosti s více incidenty byli respondenti vyzváni k odpovědím pouze ohledně toho, který oni sami považují za nejzávažnější. Je možné, že respondenti-muži jsou vůči majetkovému ohrožení vnímavější.

141 Ovšem s výhradou použití výrazu „zvědavost“ vzhledem k neutrálnímu emočnímu zabarvení (na rozdíl např. od „stalkingu“), blíže k formulaci otázek viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

142 Syndrom Fear of missing out – utkvělá obava ze zmeškání něčeho důležitého jako určitá forma závislosti, která vede k permanentní přítomnosti na sociálních sítích, soustavnému sledování zpráv atp. Blíže k tomu viz např. Roberts (2020), v českém prostředí k závislostem spojeným s internetem viz např. Blinka et al. (2015).

V.2.4 Reakce na incident a policie

Více než dvě třetiny napadených uživatelů reagovaly na zneužití jejich profilu na sociální síti změnou přihlašovacích údajů (69 %). Vezmeme-li v úvahu četnost neoprávněných přístupů umožněných znalostí hesla nebo díky zařízení s neodhlášenou aplikací (či zapamatovanými přihlašovacími údaji), jde nepochybně o správný krok. Třetina respondentů také jednala jednak obezřetně vůči svému okolí, jednak vůči sobě samým (zejména v případech převzetí identity), když informovala své kontakty na sociální síti o zneužití jejich účtu (33 %). Ostatní podoby reakce byly již výrazně méně časté a kromě jediné výjimky nepřesáhly svou četností 6 %: nahlášení správci aplikace (6 %), dále pak zrušení či zablokování profilu uživatelem (4 %), založení nového profilu (2 %), jiné (2 %). Ve 2 % případů upozornil uživatele na podezřelou aktivitu sám provozovatel sociální sítě, ať už v podobě automatického bota či správce. Uživatelé byli s reakcí provozovatelů sítí vesměs spokojeni („*napsala jsem žádost o prověření – nahlásila problém na Facebook /info/ – do cca 2 hodin to bylo vyřešeno*“), až na několik výjimek („*nahlásila účet, ten byl smazán a já si musela založit nový. Opravdu hrozný přístup k ochraně uživatelů*“).

Mezi respondenty se našlo také 18 osob (4,8 %), které nahlásily napadení jejich profilu na policii.[143] Z nich byla třetina s řešením jejich problému ze strany policie nespokojena, uvítala by především větší snahu o dopadení pachatele včetně rychlejšího jednání, ale i prosté informování respondenta. Zbývající dvě třetiny již byly převážně zcela spokojené, avšak i mezi nimi se našly osoby volající po větší snaze policie.

Všech respondentů (nejen napadených) jsme se dále zeptali, jak se podle nich daří policii objasňovat zneužití účtů na sociálních sítích.[144] Zde se již ukázala určitá nedůvěra, neboť pouze 17 % v tomto směru věří ve schopnosti policie, kdežto téměř polovina respondentů (47 %) si myslí opak, přičemž o něco více než třetina respondentů (36 %) nemá jednoznačný názor. Policii důvěřují ohledně řešení zneužívání účtů na sociálních sítích respondenti mladší 29 let a respondenti s nižším vzděláním (nejvýše vyučeni bez maturity), kdežto častěji nedůvěřují policii muži, osoby mladší 44 let a vysokoškoláci. Jednoznačný názor nemají především ženy a osoby starší 45 let.

V.2.5 Závěr ke zkušenostem se sociálními sítěmi

Sociální sítě v čele s Facebookem patří dnes mezi samozřejmé prostředky komunikace, v roce 2020* je využívalo bezmála 80 % respondentů, z toho polovina dle svého vyjádření aktivně (pochopitelně zejména mladší generace). I když někteří přestali v roce 2020* nějaký svůj účet na sociální síti používat, zpravidla nešlo o jediný jejich účet, anebo přešli na jinou sociální síť.

Profil na sociální síti může představovat určitou formu avatara – personalizaci uživatele ve virtuálním prostředí. V návaznosti na péči o vlastní digitální stopu a charakter profilu může být neoprávněný přístup k němu výrazným zásahem do soukromí, který (pravdě-

143 Jiný respondent se obrátil na státní zastupitelství.

144 Týká se jak zneužití cizího účtu na sociální síti, tak vytvoření a následné zneužití falešného účtu na sociální síti, blíže k tomu viz kapitola Falešné účty na sociálních sítích.

podobně) zakusilo v roce 2020* nejméně jednou téměř 400 respondentů (7 %). O viníkovi měla představu jen menší část z nich, podezírali obvykle osoby z úzkého rodinného kruhu, bývalé partnery nebo neznámé hackery.

Čtvrtina z nich předpokládala, že útočník uhádl jejich heslo, méně často pak, že na jejich účet vstoupil neznámý hacker prolomením jejich hesla. Ještě méně jich mělo podezření na zneužití zařízení, na kterém byli ve svém profilu přihlášeni nebo které si pamatovalo jejich přihlašovací údaje.

Respondenti detekovali zejména jednání zanechávající na první pohled viditelné stopy jako nejčastější neoprávněné vložení nějakého obsahu a/nebo převzetí jejich identity, dále pak změnu přihlašovacích údajů či smazání nějakého obsahu. Pětina zaregistrovala prohlédnutí obsahu nezvaným návštěvníkem. Nejjistěji odpovídaly v tomto směru opět osoby mladší 29 let.

Podle očekávání dominovalo jednání spadající pod virtuální násilí, z hlediska četnosti incidentů nejzávažnějších podle napadených respondentů[145] ovšem hrála nezanedbatelnou roli i majetková motivace. Z virtuálního násilí patřila k častěji předpokládaným motivacím zvědavost, pomsta nebo osobní či obecná nenávist, stalking, žert a žárlivost.

Běžnou reakcí na napadení profilu je změna přihlašovacích údajů (učinily tak dvě třetiny napadených respondentů), třetina respondentů informovala o kompromitaci účtu své kontakty. Výjimečné není ani nahlášení neoprávněných aktivit provozovateli sítě, přičemž s jeho reakcí byli respondenti vesměs spokojeni. Spíše spokojeni byli také s policií, pokud se na ni obrátili (jen zhruba 5 % napadených). Naproti tomu větší část všech respondentů (bez ohledu na jejich zkušenosti se sociálními sítěmi) se domnívá, že policii se spíše nedaří řešit incidenty spojené se zneužitím účtů na sociálních sítích.

Odpovědi 100 respondentů, kteří naopak v roce 2020* na cizí profil bez výslovného svolení jeho majitele vstoupili, ukazují poněkud odlišný obrázek. Na rozdíl od domněnek napadených jich heslo uhádlo pouze o něco více než desetina, kdežto plná třetina heslo znala od samotných majitelů účtů, na něž neoprávněně vstoupili (ať už z častějšího důvodu nějaké jednorázové aktivity v minulosti, anebo z důvodu trvalé správy daného účtu). Více než polovinu neoprávněných vstupů umožnilo zařízení se zapamatovanými přihlašovacími údaji nebo otevřeným profilem.

Většina neoprávněně vstupujících respondentů si prohlédla nějaký obsah, dílčí část z nich si nějaký obsah stáhla. Jednotlivé aktivity zanechávající viditelné stopy však v jejich případě nedosáhly ani deseti procent. Jednali převážně ze zvědavosti, ovšem sami uváděli i jiné důvody jako nuda či žert. O majetkové motivaci hovořilo pouze pár osob.

Vidíme zde tedy patrný rozdíl v odpovědích napadených vs. neoprávněně vstupujících respondentů. Mezi aktéry patrně hrají roli především stávající partneři (a dále osoby z úzkého rodinného kruhu), kdežto bývalí partneři a neznámí hackeři méně často. Přístup bývá

145 K formulaci otázek zahrnujících více incidentů viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

výrazně často umožněn fyzickým přístupem ke konkrétnímu zařízení (se zapamatovanými přihlašovacími údaji nebo právě přihlášeným profilem) a/nebo znalostí hesla z dřívějška a pachatelé si převážně prohlíží nějaký obsah.

S nadsázkou můžeme říci, že patrně dochází k řadě nedetekovaných neoprávněných přístupů na cizí profily na sociálních sítích. Děje se tak především na Facebooku, aktéry jsou stávající partneři pohánění zvědavostí a využívající dřívější znalosti hesla či sdílení zařízení s partnerem, přičemž jejich aktivita zůstává skryta, neboť si „pouze" prohlížejí jinak skrytý obsah.

Uvedené údaje mají samozřejmě své limity. Jde např. o omezení odpovědí na nejzávažnější incident (z pohledu respondenta), které nemusí odpovídat reálné šíři jednání – např. v otázce rozlišení virtuálního násilí a majetkového zájmu. Nejvýraznější slabinou je ovšem vymezení „neoprávněnosti" jednání – typickým příkladem je matka kontrolující profil svého dítěte. Nelze bez dalšího říci, zda je takové jednání oprávněné, či nikoliv.[146] Rozhodnutí ohledně oprávněnosti jsme proto záměrně ponechali na respondentech samotných. Self-reportová část dotazníku pracovala s výrazem „přístup bez výslovného svolení majitele účtu", protože posouzení „neoprávněnosti" by mohla být již příliš subjektivní a zavádějící.[147] Přesto se domníváme, že obě kategorie jsou srovnatelné, byť s uvedenou výhradou.

V.3 Falešné účty na sociálních sítích

K řadě nechtěných jednání na sociálních sítích dochází prostřednictvím zneužívání falešných účtů. Na jedné straně jde např. o falešné účty sloužící k šikaně osob, za něž se profil vydává.[148] Na straně druhé pak např. o vydávání se za někoho jiného s cílem vylákat intimní obsah, peníze či informace. Opomenout ovšem nelze ani používání falešného profilu z bezpečnostních důvodů – např. profil využívající smyšlené údaje, které neprozrazují o majiteli profilu žádné skutečné osobní údaje.[149]

Část dotazníku se proto věnovala falešným profilům na sociálních sítích, a to jak (nevyžádanému) kontaktování respondentů ze strany někoho s falešným profilem, tak používání falešných profilů samotnými respondenty. Za falešné účty považujeme ty, které využívají cizí nebo smyšlenou identitu, přičemž respondenti byli seznámeni s jejich rozlišováním následujícím textem:[150]

„*Na sociálních sítích se lze setkat i s falešnými účty. Ty využívají cizí identitu nebo smyšlenou identitu.*

146 Např. bez zohlednění aktuální situace (např. věk dítěte, náznaky podezřelé komunikace s někým online atp.).

147 Např. již zmíněná matka dítěte by své jednání zřejmě považovala za oprávněné i v pokročilém věku dítěte, kdy již lze považovat takový přístup za nepřiměřený zásah do soukromí.

148 Např. i formou zveřejňování nenávistných zpráv s cílem přisoudit jejich autorství osobě, jejíž identitu falešný profil zneužívá.

149 Přichází pochopitelně v úvahu pouze u profilů využívajících smyšlenou, a nikoliv cizí identitu.

150 Vysvětlení bylo zobrazené po celou dobu vyplňování této části dotazníku.

Účty využívající cizí identitu buď zneužijí vlastní účet člověka, za kterého se vydávají, nebo takový účet založí. Např. paní Vomáčková o sobě tvrdí, že je prezident Zeman.

Naproti tomu smyšlená identita je založená převážně na smyšlených údajích. Nejde tedy jen o zastírání vlastní identity např. smyšlenou přezdívkou. Dotyčný/á vystupuje jako někdo úplně jiný, kdo ve skutečnosti vůbec neexistuje. Např. starý pan Vomáčka se vydává za mladou slečnu, kterou si vymyslel."

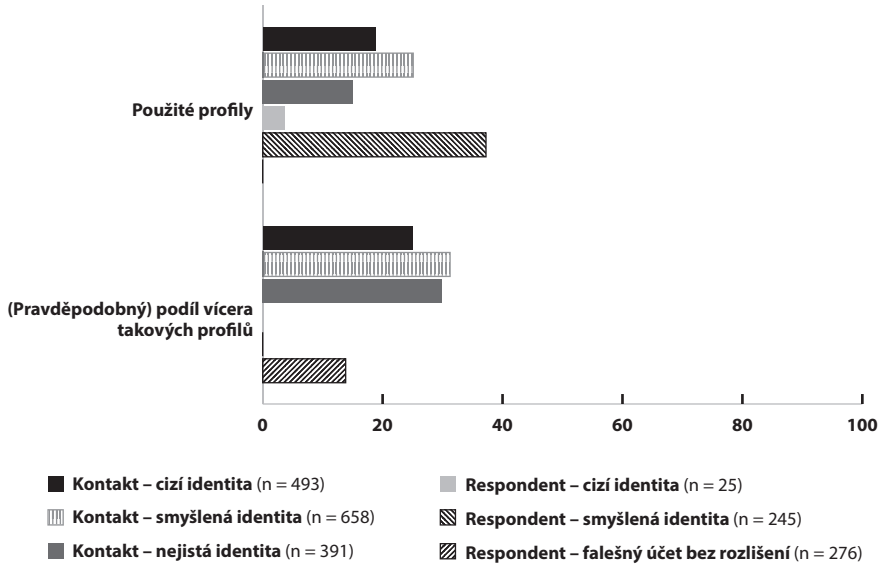
Při vyplňování dotazníku mohli respondenti odpovídat také ohledně falešného profilu, u kterého si nebyli jisti, zda využíval identitu cizí nebo smyšlenou. V konkrétních otázkách se pak vyjadřovali u daného typu falešného účtu vždy jen o jednom takovém incidentu, který považovali za nejzávažnější. Odpovídali ti, kdo používali nějakou sociální síť v roce 2020* (případně si nebyli jisti, zda v roce 2020* používali nějaký vlastní účet na sociální síti), n = 5606.

V.3.1 Používání falešných profilů vůbec

Do kontaktu s falešným profilem se v roce 2020* dostalo 12 % respondentů používajících sociální sítě, resp. 20 % společně s těmi, kteří se domnívají, že šlo o falešný účet, ale nebyli si jisti (664, resp. 1 094 respondentů)[151] (Graf 47). Významně často tak odpovídali muži a osoby mladší 29 let, kdežto senioři starší 60 let naopak významně často v takovém kontaktu nebyli. Vysokoškoláci se převážně domnívali, že s nikým takovým pravděpodobně v kontaktu nebyli. Významně často byli v kontaktu s falešným účtem využívajícím cizí identitu ženy, kdežto muži naopak s profily se smyšlenou nebo nejistou identitou. Většina osob se dostala do kontaktu s falešnými účty opakovaně (Graf 47). U účtů s cizí identitou to byli významně často respondenti mladší 29 let, u smyšlené a/nebo nejisté identity muži. Není bez zajímavosti, že senioři starší 60 let u všech tří typů falešných účtů uváděli signifikantně často pravděpodobný kontakt.

151 Ti, kteří si nebyli jisti, byli požádáni, aby odpovídali, jako by o falešný účet skutečně šlo.

Graf 47: Typy falešných účtů (%)



Naproti tomu 5 % respondentů (276 osob) používalo samo falešný účet.[152] Převážně šlo o smyšlenou identitu[153] (Graf 47). Významně často ji používaly ženy (94 % žen používajících falešný účet), kdežto cizí identitu naopak muži (12 % mužů používajících falešný účet). Zhruba třetina (31 %) používala v roce 2020* více falešných účtů. Zdaleka nejčastěji používali Facebook (75 %, významně často osoby ve věku 30–44 let),[154] dále pak Instagram (15 %), další sociální sítě už jen řádově do 4 %.

V.3.2 Podoba a domnělá motivace falešných účtů

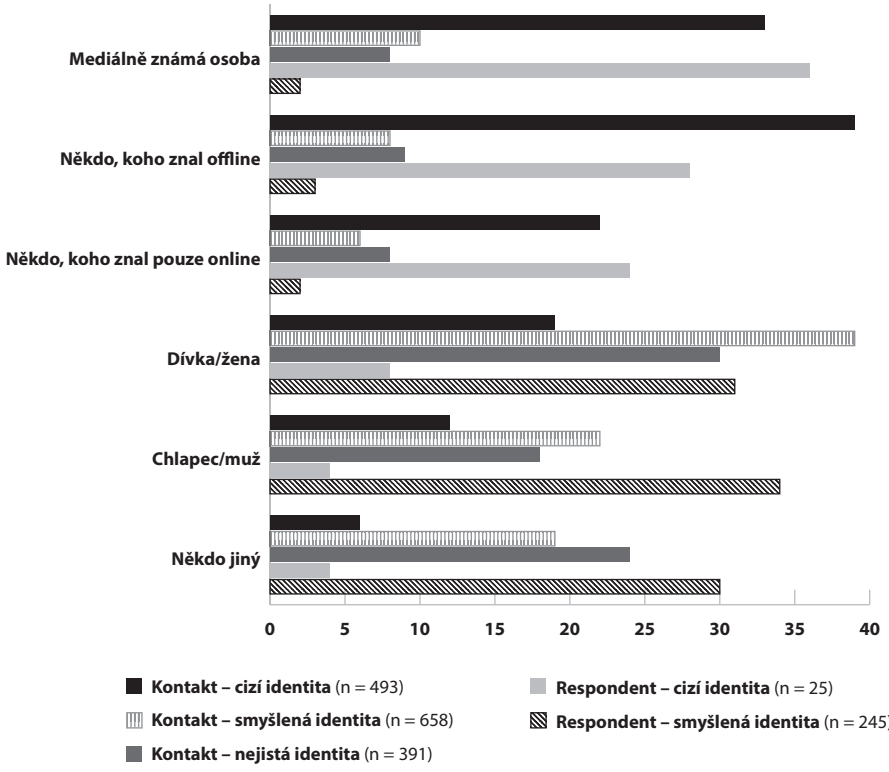
Za pozornost stojí i konkrétní podoba používaných falešných účtů.

152 Odhlédneme-li od období roku 2020*, falešný účet použilo někdy v životě 11 % respondentů (769 osob, kteří používali sociální sítě v roce 2020*).

153 Varianta nejisté identity zde pochopitelně chybí.

154 Vzhledem k ostatním odpovědím i obecnému povědomí autorů se lze domnívat, že určitou část této kategorie představují rodiče kontrolující prostřednictvím falešného profilu online komunikaci svých dětí.

Graf 48: Za koho se falešný profil vydával (%)



Nejvíce falešných profilů vedených pod cizí identitou využívá někoho známého, ať už jde o nejčastější mediálně známou osobu nebo o někoho známého dotyčnému (jak z reálného prostředí, tak i pouze online). Jiné charakteristiky vybrali respondenti jen sporadicky. Ženy byly významně často v domnělém kontaktu s jim známou osobou z reálného prostředí, respondenti mladší 29 let s dívkami. Průměrný věk osoby, jejíž identita byla zneužita, byl 33 let (s rozmezím 12–80 let).[155]

Zajímavá je disproporce u používání smyšlených identit z pohledu respondentů, kteří byli s někým takovým v kontaktu, vs. respondentů, kteří sami takový profil používali. Kontaktovaní respondenti si byli vědomi častěji falešných profilů se smyšlenou dívčí/ženskou identitou, kdežto respondenti sami používali častěji smyšlenou chlapeckou/mužskou identitu.[156] Je možné, že je snazší vytvořit věrohodný profil se smyšlenou chlapeckou/mužskou identitou, který je tudíž méně často detekovaný coby falešný. Anebo mají respondenti

155 Nejčastěji používaná sociální síť Facebook umožňuje založit profil osobám ve věku nejméně 12 let (resp. pro vytvoření profilu je nezbytné uvést věk alespoň 12 let).

156 Muži používali sami významně často chlapecké/mužské profily, kdežto ženy, osoby mladší 29 let a osoby s pouze základním vzděláním dívčí/ženské profily.

a priori více pochybností ohledně dívčích/ženských profilů.[157] Druhou z uvedených variant by mohla potvrzovat i část respondentů v kontaktu s profilem s nejistou identitou, kteří také uváděli častěji kontakt s dívčí/ženskou smyšlenou identitou. Průměrný věk kontaktující smyšlené osoby byl 30 let (s rozmezím 15–100 let).[158]

V.3.3 Jednání falešných profilů

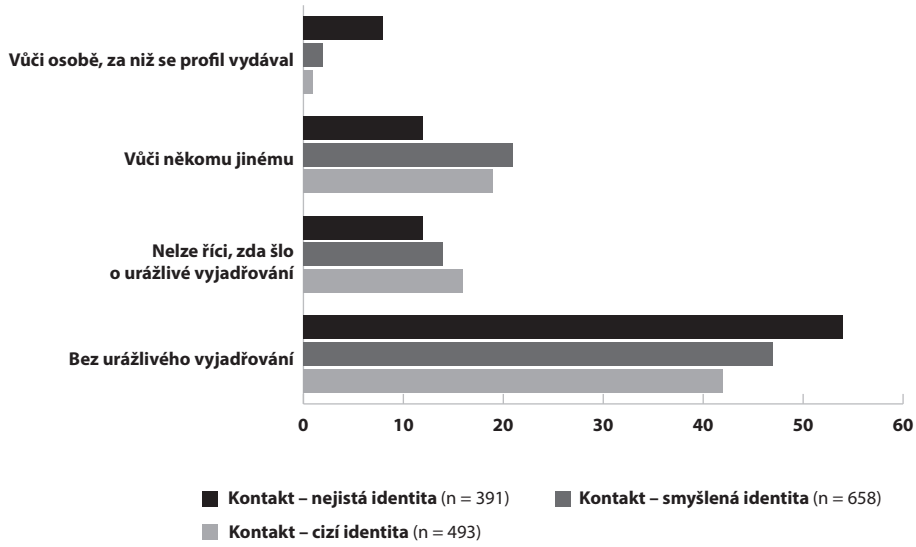
Používání falešného profilu nezřídka zahrnuje urážlivé jednání. Jednak vůči jiným osobám, ale i vůči osobě, jejíž identitu profil zneužívá.[159] Urážení je součástí komunikace u zhruba pětiny kontaktů, zejména při zneužívání cizí identity jde pak (i) o urážení osoby, za niž se profil vydával (Graf 49). Kromě běžných urážek šlo např. o „*hloupé příspěvky*", „*vydírání*", „*vtipkování o sobě*", „*sdílení nevhodného obsahu*", „*účet na twitteru se tvářil jako jeden z našich předních politiků a zároveň tvrdil že je hloupý a nadával si*," „*haněli prezidenta, pravdoláskaři*", „*nejspíš se jednalo o BOTa, který je naprogramován na sdílení sexuálních stránek*," „*trollení, rozhádat skupinu, lživá tvrzení*", ale i podrobnější jako „*napsal mi jako úchyl a potom psal i mému příteli, kde si vymýšlel, že jsem mu na jeho nabídky kývla*" nebo „*rusofilní trollové… takže komentování všeho co se týkalo Ruska, USA, NATO atd*" či naznačující jednání se značným dopadem – např. „*pošpinění dobrého jména u zaměstnavatele mé příbuzné, mělo za následek její rozvázání pracovního poměru výpovědí ze strany zaměstnavatele*" nebo „*ukradla cizi fb skupinu s 16k uzivately…*"

157 Významně často vypovídali ohledně kontaktu se smyšlenou dívčí/ženskou identitou pochopitelně muži, osoby mladší 29 let, ale také respondenti s pouze základním vzděláním. Ženy hovořily naopak o kontaktech s chlapeckými/mužskými smyšlenými profily.

158 U profilů s nejistou identitou byl průměrný věk 31,5 roku (s rozmezím opět 15–100 let).

159 Např. znevažování vlastní osoby, resp. osoby, jejíž identitu profil používá. Může jít např. i o silně vulgární vyjadřování jménem domnělého (jinak velice slušného) majitele profilu atp.

Graf 49: Urážlivé vyjadřování (%)[160]

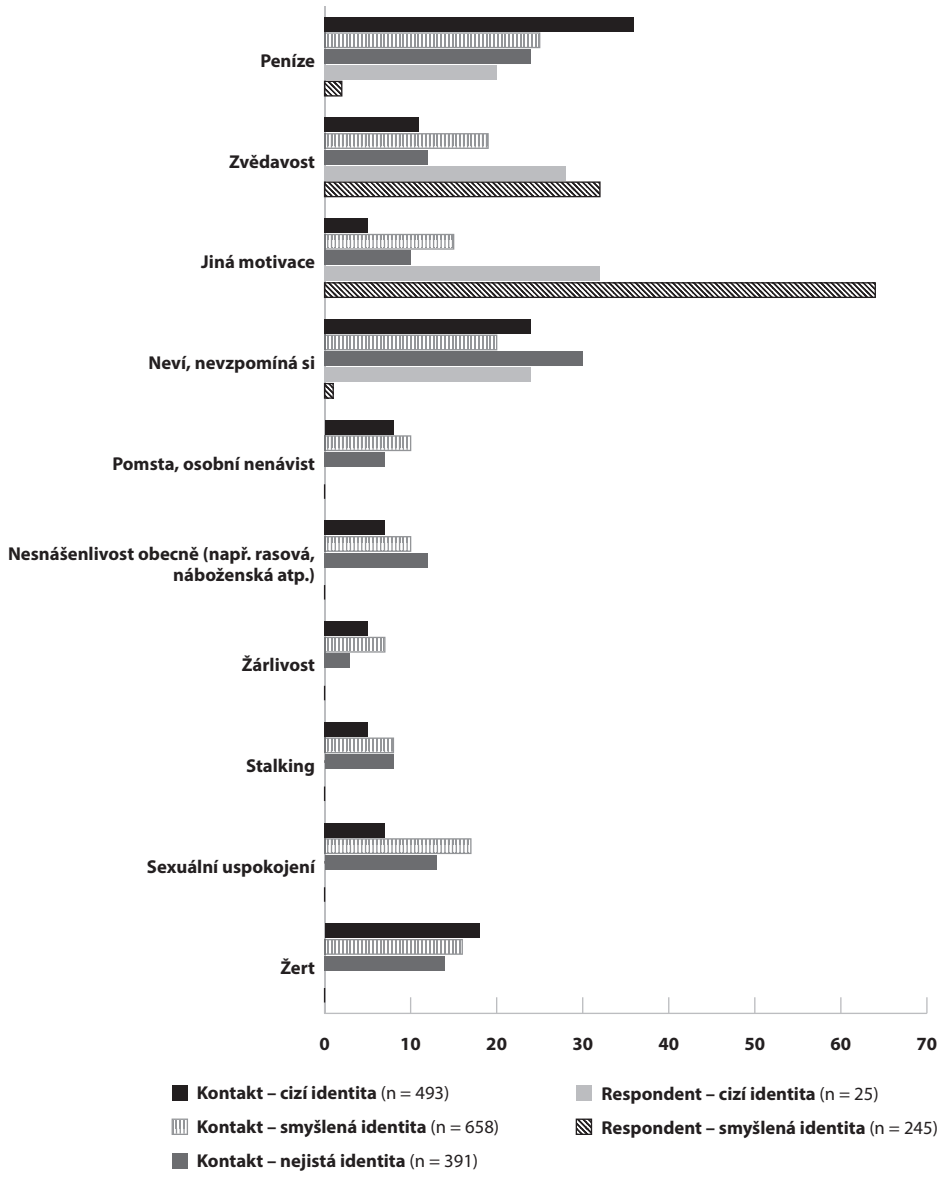


Respondenti s vlastními falešnými profily na otázky ohledně urážlivého vyjadřování neodpovídali, byli však dotázáni na motivaci vedoucí ke zřízení falešného profilu. Opět měli na výběr mezi penězi, zvědavostí či jinou, vlastní odpovědí.[161] Osoby mladší 29 let a osoby s pouze základním vzděláním uváděli významně často zvědavost, naopak vlastní odpovědi např. vysokoškoláci. Vlastní odpovědi zde uváděli respondenti poměrně často, rozdíl je patrný zejména u profilů se smyšlenou identitou, přičemž převažovala snaha o anonymitu a péče o vlastní soukromí. Respondenti, kteří byli s falešným profilem sami v kontaktu (bez ohledu na případný vlastní falešný profil), vybírali ohledně domnělé motivace z konkrétnějších odpovědí (Graf 50). Opět zde vystupuje do popředí skupina osob mladších 29 let, která významně často předpokládá jako motivaci stalking a/nebo žárlivost.

160 Otázku zodpovídali pouze respondenti, kteří byli s falešným profilem v kontaktu (bez ohledu na to, zda sami případně používali také falešný profil).

161 V případě falešných profilů není zvolená formulace zcela přiléhavá, nicméně v zájmu srovnatelnosti motivace napříč různými oblastmi jsme ponechali identické opakující se znění i zde.

Graf 50: Motivace k používání falešného účtu (%)

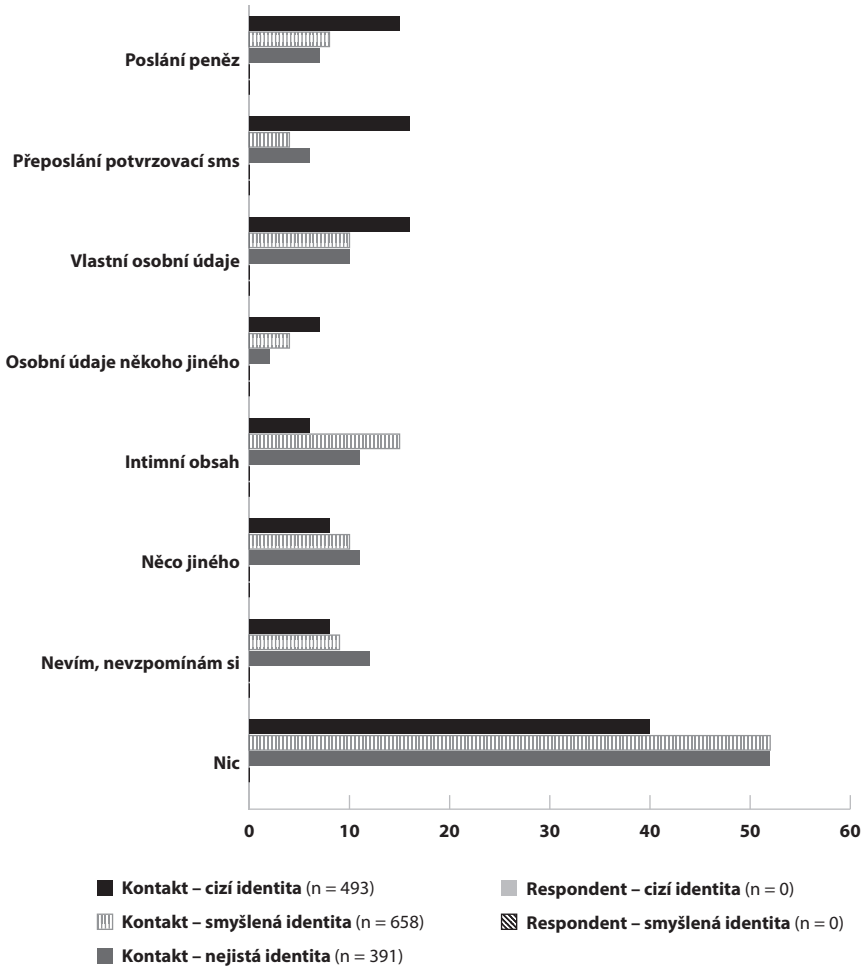


Podrobnější otázka v dotazníku směřovala na případné požadavky ze strany falešných profilů, neboť předchozí analýza trestních spisů vedených o počítačových trestných činech za rok 2015[162] mimo jiné potvrdila zneužívání sociálních sítí jak k virtuálnímu násilí (zejména vztahovému, typicky sledování ze žárlivosti, pomluvy ex-partnerů atp.), tak k podvodnému jednání (typicky vylákávání peněz pod záminkou přeposílání potvrzovacích SMS domněle známé osoby atp.). Soudě dle odpovědí respondentů, jimi odhalené

162 Zjednodušeně řečeno, podrobněji k předchozímu výzkumu viz Vlach et al. (2020).

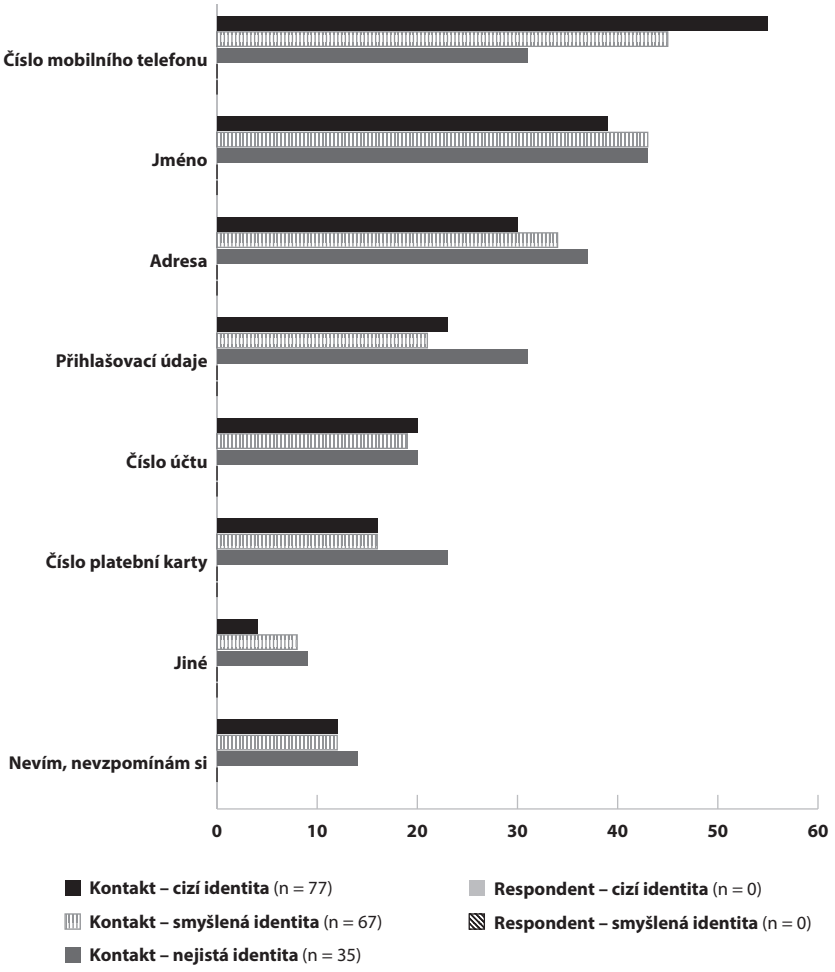
falešné profily něco požadují řádově v desetině případů, přičemž profily zneužívající cizí identitu se více soustředí na finanční vytěžení komunikace, kdežto profily se smyšlenou identitou spíše na intimní komunikaci či zneužití (Graf 51). Profily, o kterých se respondenti domnívali, že byly falešné, ale už si nebyli jisti, zda používaly cizí nebo smyšlenou identitu, opět odpovídaly převážně profilům se smyšlenou identitou.

Graf 51: Požadavky falešného účtu (%)



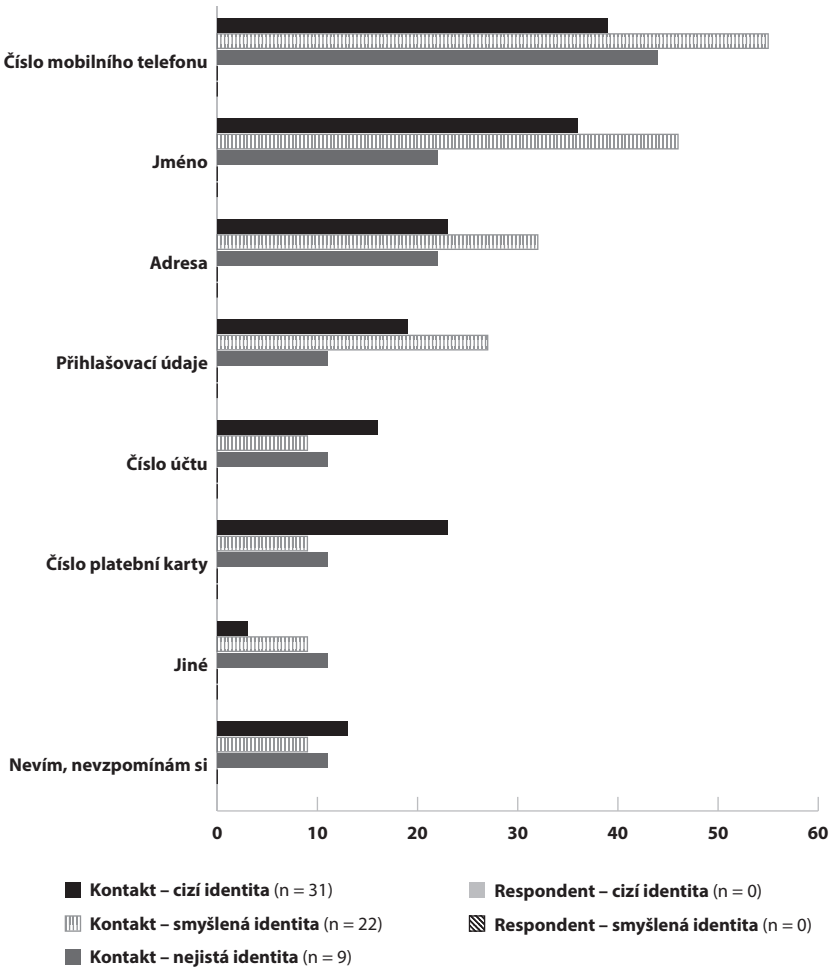
Významně často měly zkušenost s žádostí profilu s cizí identitou o intimní obsah osoby mladší 29 let a ženy, druhé jmenované pak i s žádostí o vlastní osobní údaje (muži naopak zrcadlově oproti ženám). Signifikantní setkávání se s požadavky po intimním obsahu žen se ukázalo i ze strany smyšlených profilů, u osob mladších 29 let pak u profilů se smyšlenou i nejistou identitou.

Graf 52: Požadované vlastní osobní údaje (%)



Falešné profily nejčastěji vyzvídaly z vlastních osobních údajů číslo mobilního telefonu (nepřekvapivě zejména u žen a osob mladších 29 let), dále jméno a/nebo adresu, také však další údaje jako číslo platební karty či účtu nebo přihlašovací údaje aj. (Graf 52). Podobně se snažily zjistit od respondenta osobní údaje nějakých dalších osob, a to celkově řádově v podobném poměru jako u vlastních osobních údajů (Graf 53).

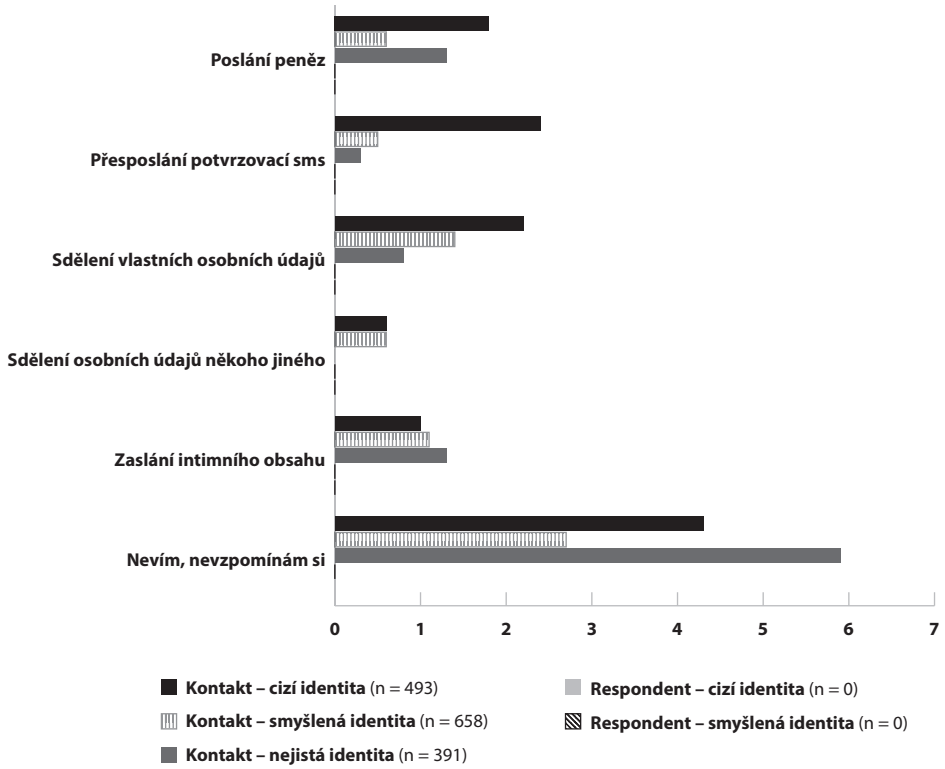
Graf 53: Požadované cizí osobní údaje (%)



V.3.4 Reakce respondentů na kontakt s falešným profilem

Drtivá většina respondentů na požadavky falešných profilů nereagovala (88–94 %), někteří jim však přece jen vyšli vstříc, řádově ovšem na úrovni 0,5–2 % dožadovaných respondentů. Přesto považujeme za vhodné je zde uvést (Graf 54). Ve většině těchto případů (67–83 %) totiž vznikla respondentům v dané souvislosti přímá finanční škoda, ať už v podobě odeslání peněz, odčerpání peněz z účtu u mobilního operátora či jinak. Pohybovala se ve výši od 100 Kč do zhruba 80 tis. Kč (průměrná výše přibližně 5 tis. Kč). Dobrou zprávou zůstává, že téměř čtvrtině poškozených (13–25 %) se podařilo získat peníze alespoň částečně či dokonce v plné výši zpět.

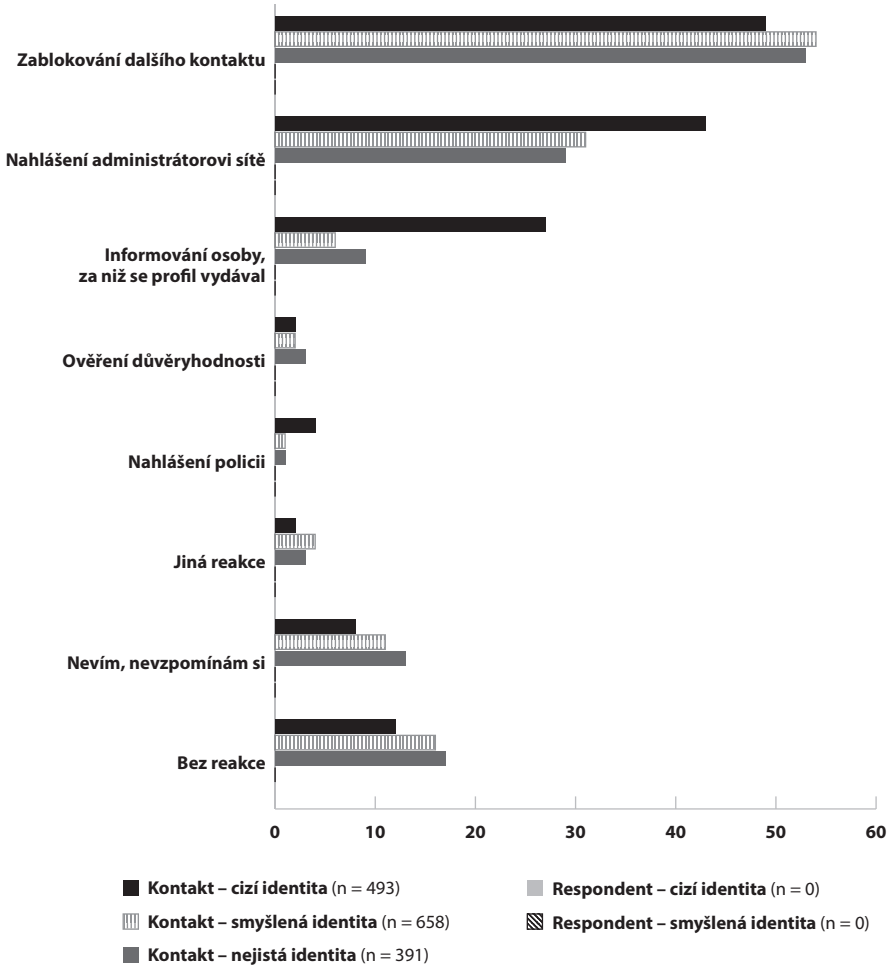
Graf 54: Jednání respondenta v kontaktu s falešným profilem (%)



Řada respondentů pojala podezření ohledně nepravosti profilu vzhledem k celkové nevěrohodnosti, spamu a/nebo útočnosti profilu (trollování, vulgarity atp.). Mnozí z nich (a to zejména v případě podezření na zneužití reálné identity někoho jiného) ověřovali pravost profilu.[163] Zdaleka nejčastěji však respondenti reagovali na kontakt s falešným profilem nahlášením administrátorovi sítě a/nebo vlastním zablokováním další komunikace s ním (Graf 55). I zde se vymyká skupina respondentů mladších 29 let, která se obrací (na rozdíl od ostatních) signifikantně často na policii, jde ovšem o mizivý počet. Naopak většina respondentů řeší situaci svépomocí, a to zablokováním dalšího kontaktu, případě kontaktováním administrátora sítě.

163 Např. telefonát domnělému majiteli, vyhledání profilových fotografií online (nejsou-li použité u více profilů s různými údaji) atp.

Graf 55: Reakce na incident (%)



Obecně však nepanuje výraznější důvěra ve schopnosti policie řešit případy spojené se zneužíváním profilů na sociálních sítích, ať už vlastních či cizích nebo smyšlených profilů. Blíže k tomu viz kapitola Latence a důvěra ve schopnosti policie.

V.3.5 Závěr k falešným účtům na sociálních sítích

S falešnými účty se setkala řada respondentů, nemálo jich samo falešný účet také používalo v roce 2020*. U některých účtů není patrné, zda využívají smyšlenou nebo cizí identitu. Rozdíly mezi těmito dvěma typy nejsou sice zásadní, rozhodně však stojí za pozornost. Podobně, jako specifická skupina osob mladších 29 let, která se mnohdy objevuje jako statisticky významná. Dle očekávání bývají součástí jednání falešných profilů i urážlivá jednání a různé požadavky, nicméně podlehla jim pouze relativně malá část respondentů.

Nutno podotknout, že v této části odpovídali pouze ti respondenti, kteří si byli vědomi nebo se alespoň domnívali, že byli v kontaktu s falešným účtem. Podaný obrázek tak nezachycuje kontakt s takovými profily, jejichž falešnost respondenti neodhalili.[164]

V.4 E-banking[165]

Při sledování používání a zneužívání e-bankingu se pozornost zaměřuje obvykle na počty uživatelů či bezpečnostní obavy s nimi spojené (sleduje např. EUROSTAT). Můžeme najít také informace o výši škod způsobených zneužitím e-bankingu. Z hlediska získání přístupu se uvažuje zejména o aktuálních podobách kyberútoků (např. pravidelně zveřejňované zprávy EU ENISA Threat Landscape nebo informace o phishingu dostupné z různých zdrojů). Jako motivace zneužití e-bankingu se nabízí samozřejmě majetkový zájem s cílem odčerpat prostřednictvím napadeného účtu peněžní prostředky, ať už v podobě částek převedených na jiný účet či vybraných v bankomatu nebo zřízením úvěru k tíži majitele napadeného účtu ve prospěch pachatele a ke škodě banky.[166] Ukázalo se, že v praxi není motivace zneužití e-bankingu tak samozřejmá.

V.4.1 Aktéři neoprávněných vstupů na e-banking

Zhruba v 15 % analyzovaných trestních spisů za rok 2015 měl být zneužit e-banking.[167] V roce 2020* měla e-banking převážná většina respondentů (93 %, 6 338 osob), zejména v produktivním věku (senioři starší 60 let tíhli k opačným odpovědím). 3 % z nich (199 osob) uvedla, že jejich e-banking někdo v roce 2020* (pravděpodobně)[168] zneužil, z toho v téměř polovině případů opakovaně.[169] Naproti tomu 9 % respondentů v rámci self-reportu vypovědělo, že v roce 2020* používali e-banking někoho jiného,[170] z toho 29 % (191 osob) tak učinilo v roce 2020* bez výslovného svolení majitele účtu.

164 Připomínáme také, že respondenti odpovídali ohledně kontaktů, které považovali za nejzávažnější, nikoliv o všech svých zkušenostech.

165 Dílčí informace obsažené v této kapitole byly již publikovány (Kudrlová & Vlach, 2023; Kudrlová, 2023).

166 Poškozená osoba se může lišit v návaznosti na vnitrostátní právní úpravu (majitel kompromitovaného účtu nebo banka, případně oba). V České republice je vlastníkem peněžních prostředků běžného spotřebitelského účtu banka, vůči níž má majitel účtu pohledávku, přičemž banka má povinnost tuto pohledávku plnit při splnění příslušných podmínek (např. dostatečný zůstatek na účtu a pokyn k převodu prostřednictvím e-bankingu) (Volevecký, 2013; Novák, 2022). Bez ohledu na postavení subjektů v případném trestním řízení (poškozený, oběť), odčerpané finanční prostředky představují pro majitele účtu vždy přinejmenším komplikaci (např. nedostupnost odčerpaných prostředků, byť případně jen krátkodobá).

167 Zneužití e-bankingu bylo zřejmě častější, a to i v praxi samotných justičních orgánů (tzn. mimo latentní kriminalitu) – některé případy mohly být právně kvalifikovány např. pouze jako podvod (české trestní právo v současnosti nerozlišuje podvody využívající kyberprostor od těch ostatních).

168 Souhrn odpovědí, kdy si respondenti byli napadením jisti spolu s odpověďmi, kdy se domnívali, že k napadení pravděpodobně došlo.

169 Pakliže bylo takových incidentů více, respondenti byli požádáni o odpovídání ohledně toho z nich, který oni sami považují za nejzávažnější.

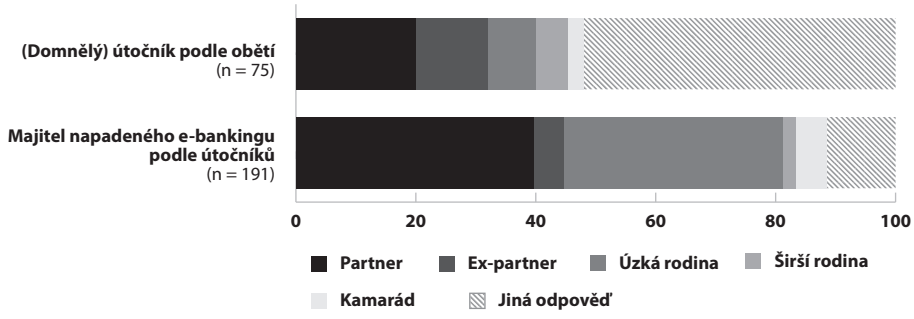
170 Nejčastěji tak činily osoby mladší 29 let, přičemž s věkem počet osob používajících e-banking někoho jiného postupně klesá.

Kupodivu více než třetina napadených respondentů věděla, kdo na jejich účet neoprávněně vstoupil (38 %, 75 osob). Mělo se jednat především o osoby z blízkého okolí včetně bývalých partnerů. Pětina respondentů označila za pachatele stávajícího partnera (20 %, 15 osob), méně často pak bývalého partnera (12 %, 9 osob) nebo někoho z úzkého rodinného kruhu mimo partnera (děti, rodiče, prarodiče, vnoučata, sourozenci, 8 %, 6 osob). Mezi častější jiné odpovědi (40 %, 30 osob) patřily převážně společnosti podnikající prostřednictvím internetu (24 %, 18 případů, typicky e-shop) nebo neznámí hackeři (17 %, 13 osob) (Graf 56).

Své partnery označovali za pachatele signifikantně často muži (29 %), kdežto ženy naopak „jiné než vyjmenované osoby" (55 %, často předpokládaly útok neznámého hackera). Jiné než vyjmenované osoby shledávali významně často jako viníky také respondenti starší 45 let (60 % napadených respondentů ve věku 45–59 let a 77 % napadených respondentů ve věku 60–74 let).

Mezi respondenty, kteří naopak v roce 2020* použili cizí e-banking bez výslovného svolení jeho majitele, se nenašel nikdo, koho bychom mohli označit za neznámého hackera.[171] I zde vidíme mezi aktéry především partnery (stávající i bývalé) a osoby z úzkého rodinného kruhu, ovšem v jiném poměru. Na účty svých bývalých partnerů totiž vstoupilo pouze 6 % respondentů neoprávněně používajících cizí účet (srov. výše uvedených 20 % domnělých útočníků předpokládaných napadenými respondenty). Naproti tomu použití účtu svého stávajícího partnera (v době použití účtu) bez jeho výslovného svolení přiznalo 45 % neoprávněně vstupujících respondentů (opět srov. 12 % domnělých útočníků předpokládaných napadenými respondenty). Výrazný rozdíl je také u ostatních příslušníků úzkého rodinného kruhu, na jejichž účet vstoupilo bez jejich výslovného souhlasu 41 % respondentů (opět srov. 8 % domnělých útočníků předpokládaných napadenými respondenty) (Graf 56).

Graf 56: Aktéři neoprávněného vstupu do e-bankingu (%)



171 Jednak se každý z nich s majitelem účtu znal, jednak nikdo nepoužil žádné zvláštní schopnosti nad rámec běžné uživatelské znalosti digitálních technologií řadového uživatele.

V.4.2 Motivace, aktivita a škody

Respondenti odpovídající v rámci self-reportové části (ti, kdo neoprávněně vstoupili na cizí účet) byli vyzváni k uvedení své motivace, přičemž mohli vybrat mezi penězi a zvědavostí nebo uvést zcela jinou odpověď (případně uvést „nevím" nebo „nechci odpovědět").[172] K našemu překvapení vybralo 45 % respondentů (85 osob) „jinou" odpověď a kromě jediné výjimky uvedli jednání na základě něčí žádosti. Nutno podotknout, že na otázku odpovídali pouze ti respondenti, kteří uvedli, že použili cizí e-banking bez výslovného svolení jeho majitele. Buď tedy pocházela ona žádost od někoho jiného než majitele účtu, anebo vědomě jednali v rámci cizího účtu nad rámec svého oprávnění vyplývajícího z oné žádosti.[173]

Mimo to uvedlo nejvíce respondentů peněžní motivaci (27 %, 52 osob), ve čtyřech případech doplněnou zvědavostí. Přestože se ukázala majetková motivace výrazně častěji než zvědavost (12 %, 22 osob), zdaleka proto nedosáhla předpokládané převahy, a to i když pomineme odpovědi poukazující na „jinou" motivaci. Signifikantně často hovořili o zvědavosti osoby mladší 29 let (22 % pachatelů v této věkové skupině).

Zvědavosti a finanční motivaci odpovídá i otázka zaměřená na samotnou aktivitu po (neoprávněném) přístupu. Respondenti uváděli nejčastěji zjištění finanční situace majitele účtu (61 %) a převod peněz na jiný účet (45 %), ostatní možnosti byly jen minoritní.

Napadených respondentů jsme se naproti tomu ptali na vznik přímé finanční škody (např. peníze převedené na jiný účet nebo úvěr ve prospěch útočníka). Došlo k ní u 55 % incidentů (110 případů)[174] s celkovou výší škody 2 436 747 Kč, průměrnou způsobenou škodou ve výši 221 523 Kč, nejnižší škodou 100 Kč, nejvyšší škodou 545 555 Kč a mediánem 2 000 Kč.[175] Většině napadených se podařilo získat ztracené peníze zpět: 62 % (68 osobám) v plné výši, 15 % (16 osobám) alespoň částečně (signifikantně málo byly v tomto ohledu úspěšné ženy a osoby mladší 29 let).

Většina majitelů neoprávněně použitých účtů (bez ohledu na případnou ztrátu peněz) se obrátila na banku (71 %, 141 osob), v 5 případech to byla naopak banka, která sama informovala respondenta o podezřelé aktivitě či rovnou zablokovala podezřelou transakci. Někteří z respondentů se obrátili na policii (14 %, 27 osob). Zřejmě s ohledem na ohrožení peněz patří neoprávněný přístup k e-bankingu z dotazníkem sledovaných jevů k nejčastěji oznamovaným jednáním, přičemž signifikantně často se na policii obraceli v roce 2020* majitelé kompromitovaných účtů mladší 29 let. Respondenti byli s policií vesměs spokojeni (více než tři čtvrtiny z nich), uvítali by nicméně větší aktivitu z její strany.

172 Šlo o jednu z otázek opakujících se pro srovnatelnost u různých jednání napříč dotazníkem.

173 Vzhledem ke konstrukci a fungování dotazníku je nepravděpodobné, že by si nebyli vědomi skutečnosti, že odpovídají ohledně použití cizího e-bankingu bez výslovného svolení jeho majitele.

174 7 % napadených respondentů (14 osob) nevědělo nebo si nevzpomnělo, zda jim nějaká škoda vznikla.

175 Respondenti, kteří odpověděli, že jim vznikla finanční škoda, museli bohužel pro pokračování v dotazníku následně uvést přibližnou částku bez možnosti odpovědi „nevím" (nebo obdobné), protože naprogramování dotazníku nedovolilo použití jiných než numerických znaků. Uvedené částky je proto nutno chápat jen jako orientační, neboť někteří respondenti mohli uvést smyšlenou částku, aby mohli pokračovat ve vyplňování dotazníku.

V.4.3 Získání přístupu

Respondentům, kteří v roce 2020* nejméně jednou vstoupili na cizí e-banking bez výslovného svolení jeho majitele, umožnila přístup v nezanedbatelném množství případů dispozice se zařízením, ve kterém byl cizí e-banking otevřený (16 %, 30 osob). Významně často toho využily osoby mladší 29 let (28 % pachatelů v této věkové skupině).

Ostatní způsoby získání přístupu byly jen sporadické, s jedinou výjimkou zdaleka převyšující všechny ostatní, a to přístupem díky dříve poskytnutým přihlašovacím údajům ze strany samotného majitele napadeného účtu (80 %, 152 osob). Zdaleka nejčastěji šlo o partnery (48 %, 73 osob) a osoby z úzkého rodinného kruhu (45 %, 69 osob). Výrazně méně často šlo o účet bývalých partnerů (6 %, 9 osob),[176] kamarádů nebo někoho z širšího rodinného kruhu (obojí po 3 %, 5 a 4 osoby) či někoho zhola jiného (8 %, 12 osob) (Grafy 57 a 58).

Nejčastějším důvodem poskytnutí byla žádost samotného majitele účtu o nějakou jednorázovou aktivitu (72 %),[177] žádáni byli především respondenti mladší 29 let (84 % osob ve věku 16–29 let, kteří neoprávněně použili cizí e-banking díky poskytnutí přihlašovacích údajů majitelem účtu, přičemž jejich poměr s věkem setrvale klesá) a vysokoškolsky vzdělané osoby (83 %). Třetina neoprávněně vstupujících respondentů (33 %) uvádí jako důvod dispozice s cizími přihlašovacími údaji trvalou péči o cizí e-banking.

Ze 75 respondentů, kteří vědí, kdo v roce 2020* nejméně jednou zneužil jejich e-banking, jich téměř polovina (45 %, 34 osob) dobrovolně pachateli poskytla své přihlašovací údaje.[178] Majitelé napadených účtů uváděli jako útočníky zneužívající dříve poskytnuté údaje partnery (32 %, 11 osob), rodinu (3 aktéři z úzkého rodinného kruhu, 9 %, a 2 z širšího, 6 %), také 2 kamarády (6 %) a 10 jiných osob (29 %) (Grafy 57 a 58).

Nejčastěji (62 %, 21 osob) jim poskytli své přihlašovací údaje z důvodu umožnění jednorázové výpomoci (např. zjištění zůstatku). Ostatní důvody byly pouze minoritní, za zmínku stojí snad jen trvalá péče o e-banking (15 %, např. vnuk spravující e-banking prarodičů).

Když se přitom podíváme na praxi sdílení přihlašovacích údajů k vlastnímu e-bankingu respondenty vůbec (bez ohledu na viktimizaci nebo neoprávněné přístupy), jde o jednání relativně časté. Své přihlašovací údaje ke svému e-bankingu někdy poskytla téměř desetina všech respondentů používajících e-banking (8 % uživatelů, 495 osob), z toho 23 % dokonce více než jednomu člověku (významně často osoby mladší 29 let, 31 %).

Své přihlašovací údaje poskytují signifikantně často osoby se základním vzděláním nebo vyučené bez maturity (12 a 10 %), osoby mladší 29 let (10 %) a ženy (9 %). Celkově jsou údaje sdíleny především se stávajícími partnery (72 %) a/nebo někým z úzkého rodinného

176 Předpokládáme, že v době poskytnutí přihlašovacích údajů šlo převážně o stávající partnery a ke zneužití údajů došlo až po skončení vztahu, nicméně nelze vyloučit opak, a tak ponecháváme kategorii jako samostatnou.

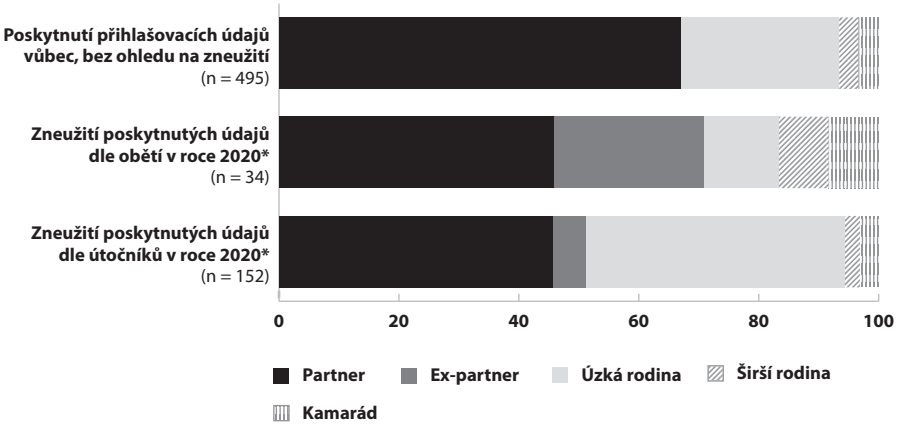
177 Zde i na jiných místech měli respondenti možnost vybrat více odpovědí, pokud se vzájemně nevylučovaly.

178 Blíže k dalším otázkám směřujícím na tzv. kyberhygienu např. síla hesla k e-mailu nebo používání antiviru (Cain et al., 2018), viz kapitoly E-mail a Fyzická vybavenost – používaná zařízení a jejich ochrana.

kruhu (29 %) (Grafy 57 a 58). S osobami z úzkého rodinného kruhu sdílí své přihlašovací údaje významně často také osoby starší 60 let (typicky prarodiče se svými dětmi či vnoučaty) a ženy i osoby mladší 29 let, kteří sdílejí či sdíleli své údaje s více osobami. Muži a osoby ve věkové skupině 30–44 let, kteří poskytnuli své přihlašovací údaje více osobám, je sdělovali významně často svým partnerům.

I v této skupině (všichni respondenti používající e-banking, kteří sdíleli své přihlašovací údaje s alespoň jednou další osobou) je nejčastějším důvodem sdílení přihlašovacích údajů jednorázové použití e-bankingu (74 %, 364 osob), zhruba pětina respondentů uvedla trvalou správu e-bankingu (21 %, 105 osob). Významně často nechávají někoho spravovat svůj e-banking trvale osoby ve věku 45–59 let. Nejstarší z respondentů (ve věku 60–74 let) uváděli nejčastěji sdílení přihlašovacích údajů s někým dalším kvůli vlastním obavám, aby blízké osoby mohly disponovat jejich prostředky v případě náhlé nehody, invalidity či jiné zdravotní překážky včetně smrti respondenta.

Graf 57: Sdílení přihlašovacích údajů k e-bankingu s vybranými osobami (%)[179]



Při srovnání uvedených tří skupin respondentů vychází najevo, že hlavními aktéry sdílení přihlašovacích údajů i neoprávněného používání cizího e-bankingu jsou partneři a osoby z úzkého rodinného kruhu. Zdá se, že méně rizikoví jsou v tomto směru partneři. Patří sice mezi nejčastější aktéry, ale jejich podíl na zneužití poskytnutých přihlašovacích údajů je nižší než podíl na poskytnutých údajích vůbec. Vyplývá to zejména z výpovědí pachatelů, a to i při zahrnutí jednání bývalých partnerů.[180] Naopak vyšší podíl zneužití

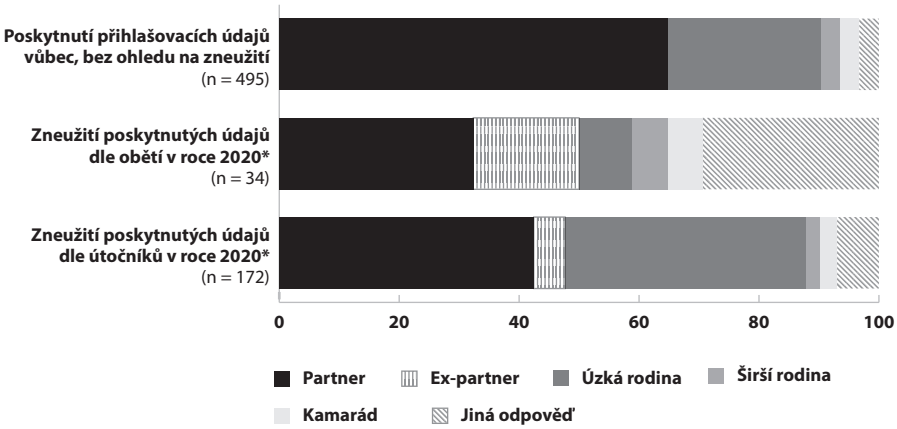
179 Graf sdružuje odpovědi od tří skupin respondentů. Zaprvé těch, kteří kdy někomu poskytnuli své přihlašovací údaje k e-bankingu. Zadruhé od respondentů, jejichž e-banking někdo nejméně jednou neoprávněně použil v roce 2020* a kteří zároveň vědí, kdo tak učinil. Zatřetí od respondentů, kteří v roce 2020* nejméně jednou použili cizí e-banking bez výslovného svolení jeho majitele. Pro názornost záměrně nezobrazuje „jiné" aktéry.

180 Lze předpokládat, že přihlašovací údaje byly sdíleny s tehdy stávajícími partnery, z nichž byli v době neoprávněného použití cizího e-bankingu již bývalí partneři.

poskytnutých přihlašovacích údajů se ukazuje mezi osobami z úzkého rodinného kruhu.[181] Sdílení přihlašovacích údajů s osobami z širšího rodinného kruhu a kamarády je poměrově spíše zanedbatelné, jiné subjekty se objevují jen sporadicky.

Z úhlu pohledu obětí se poměr poskytovaných a zneužitých přihlašovacích údajů poněkud liší, hlavní rozdíl spočívá v podílu domnělých útočníků – bývalých partnerů a osob z úzkého rodinného kruhu. Oběti také častěji ukazovaly na někoho z širšího rodinného kruhu, kamarády a především další subjekty (hacker, e-shop aj.). Při jejich začlenění se rozdílný poměr domnělých a skutečných aktérů ještě zvýrazní (Graf 58).

Graf 58: Sdílení přihlašovacích údajů k e-bankingu i s dalšími osobami (%)



Pakliže vezmeme v úvahu, že oběti si patrně nejsou vědomy části neoprávněných přístupů na jejich e-banking, a to zejména co do přístupů stávajících partnerů motivovaných zvědavostí, podíl partnerů podílejících se na neoprávněných přístupech k cizímu e-bankingu zůstává velmi zhruba stejný nebo nižší, než s kolika sdílejí respondenti své přihlašovací údaje. Naproti tomu sdílené údaje zneužívají zřejmě výrazně častěji osoby z úzkého rodinného kruhu, kdežto bývalí partneři naopak méně často.

V.4.4 Závěr k e-bankingu

Zásah do soukromí při neoprávněném použití e-mailové schránky nebo cizího profilu na sociální síti je zřejmý. Prvek zásahu do soukromí ovšem může být patrný i v tak nepředpokládaném prostředí, jakým je e-banking. Lze to přirovnat k prohlížení cizí peněženky. Jedna věc je sebrání peněz z ní nebo použití nalezené platební karty. Dotyčný, nejčastěji někdo velmi blízký, si v e-bankingu nejenže prohlédne výši obsažené částky, ale projde dopodrobna i veškeré účtenky, používané slevové karty, platební historii včetně míst a časů nákupů, zaplacených částek atd.

181 Analýza trestních spisů za roky 2015 a 2019 tento trend potvrzuje, typickým příkladem je neoprávněné jednání vnuka spravujícího e-banking svých prarodičů.

Mohlo by se zdát, že motivací neoprávněného použití cizího e-bankingu bude jednoznačně především vlastní obohacení se. Způsobené finanční škody se pohybovaly zhruba v rozmezí 100 Kč až 500 tis. Kč. Nezanedbatelná část respondentů vypovídajících ohledně svého přístupu na cizí e-banking bez výslovného souhlasu majitele účtu však jednala ze zvědavosti. Část respondentů přímo uvedla zvědavost jako svůj primární zájem (převažující nad získáním peněz). Téměř polovina respondentů (bez ohledu na to, zda na účet vstoupili oprávněně, či nikoliv) jednala po získání přístupu k cizímu e-bankingu ze zvědavosti (typicky zjištění finanční situace majitele účtu).

Hlavními aktéry na obou stranách byli partneři a/nebo osoby z úzkého rodinného kruhu. Respondenti se zneužitým e-bankingem podezírali společnosti podnikající prostřednictvím internetu, stávající partnery, neznámé hackery, bývalé partnery a osoby z úzkého rodinného kruhu (seřazeno dle četnosti). Respondenti, kteří používali v roce 2020* cizí e-banking neoprávněně (bez výslovného svolení), tak jednali zejména vůči svým stávajícím partnerům a osobám z úzkého rodinného kruhu (jiné případy byly spíše výjimečné).

Neoprávněný přístup umožnily nejčastěji přihlašovací údaje, které znal útočník přímo od majitele účtu. Poskytnuty byly převážně za účelem nějaké jednorázové aktivity někdy v minulosti, méně často pak z důvodu trvalé správy cizího e-bankingu. Za zmínku stojí respondenti mladší 29 let, kteří patřili mezi osoby častěji žádané o pomoc s e-bankingem. Také významně často získali přístup k cizímu e-bankingu díky použití zařízení, ve kterém byl účet zrovna otevřený (druhý nejčastější způsob umožňující přístup).

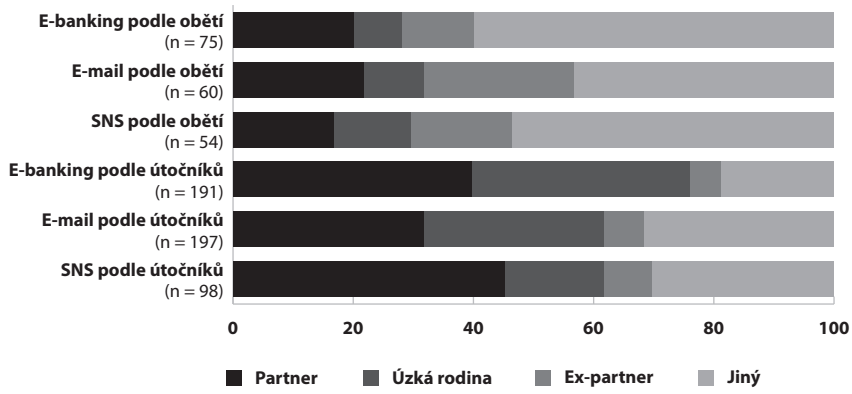
Přihlašovací údaje k e-bankingu bývají obecně sdíleny převážně s partnery a osobami z úzkého rodinného kruhu. Menší část partnerů, a naopak větší část osob z úzkého rodinného kruhu tyto údaje později využila k použití cizího e-bankingu bez výslovného svolení jeho majitele. Nejen tím se neoprávněné používání e-bankingu podobá zneužívání jiných online účtů, viz dále.

V.5 Podobnost neoprávněných přístupů k e-bankingu, e-mailovým schránkám a na sociální sítě

V dotazníkovém šetření jsme položili respondentům podobnou sérii otázek vztahujících se k neoprávněným přístupům na různé online účty. Ukázalo se, že výsledná data jsou si v několika ohledech poměrově velice podobná, a to především v podobně odlišných výpovědích obětí vs. pachatelů.[182]

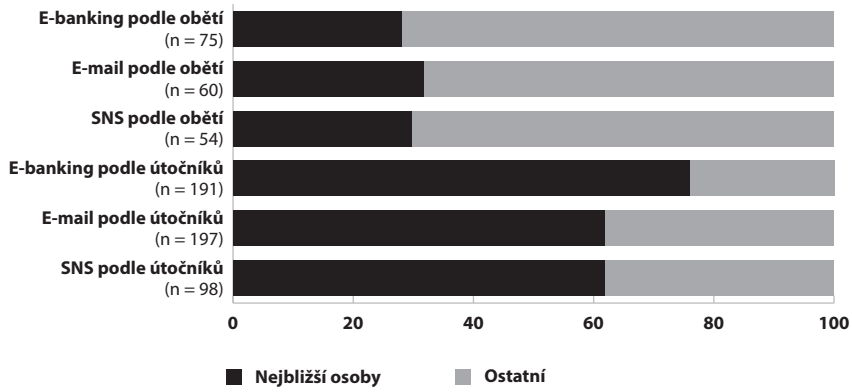
182 Údaje ohledně herních účtů zde neuvádíme jednak proto, že prvek soukromí je zde nižší než u ostatních jmenovaných, jednak vzhledem k výrazně nižší četnosti.

Graf 59: Aktéři neoprávněných přístupů k různým online účtům (%)[183]



Pachatelé oproti domněnkám obětí výrazně častěji neoprávněně vstupují na online účty svých stávajících partnerů a osob z úzkého rodinného kruhu. Naproti tomu znatelně méně často jde o bývalé partnery a další osoby (typicky neznámé hackery) (Graf 59). Podobnost v rozdílných odpovědích obětí oproti pachatelům vyvstane ještě výrazněji při rozlišení skupiny nejbližších osob vůbec (partneři a osoby z úzkého rodinného kruhu) vůči ostatním (bývalí partneři a ostatní osoby) (Graf 60).

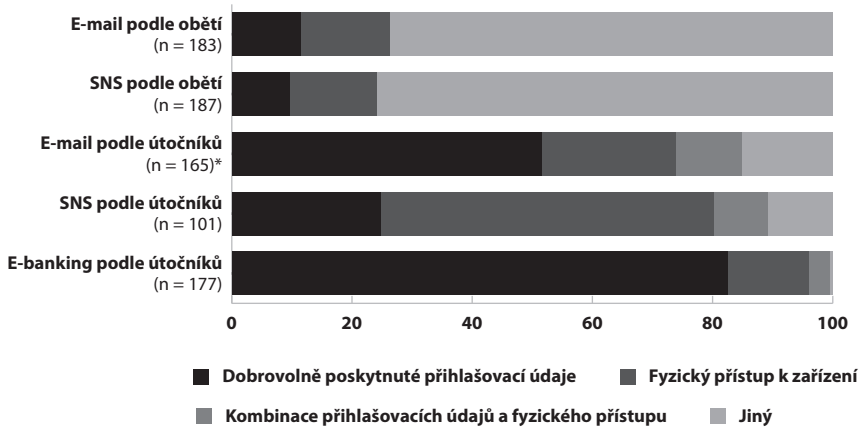
Graf 60: Skupiny aktérů neoprávněných přístupů k různým online účtům (%)



Tím ovšem podobnost nekončí. Podívejme se nyní na (domnělý) způsob získání přístupu k neoprávněně použitému účtu (Graf 61).

183 V otázkách ohledně neoprávněného použití e-mailových schránek odpovídali respondenti-oběti ohledně svého hlavního soukromého e-mailu, kdežto pachatelé ohledně přístupů na cizí e-maily bez dalšího rozlišení.

Graf 61: (Domnělé) získání přístupu k různým cizím online účtům (%)[184]



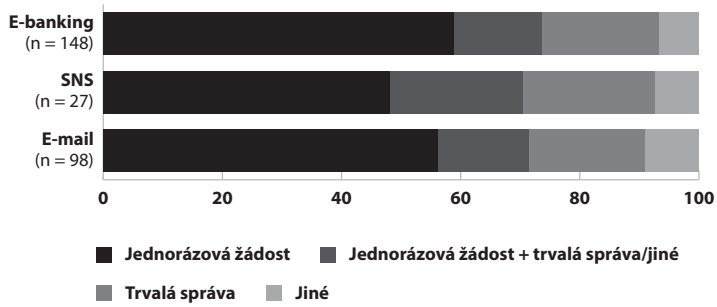
Data ohledně předpokládaného způsobu získání přístupu k e-bankingu podle majitelů napadených účtů bohužel nejsou pro srovnání k dispozici. Přesto považujeme za vhodné nastínit údaje relevantní pro oběti neoprávněného přístupu do e-mailové schránky a na sociální sítě, protože podrobnější analýza zneužívání těchto sledovaných tří online účtů ukazuje až na výjimky jejich podobnost.

Z hlediska získání přístupu dle výpovědí pachatelů se kupodivu vymykají sociální sítě s výrazně vyšším podílem zneužití přístupu umožněného konkrétním zařízením (Graf 61). Při opakování stejného průzkumu nyní by zřejmě toto prvenství připadlo již e-bankingu, vzhledem k současné povinné dvoufaktorové autentizaci podmiňující přístup k e-bankingu znalostí přihlašovacích údajů a potvrzením mobilním telefonem. Přesto je evidentní, že sdílení přihlašovacích údajů s dalšími osobami představuje z hlediska neoprávněného přístupu na online účty rizikový faktor, byť jsou tyto údaje sdíleny převážně s těmi nejbližšími.

Za pozornost stojí také důvod sdílení přihlašovacích údajů, jejichž znalost využili respondenti-útočníci k neoprávněnému užití cizího online účtu. Ve všech sledovaných online účtech převažuje zneužití přihlašovacích údajů, které pachateli sdělila oběť někdy v minulosti za účelem nějaké jednorázové aktivity (Graf 62).

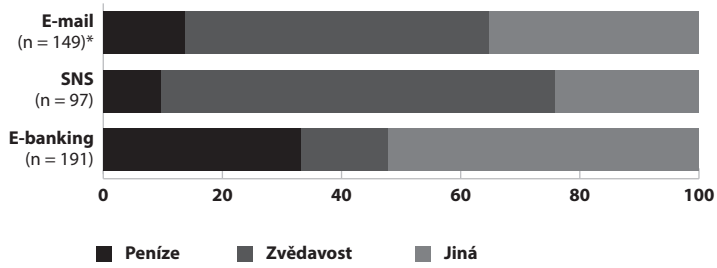
184 Respondenti měli v části věnované obětem možnost zvolit pouze jednu odpověď (tu, která nejvíce vystihovala daný incident), kdežto v self-reportové části mohli vybrat více odpovědí – proto není u obětí uvedena varianta „kombinace".

Graf 62: Důvod dobrovolného poskytnutí přihlašovacích údajů dle výpovědí útočníků, kteří je využili k nějaké aktivitě bez výslovného svolení majitele účtu (%)



Další podobný rys společný sledovaným online účtům představuje motivace, i když ne tak výrazný jako v předchozích případech. Shodu motivace neoprávněných přístupů k e-mailovým schránkám a na profily na sociálních sítích lze předpokládat, nicméně e-banking se oproti očekávání odlišuje méně – namísto zdaleka převažující finanční motivace vidíme jednání motivované zvědavostí v nezanedbatelném množství případů (Graf 63). Neoprávněné používání e-bankingu se proto zařazuje k ostatním případům narušování soukromí online a dotváří jeho obrázek.

Graf 63: Motivace podle útočníků (%)



Některé z otázek položených respondentům se zcela shodovaly (např. jakým způsobem získali k účtu přístup), některé byly položeny pouze u některého z online účtů (např. síla hesla k vlastnímu soukromému e-mailu nebo sebeprezentace na sociálních sítích). Ve svém souhrnu však naznačují odpovědi ohledně neoprávněných přístupů na různé online účty trend nikoliv výjimečného narušování soukromí, který poměrně znatelně umožňují sami uživatelé svým neopatrným chováním spočívajícím ve sdílení přihlašovacích údajů a/nebo zařízení s přihlášeným účtem (či zapamatovanými přihlašovacími údaji).

V.5.1 Závěr k podobnosti neoprávněných přístupů k různým online účtům

V oblasti neoprávněného používání cizích online účtů poskytlo odpovědi 199 obětí a 86 útočníků ohledně e-bankingu, 377 obětí a 100 útočníků ohledně sociálních sítí a 366 obětí a 169 útočníků ohledně e-mailových schránek. Na základě získaných poznatků sice

nelze statisticky vyhodnotit případný vztah mezi osobami neoprávněně vstupujícími na různé účty (může se navíc jednat o osoby spadající mezi „pachatele" více typů útoků) nebo oběťmi takových jednání, nicméně již pouhým pohledem je určitá podobnost ve struktuře pachatelů, obětí i jejich jednání patrná. Souhrn poznatků tak vytváří celkem jednoznačný obrázek narušování soukromí online, zejména ze strany nejbližších osob. A tak zatímco je ochrana soukromí mimo online prostředí vcelku samozřejmá, v online prostředí si ji řada osob neuvědomuje (např. partner sledující finanční situaci toho druhého bez jeho vědomí). Není to sice palčivé téma, jsou samozřejmě závažnější problémy online, avšak kyberprostor je již neodmyslitelnou součástí naší reality, aniž by měl za sebou dlouhou tradici morálního vývoje. Není třeba vymýšlet něco nového – stačí uvědomit si, že soukromí a jeho respekt nemají význam jen offline, ale také online.

V.6 Herní účty

Řada respondentů tráví část svého času hraním her, ať už na počítači či jiném zařízení. Nějaký svůj vlastní online herní účet použilo v roce 2020* 27 % respondentů (1 837 osob) v průměrném věku 44 let, 216 osob (3 % respondentů) si nevzpomnělo. Herní online účet používala významně často převážně zhruba třetina respondentů-mužů (35 %, průměrný věk 45 let) a naopak méně žen (18 %, průměrný věk 42 let). Věk hraje v používání online herních účtů signifikantní roli, jednak pozitivní korelací s mladšími věkovými skupinami do 44 let, jednak negativní korelací s osobami ve věku 45 let a více. Nelze říci, že by s používáním herních účtů přímo souvisela dosažená výše vzdělání, nicméně častěji o hraní vypovídali respondenti s pouze základním vzděláním či s maturitou (vyučení bez maturity ovšem naopak), kdežto významně často v roce 2020* nepoužívali herní online účet vysokoškoláci.

Třetina hráčů používala online herní účet spojený s hazardní hrou (32 %), o něco častěji pak s herní platformou, jako jsou nejčastější Steam, Xbox nebo PlayStation (39 %), dvě třetiny (62 %) pak účet spojený s konkrétní počítačovou hrou, případně jejich kombinace. Ženy významně často uváděly počítačové hry, kdežto muži hazardní hry a herní platformy. Počítačové hry a herní platformy pak uváděli především respondenti mladší 29 let, starší respondenti ve věku 45–59 let pak hazardní hry. K těm tíhli především respondenti s maturitou, podobně jako k herním platformám. Osoby se základním vzděláním se signifikantně často věnovaly počítačovým hrám, na rozdíl od vysokoškoláků.

Herní účty online mohou být stejně jako jakékoliv jiné online účty využity, případně zneužity i někým jiným než oprávněným uživatelem. Někdy v životě použilo cizí online herní účet bez výslovného svolení jeho majitele 79 respondentů (zejména osoby mladší 29 let, vysokoškoláci naopak nikoliv). Z toho 39 respondentů tak učinilo přinejmenším v roce 2020*, nadpoloviční většina z nich použila vícero cizích herních účtů (54 %, z toho dvě třetiny muži). Nejčastěji šlo o herní účet partnera (41 %) a/nebo někoho z úzkého rodinného kruhu (31 %), případně bývalého partnera (18 %). Za zmínku pak stojí již jen kamarád (13 %) či spolubydlící (10 %). Lze se proto domnívat, že k používání cizích herních účtů

dochází sice bez výslovného souhlasu jejich majitelů, ale sdílejí se poměrně běžně a spíše nepůjde o závažné jednání či zásah do soukromí.[185] Bez výslovného souhlasu majitele byly v roce 2020* používány především účty k počítačovým hrám (72 %).

V.6.1 Hazardní hry

V roce 2020* někdo zneužil účet k hazardní hře čtyř respondentů, a to dvou mužů ve věku okolo 30 let (30 a 33 let) a jednoho muže a jedné ženy ve věku okolo 60 let (60 a 59 let), z nich 1 byl vdovec a všichni ostatní rozvedení. Jeden z mladších mužů si nebyl jist, zda nedošlo ke zneužití jeho vlastního účtu v roce 2020* opakovaně, naopak výše zmíněná respondentka si byla opakovaným zneužitím jista. 6 respondentů se domnívalo, že ke zneužití jejich účtu v roce 2020* pravděpodobně došlo, nebyli si však jisti. Muži věděli, kdo jejich účet k hazardní hře (pravděpodobně) zneužil – šlo především o osoby z úzkého rodinného kruhu, o partnera ovšem nikoliv.

V důsledku zneužití přišli respondenti-hráči o do té doby dosažené bonusy, herní kredit a v jednom případě i o peníze (reálné, nikoliv herní), nemohli účet používat (tj. hrát online), potýkali se se změněnými přihlašovacími údaji. Incidenty řešili změnou přihlašovacích údajů a/nebo zrušením zneužitého účtu. Polovina se jich obrátila na policii, což představuje jednu z nejnižších pozorovaných úrovní latence.[186]

Jeden z těchto mladších mužů sám používal v roce 2020* cizí účty k hazardním i počítačovým hrám, patřící různým osobám. Druhý z mladších mužů pak cizí online herní účty sice používal, nebyl si však jist, zda tomu tak bylo v roce 2020*. Hráli, měnili přihlašovací údaje a nakupovali přes herní účet nějaký obsah, motivováni penězi, ale i zvědavostí.

V.6.2 Počítačové hry a herní platformy

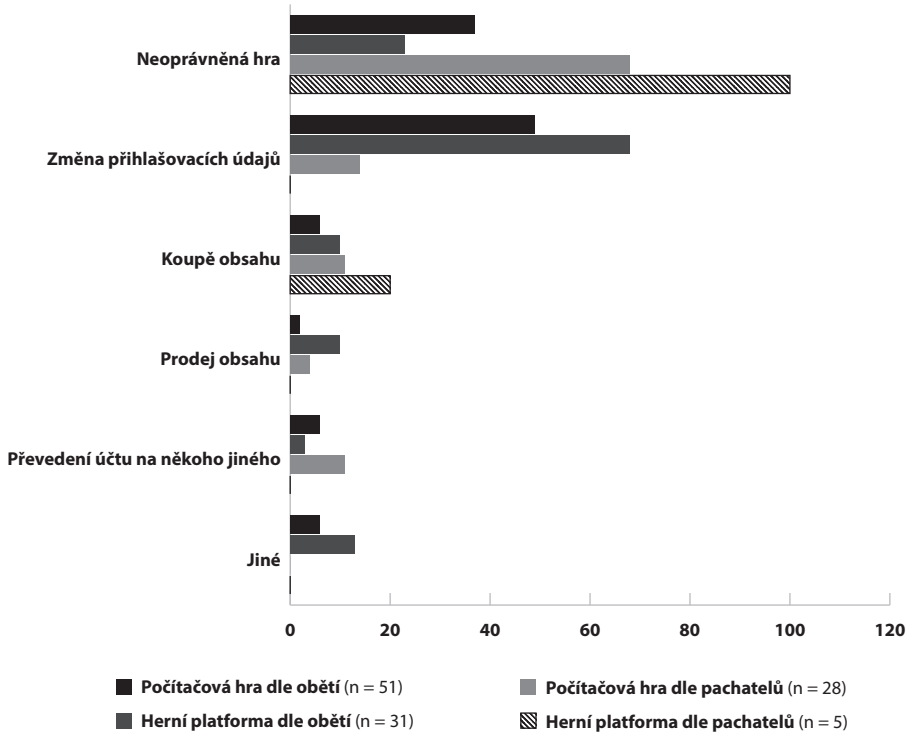
O něco více respondentů než u hazardních her se v roce 2020* potýkalo se zneužitím jejich online herního účtu k počítačové hře a/nebo na herní platformě vůbec. Údaje vztahující se k oběma těmto herním online účtům jsou velmi podobné. U počítačových her šlo o 36 respondentů a dalších 15, kteří se domnívali, že ke zneužití účtu pravděpodobně došlo (jisti si byli především osoby mladší 29 let), dohromady zhruba 5 % respondentů-hráčů. U dvou třetin z nich (67 %) šlo (pravděpodobně) o opakované zneužití herního účtu v roce 2020*, jisti si byli především muži. K (pravděpodobnému) zneužití herních platforem v roce 2020* došlo u 31 respondentů, z toho 26 si jich bylo zneužitím jisto (opět především osoby mladší 29 let), dohromady zhruba 4 %. U čtvrtiny z nich (26 %) se tak dělo v roce 2020* opakovaně. Hrající vysokoškoláci si byli významně často jisti, že ke zneužití jejich herního účtu nedošlo.

185 Nelze samozřejmě vyloučit ojedinělé závažné případy – např. vydírání v podobě vyzvídání přihlašovacích údajů pod pohrůžkou násilím, neoprávněné rozprodání herního majetku s významnou reálnou hodnotou, šikanózní zneužívání cizího účtu atp.

186 Pochopitelně s výhradou velmi nízkého počtu případů. 3 respondenti byli s policií spíše spokojeni, 2 naopak spíše nespokojeni.

Respondenti hovořili nejčastěji o změně přihlašovacích údajů neoprávněným uživatelem, časté bylo samozřejmě také neoprávněné hraní. Nikoliv ojedinělé pak bylo obchodování s obsahem, ať už jeho nákup či prodej, v méně případech pak prodej celého herního účtu (Graf 64). Jako způsobenou újmu respondenti označovali nejčastěji nemožnost hrát danou počítačovou hru či používat herní platformu, případně ve spojení se zablokováním herního účtu vůbec.[187] Řada jich zmínila pochopitelně také vliv na dosažený postup v důsledku hraní jiného uživatele, ať už v konkrétní počítačové hře či ve spojení s herní platformou (Graf 65).

Graf 64: Způsob zneužití herního účtu (%)[188]

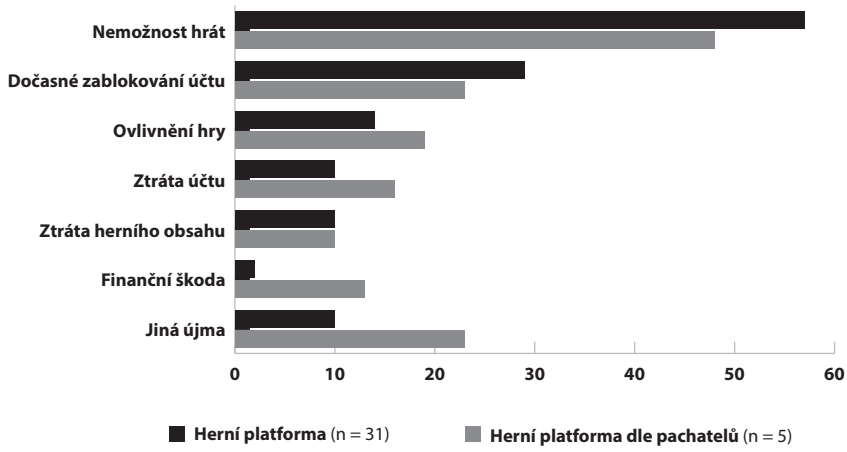


Respondenti, kteří použili v roce 2020* cizí herní účet nebo herní platformu bez výslovného svolení jeho majitele, převážně sami hráli. V některých případech ovšem i změnili přihlašovací údaje, čímž pravděpodobně přinejmenším dočasně znemožnili přístup oprávněného uživatele. Dva z nich převedli na sebe celý herní účet k počítačové hře vůbec, jiný respondent ho převedl na třetí osobu (Graf 65).

187 Nutno podotknout, že „neobvyklá" přihlášení se k hernímu účtu – např. z dosud nepoužívaného zařízení, z jiné země atp. – mohou vést k automatickému zablokování herního účtu s nutností změny přihlašovacích údajů z důvodu preventivního zabezpečení účtu a předejití jeho možného zneužití.

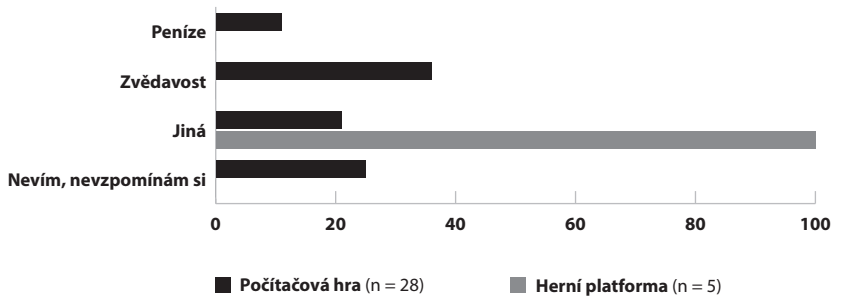
188 „Vliv na hru" znamená např. ovlivnění úrovně herní postavy, úpravu herního prostředí, změnu uložených pozic atp.

Graf 65: Forma způsobené újmy pohledem obětí (%)



Necelá polovina majitelů zneužitých herních účtů k počítačovým hrám věděla, kdo jejich účet neoprávněně použil (45 %, 23 osob), kdežto u herních platforem si byli jisti pouze 4 respondenti (13 %). Ke konkrétním aktérům viz jeden z následujících grafů (Graf 67).[189]

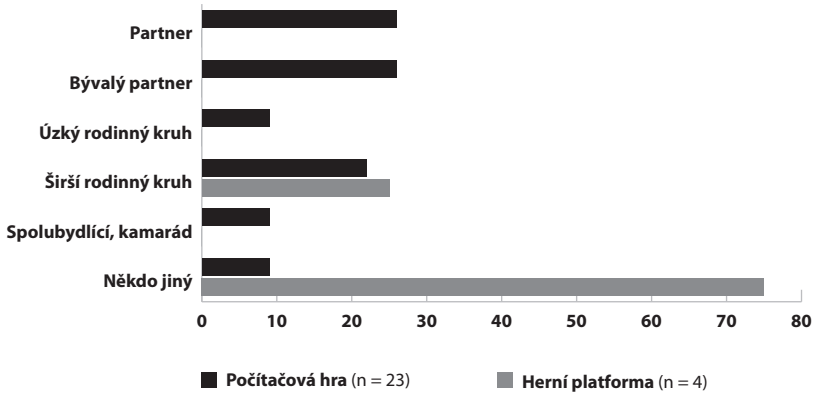
Graf 66: Motivace pachatelů (%)



Respondenti, kteří používali v roce 2020* cizí herní účty k počítačovým hrám bez výslovného svolení jejich majitelů, tak činili motivováni dílem zvědavostí, dílem penězi či jinak. Naproti tomu u herních platforem uvedli výlučně „jinou" motivaci (Graf 66). Při zohlednění ostatních odpovědí se lze domnívat, že cílem bylo převážně samotné hraní, tedy spíše volnočasová aktivita bez návaznosti na zvědavost či snad majetkový zájem (nad rámec ušetřených prostředků, které by jinak musel pachatel vynaložit na získání dané hry či herního času).

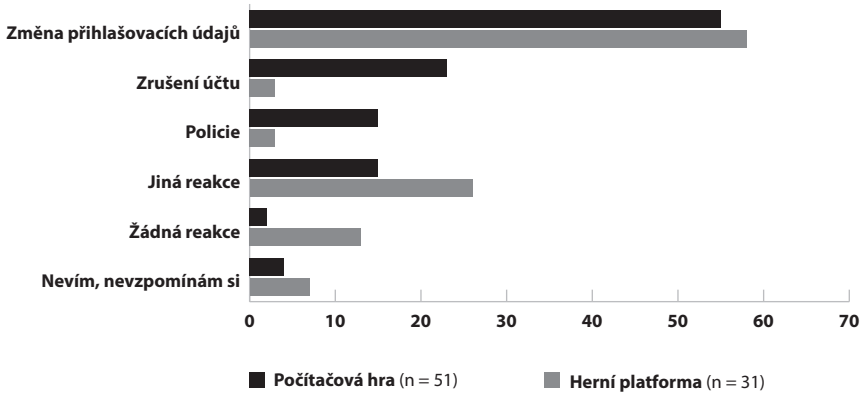
189 „Někdo jiný" v případě zneužití herní platformy zahrnovalo různé neznámé osoby bez nějakého sjednocujícího prvku.

Graf 67: Domnělí neoprávnění uživatelé herního účtu (%)



Nejčastější reakcí na zneužití herního účtu byla změna přihlašovacích údajů, u počítačových her tak činili významně často muži. Za zmínku stojí také zrušení daného účtu vůbec a oznámení policii (bez ohledu na pohlaví) (Graf 68). „Jiná reakce" zahrnovala převážně kontaktování zákaznické podpory dané hry či herní platformy. S policií byli v souvislosti s nahlášením zneužití herního online účtu k počítačové hře či herní platformě respondenti spíše spokojeni.

Graf 68: Reakce na zneužití herního účtu (%)



V.6.3 Závěr k herním účtům

I u herních účtů se ukázala disproporce mezi výpověďmi respondentů-obětí a respondentů-pachatelů.[190] Oběti jsou si vědomy zejména jednání zanechávajícího stopu (typicky změna přihlašovacích údajů). Naproti tomu pachatelé mnohem častěji hovořili výlučně o použití cizího účtu ke hraní her. Přístup u hazardních her může být odlišný, neboť samotné hraní bez dalšího může herní účet výrazně ovlivnit (např. změnit výši bonusů, zůstatek atp.), a tedy může zanechat patrnější stopy.[191]

Celkově lze říci, že používání cizích herních účtů je spojeno především s hraním samotným, kdy na jedné straně umožňuje pachatelům hru či herní platformu používat, na straně druhé v důsledku toho pak zároveň může znemožnit či omezit danou aktivitu oprávněného uživatele. Zejména tehdy, když je použití cizího účtu spojeno i se změnou přihlašovacích údajů neoprávněným uživatelem. Dochází i k neoprávněnému převádění účtů na jiné osoby, spíše však sporadicky, častější je (neoprávněná) koupě nějakého obsahu prostřednictvím herního účtu.

Z hlediska důvěry ve schopnost policie objasňovat zneužívání herních online účtů vůbec se odpovědi respondentů nijak významně neliší od jiných sledovaných oblastí, když 14 % všech respondentů věří, že se policii objasňování spíše daří (2 % daří, 12 % spíše daří), podle 42 % se jí to spíše nedaří (30 % spíše ne, 12 % nedaří) a 44 % nemá jednoznačný názor. Důvěru mají významně často osoby s pouze základním vzděláním či vyučené bez maturity, osoby mladší 29 let naopak. Respondenti starší 45 let signifikantně často nemají jednoznačný názor.[192]

V.7 Společný závěr pro online účty

Dotazníkové šetření ukázalo, že zneužívání online účtů není nijak výjimečné, ba naopak s ním má zkušenost značné množství uživatelů. Mezi hlavní aktéry na obou stranách patří kupodivu stávající partneři, případně osoby z úzkého rodinného kruhu. Není sice namístě taková jednání démonizovat, neboť v řadě případů nepůjde o nic závažného, nicméně byli to respondenti sami, kdo označil své jednání za neoprávněné.

K nejvýznamnějším zjištěním patří, že zkušenosti se zneužíváním e-mailových schránek se překvapivě hodně shodují se zneužíváním profilů na sociálních sítích (mimo falešné účty, které představují poněkud odlišné výsledky) a do jisté míry i se zneužíváním e-bankingu. Zdá se, že dochází k řadě neoprávněných přístupů, o kterých oprávnění uživatelé neví, motivovaných především zvědavostí. Pachatelé, převážně partneři, případně osoby z úzkého rodinného kruhu, získávají přístup typicky díky předchozí znalosti přihlašovacích údajů (ty jsou jim obvykle známy z dřívějška, kdy jim je sdělili sami majitelé účtů), často v kombinaci s fyzickým přístupem ke konkrétnímu zařízení oprávněného uživatele

190 Připomínáme, že respondenti jsou označováni jako „oběti" či „pachatelé" jen zjednodušeně, nejde bez dalšího o spojení s trestnou činností, viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

191 Jde ovšem pouze o domněnku, vzhledem k nízkému počtu respondentů odpovídajících v této části dotazníku.

192 Zcela pochopitelné zjištění s ohledem na to, že v tomto věku již významně často sami žádné herní účty nepoužívají.

sloužícímu pro potvrzení přístupu (typicky mobilní telefon). Nejčastější motivací neoprávněných přístupů bývá zvědavost (hraje sice nikoliv hlavní, ale přesto významnou roli kupodivu i u zneužívání e-bankingu).

Ačkoliv obvykle nejde o výrazné finanční škody, psychická újma spojená se zneužíváním online účtů (zejména v případě sociálních sítí) může být značná. O závažnosti kyberšikany, stalkingu, pomluv nebo odčerpávání finančních prostředků samozřejmě není pochyb. U většiny neoprávněných přístupů k takovému jednání naštěstí nedochází, nicméně už jen samotnou četnost neoprávněných přístupů a fakt, že k nim dochází ze strany nejbližších osob, považujeme za znepokojivou. Jde o zásah do soukromí, kterého si možná sami jednající aktéři nejsou vědomi jednoduše proto, že online prostředí je součástí společnosti pouhé roky, kdežto soukromí offline se vyvíjí od nepaměti.

VI.

Dotazník – jiné

VI.1 Obchodování online

VI.1.1 Nakupování – e-shopy

Nakupování online prostřednictvím e-shopů je již delší dobu uživateli internetu hojně využíváno. Zajímalo nás tedy, do jaké míry je služeb e-shopů využíváno našimi respondenty. Dotázali jsme se jich, zda v roce 2020* nakoupili nějaké zboží prostřednictvím e-shopu. Téměř 92 % respondentů (6 238 osob) na tuto otázku odpovědělo kladně, což potvrzuje předpoklad, že mezi uživateli internetu je nakupování online masivně rozšířeno. Nákup prostřednictvím e-shopu ve vymezeném období negovalo necelých 7 % respondentů (464 osob) a pouze necelá 2 % (109 osob) odpověděla, že neví či si nevzpomínají. Respondentů, kteří na tuto otázku odpověděli kladně, jsme se dále dotazovali, zda se v roce 2020* setkali s tím, že jim bylo při jejich online nákupech v e-shopech dodáno vadné zboží. Za vadné zboží zde bylo považováno zboží výrazně horší kvality, zboží v jiném než deklarovaném množství, dodání zcela jiného zboží bez předchozího informování e-shopem, jakož i nedodání zboží vůbec. Takovou zkušenost připustila necelá čtvrtina respondentů, což představuje 1 347 osob. Respondenti odpovídali na otázku „*bylo Vám v uplynulých 12 měsících dodáno vinou e-shopu vadné zboží? Jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží, a to bez předchozího informování e–shopem*“ (Tabulka 7).

Tabulka 7: Dodání vadného zboží vinou e-shopu

	Počet	%
Ano	1 347	21,6
Ne	4 657	74,7
Nevím, nevzpomínám si	234	3,8
Celkem	6 238	100

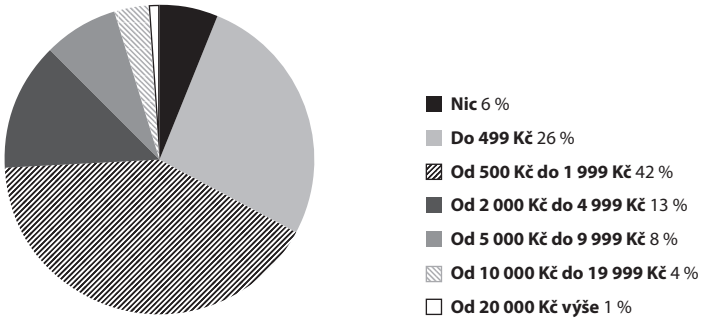
Z těch, kteří odpověděli kladně, dále třetina uvedla, že se tak v roce 2020* stalo vícekrát než jednou (Tabulka 8).

Tabulka 8: Opakovaná zkušenost s dodáním vadného zboží vinou e-shopu

	Počet	%
Ano	456	33,9
Ne	827	61,4
Nevím, nevzpomínám si	64	4,8
Celkem	1 347	100

Zajímalo nás též, kolik za vadné zboží z e-shopu respondenti zaplatili. Tři čtvrtiny respondentů, kteří se k této otázce vyjádřili (celkem 1 159 osob),[193] zaplatily za vadné zboží do 2 000 Kč. Více než dvě pětiny respondentů (482 osob, tj. 42 %) zaplatily částku od 500 Kč do 2 000 Kč. Cenovou strukturu ilustruje následující graf (Graf 69).

Graf 69: Cena vadného zboží z e-shopu (n = 1 159)



Dále jsme se respondentů dotazovali, zda se jim v případě dodání vadného zboží podařilo sjednat nápravu. A to ať již tím, že se jim podařilo získat žádané zboží, nebo získat zpět své peníze. Tohoto výsledku se podařilo dosáhnout přibližně dvěma třetinám z nich. Podrobněji jsou odpovědi na tuto otázku uvedeny níže (Tabulka 9).

Tabulka 9: Sjednání nápravy vadného zboží z e-shopu

	Počet	%
Ano, zcela	872	64,7
Pouze částečně	153	11,4
Ne	291	21,6
Nevím, nevzpomínám si	31	2,3
Celkem	1 347	100

Povzbudivým zjištěním bylo, že se více než třem čtvrtinám z těchto respondentů (76 %) podařilo dosáhnout úplné či alespoň částečné nápravy, přičemž úplné nápravy se pak podařilo dosáhnout přibližně dvěma třetinám.

Zajímali jsme se též o to, v čem zmíněná vada zboží spočívala. Ve více než polovině případů se jednalo o dodání zboží ve výrazně horší kvalitě. V přibližně pětině případů bylo dodáno zcela jiné zboží. Ve více než polovině případů se jednalo o dodání zboží ve

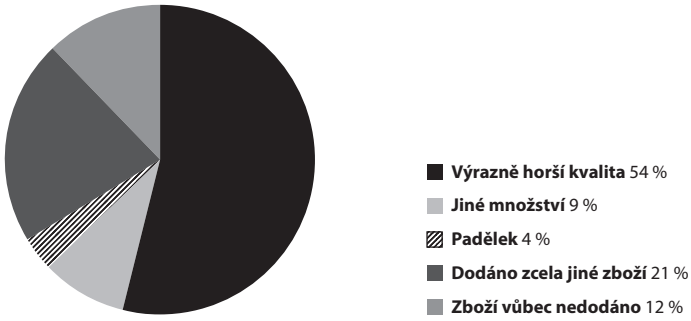
193 188 respondentů uvedlo, že již neví, kolik za vadné zboží z e-shopu zaplatilo.

výrazně horší kvalitě. V přibližně pětině případů bylo dodáno zcela jiné zboží. Naproti tomu nejméně bylo respondenty uváděno dodání padělku, kdy se tak stalo ve čtyřech procentech případů. Blíže viz (Tabulka 10 a Graf 70).[194]

Tabulka 10: Vady zboží z e-shopu

	Počet	%
Výrazně horší kvalita	776	57,6
Jiné množství	125	9,3
Padělek	52	3,9
Dodáno zcela jiné zboží	307	22,8
Zboží vůbec nedodáno	173	12,8
Celkem	1 433	100

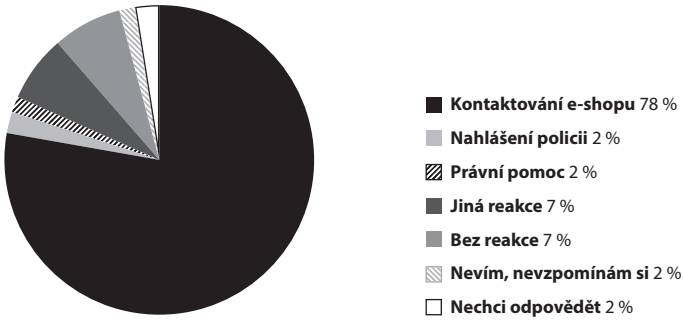
Graf 70: V čem spočívala vada zboží z e-shopu (n = 1 433)



Zjišťovali jsme také, jak respondenti vadu zboží konkrétně řešili (Graf 71). Nejčastěji uváděli, že se snažili získat požadované zboží nebo peníze zpět kontaktováním prodejce. Učinily tak více než tři čtvrtiny respondentů. Na policii se obrátila přibližně dvě procenta respondentů a právní pomoc vyhledala necelá dvě procenta respondentů. Sedm procent se rozhodlo situaci nijak neřešit. Čtyři procenta dotazovaných si již nevzpomněla, jak zmíněnou situaci řešili, nebo nechtěla odpovědět.

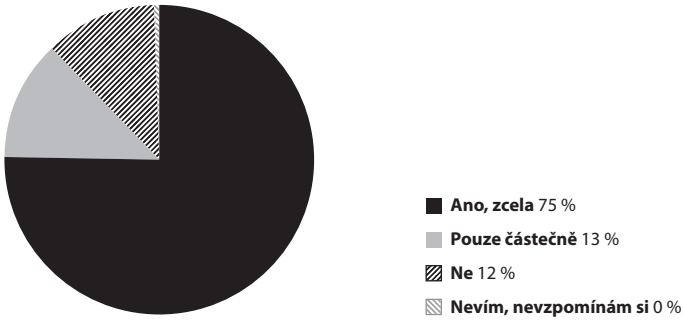
194 Respondenti mohli zvolit více odpovědí, pokud se vzájemně nevylučovaly.

Graf 71: Reakce na dodání vadného zboží z e-shopu (n = 1 399)



Těch, kteří se při řešení zmíněné situace obrátili na prodejce, jsme se následně dotazovali, zda e-shop vyhověl jejich požadavkům (Graf 72).

Graf 72: Vyhovění požadavkům e-shopem (n = 1 090)



Celým třem čtvrtinám respondentů vyhověl e-shop zcela a přibližně jedné osmině alespoň částečně.

VI.1.2 Nakupování – inzertní portály

Uživatelé internetu však nenakupují online pouze v e-shopech. Využívají při svých nákupech také služeb inzertních portálů, byť se tak neděje v tak hojné míře jako při nakupování v e-shopech. Dotázali jsme se jich proto, zda v roce 2020* nakoupili nějaké zboží prostřednictvím inzertního portálu. Kladně na tuto otázku odpověděly dvě pětiny respondentů (41 %, tj. 2 775 osob). Zamítavě na tuto otázku odpověděla více než polovina respondentů (54 %, tj. 3 673 osob).

Respondentů, kteří na tuto otázku odpověděli kladně, jsme se dále dotazovali, zda se v roce 2020* setkali s tím, že jim bylo při jejich online nákupech prostřednictvím inzertních portálů dodáno vadné zboží. Za vadné zboží bylo (obdobně jako při nakupování

v e-shopech) považováno zboží výrazně horší kvality, zboží v jiném než deklarovaném množství, dodání zcela jiného zboží bez předchozího informování prodejcem, jakož i nedodání zboží vůbec (Tabulka 11).

Tabulka 11: Dodání vadného zboží vinou prodávajícího na inzertním portálu

	Počet	%
Ano	490	17,7
Ne	2 201	79,3
Nevím, nevzpomínám si	84	3
Celkem	2 775	100

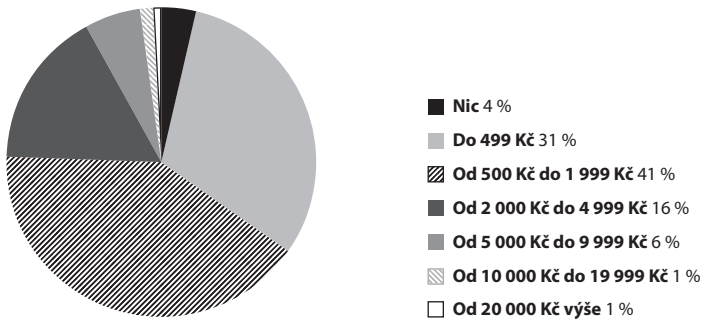
Přibližně třetina respondentů, které bylo dodáno vadné zboží, připustila, že se tak stalo v roce 2020* opakovaně (Tabulka 12).

Tabulka 12: Opakované dodání vadného zboží vinou prodávajícího na inzertním portálu

	Počet	%
Ano	175	35,7
Ne	289	59
Nevím, nevzpomínám si	26	5,3
Celkem	490	100

Co se týče ceny, kterou respondenti za vadné zboží z inzertních portálů zaplatili, obdobně jako u nákupů v e-shopech, tři čtvrtiny respondentů (75,7 %, tj. 305 osob), zaplatily za vadné zboží do 2 000 Kč a dvě pětiny zákazníků (164 osob, tj. 40,7 %) zaplatily částku od 500 Kč do 2 000 Kč. Cenovou strukturu ilustruje následující graf (Graf 73).

Graf 73: Cena vadného zboží z inzertního portálu (n = 1 159)



Dále jsme se klientů inzertních portálů dotazovali, zda se jim v případě dodání vadného zboží podařilo sjednat nápravu. A to ať již tím, že se jim podařilo získat žádané zboží, nebo získat zpět své peníze. Pozitivním zjištěním je, že se tohoto výsledku podařilo zcela či alespoň částečně dosáhnout přibližně třem pětinám z nich (61 %, tj. 298 osob). Podrobněji jsou odpovědi na tuto otázku uvedeny níže (Tabulka 13).

Tabulka 13: Sjednání nápravy vadného zboží z inzertního portálu

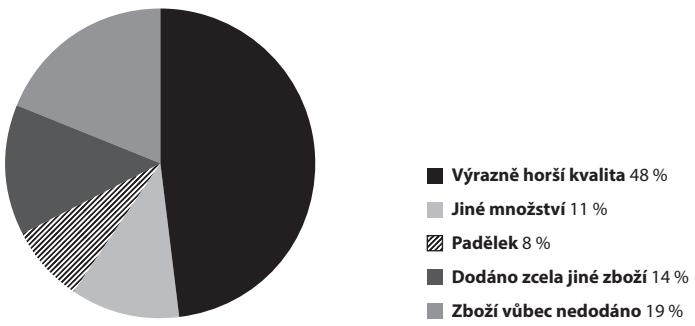
	Počet	%
Ano, zcela	198	40,4
Pouze částečně	100	20,4
Ne	180	36,7
Nevím, nevzpomínám si	12	2,4
Celkem	490	100

Vada zboží spočívala nejčastěji, tj. téměř v polovině případů v dodání zboží výrazně horší kvality. V přibližně pětině případů nebylo zboží dodáno vůbec. Naproti tomu nejméně bylo respondenty uváděno dodání padělku, kdy se tak stalo v osmi procentech případů (Tabulka 14 a Graf 74).[195]

Tabulka 14: V čem spočívala vada zboží z inzertního portálu

	Počet	%
Výrazně horší kvalita	256	48,3
Jiné množství	60	11,3
Padělek	43	8,1
Dodáno zcela jiné zboží	72	13,6
Zboží vůbec nedodáno	99	18,7
Celkem	530	100

Graf 74: V čem spočívala vada zboží z inzertního portálu



195 Respondenti mohli zvolit více odpovědí, pokud se vzájemně nevylučovaly.

Nejčastějším způsobem, jakým bylo řešeno dodání vadného zboží, bylo kontaktování prodávajícího. Učinilo tak 73 % (381 osob) nakupujících. Necelá desetina kupujících (9 %, tj. 46 osob) řešila situaci kontaktováním Policie ČR a přibližně stejně velká skupina kupujících (45 osob, tj. 9 %) se rozhodla situaci nijak neřešit. Právní pomoc vyhledalo pouze devět kupujících (tj. 2 %). Respondenti, kteří zvolili jiný způsob řešení (21 osob, tj. 4 %), byli dotazováni, jak konkrétně postupovali. Celkem se ke zvolenému způsobu řešení vyjádřilo 19 z nich. Nejčastěji (ve 12 případech) se obraceli přímo na inzertní portál: např. *„kontaktoval jsem podporu inzertního portálu" nebo „portál mi sám vrátil peníze po uplynutí ochranné lhůty."*

Tři z respondentů se obrátili na svou banku, respektive na provozovatele internetového platebního systému: např. *„u banky jsem chtěla zrušit platbu" nebo „pojištění přes Pay-Pal."*

Někteří z respondentů (ve třech případech) zvolili řešení nastalé situace fyzickým kontaktováním prodejce: např. „*dojel jsem si za tímto člověkem…Pracuji u MP*" nebo „*našel jsem podvodníka a rozbil mu tlamu…*"

Také ti z respondentů, kteří dodání vadného zboží nijak neřešili, dostali příležitost upřesnit, proč k dané situaci zvolili takový přístup. Této příležitosti využilo celkem 40 respondentů. Nejčastěji (ve 14 případech) zastávali názor, že by šlo pouze o zbytečně vynaložený čas a úsilí: např. *„nemělo to cenu. Bylo to z ciziny"* nebo *„neměl jsem na to čas a výsledek byl pochybný."*

*H*ojně (v 11 případech) bylo mezi odpověďmi zastoupeno též stanovisko, že i přes zjištěnou vadu jsou ochotni takové zboží akceptovat: např. *„pouze vizuální poškození, nemá vliv na funkčnost"* nebo *„opotřebení bylo horší, než uváděl inzerující, ale stále se koupě vyplatila. Proto jsem to neřešil."*

Část respondentů (9 osob) neřešilo dodání vadného zboží proto, že se jednalo o zanedbatelnou částku: např. *„nemělo to cenu vzhledem k hodnotě zboží."*

*Z*bývající odpovědi (6 osob) k této problematice poukazovaly na nemožnost reklamace či jiné faktory, které je od řešení odradily.

VI.1.3 Prodej

Stranou našeho zájmu samozřejmě nezůstaly ani zkušenosti uživatelů internetu s pozicí prodávajícího prostřednictvím e-shopu či inzertního portálu. Na otázku, zda v roce 2020* prodali nějaké zboží přes e-shop, odpovědělo kladně pouze 439 respondentů (tj. 6 %). O poznání více respondentů připustilo dle očekávání zkušenost s prodejem prostřednictvím inzertního portálu. Takovou zkušenost připustila téměř třetina dotazovaných (28 %, 1 926 osob). Navazující otázka byla směřována na to, zda při prodeji dodali kupujícímu vadné zboží, aniž by ho o tom informovali předem. Více než tři čtvrtiny prodávajících prostřednictvím e-shopu (76 %, tj. 335 osob) a téměř všichni prodávající prostřednictvím inzertních portálů (93 %, tj. 1 786 osob) takové jednání popírají. Blíže viz (Tabulka 15).

Tabulka 15: Dodání vadného zboží při prodeji prostřednictvím e-shopu či inzertního portálu bez předchozího informování kupujícího v roce 2020*

	E-shop		Inzertní portál	
	Počet	%	Počet	%
Ano, jednou	55	12,5	59	3,1
Ano, několikrát	23	5,2	34	1,8
Ne	335	76,3	1 786	92,7
Nevím, nevzpomínám si	21	4,8	41	2,1
Nechci odpovědět	5	1,1	6	0,3
Celkem	439	100	1 926	100

K tomu, v čem tkvěla vada zboží, se vyjádřilo pouze 73 prodejců prostřednictvím e-shopů a 72 prodávajících na inzertních portálech. Vada zboží nejčastěji spočívala v jeho výrazně horší kvalitě, v jiném množství či v dodání zcela jiného zboží. Odpovědi respondentů k této problematice jsou ilustrovány následovně (Tabulka 16).

Tabulka 16: Vady prodávaného zboží

	E-shop		Inzertní portál	
	Počet	%	Počet	%
Výrazně horší kvalita	40	54,8	41	56,9
Jiné množství	20	27,4	13	18,1
Padělek	2	2,7	6	8,3
Dodáno zcela jiné zboží	7	9,6	8	11,1
Zboží vůbec nedodáno	4	5,5	4	5,6
Celkem	73	100	72	100

Důvod prodeje vadného zboží uvedlo pouze 68 prodejců z obou skupin. Dle jejich tvrzení nejčastěji došlo k prodeji vadného zboží omylem (přibližně ve dvou třetinách odpovědí) a přibližně čtvrtina uvedla, že vadné zboží dodali kvůli výdělku.

VI.1.4 Kazuistika

Nástrahy, s nimiž se kupující či prodávající mohou setkat při obchodování v online prostředí, jsou pro lepší představu ilustrovány následujícími případy, převzatými z analýzy trestních spisů za rok 2019.[196]

196 Blíže k analyzovaným spisům viz kapitola Metodologie.

VI.1.4.1 Nepoctivý prodejce

Pětadvacetiletý, již šestkrát trestaný J. P., odcizil své náhodné známé mobilní telefon, v němž měla nainstalovánu aplikaci e-bankingu a uloženy přihlašovací údaje. Počátkem dubna 2017 si na aukčním portálu Aukro.cz zaregistroval uživatelský účet na jméno poškozené a aktivoval ho platbou z e-bankingu. V průběhu května 2017 nabídl prostřednictvím aukčního portálu k prodeji dva mobilní telefony. Zájemci poukázali kupní cenu včetně poštovného v celkové výši 5 180 Kč na účet vedený na jméno A. M., s nímž se pachatel seznámil ve výkonu trestu. Zaplacené zboží však pachatel nikdy kupujícím nedodal a na výzvy o vrácení peněz nereagoval. Škodu kupujícím uhradila společnost Aukro, s. r. o. v rámci finančního odškodnění z programu ochrany kupujících. Obdobným způsobem si J. P. počínal i v dalších případech, a společnosti Aukro tak způsobil škodu v celkové výši 14 930 Kč. Městský soud v Brně ho shledal vinným z trestných činů podvodu (dle § 209 odst. 1 a 2 TZ), neoprávněného přístupu k počítačovému systému a nosiči informací [dle § 230 odst. 2 písm. a) a odst. 3 písm. a) TZ] a neoprávněného opatření, padělání a pozměnění platebního prostředku (dle § 234 odst. 3 TZ), za což jej odsoudil k souhrnnému trestu odnětí svobody v trvání čtyři roky.

VI.1.4.2 Skladník

Třiatřicetiletý J. K. nastoupil jako agenturní pracovník na pozici skladníka ve společnosti Zásilkovna. Z titulu své funkce obdržel přístupové heslo do systému, kterým se zákazníkům zasílalo oznámení, že je jejich objednávka připravena k vyzvednutí a kód pro její vyzvednutí. Po čase se od kolegů dozvěděl, že lze v systému snadno změnit e-mailové adresy zákazníků. Počátkem února 2017 se v hostelu, kde byl tehdy ubytován, přes místní wi-fi přihlásil do systému Zásilkovny a u pěti zákazníků změnil e-mailové adresy na adresy, které si předem založil. Poté, co obdržel kódy pro vyzvednutí již zaplacených zásilek, objel příslušné výdejny a zboží vyzvedl. Konkrétně se jednalo o dvě počítačové hry, hodinky, mixážní pult a robotický vysavač v celkové hodnotě 12 100 Kč. Poté v systému změnil kontaktní e-mailové adresy zpět na původní adresy zákazníků s cílem zakrýt své jednání. Získané zboží rozprodal pod cenou po hospodách a obdržené peníze prohrál v automatech. Poté, co se dozvěděl od známých, že je hledán policií, se sám dostavil k podání vysvětlení. Jak se však ukázalo, nešlo o jedinou jeho nelegální aktivitu. Agentura, pro kterou J. K. pracoval, na něj podala trestní oznámení, že v období od prosince 2016 do ledna 2017 objednal postupně na fiktivní jméno celkem devět notebooků a jeden iPhone s dodáním na pobočku společnosti Zásilkovna. V rámci výkonu práce skladníka u této společnosti zaměnil původní štítky s cenovkou za štítky z jiných zásilek nižší hodnoty. Následně po zaplacení takto snížené kupní ceny zboží převzal, čímž způsobil společnosti Zásilkovna škodu v celkové výši 214 657 Kč. Obvodní soud pro Prahu 9 shledal pana J. K. vinným z trestného činu podvodu (dle § 209 TZ) a neoprávněného přístupu k počítačovému systému a nosiči informací [dle § 230 odst. 2 písm. b), odst. 3 písm. a) TZ], za což mu uložil podmíněný trest odnětí svobody v trvání jednoho roku se zkušební dobou v trvání tří let. Zároveň mu byla uložena povinnost nahradit poškozeným škodu, kterou jim způsobil.

VI.2 Porušování autorských práv

Stahování audiovizuálních děl či softwaru je v online prostředí poměrně častým jevem.[197] Proto jsme se zajímali o to, zda respondenti v roce 2020* stáhli z internetu takový obsah, jako jsou hudba, filmy nebo software.[198] Téměř dvě třetiny respondentů (60,9 %, tj. 4 146 osob) připustily, že tak v uplynulých 12 měsících učinily. Blíže je tato problematika ilustrována následovně (Tabulka 17).

Tabulka 17: Stahování audiovizuálních děl nebo softwaru v roce 2020*

	Počet	%
Ano	4 146	60,9
Ne	2 186	32,1
Nevím, nevzpomínám si	386	5,7
Nechci odpovědět	93	1,4
Celkem	6 811	100

U těch respondentů, kteří odpověděli kladně, jsme se následně zajímali o to, zda je při stahování omezovaly obavy, že jednají protiprávně.[199] Z odpovědí je zřejmé, že více než čtyři pětiny respondentů (87 %, tj. 3 604 osob) odpovídajících na tuto otázku žádné takové obavy nepociťovaly (Tabulka 18).

Tabulka 18: Obavy z protiprávnosti stahování

	Počet	%
Ano	448	10,8
Ne	3 604	86,9
Nechci odpovědět	94	2,3
Celkem	4 146	100

Následující otázka byla zaměřena na to, zda při stahování respondenti pociťovali obavy z nechtěného stažení škodlivého obsahu, typicky ve formě malwaru.[200] Téměř tři pětiny

197 Vzhledem k již tak značné rozsáhlosti dotazníku jsme se v souvislosti s porušováním autorských práv dotazovali pouze na software, hudbu a film.

198 Otázka byla položena v tomto znění: *„stáhl/a jste v uplynulých 12 měsících z internetu obsah jako je hudba, filmy nebo software? Nemusí jít o stahování všeho vyjmenovaného, stačí např. stahování hudby, aniž byste stahoval/a i filmy a software. Software je např. i počítačová hra."*

199 Otázka byla položena v tomto znění: *„omezovaly Vás při stahování obavy, že jednáte protiprávně? Bez ohledu na to, zda bylo stahování ve skutečnosti protiprávní či nikoliv."* Naše dotazy zde a dále směřovaly záměrně právě na obavy respondentů z protiprávnosti, a nikoliv na jejich posouzení, zda jednali protiprávně.

200 Otázka byla položena v tomto znění: *„omezovaly Vás při stahování obavy, že nechtěně stáhnete i škodlivý obsah (např. virus)?"*

respondentů, kteří v roce 2020* stáhli z internetu audiovizuální díla či software (58 %, tj. 2 387 osob), takové obavy nepociťovaly. Z toho bylo 1 432 mužů (tj. 60 %) a 955 žen (tj. 40 %) (Tabulka 19).

Tabulka 19: Obavy z nechtěného stažení škodlivého obsahu

	Počet	%
Ano	1 725	41,6
Ne	2 387	57,6
Nechci odpovědět	34	0,8
Celkem	4 146	100

Na otázku, zda v roce 2020* stáhli z internetu nelegálně nějakou hudbu či film, odpověděla kladně téměř čtvrtina respondentů (24 %, tj. 996 osob), přičemž více než čtyři pětiny z nich tak v roce 2020* učinily dokonce několikrát. Naproti tomu na otázku týkající se nelegálního stažení softwaru takové počínání připustila pouze necelá osmina respondentů stahujících z internetu. Podrobněji jsou jejich odpovědi ilustrovány následovně (Tabulka 20).[201]

Tabulka 20: Nelegální stahování zvukových či audiovizuálních děl nebo softwaru[202]

	Hudba či film		Software	
	Počet	%	Počet	%
Ano, jednou	180	4,3	156	3,8
Ano, několikrát	816	19,7	331	8,0
Nejsem si jistý, zda bylo stažení nelegální	902	21,8	461	11,1
Ne	1 803	43,5	2 736	66,0
Nevím, nevzpomínám si	293	7,1	316	7,6
Nechci odpovědět	152	3,7	146	3,5
Celkem	4 146	100	4 146	100

Jedno stažení hudby či filmu připustilo přibližně stejně mužů i žen (91 mužů, 89 žen). K opakovanému stahování zmíněného obsahu se však již hlásilo výrazně více mužů (63 %, tj. 513 mužů oproti 303 ženám). V případech nelegálního stahování softwaru lze konstatovat, že se jedná jednoznačně o doménu mužů. K jednomu stažení softwaru se přihlásily dvě třetiny (65 %, tj. 102 mužů oproti 54 ženám) a k opakovanému dokonce tři čtvrtiny mužů (74 %, tj. 245 mužů oproti 86 ženám). Muži se též oproti ženám výrazně více odmítali

201 Na rozdíl od předchozích otázek zde již (opět záměrně) vycházíme z vlastního dojmu respondentů ohledně případné protiprávnosti jejich jednání.

202 Otázka byla položena v tomto znění: *„stáhl/a jste v uplynulých 12 měsících z internetu hudbu nebo filmy či software nelegálně?“*

k problematice nelegálního stahování vyjadřovat. Z respondentů, kteří zvolili variantu „*nechci odpovědět*" byl podíl mužů více než dvoutřetinový (71 % u stahování hudby či filmu, tj. 108 mužů oproti 44 ženám, a 72 % u stahování softwaru, tj. 105 mužů oproti 41 ženám).

Respondenti byli dotazováni též na to, zda zpřístupnili v roce 2020* na internetu obsah audiovizuální povahy nebo software, přičemž se mohlo jednat jak o legální, tak také nelegální zpřístupnění[203] (Tabulka 21).

Tabulka 21: Zpřístupnění hudby, filmů nebo softwaru

	Počet	%
Ano	502	7,4
Ne	5 733	84,2
Nevím, nevzpomínám si	490	7,2
Nechci odpovědět	86	1,3
Celkem	6 811	100

Celkem takové zpřístupnění uvedlo 502 respondentů, z čehož se ze tří pětin jednalo o respondenty mužského pohlaví (61 %, tj. 304 mužů oproti 198 ženám). S přihlédnutím k věkové struktuře lze konstatovat, že zpřístupnění zmíněného obsahu připustily přibližně dvě pětiny respondentů mladších 35 let (211 osob, tj. 42 %), přičemž nejvíce byla zastoupena věková skupina od 25 do 35 let (117 osob, tj. 23 %).

Dále byly otázky zaměřeny již jen na nelegální zpřístupnění hudby, filmů nebo softwaru. Z těch, kteří uvedli, že zpřístupnili v roce 2020* na internetu obsah audiovizuální povahy nebo software, se k nelegálnímu zpřístupnění hudby či filmů přihlásilo 117 respondentů a k nelegálnímu zpřístupnění softwaru 40 respondentů. Podrobněji je rozložení odpovědí ke zmíněné problematice ilustrováno následovně (Tabulka 22).

Tabulka 22: Nelegální zpřístupnění hudby, filmů nebo softwaru

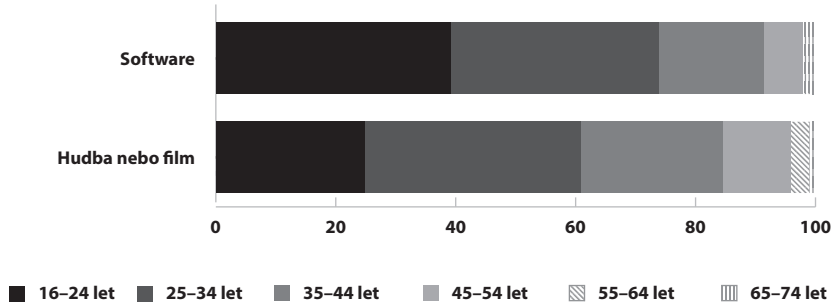
	Hudba či film		Software	
	Počet	%	Počet	%
Ano	59	11,8	24	4,8
Ano, několikrát	38	7,6	22	4,4
Nejsem si jistý, zda bylo zpřístupnění nelegální	78	15,5	29	5,8
Ne	304	60,6	405	80,7
Nevím, nevzpomínám si	20	4,0	20	4,0
Nechci odpovědět	3	0,6	2	0,4
Celkem	502	100	502	100

203 Otázka byla položena v tomto znění: *„zpřístupnil/a jste v uplynulých 12 měsících na internetu obsah jako je hudba, filmy nebo software? Nemusí jít o vše vyjmenované a jde o legální i nelegální zpřístupnění."*

Skupina respondentů, kteří alespoň jednou nelegálně zpřístupnili obsah audiovizuální povahy, sestávala ze dvou třetin z mužů (67 %, tj. 65 ku 35 ženám), a mezi těmi, kteří tak učinili dokonce několikrát, tvořili muži dokonce téměř tři čtvrtiny (71 %, tj. 27 mužů ku 11 ženám). Také mezi respondenty, kteří alespoň jednou zpřístupnili nelegálně software, šlo ve dvou třetinách o muže (74 %, tj. 34 mužů). U těch respondentů, kteří odpověděli, že software nelegálně zpřístupnili dokonce několikrát, byl podíl mužů dokonce více než čtyřpětinový (86 %).

Lze konstatovat, že nelegální zpřístupnění je doménou mladších respondentů. Zpřístupnění audiovizuálních děl tvořili respondenti ve věku do 35 let celé tři pětiny (61 %, tj. 59 osob), přičemž nejsilněji byla zastoupena věková skupina 25–34 let (36 %, tj. 35 osob). U nelegálního zpřístupnění softwaru se pak osoby ve věku do 35 let podílely téměř třemi čtvrtinami (74 %, tj. 34 osob), nicméně oproti zpřístupňování audiovizuálních děl zde byla nejpočetněji zastoupena nejmladší věková skupina osob do 24 let (39 %, tj. 18 osob). Zastoupení jednotlivých věkových skupin mezi respondenty, kteří nelegálně zpřístupnili hudbu, film nebo software, je přehledně ilustrováno následovně (Graf 75).

Graf 75: Věková struktura respondentů, kteří nelegálně zpřístupnili hudbu, film nebo software (%)



Stranou zájmu nezůstaly ani pohnutky, které respondenty vedly k nelegálnímu zpřístupnění audiovizuálního obsahu či softwaru (Tabulka 23).

Tabulka 23: Motivace nelegálního zpřístupnění hudby, filmů nebo softwaru

	Hudba/film		Software	
	Počet	%	Počet	%
Protože to dokážu	43	18,4	32	30,2
Protože legální přístup je příliš drahý	74	31,6	40	37,7
Protože produkující společnosti mají nepřiměřeně velké zisky	41	17,5	17	16
Protože na internetu by mělo být vše zdarma	45	19,2	10	9,4
Z jiného důvodu	31	13,2	7	6,6
Celkem	234	100	106	100

Ti z respondentů, kteří zpřístupnili audiovizuální obsah či software z jiného důvodu, měli možnost ozřejmit, proč tak učinili. U audiovizuálního obsahu nejčastěji, v osmi případech, uváděli, že k zpřístupnění došlo v rámci využívání sítě BitTorrent:[204] např. *„stahoval jsem… přes torrenty, které současně se stahováním obsah sdílí a umožní stahovat dalším lidem“* nebo *„Torrenty – je potřeba sdílet, ne jen stahovat.“*

*D*alším důvodem, uváděným více respondenty, bylo zpřístupnění obsahu, který je jinak obtížně či zcela nedostupný: např. *„kolikrát je velmi složité se k nějakým filmům/písničkám dostat i legální cestou“* nebo *„protože jde o vzácné kousky, které jinak na internetu nejsou, nebo jsou těžce dohledatelné.“*

*N*ěkolik respondentů zmínilo též ekonomický faktor: např. *„produkující společnosti by si měli uvědomit, že ne každý si to může dovolit.“*

*Z*ajímavě odůvodnila nelegální zpřístupnění audiovizuálního obsahu 58letá respondentka: *„Protože mi to vnuk ukázal.“*

*T*aké zpřístupnění softwaru bylo respondenty zmiňováno v souvislosti se sítí BitTorrent (Jirovský, 2007, s. 73) a zpřístupněním nedostupného obsahu: např. *„zpřístupnil ve stylu seedování přes torrenty. Sám o sobě ne“ nebo „archivace – legální kopie již není dostupná.“*

VI.3 Zaměstnanci jako rizikový faktor

Odborná veřejnost již delší dobu poukazuje na skutečnost, že nejslabším článkem zabezpečení informačního systému je obvykle člověk (Smejkal, 2015). Organizace či firmy však mnohdy tuto skutečnost opomíjejí. Vlastní zaměstnanci tak mohou představovat, ať již z nedbalosti či dokonce úmyslně, bezpečnostní hrozbu pro firemní sítě a data.

V rámci provedeného výzkumného šetření byli též předmětem zájmu uživatelé v pozici zaměstnanců, jakož i jejich bezpečnostní návyky a chování při používání ICT. Konkrétně se jednalo o problematiku přístupu zaměstnanců k neveřejným informačním systémům.

Respondentům z řad zaměstnanců tak byla mimo jiné položena otázka, zda ve své pracovní pozici využívají informační systém, který není veřejně přístupný.

K této otázce se vyjádřilo celkem 3 974 respondentů (tj. 58 % všech respondentů), přičemž přibližně 44 % (1 740 osob) z nich odpovědělo, že takový informační systém v zaměstnání používají (Tabulka 24).

204 BitTorrent umožňuje tzv. peer-to-peer (P2P) distribuci souborů, kdy klient zároveň stahuje a dále sdílí.

Tabulka 24: Používání neveřejného informačního systému zaměstnanci

	Počet	%
Ano	1 740	43,8
Ne	2 110	53,1
Nechci odpovědět	124	3,1
Celkem	3 974	100,0

Těchto respondentů jsme se následně dotázali, zda v roce 2020* tento informační systém využili nad rámec jejich oprávnění. Kladně na tuto otázku odpověděla necelá čtyři procenta (66 osob) (Tabulka 25).

Tabulka 25: Využití neveřejného informačního systému zaměstnanci nad rámec oprávnění

	Počet	%
Ano	66	3,8
Ne	1 621	93,2
Nevím, nevzpomínám si	43	2,5
Nechci odpovědět	10	0,6
Celkem	1 740	100

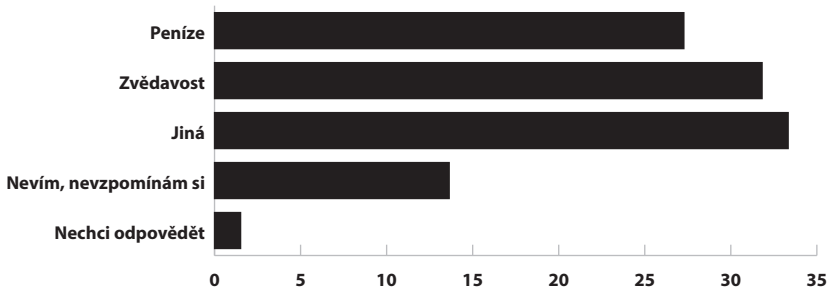
Kladně odpovědělo pouze 66 dotazovaných (tedy necelá 4 %), přičemž tři čtvrtiny z nich uvedly, že tak v roce 2020* činili opakovaně (42 respondentů). Zajímala nás samozřejmě také jejich motivace k takovému jednání (Tabulka 26 a Graf 76).[205]

Tabulka 26: Motivace k využití neveřejného informačního systému zaměstnanci nad rámec jejich oprávnění

	Počet	%
Peníze	18	27,3
Zvědavost	21	31,8
Jiná	22	33,3
Nevím, nevzpomínám si	9	13,6
Nechci odpovědět	1	1,5
Celkem	71	107,6

205 Respondenti mohli zvolit více odpovědí, pokud se vzájemně nevylučovaly.

Graf 76: Motivace k využití neveřejného informačního systému zaměstnanci nad rámec jejich oprávnění (%, n = 71)



Odhlédneme-li od odpovědí „*nevím, nevzpomínám si*“ a „*nechci odpovědět,*“ zbývají tři přibližně stejně velké skupiny odpovědí, kdy respondenti uváděli jako motivaci pro zmíněné jednání peníze (v 18 případech), zvědavost (v 21 případech) a jinou motivaci (ve 22 případech). U varianty „*jiná*“ uváděli dotazovaní nejčastěji potřebu získat informace a rychlost jejich získání v porovnání s oficiální cestou, např. „*potřeba práce s informacemi, ke kterým jsem zrovna neměl oprávnění a odmítl jsem se zdržovat vyřizováním žádost o přístup v IT,*“ „*vyřešit problém, který bych jinak musel řešit složitou oficiální cestou*“ nebo „*nemusím otravovat IT (trvá jim to).*“

Několik respondentů též připustilo, že je k využití informačního systému nad rámec jejich oprávnění motivovala snaha pomoci jiné osobě, např. „*prosba kamaráda*“ nebo „*nikomu to neuškodilo (max zanedbatelná ztráta zisku zaměstnavatele, známému to dost pomohlo).*“

Dále jsme se dotazovali, zda někdy v roce 2020* k přístupu do neveřejného informačního systému použili cizího přístupu bez vědomí oprávněné osoby. Kladně na tuto otázku odpovědělo pouze 62 osob, přičemž necelé tři čtvrtiny z nich (44 osob, tj. 71 %) tak učinily vícekrát než jednou (Tabulka 27).

Tabulka 27: Využití cizího přístupu k neveřejnému informačnímu systému zaměstnancem

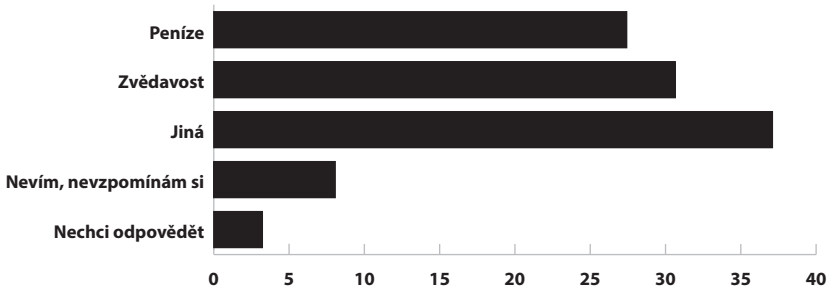
	Počet	%
Ano	62	1,6
Ne	3 776	95
Nevím, nevzpomínám si	97	2,4
Nechci odpovědět	39	1
Celkem	3 974	100

Co se týče jejich motivace k takovému počínání, tak i zde byly přístupy motivované penězi a zvědavostí zastoupeny obdobně. Podrobněji je motivace těchto zaměstnanců ilustrována následovně (Tabulka 28 a Graf 77).[206]

Tabulka 28: Motivace k využití cizího přístupu k neveřejnému informačnímu systému zaměstnancem

	Počet	%
Peníze	17	27,4
Zvědavost	19	30,6
Jiná	23	37,1
Nevím, nevzpomínám si	5	8,1
Nechci odpovědět	2	3,2
Celkem	66	106,5

Graf 77: Motivace k využití cizího přístupu k neveřejnému informačnímu systému zaměstnancem (%)



Těmi, kteří zvolili variantu „*jiná, uveďte jaká…*," byla nejčastěji zmiňována potřeba přístupu k výkonu práce i přesto, že respondent sám vlastními přístupovými údaji do systému nedisponuje, např. „*pro práci jsem potřeboval dočasně (náhrada za nepřítomnosti) práva, která nemám*" nebo „*pracovní, neměla jsem ještě svoje přihlašovací údaje.*"

Část respondentů uvedla, že využívání cizích přihlašovacích údajů je na jejich pracovišti běžnou, či přinejmenším tolerovanou praxí, např. „*je to více méně v zájmu všech, nikomu to nevadí, usnadňuje a zrychluje to práci*" nebo „*jde o povoleny postup.*"

VI.3.1 Kazuistika

VI.3.1.1 Kolegiální výpomoc

Přístup do neveřejného systému s použitím cizích přihlašovacích údajů lze pro lepší představu ilustrovat následujícími konkrétními případy.

206 Respondenti mohli zvolit více odpovědí, pokud se vzájemně nevylučovaly.

Paní Martině Ch. (39) nebylo po ztrátě zaměstnání bývalým zaměstnavatelem vyplaceno odstupné a v následujících třech měsících neměla nárok na podporu v nezaměstnanosti, v důsledku čehož se nezaviněně dostala do tíživé finanční situace. Přibližně po roce nastoupila na Úřad práce jako referentka dávek státní sociální podpory, kde měla příležitost se seznámit s postupem při jejich schvalování a vyplácení. Po čase byla přeřazena na pozici metodika a ověřovatele dávek státní sociální podpory. V té době jí však již hrozily exekuce ve výši kolem jednoho milionu korun. Takové závazky nebyla schopna ze svých příjmů hradit, a proto ji napadlo, jak tuto situaci řešit. Z titulu své aktuální pracovní pozice však již nemohla zadávat nové žádosti o dávky. Pod záminkou kolegiální výpomoci si tak od kolegyň půjčovala jejich identifikační karty. Kolegyně jí též sdělovaly PIN, který je nezbytný pro přihlášení do systému. Přestože to bylo přísně zakázáno, v praxi byl na tomto pracovišti Úřadu práce takový postup celkem běžný. Paní Martina si z databáze vybírala osoby z okruhu svých známých, kteří si v minulosti o nějakou dávku či příspěvek žádali. Tak získala všechny potřebné údaje. Poté, co jejich jménem podala žádost, ji z titulu své funkce metodičky v systému odsouhlasila a povolila její výplatu na jí zadané bankovní účty. Celkem takto od června 2014 do září 2018 získala na neoprávněně vyplacených dávkách státní sociální podpory ve formě příspěvku na bydlení finanční prostředky ve výši 1 686 454 Kč. Poté, co tato skutečnost vyšla v rámci interní kontroly najevo, byla věc nahlášena Policii ČR. Posléze byla úřednice obviněna z podvodu dle ustanovení § 209 odst. 1, odst. 4 písm. d) TZ a neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 odst. 1, odst. 2 písm. a), písm. d) a odst. 4 písm. b) a d) TZ. Okresní soud ji za tyto trestné činy odsoudil k úhrnnému trestu odnětí svobody v trvání tří let, podmíněně odloženému na zkušební dobu v trvání čtyř let. Dále jí byla uložena povinnost nahradit způsobenou škodu.

V souvislosti s tímto případem je vhodné si připomenout výrok jednoho z respondentů k problematice přihlášení se do neveřejného systému cizími přihlašovacími údaji: „*je to více méně v zájmu všech, nikomu to nevadí, usnadňuje a zrychluje to práci.*“

Ve světle prezentovaného případu lze konstatovat, že taková praxe možná práci zrychluje, ale rozhodně není v zájmu všech.

VI.3.1.2 Neoprávněná lustrace

Nadpraporčík Š. P. pracoval jako inspektor Krajského ředitelství policie Moravskoslezského kraje na Obvodním oddělení Policie ČR. Postupně se s celou rodinou dostali do značné finanční nouze a hrozila jim exekuce. Napadlo ho situaci řešit poskytováním informací o probíhajících trestních řízeních za úplatu. V několika případech poskytoval za drobné finanční částky, poskytnutí bezúročné půjčky či příslib sjednání úvěru informace z policejního informačního systému ETŘ (Evidence trestního řízení), k němuž měl jako policista zřízen přístup. Jednalo se především o informace, zda nebylo trestní řízení zastaveno, jaké svědky již policie v dané věci vyslechla atp. Poté, co se jeho jednání provalilo, šetřila věc Generální inspekce bezpečnostních sborů (GIBS) a následně na něj podal státní zástupce obžalobu pro spáchání trestného činu zneužití pravomoci úřední osoby (§ 329 TZ), přijetí úplatku (§ 331 TZ) a neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ). Okresní soud odsoudil policistu Š. P. k úhrnnému trestu odnětí

svobody v trvání tří let nepodmíněně, pro jehož výkon byl zařazen do věznice s dozorem. Dále mu byl uložen trest zákazu činnosti spočívající v zákazu služebního a pracovního poměru u bezpečnostních sborů po dobu pěti let.

Uvedený případ o „kolegiální výpomoci" vhodně ilustruje, že zaměstnanec může být bezpečnostní hrozbou jak zcela záměrně a promyšleně, tak také vlivem nedbalosti či neznalosti.

Možnost ohrožení informačního systému zaměstnanci z nedbalosti či neznalosti lze předcházet především jejich průběžným školením v oblasti kybernetické bezpečnosti. Poněkud nákladnější cestou je testování odolnosti zaměstnanců proti kybernetickým hrozbám, ať již jde o simulované phishingové kampaně, penetrační testování nebo techniky sociálního inženýrství. V poslední době se do popředí dostává pokročilá správa přístupů v rámci informačního systému.[207] Taková technologie pak může do značné míry snížit možnost úmyslného ohrožení či poškození systému ze strany zaměstnanců.[208]

VI.3.2 Baiting

Jak již bylo zmíněno v souvislosti s bezpečností firemních dat, nejslabším článkem bývá zaměstnanec.[209] Jedním ze způsobů, kterým může potenciálně škodlivý software proniknout do počítačového systému, je tzv. baiting, spočívající v nastražení vhodného datového nosiče[210] s příslušným malwarem na vhodné místo, kde má být nalezeno.

Proto byla součástí provedeného výzkumného šetření série otázek věnovaná právě této problematice. Nejprve jsme se dotazovali, zda již někdy cizí flashdisk či paměťovou kartu nalezli. Kladně se vyjádřila necelá pětina respondentů (1 248 osob, tj. 18 % vzorku). Tři čtvrtiny dotázaných odpověděly zamítavě (5 103 osob, tj. 75 % vzorku) a zbývající respondenti odpovídali, že neví nebo si nevzpomínají (460 osob, tj. 7 % vzorku).

Těm, kteří nález zmíněných datových nosičů připustili, byla následně položena otázka, zda je použili. Přibližně dvě pětiny z nich (496 osob, tj. 40 %) odpověděly, že tak učinily. Jednalo se celkem o 355 mužů (72 %) a 141 žen (28 %). Více než polovina použití nalezených nosičů negovala. Pouze 41 osob (3 %) odpovědělo, že neví, nebo si nevzpomínají.

Zajímalo nás též to, zda respondenti, kteří nalezený cizí paměťový nosič použili, tak učinili bez prvotní kontroly ochranným softwarem (např. antivirem). Téměř polovina dotazovaných (245 osob, tj. 49 %) se k této otázce vyjádřila zamítavě, přičemž takové jednání negovalo 187 mužů (76 %) a 58 žen (24 %). Kladně odpověděly dvě pětiny respondentů (207 osob, tj. 42 %) a 44 osob odpovědělo, že neví nebo si již nevzpomínají (9 % dotázaných).

207 Jedná se o tzv. zero trust model, kdy je i po prvotním přihlášení stále prověřováno, zda se uživatel či zařízení připojuje oprávněně.

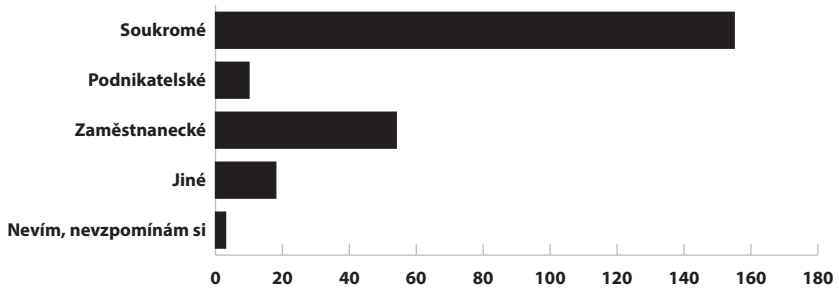
208 Blíže viz např. World Economic Forum. (2022). The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment. https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf.

209 Blíže viz např. Computerworld. (2020). Potvrzeno. Nejslabším článkem kyberbezpečnosti je člověk. https://www.computerworld.cz/clanky/potvrzeno-nejslabsim-clankem-kyberbezpecnosti-je-clovek/.

210 Obvykle se jedná o flashdisk či paměťovou kartu.

Navazující otázka byla zaměřena na to, v jakém zařízení byl nalezený paměťový nosič použit bez kontroly. Zda se tak stalo na některém ze zařízení soukromých, zaměstnaneckých, podnikatelských či jiných. Z odpovědí je zřejmé, že se tak nejčastěji dělo na soukromých zařízeních (ve 155 případech). Zaměstnanecká zařízení byla ohrožena v 54 případech a podnikatelská jen v deseti případech. Blíže je rozložení odpovědí na tuto otázku ilustrováno grafem (Graf 78).

Graf 78: V jakém zařízení byl použit nalezený paměťový nosič bez předchozí kontroly



VII.

Dotazník – souhrnné

V předchozích kapitolách jsme se podrobně věnovali dílčím deliktům, ať už z pohledu viktimizace či páchání. Jak se ukázalo, obě tyto kategorie nemají příliš ostrou a jednoznačnou hranici. Do dotazování tedy prostupovalo mnoho proměnných, díky kterým se mohlo ukázat, že se jednalo o nezávadné chování online nebo naopak nelegální činnost. Nyní představíme indexy online pachatelů a obětí, které jsme dotazníkem byli schopni identifikovat. Na základě chí-kvadrát statistiky pak popíšeme jejich sociodemografická specifika. Následně tyto dvě kategorie respondentů porovnáme a zaměříme se na možný překryv viktimizace a páchání. Online viktimizaci budeme dále zkoumat z pohledu dělení na virtuální násilí a majetkový zájem. Následovat bude kapitola o reakcích na incidenty a v závěru této části se budeme věnovat latenci této trestné činnosti včetně důvěry ve schopnost policie kyberkriminalitu řešit.

VII.1 Pachatelé[211]

Největší podíl pachatelů tvoří respondenti, kteří za poslední rok nelegálně stáhli hudbu nebo film. Obecně se ukazuje, že delikty spojené s porušováním autorských práv jsou poměrně častou aktivitou uživatelů internetu.[212] Celkově 15 % respondentů někdy nelegálně stáhlo hudbu nebo film a 7 % software, přičemž většina tak činí opakovaně. Zpřístupňování tohoto obsahu již tak běžné není a pohybuje se kolem jednoho procenta. Celkově se 16 % dotazovaných dopustilo nějakého porušení autorského práva, kdy všechny proměnné navzájem korelují. Nejvíce však mezi lidmi, kteří obsah stahují nebo naopak nahrávají.

Ostatní delikty byly zastoupeny v poměrně malé či úplně zanedbatelné míře. Za zmínku ještě stojí použití e-bankingu (23 %), či e-mailu bez výslovného souhlasu majitele (3 %), nebo účtu na sociálních sítích (2 %).[213] Ke zneužití cizí identity či online herního účtu bez svolení majitele došlo již minimálně.

Nezanedbatelné množství respondentů se přiznalo i k využití informačního systému nad rámec oprávnění nebo přes účet někoho jiného (obojí 1 %). Tato skupina respondentů spolu taktéž silně koreluje a celkem tvoří 2 % dotazovaných.

K podvodům jak sofistikovanějším v podobě ransomware či phishingu, tak méně sofistikovaným v rámci online obchodování se přiznal velmi malý podíl respondentů. Nejmenší zastoupení však mělo skrytí identity za účelem nelegální činnosti.

Celkově se tedy 21 % respondentů přiznalo k některému z výše zmíněných deliktů. Je však nutné připomenout, že většinu z nich tvoří lidé, kteří se dopustili nějakého porušení autorského práva.

211 Podrobnější informace k pachatelům budou publikovány jako samostatný článek.

212 Blíže k tomu viz kapitola Porušování autorských práv.

213 Viz kapitolyE-banking E-banking, E-mail a Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily.

Tabulka 29: Složení indexu páchání za poslední rok (n = 6 811)

	Celkem		Jednou		Několikrát	
	n	%	n	%	n	%
Nelegální stažení hudby/filmu	996	14,6	180	2,6	816	12,0
Nelegální stažení softwaru	487	7,2	156	2,3	331	4,9
Nelegální zpřístupnění hudby/filmu	97	1,4	59	0,9	38	0,6
Nelegální zpřístupnění softwaru	24	0,7	24	0,4	22	0,3
Použití e-bankingu bez výslovného svolení jeho majitele	191	2,8	166[214]	2,4	25[215]	0,4
Použití e-mailu bez výslovného svolení jeho majitele	169	2,5	142[216]	2,1	27[217]	0,4
Použití profilu na SNS bez výslovného svolení jeho majitele	100	1,5				
Použití falešného profilu na SNS zneužívajícího cizí identitu	25	0,4				
Použití online herního účtu bez svolení jeho majitele	39	0,6				
Využití cizího přístupu do informačního systému	62	0,9				
Využití informačního systému nad rámec vlastního oprávnění	66	1,0				
Ransomware[218]	37	0,5				
Phishing[219]	28	0,4				
Dodání vadného zboží přes e-shop kvůli výdělku	19	0,3				
Dodání vadného zboží přes inzertní portál kvůli výdělku	16	0,2				
Skrytí identity za účelem nelegální činnosti online	17	0,2				

Takto určené pachatele jsme podrobili chí-kvadrát testu sociodemografických ukazatelů. Je předpokládatelné, že značnou roli bude hrát ochota přiznat se k dílčím deliktům. Nicméně z analýzy našich dat vyplývá, že kyberkriminality se dopouštějí především mladší respondenti do 35 let. Nízký věk se odráží i na tom, že se jedná o svobodné jedince, případně ty, co žijí v nesezdaném partnerství, se základním vzděláním. Na druhou stranu se mezi pachateli objevuje i výrazně více vysokoškoláků. Lze předpokládat, že některé delikty vyžadují odbornější znalost užívání informačních technologií, nebo se vážou na pracovní pozice, které jsou spojeny s vysokoškolským vzděláním. Tento paradox je pak vidět i v případě testování sociálního statusu, kdy se jedná především o studenty, nebo naopak zaměstnance, kteří mají na starosti další podřízené.

214 Jednorázové použití e-bankingu bez výslovného svolení majitele.

215 Opakované použití e-bankingu bez výslovného svolení majitele.

216 Jednorázové použití e-mailu bez výslovného svolení majitele.

217 Opakované použití e-mailu bez výslovného svolení majitele.

218 Navazující otázky: *„zablokoval/a jste někdy v životě něčí zařízení a požadoval/a za jejich zpřístupnění výkupné?"* ➜ *„Došlo k tomu v uplynulých 12 měsících?"*

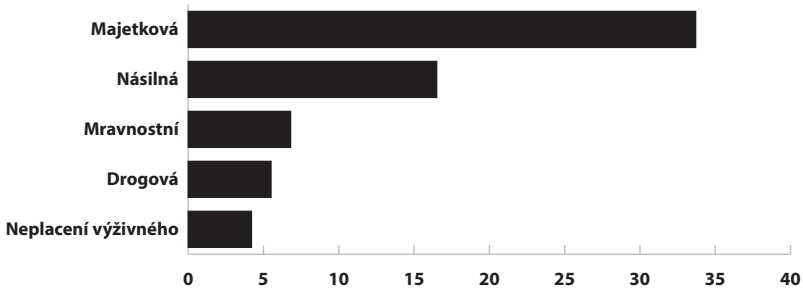
219 Navazující otázky: *„poslal/a jste někdy v životě někomu falešný nevyžádaný e-mail? Zajímá nás vydávání se za někoho jiného a požadování poslání peněz nebo sdělení osobních údajů."* ➜ *„Došlo k tomu v uplynulých 12 měsících?"*

Pokud se jednalo o zaměstnané pachatele, tak především v IT oboru. To se projevuje například v tom, že většina pachatelů ví, co je to darkweb či darknet, spíše než ostatní někdy v životě použili Tor, byli na školení bezpečného užívání IT technologií a svá zařízení si spíše zabezpečují. Na druhou stranu jsou více než ostatní respondenti ochotni nechat někoho svá zařízení používat nebo například použili cizí paměťovou kartu či flashdisk.

VII.1.1 Pachatelé další trestné činnosti vs. kyberkriminalita

Respondentů jsme se taktéž ptali, zda proti nim bylo zahájeno trestní stíhání nehledě na to, zda se jednalo o online či offline činnost, na což kladně odpovědělo 5 % (n = 309). Z toho dvě pětiny byly z některého skutku obviněny a dalších 16 % nechtělo na možné obvinění odpovědět. Dotazovaní, kteří dokázali určit, o jaký typ skutku šlo, ve třetině uvedli, že trestní stíhání proti nim bylo zahájeno za majetkovou činnost a dalších 17 % za násilnou. Mravnostní delikty a ty, co byly spojené s drogami, již byly uváděny méně. Respondenti dále mohli i konkrétně zvolit možnost neplacení výživného, což se týkalo 4 % dotazovaných (Graf 79).

Graf 79: Typ trestné činnosti, za niž bylo proti respondentovi zahájeno trestní stíhání, (%, n = 309)



Jedná se především o muže ve věkové kategorii 45–54 let s nižším vzděláním bez maturity, kteří se živí nějakým soukromým podnikáním. Pocházejí především ze severozápadní části republiky (tedy z Karlovarského, Ústeckého či Libereckého kraje), nehledě na velikost obce.

Sice se jedná o slabé tendence (míry asociací jsou velmi nízké), ale charakteristiky relativně odpovídají zjištěním ze self-reportové části aktuálního reprezentativního viktimologického výzkumu (Roubalová et al. 2023). Zde byli zkoumáni respondenti, kteří byli dotazováni, zda v průběhu života porušili zákon, což uvedla necelá pětina respondentů. Celkově pak 12 % dotazovaných uvedlo, že pro porušení zákona byli řešeni policií. Náš výzkum tedy na tento řetězec pachatelů navazuje.

Pokud ale charakteristiky (ať už z našeho nebo ze zmíněného viktimologického výzkumu) srovnáme s jedinci, kteří se doznali k nějakému deliktu spáchanému online, pak zjistíme, že jde o velmi specifickou skupinu. Sice je větší poměr trestně stíhaných mezi námi identifikovanými kyberpachateli než ve zbytku populace, ale jedná se o poměr 7 % ku 4 %. Vztah je tedy opět velmi slabý.

VII.1.2 Závěr k pachatelům vůbec

Naše data tedy ukázala, že pachatelé online trestné činnosti jsou oproti té offline výrazně specifičtí, a to především v koncentraci mladších jedinců. Vzhledem k tomu, že se ale většina deliktů týká online pirátství, tak to není až tak překvapivé zjištění. Kriminologové ve vztahu k takovému porušování autorských práv, ale i obecně k online kriminalitě (Bossler, 2021; Brewer & Miller, 2020) obvykle využívají teorie z 60. let Sykese a Matzy (1957) o technikách neutralizace, která navazuje na tradici teorií sociálního učení chicagské školy zaměřené na delikvenci mládeže, nebo naopak na zločiny tzv. bílých límečků.

To v podstatě odpovídá nám zjištěným pachatelům. Ve zkratce a s velkou nadsázkou by se dalo uvažovat nad tím, že se jedná buď o studenty, kteří nemají dostatek prostředků, aby si stáhli hudbu nebo film. Mohou nad tím uvažovat tak, že hudební a filmové produkce mají beztak nehorázné obraty (jejich chování tedy nikomu neubližuje), a dělají to i jejich vrstevníci, tak se k tomu ani nestydí přiznat. Nebo jde o mladé již pracující jedince, kteří využívají svých znalostí online prostředí k nelegální činnosti, případně přístupu do informačního systému, který zneužijí nad rámec svých oprávnění.

VII.2 Oběti

V této kapitole se naopak zaměříme na specifika obětí kyberkriminality.[220] Nejprve představíme různé formy viktimizace, které jsme dotazníkem sledovali: podvody při online nákupu, zneužití e-bankingu a dalších účtů od e-mailu přes sociální sítě až po herní prostředí, phishing, ransomware a další.

Ze sledovaných forem jsme vytvořili index viktimizace, který jsme dále podrobili hlubší analýze, přičemž cílem bylo porozumět, kdo jsou tyto oběti, jaké jsou jejich charakteristiky a jaké faktory mohou přispívat k jejich viktimizaci. Hledáme souvislosti mezi oběťmi kyberkriminality a různými sociodemografickými faktory, chováním online a mírou zabezpečení. Zjišťujeme například, zda jsou některé skupiny obyvatelstva náchylnější k viktimizaci a jaký vliv má zkušenost s technologiemi na riziko viktimizace.

VII.2.1 Sledované typy online viktimizace

Jak už bylo řečeno, v dotazníkovém šetření jsme se zabývali širokou škálu online viktimizace v roce 2020*. Vzhledem k tomu, že respondentům nemuselo být vždy zřejmé, zda se stali, či nestali obětí dané nelegální aktivity, nebo to ani nelze z odpovědí jednoznačně určit, tak jsme u některých typů viktimizace rozlišovali mezi jistou a nejistou viktimizací. Chronologický přehled všech typů viktimizace dle skladby dotazníku je prezentován prostřednictvím tabulky (Tabulka 30).

220 V roce 2023 končil závěrečnou publikací také jeden z výzkumných úkolů IKSP věnovaný obětem trestné činnosti vůbec (Roubalová et al. 2023).

Nejprve jsme se věnovali podvodům při online nakupování.[221] Zde jsme se dotazovali na to, zda bylo respondentům dodáno vadné zboží[222] vinou e-shopu nebo prodávajícího. Jako oběť podvodu jsme považovali pouze ty respondenty, kteří se snažili zboží nebo peníze získat kontaktováním e-shopu (n = 1 090) či prodejce (n = 366) zpět, ale daný subjekt jim nevyhověl.

Méně úspěšní byli zákazníci, kteří nakupovali přes prodejce, kdy 28 % nebylo vyhověno vůbec a dalším 23 % pouze částečně. V prostředí e-shopů nebylo vyhověno 12 % respondentů, kteří se o náhradu snažili, a dalším 13 % bylo vyhověno pouze částečně. Tedy celkově polovině zákazníků, kteří se chtěli domoci vrácení zboží či peněz od prodejce, nebylo plně vyhověno, podobně jako čtvrtině zákazníků e-shopů. V tabulce jsou však validní procenta vztažena ke všem nakupujícím, tedy 2 % zákazníků e-shopů a 4 % zákazníků u prodávajících bylo při nakupování podvedeno nevyhovujícím či nedodaným zbožím (Tabulka 30). Alespoň částečně byla škoda nahrazena u 2 % nakupujících přes e-shop a 3 % přes prodávajícího. Celkově mělo tedy špatnou zkušenost 4 % s e-shopy a 7 % s prodejci. V celém reprezentativním vzorku bylo takto konstruovaných obětí podvodů při online nákupech zaznamenáno 4 % alespoň částečně neuspokojených zákazníků e-shopů a 3 % zákazníků na inzertních portálech.

Dalším tématem bylo zneužití e-bankingu. 2 % majitelů těchto účtů (n = 6 338) měla s takovým jednáním zkušenosti a další 1 % pravděpodobně také. Vzhledem k tomu, že pouze 7 % respondentů nevyužívá elektronické bankovnictví, tak se procenta vztahující se k celkové populaci příliš neliší.[223]

Neoprávněný přístup jsme taktéž sledovali ve vztahu k e-mailovým účtům, účtům na sociálních sítích a herním účtům.[224] Na základě srovnání validních procent, která se v těchto případech vždy odvíjí od vlastnictví daného účtu, lze konstatovat, že nejčastěji bývají zneužívány účty na sociálních sítích (5 % a 2 % pravděpodobně), soukromé e-maily (3 % a 2 % pravděpodobně), k počítačové hře (3 % a 1 pravděpodobně) a na herní platformě (4 % a 1 % pravděpodobně). Ostatní účty (zaměstnanecký a podnikatelský e-mail a účet k hazardní hře) jsou zneužívány spíše výjimečně.

Taktéž jsme zjišťovali míru útoků ransomwarem – zablokování mobilního telefonu, PC notebooku či jiného zařízení spojené s požadavkem výkupného. Takovou zkušenost má 4,5 % vlastníků některého z těchto typů IT technologie.[225]

V neposlední řadě jsme sledovali, do jaké míry mají respondenti zkušenost s doručením e-mailu požadujícího peníze (n = 3 040) či osobní údaje (n = 1 695). Jako oběti těchto útoků jsme považovali ty, kteří tomuto podvodnému e-mailu vyhověli. Obdobně jsme

221 Viz kapitola Obchodování online.

222 V dotazníku bylo upřesněno: *„jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží."*

223 Podrobněji viz kapitola E-banking.

224 Viz kapitoly E-mail, Zkušenosti se sociálními sítěmi a neoprávněné vstupy na cizí profily, Falešné účty na sociálních sítích, Herní účty a E-banking.

225 Bližší informace k tomuto tématu nabízí kapitola Ransomware.

dotazovali i uživatele sociálních sítí, kteří byli v kontaktu s některým z falešných účtů (účet zneužívající cizí identitu, účet se smyšlenou identitou, účet s nejistou identitou), zda danému účtu poslali peníze, potvrzovací SMS, osobní údaje či intimní obsah.

Podvodníci jsou obecně nejúspěšnější, pokud se na sociálních sítích vydávají za někoho reálného (zneužívají cizí identitu). Takto se nejčastěji domohou potvrzovacích SMS (2 %), osobních údajů (2 %, podobně jako v případě zasílání falešných e-mailů – 2 %) a peněz (2 %). Obecně lze však říci, že na tyto útoky respondenti málokdy „naletí". Ve všech případech se jedná o velmi malé absolutní četnosti, kdy u většiny sledovaných položek můžeme hovořit o několika jednotlivcích.[226]

Tabulka 30: Složení indexu viktimizace (jistá, nejistá a celkem) za rok 2020*

	Jistá viktimizace			Nejistá viktimizace			Viktimizace celkem		
	n	%	V%	n	%	V%	n	%	V%
Pokud bylo dodáno vadné zboží vinou e-shopu:[227] Vyhověl e-shop Vašim požadavkům? (n = 6 238)	Ne			Pouze částečně					
	126	1,8	2,0	137	2,0	2,2	263	3,8	4,2
Pokud bylo dodáno vadné zboží vinou prodávajícího: Vyhověl prodávající Vašim požadavkům? (n = 2 775)	Ne			Pouze částečně					
	101	1,5	3,6	85	1,2	3,1	186	2,7	6,7
Zneužil někdo v uplynulých 12 měsících Váš e-banking? (n = 6 338)	Ano			Pravděpodobně ano					
	143	2,1	2,3	56	0,8	0,9	199	2,9	3,2
Napadl někdo v uplynulých 12 měsících Vaše zařízení ransomwarem? (n = 6 396)	Ano								
	290	4,3	4,5	–	–		290	4,3	4,5
Phishing požadující poslání peněz (n = 3 040)/ osobních údajů (n = 1 695): odeslal jsem:[228]	Peníze								
	28	0,4	0,9	–	–		28	0,4	0,9
	Osobní údaje								
	35	0,5	2,1	–	–		35	0,5	2,1
Zneužil někdo v uplynulých 12 měsících Váš soukromý e-mail? (n = 6 584)	Ano			Pravděpodobně ano					
	220	3,2	3,3	146	2,1	2,2	366	5,3	5,5
Zneužil někdo v uplynulých 12 měsících Váš zaměstnanecký e-mail? (n = 2 650)	Ano			Pravděpodobně ano					
	38	0,6	1,4	31	0,5	1,2	69	1,1	2,6
Zneužil někdo v uplynulých 12 měsících Váš podnikatelský e-mail? (n = 475)	Ano			Pravděpodobně ano					
	5	0,1	1,1	3	0,0	0,6	8	0,1	1,7
Zneužil někdo v uplynulých 12 měsících Váš účet na sociální síti? (n = 5 606)	Ano			Pravděpodobně ano					
	257	3,8	4,6	119	1,7	2,1	376	5,5	6,7

226 Blíže ke zneužívání e-mailů a profilů na sociálních sítích viz kapitoly Phishing a Falešné účty na sociálních sítích.

227 Navazující otázky: *„bylo Vám v uplynulých 12 měsících dodáno vinou e-shopu/prodávajícího vadné zboží? Jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží."* ➔ *„Jak jste vadné zboží řešil/a?"* Při odpovědi *„snažil/a jsem se získat žádané zboží nebo peníze zpět kontaktováním e-shopu/prodávajícího"* následovala otázka *„vyhověl e-shop Vašim požadavkům?"* Index viktimizace zahrnuje odpovědi *„ne"* a *„pouze částečně"*.

228 Navazující otázky: *„přišel Vám v uplynulých 12 měsících falešný e-mail požadující poslání peněz/sdělení osobních údajů?"* ➔ *„Jak jste tento falešný e-mail řešil/a?"* Index zahrnuje odpovědi *„odeslal/a jsem požadované peníze/ osobní údaje."*

	Jistá viktimizace			Nejistá viktimizace			Viktimizace celkem		
	n	%	V%	n	%	V%	n	%	V%
Falešný profil na SNS zneužívající cizí identitu: poslal jsem:[229] (n = 493)	Peníze								
	9	0,1	1,8	–	–		9	0,1	1,8
	Potvrzovací SMS								
	12	0,2	2,4	–	–		12	0,2	2,4
	Osobní údaje								
	11	0,2	2,2	–	–		11	0,2	2,2
	Intimní obsah								
	5	0,1	1,0	–	–		5	0,1	1,0
Falešný profil na SNS se smyšlenou identitou: poslal jsem: (n = 658)	Peníze								
	4	0,1	0,6	–	–		4	0,1	0,6
	Potvrzovací SMS								
	3	0,0	0,5	–	–		3	0,0	0,5
	Osobní údaje								
	9	0,1	1,4	–	–		9	0,1	1,4
	Intimní obsah								
	7	0,1	1,1	–	–		7	0,1	1,1
Falešný profil na SNS s nejistou identitou: poslal jsem: (n = 391)	Peníze								
	5	0,1	1,3	–	–		5	0,1	1,3
	Potvrzovací SMS								
	1	0,0	0,3	–	–		1	0,0	0,3
	Osobní údaje								
	3	0,0	0,8	–	–		3	0,0	0,8
	Intimní obsah								
	5	0,1	1,3	–	–		5	0,1	1,3
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet k počítačové hře? (n = 1 142)	Ano			Pravděpodobně ano					
	36	0,5	3,2	15	0,2	1,3	51	0,7	4,5
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet k hazardní hře? (n = 593)	Ano			Pravděpodobně ano					
	4	0,1	0,7	6	0,1	1,0	10	0,2	1,7
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet na herní platformě? (n = 719)	Ano			Pravděpodobně ano					
	26	0,5	3,6	5	0,1	0,7	31	0,6	4,3
INDEX VIKTIMIZACE	1 013	**14,9**		521	**7,6**		1 364	**20,0**	

Pozn: Sloupce označené % se vztahují k celkovému počtu respondentů (n = 6 811). Sloupce označené V% odpovídají validním procentům. Počet respondentů (uvedený v závorce za sledovanou položkou), z něhož podíl vychází, odpovídá těm, kteří měli tuto otázku zodpovědět (např. nakupují online, vlastní daný účet nebo obdrželi falešný e-mail atp.).

229 Pro účet zneužívající cizí identitu, účet se smyšlenou identitou a účet s nejistou identitou platí, že respondenti odpovídali na otázku *„učinil/a jste v rámci kontaktu s falešným účtem některý z následujících kroků?“* Zahrnuty jsou odpovědi *„poslal/a jsem peníze,“ „přeposlal/a jsem potvrzovací SMS,“ „sdělil/a jsem své osobní údaje,“ „zaslal/a jsem intimní obsah.“*

Ze všech těchto sledovaných položek byl tedy vytvořen index viktimizace, kam byl započítán každý respondent, který má zkušenost alespoň s jedním typem výše uvedené online viktimizace. Takto jsme identifikovali 15 % respondentů, kteří byli viktimizováni některou z forem online útoku. Dalších 8 % si nebylo jisto, zda bylo viktimizováno, nebo utrpělo alespoň částečnou škodu. Celkově se tedy každý pátý respondent stal a/nebo možná stal obětí kyberútoku.

VII.2.2 Specifika obětí kyberkriminality

Indexy viktimizace jsme podrobili analýze chíkvadrát testu s mnoha sociodemografickými proměnnými a dalšími proměnnými, které sledují různorodá specifika respondentů (od míry zabezpečení po rizikové chování spojené s online prostředím). Obecně lze konstatovat, že se potvrzuje fakt, že obětí kyberkiminality se může stát každý, jelikož žádný ze signifikantních vztahů se neukázal být příliš silný. Vztahy se nejvíce projevovaly v rámci celkového indexu viktimizace, kde jsou započítány jisté i nejisté oběti. V následujících odstavcích tedy budeme prezentovat pouze slabé náznaky tendencí, které se vážou na celkovou viktimizaci.

Ze sociodemografických proměnných se ukazuje, že jsou spíše viktimizováni mladí lidé, přičemž s vyšším věkem viktimizace klesá. To může být způsobeno tím, že se mladí lidé v online prostředí více pohybují a vystavují rizikům viktimizace. Dále jsou spíše ohroženi nejméně vzdělaní lidé oproti vysokoškolákům. Do nejméně vzdělané kategorie samozřejmě spadají především i již zmínění mladí lidé. S tím souvisí i častější viktimizace studentů. Oběťmi online kriminality se také častěji stávají lidé v domácnosti. Naopak nejméně viktimizováni jsou zaměstnanci bez podřízených a nepracující důchodci. S nízkým věkem pravděpodobně souvisí i vyšší viktimizace svobodných respondentů nebo těch, kteří žijí v nesezdaném páru, a to především ve srovnání s jedinci v manželském vztahu. Na druhou stranu závislost viktimizace na rodinném vztahu je opravdu velmi slabá. Pohlaví, obor, v němž respondent pracuje, a velikost obce bydliště dotazovaného na viktimizaci nemají vliv.

Co se týče bezpečného užívání informačních technologií, tak jsou spíše viktimizováni ti, kteří někdy použili nalezenou cizí paměťovou kartu či flashdisk (35 % oproti 30 %)[230] a o něco více respondenti, kteří je před použitím nezkontrolovali.[231] Tento rozdíl se však nejvíce projevuje u nejistých obětí (21 % oproti 10 %). A téměř zanedbatelný (byť signifikantní) rozdíl je i u vyšší viktimizace respondentů, kteří nechávají používat své zařízení někoho jiného (21 % oproti 18 %). V tomto kontextu se ukazuje paradoxní, nicméně stále slabá tendence, že větší riziko viktimizace se ukazuje u respondentů, kteří byli na kurzu bezpečného užívání informačních technologií (24 % oproti 19,1 %). Zde však nemůžeme určit kauzalitu, zda byly oběti kyberkriminality nejprve viktimizovány, a pak se kurzu účastnily, nebo zda byly na kurzu a pak se teprve staly oběťmi a pouze například spadají do rizikové skupiny. To, jestli se někdo stará o bezpečnost svého zařízení či jej zabezpečuje,

230 Počítáno pouze z obětí, které některý z těchto paměťových nosičů nalezly a zároveň si pamatují, zda jej (ne) použily (n = 385).

231 Počítáno pouze z obětí, které paměťový nosič našly, použily a pamatují si, zda jej (ne)zkontrolovaly (n = 163).

na viktimizaci dle našich dat nemá vliv. Co se však projevuje jako velmi slabý rizikový faktor, je znalost darkwebu či darknetu (22 % oproti 19 %) a zkušenost s využitím Toru (24 % oproti 19 %).

VII.2.3 Čtyři úrovně viktimizace

Index jisté viktimizace v sobě skrývá možnou polyviktimizaci – zkušenost s více různými formami viktimizace (Näsi et al., 2021). V rámci kyberútoků může docházet i k řetězcům, kdy je např. phishing nebo hacking následován krádeží identity k vykradení bankovního účtu (Holt & Turner, 2012).

Ukázalo se, že téměř čtvrtina jistých obětí (24 %) uvedla dva a více typů útoku. Dvanáct respondentů sdílelo zkušenost dokonce s pěti až osmi incidenty. Nebude překvapivé, že v kombinaci spíše bývají útoky, které jsou si vzájemně podobné. Jde například o podvody při online nakupování, nebo falešné e-maily požadující peníze v kombinaci s požadováním osobních údajů či útoky falešných účtů na sociálních sítích. Pokud respondentovi někdo neoprávněně vstoupil do účtu k počítačové hře či herní platformě, tak má pravděpodobně také zkušenost s další viktimizací především na sociálních sítích. A v kombinaci s dalšími útoky také často dochází ke zneužití e-bankingu.

Dále jsme měli možnost sledovat reviktimizaci – opakovanou viktimizaci stejným trestným činem, kterou jsme s jistotou mohli určit pouze u některých položek.[232] V rámci výzkumu kyberkriminality se v literatuře spíše diskutují opakované útoky na webové stránky (Moneva et al., 2022), ale my se zde zaměříme na opakovanou viktimizaci našich respondentů. Zjistili jsme tak, že čtvrtina (25 %) se za poslední rok stala obětí stejného útoku, přičemž u všech sledovaných položek šlo v naprosté většině o jistou viktimizaci.

Tyto indikátory, které dávají viktimizaci nový rozměr a intenzitu, jsme tedy vyhodnocovali pouze u obětí s jistou viktimizací. Díky tomu jsme na základě zjištěných indexů viktimizace, identifikované polyviktimizace a reviktimizace vytvořili čtyři úrovně viktimizace, viz Obrázek 1: Čtyři úrovně viktimizace.

232 Zneužití bankovních, e-mailových či herních účtů a ransomware.

Obrázek 1: Čtyři úrovně viktimizace

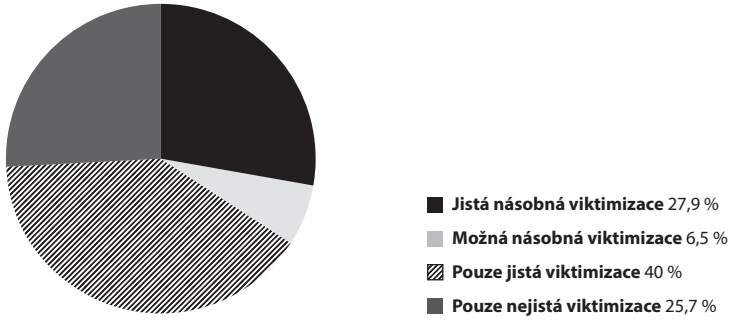
1. Jistá násobná viktimizace[233] (n = 380)
2. Možná násobná viktimizace[234] (n = 88)
3. Pouze jistá viktimizace (n = 545)
4. Pouze nejistá viktimizace (n = 351)

Struktura obětí z indexu celkové viktimizace dle její úrovně je zobrazena v grafu (Graf 80). Přesné dvě pětiny a zároveň nejvíce „obětí" bylo zařazeno do skupiny s jistou viktimizací. Nicméně třetina respondentů tvoří dvě výrazněji zasažené rizikové skupiny kyberkriminalitou – 28 % bylo buď polyviktimizováno různými a/nebo opakovaně stejnými typy incidentů, které jsme zařadili do jisté viktimizace; a dalších 7 % uvedlo jeden typ jisté viktimizace a zároveň jeden či více typů nejisté viktimizace, tedy pravděpodobně mohlo dojít k násobné viktimizaci. Na druhou stranu u čtvrtiny „obětí" (26 %) z celkového indexu viktimizace si nemůžeme být jisti, zda opravdu došlo k viktimizaci, buď kvůli tomu, že si tím není jistý samotný respondent, nebo nám chybí další informace. Nicméně určitá pravděpodobnost, že se dotyčný stal obětí, tu je.

233 Polyviktimizace různými incidenty a opakovaná viktimizace stejnými incidenty v rámci jisté viktimizace.

234 Viktimizace jistou viktimizací v kombinaci s jednou a více nejistými incidenty.

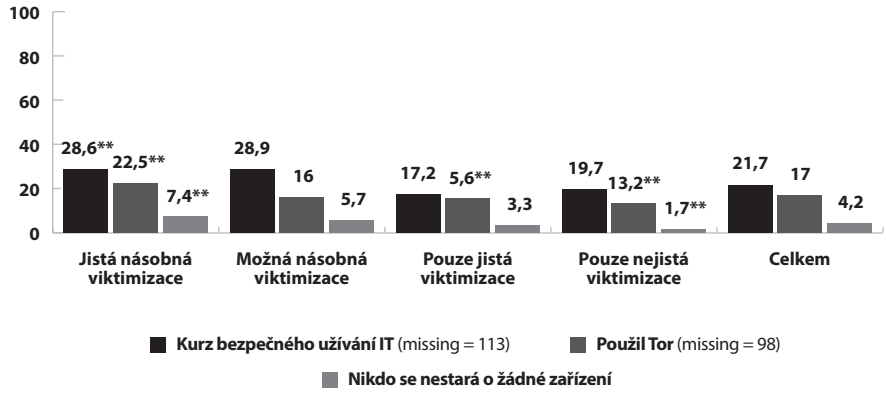
Graf 80: Struktura online obětí (index celkové viktimizace) dle úrovně viktimizace (n = 1 364)



Čtyři úrovně viktimizace jsme otestovali v závislosti na sociodemografikách a bezpečnostních návycích. Stupně viktimizace považujeme za ordinální proměnnou ve vztahu k možným dopadům na oběť.

Zatímco u sociodemografik se neobjevila žádná závislost, tak na bezpečnostní návyky ukazují určité, byť ne příliš silné tendence. Z grafu lze vypozorovat, že zjištěné tendence se nejvíce projevují u jisté násobné viktimizace (Graf 80). Opakovanou či vícenásobnou obětí kyberkriminality se tedy spíše stali jedinci, kteří byli na kurzu bezpečného užívání informačních technologií, použili Tor, ale zároveň také ti, o jejichž zařízení se nikdo nestará. Ukázalo se také, že s vyšší zjištěnou úrovní viktimizace respondenti spíše některý z incidentů ohlásili na policii.

Graf 81: Vliv bezpečnostních návyků na viktimizaci (%, n = 1 364)[235]



235 Chybějící hodnoty (missing) u dílčích bezpečnostních návyků jsou způsobeny možností nevím/nedokážu odpovědět/ nebo neodpověděl/a. * p < 0,05; ** p < 0,01; *** p < 0,001.

VII.2.4 Závěr k obětem vůbec

Obecně lze tedy říci, že nejčastěji dochází ke zneužití účtu na sociálních sítích (6 %, respektive 7 % z těch, co takový účet mají), soukromého e-mailu (5 %) nebo útoku ransomwarem (4 %). Výraznější viktimizace je i v rámci útoků na e-banking (3 %) a podvodů při online obchodování jak přes e-shopy (3 %) tak inzertní portály (4 %). Pokud bychom se však zaměřili pouze na respondenty, kteří takto nakupují, pak tato skupina patří mezi nejrizikovější, a to jak u zákazníků e-shopů (4 %), kde čtvrtině není na aktivní stížnost plně vyhověno, ale především u nakupujících přes inzertní portály (7 %), kteří mají špatnou zkušenost v polovině případů. Ostatní formy viktimizace byly ve vztahu k celému vzorku velmi nízké. Za zmínku však stojí specifická skupina online hráčů, kteří se v 5 % případů stali obětí zneužití účtu k počítačové hře a 4 % k herní platformě.

Z analýzy vztahů žádná výrazná sociodemografická specifika obětí nevyplynula, na což poukazují i další autoři (Guerra & Ingram, 2020; Leukfeldt & Yar, 2016). Potvrzuje se tedy premisa, že obětí online útoku se může stát každý z nás.

Ve slabých náznacích však lze shrnout, že jsou kyberkriminalitou ohroženi spíše mladí lidé. To se ukázalo i v dalších zahraničních výzkumech (Ngo et al., 2020; van de Weijer & Leukfeldt, 2017). V našem dotazníkovém šetření je pro mladší respondenty specifické například to, že výrazně častěji uvedli znalost prostředí darkwebu či darknetu. A co se týče vyloženě rizikového chování, tak spíše nechávají používat svá zařízení někoho jiného. Naopak si ale svá zařízení více zabezpečují, v menší míře použili cizí paměťovou kartu či flashdisk,[236] spíše prošli nějakým kurzem bezpečného užívání informačních technologií a více užívají Tor. Nelze tedy říci, že by se chovali pouze rizikově či protektivně. Lze spíše uvažovat nad tím, že jakožto jedinci, kteří s informačními technologiemi vyrůstali, jsou však díky intenzitě jejich využívání více vystavováni jejich rizikům.

Z bezpečnostních návyků mělo na viktimizaci silnější vliv pouze to, zda respondent použil cizí paměťovou kartu či flashdisk bez předchozí kontroly.[237] Naopak (a možná i překvapivě) na viktimizaci nemá vůbec vliv míra zabezpečení či péče o bezpečnost užívaných technologií. Podobné výsledky se ukázaly například i v nedávno publikované nizozemské studii založená na longitudinálních datech (van 't Hoff-de Goede et al., 2023). Z toho je možné usoudit, že kybernetické útoky jsou specifické tím, že cílí na celou populaci a není snadné se jim ubránit.

Po sestrojení čtyř úrovní viktimizace, které mohou odrážet závažnost dopadu na oběť, se již bezpečnostní návyky alespoň náznakem projevují. Nicméně opačným směrem, než by se možná očekávalo – násobnou obětí kyberkriminality se například spíše stali jedinci, kteří byli na kurzu bezpečného užívání informačních technologií a ti, co použili Tor. Výše zmínění nizozemští výzkumníci to vysvětlují tím, že lidé s vyššími IT schopnostmi si spíše kyberútoku všimnou (ibid.). V našich datech jsou však taktéž ve větší míře násobně

236 Počítáno pouze z těch respondentů, kteří některý z těchto paměťových nosičů nalezli a zároveň si pamatují, zda jej (ne)použili (n = 1 207).

237 Počítáno pouze z obětí, které některý z těchto paměťových nosičů nalezly a zároveň si pamatují, zda jej při použití (ne)zkontrolovaly (n = 163).

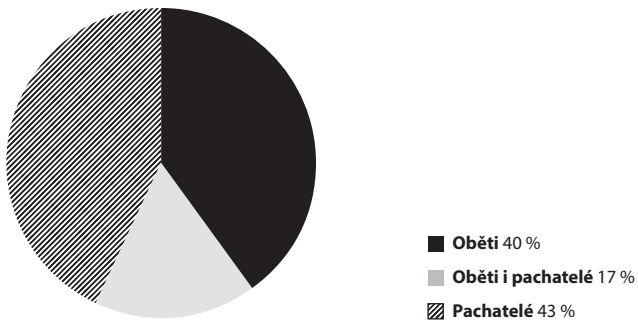
viktimizováni ti, o jejichž zařízení se nikdo nestará. Bohužel se ukázala i vysoká míra latence, kdy pouze 10 % obětí jisté viktimizace ohlásilo alespoň jeden případ online útoku policii. Na druhou stranu násobně viktimizovaní respondenti tak učinili výrazně častěji.[238]

VII.3 Pachatelé vs. oběti

Nyní se podíváme na to, do jaké míry se mezi online oběťmi objevují respondenti, kteří se přiznali, že se dopustili některého z deliktů v kyberprostoru. Ukázalo se, že je tento překryv mezi online oběťmi a pachateli téměř třetinový (30 % jistých či nejistých obětí se dopustilo některého ze zkoumaných deliktů, oproti 19 % zbylých respondentů). Dokonce lze i do určité míry říci, že se oproti běžné populaci oběti signifikantně častěji dopouštějí nějaké nelegální činnosti online, a naopak spíše jsou online viktimizováni jedinci, kteří se sami něčeho dopustili. Především se to projevuje u jistých obětí, ať už byli viktimizováni jednou či násobně.

V našem vzorku takto můžeme identifikovat skupinu respondentů, kteří mají dost pravděpodobně zkušenost s kyberkriminalitou (Graf 82), ať už v pozici:
1) pouze oběti[239] (n = 961),
2) oběti i pachatele (n = 403),
3) pouze pachatele (n = 1 038).

Graf 82: Tři typy respondentů s možnou zkušeností s kyberkriminalitou



Respondenti, kteří v našem dotazníku byli identifikováni pouze jako možné oběti online viktimizace, jsou specifičtí tím, že se jedná především o starší ženy, spíše rozvedené, případně vdovy s vyučením bez maturity, které jsou v domácnosti či v důchodu. Mohou být tedy snadným terčem online podvodníků. Spíše neabsolvovali kurz bezpečného užívání online technologií a nevykazují hlubší znalosti online prostředí. Jejich zařízení většinou ani nemají žádné zabezpečení. Online viktimizaci však nahlásilo výrazně více těch, kdo se stali obětí i něco online spáchali (viz následující odstavec) než jedinci, kteří byli pouze viktimizováni.

238 Více o latenci viz kapitola Latence a důvěra ve schopnosti policie.

239 Počítáno z jistých i nejistých obětí.

Ti, kdo uvedli některou z jistých či nejistých forem viktimizace, i páchání patří především do nejmladší věkové skupiny. Jsou to tedy zejména svobodní, studující, případně zaměstnaní jedinci se základním, případně středoškolským vzděláním s maturitou. Z těchto tří skupin respondentů byli na jednu stranu tito jedinci ve větší míře na kurzu bezpečného užívání IT technologií, na druhou stranu vykazují více než ostatní některá riziková chování – například ve větší míře použili TOR nebo cizí paměťovou kartu či flashdisk. Na druhou stranu, pokud se jim něco nepříjemného v kyberprostoru stane, častěji se obracejí na policii.

Námi označení online pachatelé, kteří však neuvedli žádnou z forem viktimizace, jsou především muži v mladším produktivním věku (25–44 let), taktéž především svobodní a vysokoškolsky vzdělaní jedinci, ať už ještě studující, či již zaměstnaní, a to především v oboru IT. Není tedy překvapivé, že vykazují hlubší znalosti internetu a využívají zabezpečení svých zařízení.

VII.3.1 Závěr k pachatelům vs. obětem

Tato typologie nám nabídla poměrně stereotypní pohled na kyberkriminalitu. Zde si můžeme představit skupinu online hackerů. Oproti naivním postarším ženám bez znalosti kyberprostoru. A jakousi skupinku teenagerů, kteří se v důsledku svého nekontrolovaného chování mohou stát jak obětí, tak i pachateli nelegální činnosti online. Zde je však nutné mít na paměti, kterých deliktů se náš výzkum týká a v jakém zastoupení se odehrával, aby tyto generalizace nezpůsobovaly mýty v oblasti kyberkriminality.

VII.4 Rozlišování virtuálního násilí a majetkového zájmu

Nyní se podíváme na jinou typologii, kdy incidenty, jimiž byli respondenti viktimizováni, jsme rozdělili do dvou skupin dle motivace pachatele, a to na *virtuální násilí* a *majetkový zájem* (Vlach et al., 2020). Pro každou z těchto skupin jsme vytvořili samostatný index. Do indexu majetkového zájmu patří útoky, které cílí především na získání finančního obnosu nebo osobních údajů či online vlastnictví, které lze zpeněžit prodejem. Index virtuálního násilí obsahuje činy, které útočí na osobu oběti. Motivace je u některých případů zřejmá z podstaty útoku. U dalších incidentů bylo potřeba využít doplňující otázky, které nám dodaly kontext incidentu, nebo názor respondenta, jehož jsme se u některých útoků doptávali na pravděpodobnou motivaci pachatele.

V dotazníku se také vyskytovaly případy, u nichž ani nešlo se sebemenší jistotou motivaci určit. Navíc jsme vycházeli ze všech, ať už jistých či nejistých obětí, jelikož oba typy obětí mohly odpovědět, zda vyhověly požadavkům útočníka, zda dokážou posoudit jeho motivaci atp. Pokud bylo možné takto určit motivaci, tak se zároveň zvýšila pravděpodobnost, že byli nakonec opravdu kyberkriminalitou viktimizováni i ti respondenti, kteří jsou v současné chvíli zařazeni do skupiny nejistých obětí (viz kapitola Oběti). Tvorba indexů tedy skýtá různé metodologické obtíže, které je třeba brát při interpretaci v potaz a vnímat je spíše jako náhled do problematiky než jako neměnná fakta.

VII.4.1 Majetkový zájem

V indexu majetkového zájmu jsou ponechány v kontextu nakupování online stejné položky, jako byly v indexu viktimizace (Tabulka 31), viz kapitola Oběti. Tedy, zda vyhověl daný subjekt požadavkům respondenta, v případě, že bylo dodáno vadné zboží vinou prodávajícího. Započítávali jsme pouze ty respondenty, kterým nebylo vyhověno vůbec. Jednalo se tedy o 12 % těch, kterým nevyhověl e-shop, a o téměř třetinu (28 %), kterým nevyhověl prodávající. Stejně tak byla ponechána položka napadnutí zařízení ransomwarem, k němuž došlo v případě 5 % majitelů některého z IT zařízení. Neměnná zůstala i položka sledující phishing – útok falešným e-mailem požadující poslání peněz či osobních údajů, kdy byly jako oběti identifikováni pouze ti respondenti, kteří žádosti vyhověli a útočníkovi tak „naletěli". Do indexu majetkového zájmu byli zařazeni samozřejmě respondenti, kteří zaslali požadované peníze (1 %), ale také i ti, kdo poslali osobní údaje (2 %).[240] U všech těchto položek je tedy podíl majetkového zájmu stoprocentní.

Zneužití e-bankingu jsme do indexu zařadili, pokud vznikla finanční škoda. Jednalo se o více než polovinu „obětí" (55 %), které byly zařazeny jak do jisté, tak nejisté viktimizace.[241] Podobně jsme přistupovali ke zneužití e-mailového či herního účtu a profilu na sociálních sítích, nebo při zneužití osoby na sociálních sítích s falešným profilem. Zde bylo rozhodující respondentovo zhodnocení motivace pachatele, kterou mohlo být majetkové obohacení. U herních účtů šlo alespoň o jednu z těchto možností: dotyčný koupil nějaký obsah, prodal nějaký obsah nebo prodal herní účet.

240 Osobní údaje získané phishingem bývají monetizovány např. prodejem na černém trhu.

241 Respondent uvedl, že se stal nebo pravděpodobně stal obětí útoku (viz kapitola E-banking).

Tabulka 31: Složení indexu majetkového zájmu

	n	%	V%		n	%	V%
	Ne				**Ne**		
Pokud bylo dodáno vadné zboží vinou e-shopu:[242] Vyhověl e-shop Vašim požadavkům? (n = 126)	126	1,8	100	**Pokud bylo dodáno vadné zboží vinou prodávajícího: Vyhověl prodávající Vašim požadavkům? (n = 101)**	101	1,5	100
	Ano				**Ano**		
Zneužití e-bankingu: Vznikla finanční škoda? (n = 199)	110	1,6	55,3	**Napadl někdo v uplynulých 12 měsících Vaše zařízení (mobil, PC, notebook, tablet) ransomwarem? (n = 290)**	290	4,3	100
	Peníze				**Osobní údaje**		
Phishing požadující poslání peněz (n = 28): odeslal jsem:[243]	28	0,4	100	**Phishing požadující poslání osobních údajů (n = 35): odeslal jsem:**	35	0,5	100
	Majetkově se obohatit				**Majetkově se obohatit**		
Důvod zneužití soukromého e-mailu (n = 366):	92	1,4	25,1	**Důvod zneužití zaměstnaneckého e-mailu (n = 69):**	19	0,3	27,5
	Majetkově se obohatit				**Majetkově se obohatit**		
Důvod zneužití podnikatelského e-mailu (n = 8):	3	0,0	37,5	**Důvod zneužití účtu na SNS (n = 376):**	55	0,8	14,6
	Majetkově se obohatit				**Majetkově se obohatit**		
Důvod zneužití falešným účtem s cizí identitou (n = 36):	15	0,2	41,6	**Důvod zneužití falešným účtem se smyšlenou identitou (n = 22):**	7	0,1	31,8
	Majetkově se obohatit				**Majetkově se obohatit[244]**		
Důvod zneužití falešným účtem s nejistou identitou (n = 14):	6	0,9	42,9	**Důvod zneužití účtu k počítačové hře (51):**	7	0,1	13,7
	Majetkově se obohatit				**Majetkově se obohatit**		
Důvod zneužití účtu k hazardní hře (n = 10)	1	0,0	10,0	**Důvod zneužití účtu k herní platformě (n = 31):**	7	0,1	22,6
INDEX MAJETKOVÉHO ZÁJMU					**680**	**10,0**	

Pozn: Sloupce označené % se vztahují k celkovému počtu respondentů (n = 6 811). Sloupce označené V% odpovídají validním procentům. Počet respondentů (uvedený v závorce za sledovanou položkou), z něhož podíl vychází, odpovídá těm, kteří se stali obětí daného útoku.

242 Návazné otázky: *„bylo Vám v uplynulých 12 měsících dodáno vinou e-shopu/prodávajícího vadné zboží? Jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží.“* ➔ *„Jak jste vadné zboží řešil/a?“* Při odpovědi *„snažil/a jsem se získat žádané zboží nebo peníze zpět kontaktováním e-shopu/prodejce“* navázala otázka zahrnutá do tabulky: *„vyhověl e-shop Vašim požadavkům?“*

243 Návazné otázky: *„přišel Vám v uplynulých 12 měsících falešný e-mail požadující poslání peněz/sdělení osobních údajů?“* ➔ *„Jak jste tento falešný e-mail řešil/a?“* Zahrnuty jsou odpovědi *„odeslal/a jsem požadované peníze/ osobní* údaje.“

244 V případě herních účtů (k počítačové hře, hazardní hře či na herní platformě) se jednalo o jednu či více z těchto možností: dotyčný koupil nějaký obsah, prodal nějaký obsah nebo prodal herní účet.

U zneužití uživatelů sociálních sítí falešnými účty je poměr majetkového zájmu poměrně vysoký, a to především u zneužití účtem s cizí (42 %) a nejistou identitou (43 %). Nicméně je třeba brát v potaz relativně nízkou prevalenci této viktimizace, což platí především v případě zneužití podnikatelského účtu, kde se jedná pouze o tři případy z osmi. Jako důvod majetkově se obohatit dále bylo uvedeno v 32 % zneužití smyšlenou identitou a přibližně ve čtvrtině případů zneužití zaměstnaneckého (28 %) a soukromého e-mailu (25 %), nebo účtu k herní platformě (23 %).

Menší podíl této motivace vyšel v kontextu zneužití účtu k počítačové hře (14 %) a účtu na sociálních sítích (14 %). Nejmenší podíl majetkového zájmu byl zaznamenán u zneužití účtu k hazardní hře, ale zde šlo pouze o jeden případ z deseti.

Jak již bylo výše zmíněno, tak z těchto položek byl vytvořen index majetkového zájmu. Ukázalo se, že každý desátý respondent splňoval alespoň jednu z definovaných podmínek, tedy byl viktimizován alespoň jedním z online útoků, jehož cílem bylo obohacení pachatele. Specifika těchto obětí budou ještě níže popsána.

VII.4.2 Virtuální násilí

V indexu virtuálního násilí (Tabulka 32) je podstatně méně sledovaných položek oproti indexu majetkového zájmu. Bylo možné pracovat pouze s viktimizací zneužití některého z účtů či útoku přes sociální sítě, kde jsme dle navazujících otázek mohli identifikovat, zda bylo cílem poškodit osobu oběti.

V rámci zneužití účtu k e-mailu a sociálním sítím a zneužití falešným profilem přes sociální sítě jsme takto označili případy, kdy respondent uvedl alespoň jeden z těchto důvodů: žárlivost, pomsta či osobní nenávist, nesnášenlivost obecně, stalking, žert, zvědavost, a/nebo sexuální uspokojení. Největší podíl virtuálního násilí byl zaznamenán v kontextu zneužití herních účtů, a to k počítačové hře (88 %), herní platformě (81 %) a hazardní hře (80 %). U poslední položky se však v absolutních četnostech jednalo o osm respondentů z deseti. Nízké četnosti s vysokým podílem jsou také u zneužití podnikatelského účtu (pět z osmi, tedy 63 %) a zneužití falešným profilem s cizí identitou (osm z čtrnácti, tedy 57 %). Nicméně více než poloviční podíly virtuálního násilí byly také naměřeny u zneužití falešným profilem se smyšlenou identitou na sociálních sítích (59 %) a zneužití zaměstnaneckého e-mailu (54 %).

Menší, ale stále velmi vysoké podíly virtuálního násilí můžeme pozorovat u zneužití falešným účtem s cizí identitou na sociálních sítích (44 %), zneužití respondentova účtu na sociálních sítích (35 %) a zneužití soukromého e-mailu (29 %).

S ohledem na validní procenta (podíl typu motivace na viktimizaci daným útokem) se zdá být virtuální násilí ve srovnání s majetkovým zájmem velmi silně zastoupené. Nesmíme však zapomenout na nižší počet sledovaných proměnných, u kterých byla zároveň nižší prevalence viktimizace. Takto zkonstruovaný index virtuálního násilí zahrnující případy, kdy byl respondent viktimizován alespoň jedním z některých online útoků cíleným proti jeho osobě, tedy tvořil 4 % z celkového vzorku. Hlubší analýza tohoto typu obětí je provedena níže.

Tabulka 32: Složení indexu virtuálního násilí[245]

	n	%	V%		n	%	V%
	Virtuální násilí[246]				Virtuální násilí		
Důvod zneužití soukromého e-mailu (n = 366)	105	1,5	28,7	Důvod zneužití zaměstnaneckého e-mailu (n = 69)	37	0,5	53,6
	Virtuální násilí				Virtuální násilí		
Důvod zneužití podnikatelského e-mailu (n = 8)	5	0,1	62,5	Důvod zneužití profilu na SNS (n = 376)	130	1,9	34,6
	Virtuální násilí				Virtuální násilí		
Důvod zneužití falešným účtem s cizí identitou (n = 36)	16	0,2	44,4	Důvod zneužití falešným účtem se smyšlenou identitou (n = 22)	13	0,2	59,1
	Virtuální násilí				Virtuální násilí[247]		
Důvod zneužití falešným účtem s nejistou identitou (n = 14)	8	0,1	57,1	Důvod zneužití účtu k počítačové hře (n = 51)	45	0,7	88,2
	Virtuální násilí				Virtuální násilí		
Důvod zneužití účtu k hazardní hře (n = 10)	8	0,1	80,0	Důvod zneužití účtu k herní platformě (n = 31)	25	0,4	80,6
Index virtuálního násilí					299	4,4	

VII.4.3 Porovnání skupin obětí podle motivace pachatele

Tyto dva indexy nám umožňují oběti útoků kyberkriminality, ať už jisté či nejisté (n = 1 364, viz kapitola Oběti), rozdělit do 4 skupin podle dotazníkem zjištěné motivace, viz Obrázek 2: Skupiny obětí podle motivace pachatele. Tedy na ty respondenty, kteří pravděpodobně mají zkušenost s:

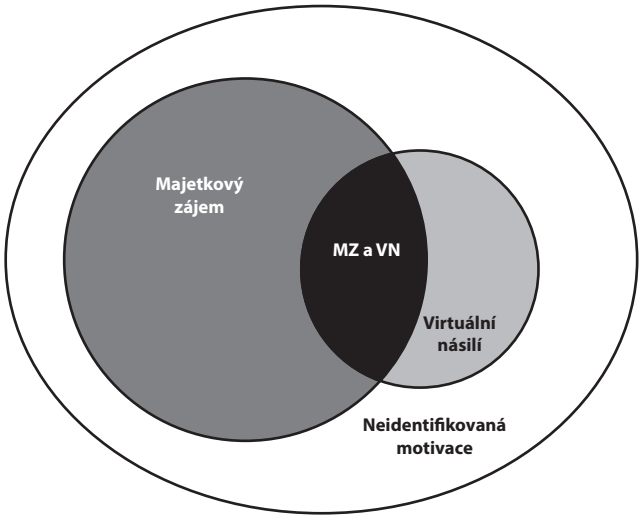
1. pouze majetkovým zájmem (n = 568);
2. pouze virtuálním násilím (n = 187);
3. majetkovým zájmem i virtuálním násilím (n = 112);
4. incidentem s neidentifikovanou motivací pachatele (n = 497).

245 Sloupce označené % se vztahují k celkovému počtu respondentů (n = 6 811). Sloupce označené V% odpovídají validním procentům. Počet respondentů (uvedený v závorce za sledovanou položkou), z něhož podíl vychází, odpovídá těm, kteří se stali obětí daného útoku.

246 Pokud v případě zneužití e-mailového účtu, účtu na sociálních sítích nebo zneužití falešným účtem na sociálních sítích respondent uvedl alespoň jeden z následujících důvodů: žárlivost, pomsta či osobní nenávist, nesnášenlivost obecně, stalking, žert, zvědavost, sexuální uspokojení.

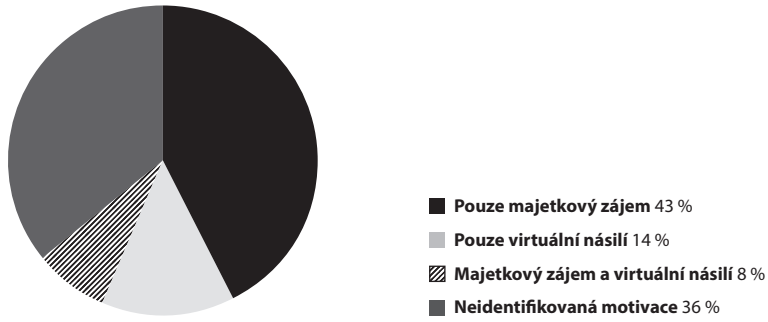
247 Pokud v případě zneužití některého z herních účtů respondent uvedl alespoň jeden z následujících způsobů zneužití: dotyčný hrál bez mého svolení, dotyčný ovlivnil mé hraní (např. změnil uložené pozice), dotyčný změnil mé přihlašovací údaje.

Obrázek 2: Skupiny obětí podle motivace pachatele



Struktura obětí celkového indexu viktimizace dle motivace pachatele útoku je zobrazena následovně (Graf 83). Více než dvě pětiny obětí (43 %) mají zkušenost s viktimizací pouze s majetkovým zájmem pachatele, oproti 14 %, která se stala oběťmi virtuálního násilí. 8 % obětí buď určilo motivaci útoku jako cílenou proti jejich osobě a zároveň majetkově motivovanou, nebo se stalo obětí vícera útoků, z čehož každý byl jinak motivovaný. U více než třetiny obětí (36 %) nebylo možné motivaci identifikovat, a to buď kvůli chybějící doplňující otázce, nebo kvůli tomu, že respondent nedokázal motivaci určit.

Graf 83: Struktura obětí (celkový index celkové viktimizace) dle motivace pachatele (n = 1 364)



Co se týče genderového rozložení, tak muži byli více viktimizováni kombinací majetkového zájmu a virtuálního násilí než ženy (10 % oproti 6 %). Naopak u žen bylo výrazně více případů, jejichž motivaci nebylo možné identifikovat (41 % oproti 32 %). Z pohledu věkové struktury respondentů se ukázalo být specifické především virtuální násilí, které

je charakteristické především pro mladší respondenty, a to především pro nejmladší věkovou kategorii do 24 let. Naopak viktimizace majetkovým zájmem není pro tuto skupinu respondentů tak častá jako u ostatních.

Lze předpokládat, že s věkem souvisí i další sledované sociodemografické proměnné. Například svobodní respondenti mají spíše zkušenost s virtuálním násilím. Virtuální násilí naopak není běžné pro ženaté, potažmo vdané jedince či rozvedené. Rozvedení naopak spíše bývají viktimizováni majetkovým zájmem.

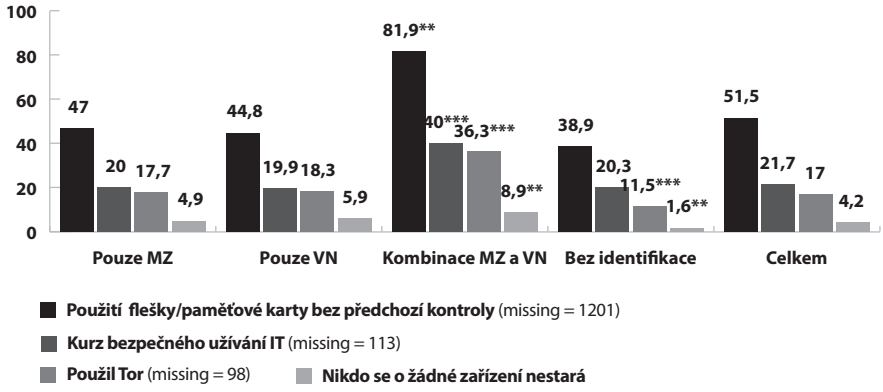
Věk se odráží i v socioekonomickém statusu respondenta, kdy virtuálním násilím jsou nejvíce viktimizováni studenti, oproti ostatním skupinám, a to zejména ve srovnání se zaměstnanci bez podřízených. Ti jsou virtuálním násilím (stejně jako kombinací s majetkovým zájmem) viktimizováni méně. Pro lidi v domácnosti je dále specifické, že se méně stávají oběťmi majetkového zájmu, a naopak zakusili více incidentů, u nichž nebylo možné určit motivaci.

Pokud bychom se zaměřili pouze na zaměstnané respondenty, kteří se identifikovali s některou z možností definující obor jejich zaměstnání (včetně „jiné", n = 834), tak se ukazuje, že lidé pracující v bezpečnostních službách, v bankovnictví, finančnictví či pojišťovnictví, se spíše stanou obětí útoku s kombinovanou motivací či vícero různě motivovaných útoků. Jedinci, kteří uvedli jiný než v možnostech nabízený obor,[248] se zase spíše stali obětí majetkového zájmu.

Kromě sociodemografik jsme také sledovali závislost typu viktimizace dle motivace pachatele na bezpečnostních návycích respondenta. Z grafu je zřejmé, že nejvíce se tyto sledované proměnné projevovaly u obětí, které byly viktimizovány jak majetkovým zájmem, tak virtuálním násilím (Graf 84). Mohlo jít o útoky s kombinovanou motivací nebo o násobnou viktimizaci. Z toho lze usuzovat, že se jednalo o nejzávažnější viktimizaci.

248 V dotazníku jsme sledovali tyto obory: státní správa či samospráva, bezpečnostní služby, bankovní/finanční sféra/pojišťovnictví (pojišťovnictví bylo sledováno zvlášť, ale při analýze bylo z důvodu malého zastoupení sloučeno s bankovní/finanční sférou), IT, jiný.

Graf 84: Vliv bezpečnostních návyků na viktimizaci (%, n = 1 364)[249]



Pokud se zaměříme na dílčí proměnné, u nichž byl zjištěn signifikantní vztah, tak nejvíce je kombinovaná viktimizace asociována s použitím neověřené flešky/paměťové karty. Toto rizikové chování je však počítáno pouze z těch obětí celkového indexu viktimizace, kteří paměťový nosič našli, použili a pamatují si, zda jej ne/zkontrolovali (n = 163). Dále mělo na vyšší míře kombinované viktimizaci vliv to, zda se respondent účastnil kurzu bezpečného užívání informačních technologií, použil Tor nebo zda uvedl, že se o žádné z jím užívaných zařízení nikdo nestará.

Nebude tedy překvapivé, že oběti útoků kombinujících majetkový zájem a virtuální násilí, ve výrazně větší míře v roce 2020* nahlásili alespoň některou formu kyberútoku (42 %), a to především v porovnání s těmi, u jejichž viktimizace nebylo možné zhodnotit pachatelovu motivaci (3 %).

VII.4.4 Závěr k rozlišování virtuálního násilí a majetkového zájmu

V této kapitole jsme sledovali specifika respondentů, kteří byli alespoň pravděpodobně viktimizováni útoky s motivací majetkově se obohatit a/nebo oběti ublížit. V offline světě bychom mluvili o rozdílech mezi násilnou a majetkovou trestnou činností. Na druhou stranu existuje i trestná činnost, která tyto dva prvky kombinuje – například loupežné přepadení. Případně existují lidé, kteří se v rámci polyviktimizace stali obětí jak majetkové, tak násilné trestné činnosti. Proto jsme testovali skupinu obětí, které byly viktimizovány pouze majetkovým zájmem, pouze virtuálním násilí, kombinací obojího a útoky, jejichž motivaci nebylo možné určit.

Virtuální násilí se ukázalo být specifické pro nejmladší kategorii respondentů, což bývají většinou studenti a lidé bez vážného vztahu. Vzhledem k operacionalizaci virtuál-

249 Chybějící hodnoty (missing) u dílčích bezpečnostních návyků jsou způsobeny možností nevím/nedokážu odpovědět/bez odpovědi. V případě použití paměťového nosiče se vycházelo z celkového indexu obětí, kteří tento nosič našli a ví, zda jej (ne)použili bez předchozí kontroly. * p < 0,05; ** p < 0,01; *** p < 0,001.

ního násilí[250] lze předpokládat, že se jednalo o nějakou formu pravděpodobně i závažnější kyberšikany, která je specifická především pro děti, ale může snadno překročit hranici trestné činnosti.

Většina položek z indexu majetkového zájmu zároveň vychází z prostředí sociálních sítí a objevují se zde i incidenty majitelů herních účtů, což opět výrazně souvisí s mladší generací. Na to také navazuje teorie využití internetu nejen jako nástroje, ale i jako místa (place), kde je možné dokonce vyjadřovat vlastní životní styl (way of being) (Markham, 2003). V tomto prostoru může také docházet k virtuálnímu násilí. U uživatelů internetu, kteří se zde pohybují jako v prostoru, kde žijí svůj online život (typicky na sociálních sítích či herních platformách), číhá vyšší riziko viktimizace virtuálním násilím.

Nově vzniklá kategorie kombinující jak majetkový zájem, tak virtuální násilí je charakteristická pro skupinu respondentů, kteří pracují v bezpečnostních službách nebo bankovnictví, finančnictví či pojišťovnictví. U této kategorie se zároveň nejvíce projevoval vliv bezpečnostních návyků. Z proměnných, které se ukázaly být jako signifikantní a nejvíce ovlivňovaly právě kombinovanou viktimizaci, lze vyčíst, že se se jedná o jedince, kteří mají hlubší znalosti online světa včetně využití Toru, dost možná byli i na kurzu bezpečného užívání informačních technologií, ale zároveň se chovají i rizikově. Použili například nalezený paměťový nosič nebo flashdisk bez předchozí kontroly nebo neřeší bezpečnost svých zařízení. Přitom dost možná pracují s financemi či důležitými dokumenty. Jako pozitivní můžeme vnímat zjištění, že téměř každá druhá oběť kombinované viktimizace za rok 2020* nahlásila některý z kyberútoků na policii.

VII.5 Reakce na incident

Respondentům, kteří se (pravděpodobně) stali v roce 2020* obětí některého ze sledovaných jednání, jsme vždy položili otázku, jakým způsobem daný incident řešili – např. „*jak jste zneužití Vašeho internetového bankovnictví řešil/a?*“ Měli možnost vybrat si z nabízených odpovědí zahrnujících nějakou formu vlastní iniciativy (např. „*kontaktoval/a jsem banku*“), dále nahlášení policii a/nebo vyhledání právní pomoci. Mohli také uvést jakoukoliv jinou, vlastní odpověď, případně uvést, proč incident žádným způsobem neřešili. Obvykle také alespoň několik respondentů uvedlo, že neví nebo si nevzpomínají, anebo že nechtějí odpovědět.[251]

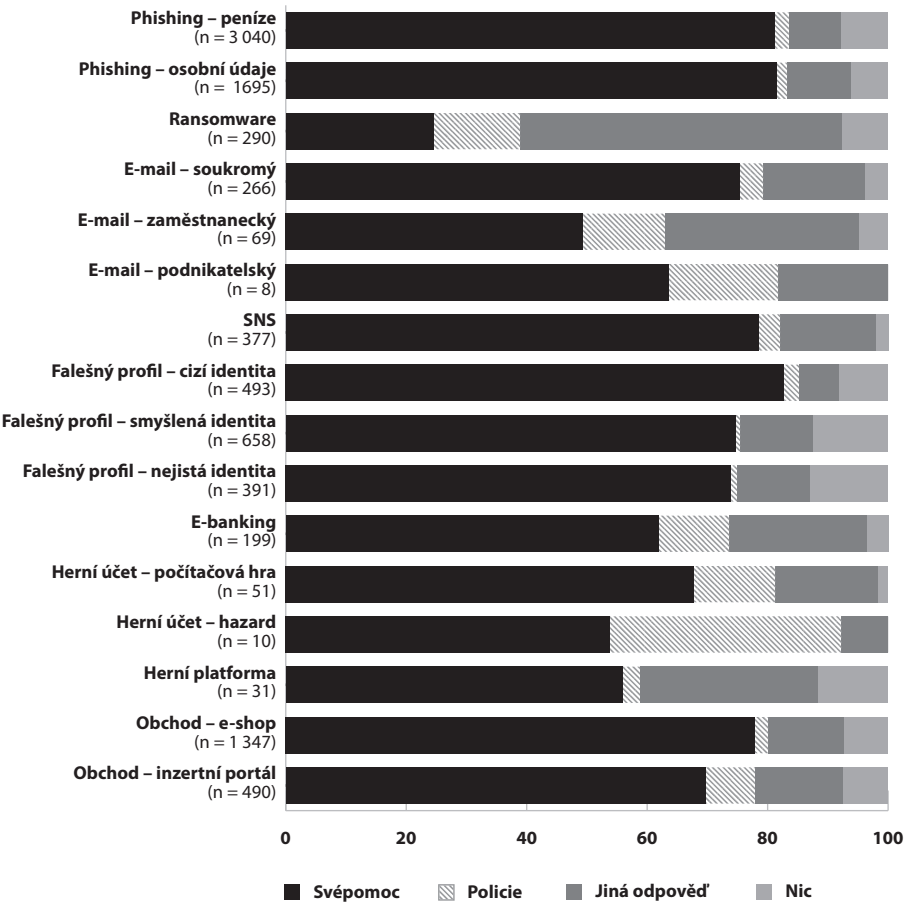
V drtivé většině sledovaných jevů hrála významnou roli snaha řešit nastalý incident vlastními silami (Graf 85). Výjimku představuje negativní zkušenost s ransomwarem, zcela pochopitelná s ohledem na nezbytné IT schopnosti nad rámec běžných uživatelských dovedností. Konkrétně šlo o pokus ověřit důvěryhodnost e-mailu či profilu (phishing a kontakt s falešným profilem na sociální síti), změnu přihlašovacích údajů (zneužití e-mailu, profilu na sociální síti a herních účtů), zrušení online účtu (herní účty), kontaktování osoby kompetentní řešit daný incident (administrátor sociální sítě při kontaktu s falešným profilem, banka při zneužití e-bankingu, prodejce při obchodování online),

250 Ve většině případů definováno jednou z následujících možností: žárlivost, pomsta či osobní nenávist, nesnášenlivost obecně, stalking, žert, zvědavost, sexuální uspokojení.

251 Respondenti mohli uvést vícero odpovědí, pokud se vzájemně nevylučovaly.

smazání phishingového e-mailu, pokus dešifrovat obsah vlastními silami (ransomware), zablokování komunikace s falešným profilem na sociální síti. Někteří respondenti také informovali osoby, jejichž údaje měl někdo zneužít pro falešný profil na sociální síti, či informovali své kontakty o zneužití vlastního e-mailu nebo profilu na sociální síti, potažmo o riziku podvržené komunikace.

Graf 85: Reakce na incident souhrnně (%)



Kategorie „*jiná odpověď*“ zahrnuje jiné než v grafu výslovně uvedené odpovědi, včetně „*nevím, nepamatuji si*“ a „*nechci odpovědět*“ (Graf 85).

Signifikantně významné reakce na incident vykazuje několik skupin respondentů, vždy ovšem pouze ve spojení s konkrétním jevem, případně několika jevy. Za zmínku stojí 36 % respondentů ve věku 30–44 let, kteří nahlásili administrátorovi sociální sítě svůj kontakt s falešným profilem, u kterého si ovšem nebyli jisti, zda využíval cizí nebo zcela smyšlenou identitu, kdežto o něco starší respondenti (21 % osob ve věku 45–59 let) tak naopak významně často nečinili, ba nereagovali na incident vůbec nijak (29 % respondentů v této věkové skupině), podobně jako muži (21 % jich nereagovalo).

Nejmladší věková skupina se významně často obracela na policii v souvislosti se zneužitím jejich e-bankingu (26 % respondentů mladších 29 let).

Signifikantní vztahy v souvislosti s reakcí na incident můžeme nalézt i u obchodování online, liší se nicméně v závislosti na tom, zda šlo o nákup na e-shopu nebo na inzertním portálu. U e-shopu významně často muži dodání vadného zboží nijak neřešili (9 % mužů), kdežto ženy volily tuto odpověď naopak signifikantně méně často (6 %). Respondenti mladší 29 let patřili mezi těch několik málo, kdo vyhledali právní pomoc (3 % respondentů v této věkové skupině). Respondenti vyučení bez maturity významně málo často řešili nastalou situaci kontaktováním e-shopu (76 % v této skupině), naproti tomu respondenti s maturitou (bez vyššího vzdělání) tak činili významně často (85 % osob s nejvýše dosaženou maturitou).

V případě nakupování na inzertních portálech jsou to především ženy, kdo významně často kontaktují kvůli vadnému zboží prodejce (79 % žen), kdežto muži naopak nikoliv (prodejce kontaktuje pouze 71 % mužů). Osoby vyučené bez maturity si významně často nevzpomínají, jak vadné zboží řešily (11 % respondentů v této skupině), vysokoškolsky vzdělaní respondenti jsou si naproti tomu jistí, že vadné zboží nijak neřešili (13 % vysokoškoláků).

Lze shrnout, že většina viktimizovaných respondentů reaguje na incident vlastním řešením a nespoléhá se pouze na iniciativu jiných institucí či organizací. Jen velmi malá část se jich obrací na policii, což potvrzuje předpokládanou vysokou latenci sledovaných jevů, jak ukazuje podrobněji následující kapitola Latence a důvěra ve schopnosti policie.

VII.6 Latence a důvěra ve schopnosti policie

U každého zkoumaného typu jisté viktimizace[252] jsme dále zjišťovali, zda byl útok oznámen policii. Ve sloupci „nahlášeno" přehledové tabulky (Tabulka 33) vidíme počty událostí, které byly policii oznámeny a zároveň jsme je identifikovali jako online viktimizaci. Validní procenta, která jsou uvedena v následujícím sloupci, jsou počítána z počtu obětí dané formy útoku. Obdobně tomu je i v prostřední sekci, kde jsou uvedeny počty dalších nahlášených incidentů, které se týkají dané zkoumané oblasti, ale jako kyber viktimizaci jsme je neidentifikovali. Respondenti totiž mohli nahlásit útok, byť se ve finále nestali jeho obětí (např. neposlali požadované peníze atp.), nebo jsme nemohli jejich viktimizaci objektivně zhodnotit (např. jim bylo dodáno vadné zboží, ale respondent nekontaktoval e-shop či prodejce – nemůžeme tedy s jistotou určit, zda šlo o podvod či pouhou chybu v procesu doručování zboží). Poslední sekce uvádí celkové počty nahlašování v dané oblasti.

Pokud bychom se zaměřili čistě na validní procenta, pak se ukazuje, že nejvíce byly policii oznamovány případy zneužití falešným účtem na sociálních sítích, a to především tehdy, pokud šlo o cizí identitu a došlo k poslání peněz či potvrzovací SMS, případně v případech zneužití podnikatelského e-mailu nebo účtu k hazardní hře. Na druhou stranu u všech těchto případů se jednalo o velmi malé absolutní četnosti.

252 Vysvětlení pojmu „jisté viktimizace" viz kapitola Oběti.

Z těch incidentů, kde byla vyšší prevalence viktimizace, bylo nejvíce nahlášeno napadení zařízení ransomwarem (15 %), zneužití účtu k počítačové hře (10 %), e-bankingu (9 %) či zaměstnaneckého e-mailu (9 %). Ostatní incidenty byly nahlášeny v menší či zanedbatelné míře.

Největší podíl nahlášených incidentů (9 %), které jsme nezařadili mezi online viktimizaci, byl u případů dodání vadného zboží vinou prodejce. Tito respondenti totiž nesplnili podmínku, že by kontaktovali e-shop, nebo jim při případném kontaktu nebylo alespoň částečně vyhověno. Nevíme tedy, jaká by byla případná reakce prodejce. Mohlo se například jednat o nedorozumění či chybu. I přesto však byl případ nahlášen policii, jelikož se respondent mohl domnívat, že kontaktování prodejce nic nevyřeší. V absolutních hodnotách pak bylo nahlášeno dalších 29 případů nakupování přes e-shop, kde obdobně jako při nakupování na inzertním portálu nebyla zřejmá viktimizace podvodem. Z celkového počtu nakupujících přes e-shopy to však tvořila pouhá 3 %.

Početně byly nejvíce hlášeny falešné e-maily požadující poslání peněz. Jednalo se o 77 útoků tohoto typu a dalších 32 e-mailů požadujících osobní údaje. Uvedené zjištění je o to více zajímavé v kontrastu s tím, že byl nahlášen pouze jeden případ, kdy respondent na e-mail „naletěl" a peníze útočníkovi poslal. Zároveň je počet nahlášených útoků požadujících peníze téměř trojnásobný ve srovnání s počtem obětí. Dalo by se tedy říci, že nemalá část respondentů je v případech phishingu uvědomělá a nejen, že se vyhne viktimizaci, ale snaží se i dalším útokům zabránit. V menší míře, ale podobným způsobem, se chovají i někteří uživatelé sociálních sítí, na které někdo takto zaútočil.

Celkově tedy policii nahlásilo alespoň jeden incident 10 % obětí jisté online viktimizace. Dalších 3 % respondentů z celého vzorku tak učinilo i přesto, že jsme je neidentifikovali jako oběti daného deliktu. Z našich dat tedy vyplývá, že 3 % respondentů během posledního roku s policií řešila alespoň jeden online útok, nehledě na to, zda se ve finále stala jeho obětí.

Tabulka 33: Index nahlašování, prevalence za poslední rok

		Nahlášeno		Jisté oběti	Další nahlášení ve zkoumané oblasti		Oblast	Nahlášení celkem
		n	V%	n	n	V%	n	n
Pokud bylo dodáno vadné zboží vinou e-shopu:[253] Vyhověl e-shop Vašim požadavkům? (ne)		2	1,6	126	29	2,7	1 090	31
Pokud bylo dodáno vadné zboží vinou prodávajícího: Vyhověl prodávající Vašim požadavkům? (ne)		10	9,9	101	33	9,0	366	43
Zneužil někdo v uplynulých 12 měsících Váš e-banking?		18	12,6	143	9	0,1	6 338	27
Napadl někdo v uplynulých 12 měsících Vaše zařízení (mobil, PC, notebook, tablet) ransomwarem?		42	14,5	290	0	0,0	6 396	42
Phishing požadující poslání peněz/osobních údajů: odeslal jsem:[254]	*Peníze*	1	3,6	28	77	2,5	3 040	78
	Osobní údaje	0	0,0	35	32	1,9	1 695	32
Zneužil někdo v uplynulých 12 měsících Váš soukromý e-mail?		12	5,5	220	5	0,1	6 584	17
Zneužil někdo v uplynulých 12 měsících Váš zaměstnanecký e-mail?		6	15,8	38	5	0,2	2 650	11
Zneužil někdo v uplynulých 12 měsících Váš podnikatelský e-mail?		2	40,0	5	0	0,0	475	2
Zneužil někdo v uplynulých 12 měsících Váš profil na SNS?		11	4,3	257	7	0,1	5 606	18
Falešný profil na SNS zneužívající cizí identitu: poslal jsem:[255]	*Peníze*	4	44,4	9	18	3,7	493	18
	Potvrzovací SMS	5	41,7	12				
	Osobní údaje	2	18,2	11				
	Intimní obsah	1	20,0	5				
Falešný profil na SNS se smyšlenou identitou: poslal jsem:	*Peníze*	1	25,0	4	7	1,	658	7
	Potvrzovací SMS	1	33,3	3				
	Osobní údaje	1	11,1	9				
	Intimní obsah	0	0,0	7				

253 Návazné otázky: *„bylo Vám v uplynulých 12 měsících dodáno vinou e-shopu/prodávajícího vadné zboží? Jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží."* ➔ *„Jak jste vadné zboží řešil/a?"* Při odpovědi *„snažil/a jsem se získat žádané zboží nebo peníze zpět kontaktováním e-shopu/prodejce"* navázala otázka zahrnutá do tabulky *„vyhověl e-shop/prodávající Vašim požadavkům?"*

254 Návazné otázky: *„přišel Vám v uplynulých 12 měsících falešný e-mail požadující poslání peněz/sdělení osobních údajů?"* ➔ *„Jak jste tento falešný e-mail řešil/a?"* Do tabulky jsou zahrnuty odpovědi *„odeslal/a jsem požadované peníze/osobní údaje."*

255 Pro účet zneužívající cizí identitu, účet se smyšlenou identitou a účet s nejistou identitou platí, že respondenti odpovídali na otázku *„učinil/a jste v rámci kontaktu s falešným účtem některý z následujících kroků?"* jednou z uvedených možností: *„poslal/a jsem peníze,"* *„přeposlal/a jsem potvrzovací SMS,"* *„sdělil/a jsem své osobní údaje,"* *„zaslal/a jsem intimní obsah."*

		Nahlášeno		Jisté oběti	Další nahlášení ve zkoumané oblasti		Oblast	Nahlášení celkem	
		n	V%	n	n	V%	n	n	
Účet s nejistou identitou: poslal jsem:	*Peníze*	2	40,0	5	5	1,3	391	5	
	Potvrzovací SMS	0	0,0	1					
	Osobní údaje	1	33,3	3					
	Intimní obsah	0	0,0	5					
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet k počítačové hře?		5	13,9	36	3	0,3	1 142	8	
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet k hazardní hře?		2	50,0	4	3	0,5	593	5	
Zneužil někdo v uplynulých 12 měsících nějaký Váš účet na herní platformě?		0	0,0	26	1	0,1	719	1	
					N		%	N	%
Index nahlašování		96	**9,5**	1 013	171		**2,5**	233	**3,4**

VII.6.1 Charakteristika (jistých) obětí nahlašujících incidenty

Některý z incidentů v posledním roce nahlásili spíše lidé ve věkové kategorii 25–44 let a pracovníci v bankovní, finanční či pojišťovací sféře, kteří se stali (jistou) obětí některého z online útoků.

Incidenty také více oznamují jedinci, kteří byli na kurzu bezpečného užívání informačních technologií (37 % oproti 21 % těch, kteří jej neabsolvovali) nebo někdy v životě použili Tor (36 % oproti 17 % těch, kteří Tor nepoužili) či cizí paměťovou kartu nebo flashdisk (obzvlášť pokud nebyly předem zkontrolované). Slabší tendence se projevila i v případě vyšší míry nahlašování v případě, že oběť zná darkweb a že se ohledně bezpečnosti nikdo nestará o žádné z užívaných zařízení.

Ze čtyř skupin obětí dle motivace pachatele (viz kapitola Rozlišování virtuálního násilí a majetkového zájmu), výrazně častěji (29 %) některý z útoků nahlásili ti, kdo byli viktimizováni kombinací majetkového zájmu a virtuálního násilí. To se projevuje i při testování úrovně viktimizace (viz kapitola Oběti), kde ze čtyř úrovní logicky vypadla skupina nejistých obětí. Pokud tedy srovnáme jistou násobnou, možnou násobnou a jednoduchou jistou viktimizaci, pak se ukazuje ne příliš silný, ale signifikantní trend: čím vyšší úroveň viktimizace byla zjištěna, tím spíše respondent některý z online incidentů nahlásil.

VII.6.2 Ostatní ohlašování

V našich datech se ukázal nezanedbatelný podíl respondentů (3 %), kteří policii oznámili některý z kyberútoků, zároveň ale jistě nevíme, že by se stali jeho obětí. Například je poměrně běžné, že respondenti, které jsme označili za jisté oběti, nahlásili jak daný incident, tak ještě nějaký další útok, u něhož jsme viktimizaci již s jistotou nemohli určit (35 %). Naopak jisté oběti, které danou viktimizaci s policií neřešili, nahlásili nějaké další alespoň podezřelé online chování spíše výjimečně (2 %).

Vzhledem k tomu, že se tato ostatní ohlašování vztahují k celému vzorku respondentů, tak zjištěné míry asociací jsou u všech indikátorů velmi slabé. Můžeme tedy hovořit pouze o slabých náznacích. Např. se ukazuje, že kyberútoky takto nahlašují spíše muži, mladší respondenti do 35 let, lidé v nesezdaném partnerském vztahu, studenti, zaměstnanci s podřízenými a podnikatelé, pracovníci v bankovnictví, finančnictví či pojišťovnictví. Z bezpečnostních návyků jde spíše o lidi, kteří někdy byli na kurzu bezpečného užívání informačních technologií, znají darkweb, někdy použili Tor, nemají nikoho, kdo se stará o některé z jejich zařízení, nezabezpečují se, či použili nalezenou flešku bez její následovné kontroly.

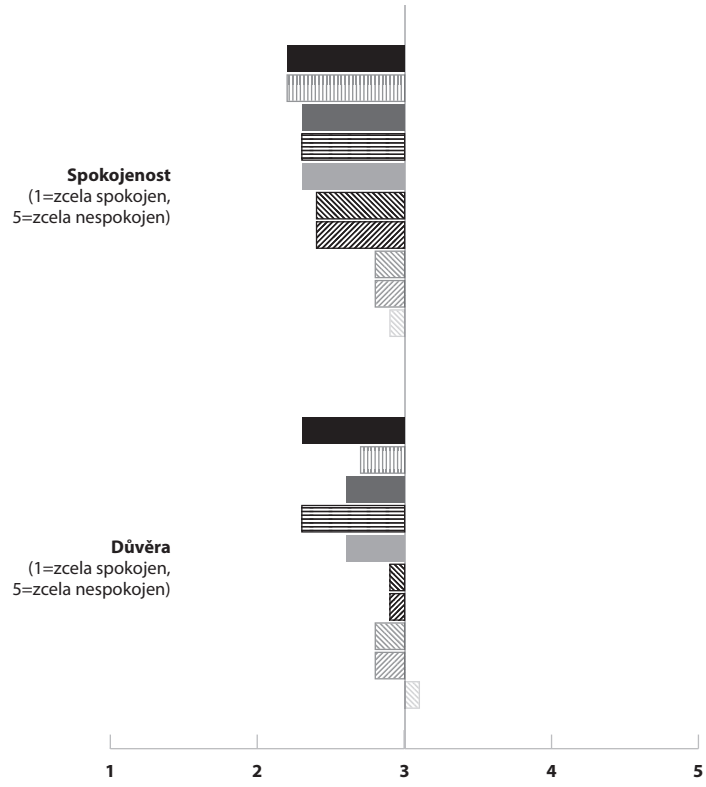
VII.6.3 Spokojenost s přístupem policie

Respondentů jsme se následovně ptali, zda byli spokojeni s policií, a to na škále od zcela spokojen po zcela nespokojen, kdy jsme na střed škály přidali respondenty, kteří nemají jednoznačný názor. Obecně by se dalo říci, že respondenti byli až na výjimky relativně spokojeni (Graf 86). Detailní přehled hodnocení je k vidění v následující tabulce (Tabulka 34).

V rámci hodnocení policie se objevuje i zdánlivý paradox. Například můžeme pozorovat poměrně značný rozdíl v hodnocení policie u obětí podvodu při nákupu na e-shopu (2,2) oproti těm, které podvedl prodávající (2,9). Vysvětlující mohou být rozdílné možnosti policie při řešení daných případů, což naznačuje i důvěra těchto obětí ve schopnost policie daný případ vyřešit.[256] Zatímco oběti podvodu na e-shopu spíš policii věří (2,7), tak oběti podvodu u prodejce se překlápějí do více negativního hodnocení (3,1).

256 Měřeno otázkou *„daří se podle Vás policii objasňovat… (pozn.: doplněn vždy daný typ jednání, např. zneužití internetového bankovnictví)?"* Hodnoceno na škále 1 = rozhodně ano, 5 = rozhodně ne, blíže k tomu viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

Graf 86: Spokojenost s policií a důvěra ve schopnosti policie očima obětí dílčích útoků[257]



- **Zneužití e-bankingu** (n=27)
- **Vadné zboží** (e-shop, n=31)
- **Zneužití profilu na SNS** (n=18)
- **Zneužití e-mailu** (zaměstnanecký, n=11)
- **Ransomware** (n=42)
- **Phishing** (osobní údaje, n=32)
- **Phishing** (peníze, n=78)
- **Zneužití falešným profilem** (cizí identita, n=18)
- **Zneužití e-mailu** (soukromý, n=17)
- **Vadné zboží** (inzertní portál, n=43)

257 Graf nezobrazuje hodnocení obětí útoků, které se vyskytnuly v počtu menším než 10.

Tabulka 34: Přehled hodnocení spokojenosti s policií a důvěry ve schopnost policie objasňovat dané typy kyberkriminality očima obětí dílčích útoků

		Nahlášení celkem				
			Spokojenost		Důvěra	
		n	Ø	SD	Ø	SD
Pokud bylo dodáno vadné zboží vinou e-shopu:[258] Vyhověl e-shop Vašim požadavkům?		31	2,2	1,3	2,7	1,5
Pokud bylo dodáno vadné zboží vinou prodávajícího: Vyhověl prodávající Vašim požadavkům?		43	2,9	1,4	3,1	1,3
Zneužil někdo v roce 2020* Váš e-banking?		27	2,2	1,4	2,3	1,4
Napadl někdo v roce 2020* Vaše zařízení ransomwarem?		42	2,3	1,3	2,6	1,5
Phishing požadující poslání peněz/ osobních údajů: odeslal jsem:[259]	*Peníze*	78	2,4	1,4	2,9	1,3
	Údaje	32	2,4	1,4	2,9	1,6
Zneužil někdo v roce 2020* Váš soukromý e-mail?		17	2,8	1,8	2,8	1,3
Zneužil někdo v roce 2020* Váš zaměstnanecký e-mail?		11	2,3	1,0	2,3	1,4
Zneužil někdo v roce 2020* Váš profil na SNS?		18	2,3	1,4	2,6	1,5
Profil na SNS zneužívající cizí identitu:		18	2,8	1,7	2,8	1,4

VII.6.4 Důvěra ve schopnosti policie

Důvěra v policii[260] je oproti spokojenosti o něco slabší. Obecně se pohybovala spíše ve druhé polovině hodnotící škály (Graf 87). Výjimku tvořili právě ti respondenti, kteří měli s policií osobní zkušenost, protože útok nahlásili. Pravděpodobně i díky tomu se ukázaly být více důvěřivé oběti kombinace majetkového zájmu a virtuálního násilí,[261] které útoky více nahlašovaly. Oběti, které policii nekontaktovaly, naopak spíše nevěřily, že by byla schopna daný případ vyřešit, což může být i důvodem nenahlášení daného incidentu.

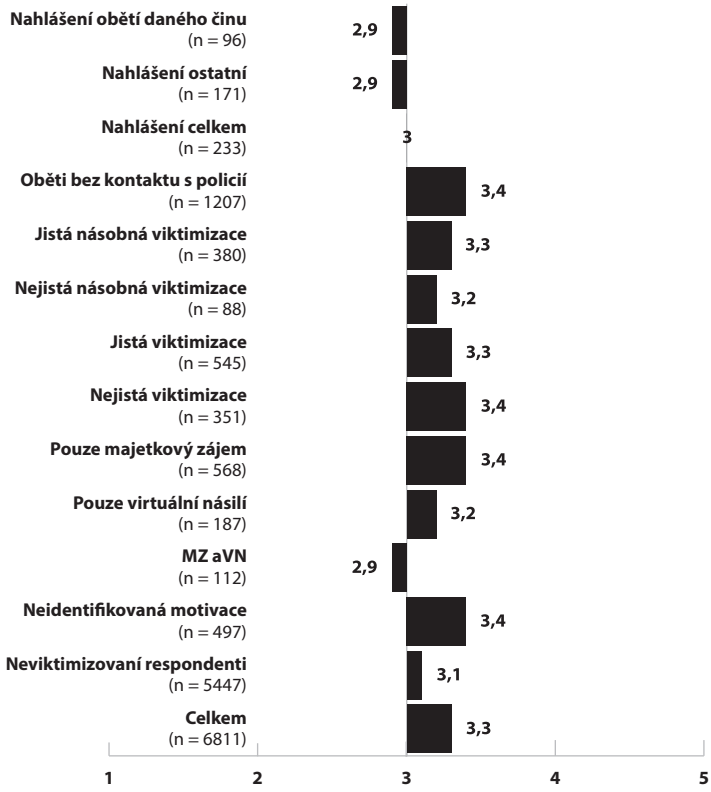
258 Návazné otázky: *„bylo Vám v uplynulých 12 měsících dodáno vinou e-shopu/prodávajícího vadné zboží? Jde o výrazně horší kvalitu, jiné množství, nedodání zboží nebo dodání zcela jiného zboží.“* ➔ „Jak jste vadné zboží řešil/a?“ Při odpovědi *„snažil/a jsem se získat žádané zboží nebo peníze zpět kontaktováním e-shopu/prodejce“* navázala otázka zahrnutá do tabulky *„vyhověl e-shop/prodávající Vašim požadavkům?“*

259 Návazné otázky: *„přišel Vám v uplynulých 12 měsících falešný e-mail požadující poslání peněz/sdělení osobních údajů?“* ➔ *„Jak jste tento falešný e-mail řešil/a?“* Do tabulky jsou zahrnuté odpovědi *„odeslal/a jsem požadované peníze/osobní údaje.“*

260 Jak je již uvedeno výše, měřeno otázkou *„daří se podle Vás policii objasňovat (…)?“* Hodnoceno na škále 1 = rozhodně ano, 5 = rozhodně ne, blíže k tomu viz kapitola Tematické okruhy, formulace otázek a používaná terminologie.

261 Vysvětlení pojmů viz kapitola Rozlišování virtuálního násilí a majetkového zájmu.

Graf 87: Důvěra ve schopnosti policie objasňovat dané typy kyberkriminality ve vztahu k různým typům obětí[262]



VII.6.5 Závěr k latenci a důvěře ve schopnosti policie

Podle našich dat je kyberkriminalita v České republice značně latentním jevem. Méně než každá desátá oběť ohlásí některý z útoků na policii. Například ve srovnání s aktuálním obecným viktimizačním výzkumem (Roubalová et al., 2023) byla nejvyšší latence zjištěna v případech domácího násilí či sexuálního násilí, které jsou ohlašovány v přibližně 15 %. Na druhou stranu některý z incidentů s policií řešila necelá třetina obětí kombinovaného útoku majetkového zájmu a virtuálního násilí. Zároveň existuje i nezanedbatelná skupina dotazovaných, která nějaký podezřelý případ policii nahlásila, ale nelze s jistotou určit, zda se stali či nestali obětí daného útoku. Část z nich se dokonce s jistotou obětí nestala, ale přesto policii např. pokus o phishing či jiný typ útoku nahlásila.

Práci policie hodnotí respondenti, kteří s ní mají zkušenost, poměrně pozitivně. V rámci řešení většiny sledovaných útoků bylo průměrné hodnocení policie spíše v první půlce hodnotící škály. To je lepší výsledek, než ukazuje reprezentativní výzkum na celé české populaci, kde respondenti na pětibodové škále v průměru hodnotili spokojenost s policií

262 K vysvětlení typologie jisté a nejisté viktimizace viz kapitola Oběti, k typologii čtyř typů viktimizace dle motivace pachatele viz kapitola Rozlišování virtuálního násilí a majetkového zájmu.

známkou 3,3 (Krulichová & Buriánek Eds., 2020). Pozitivní hodnocení policie v kontextu řešení kyberútoků se odráží i na větší důvěře, že se jim daný případ podaří vyřešit. To ovšem nelze říci o obětech, které policii nekontaktovaly, které spíše projevovaly nedůvěru ve schopnost policie daný případ vyřešit. To mohlo být i jedním z důvodů, proč případ nenahlásily.

VIII.

Závěr

Poznatky získané dotazníkovým šetřením rezonují s výsledky jiných studií, ať už se podíváme na jiné české projekty, zejména viktimologický výzkum realizovaný v IKSP (podílí se na něm např. M. Roubalová nebo H. Přesličková), nebo na zahraniční studie nahlížející kyberkriminalitu prizmatem sociálních věd (např. R. Leukfeldt, S. van t'Hoff nebo A. Bossler). Společně ukazují obrázek kyberkriminality, která může bez dalšího rozlišení zasáhnout prakticky kohokoliv. Probíhají samozřejmě snahy identifikovat významné kriminogenní faktory, ale prozatím se zdá, že nic takového není, resp. dosud odhalené kriminogenní faktory mají jen relativně malý vliv, jak ukazují i naše analýzy zde nastíněné (zejména shrnující závěrečné kapitoly věnující se pachatelům a obětem).

Situace se však změní v okamžiku, kdy opustíme všeobjímající hledisko kyberkriminality jako takové a zaměříme pozornost na konkrétní oblasti, jako jsou phishing nebo ransomware, zneužívání online účtů, porušování autorských práv atp.[263] Do popředí vystupují určité skupiny, typicky ženy nebo muži, různé věkové kategorie (nejčastěji osoby mladší 29 let a/nebo naopak starší generace), úroveň vzdělání (opět především krajní strany škály – základní a/nebo vysokoškolské vzdělání), profesní zaměření (nejvýrazněji IT odborník nebo u analýzy trestních spisů řidič spediční firmy). Určitou roli mohou hrát také vlastní bezpečnostní návyky uživatelů, typicky ne/sdílení přihlašovacích údajů.

Pakliže dochází k viktimizaci či neoprávněnému jednání, mezi aktéry převažují vzájemně si nejbližší osoby, ať už partneři nebo členové úzkého rodinného kruhu. Nemusí přitom vždy jít o jednání trestné, přesto ho sami respondenti označili za nějak neoprávněné. Jako možné vysvětlení se nabízí pokulhávající institut soukromí, jehož koncept a především vnímání aktéry se v offline prostředí vyvíjí odnepaměti, kdežto online svět nabízí ještě donedávna netušené možnosti sledování. Domníváme se, že mnozí uživatelé nad respektem vůči soukromí druhého online vůbec neuvažují a bez váhání jednají tak, jak by je v offline prostředí ani nenapadlo (např. ze zvědavosti si detailně prohlédnou finanční situaci partnera, čtou soukromou komunikaci dospívajících dětí, žertem přebírají identitu jiného atp.). Dotčené osoby přitom mohou právem pociťovat jednání jako újmu a zásah do vlastního soukromí. Něco zhola jiného je samozřejmě záměrné protiprávní jednání, ať už motivované penězi, zvědavostí, žárlivostí či jinak.

Pohled na kyberkriminalitu, resp. počítačové trestné činy doplňují poznatky z analýzy trestních spisů. Jen pro úplnost zdůrazňujeme, že jde výlučně právě o počítačové trestné činy (§ 230–232 TZ), tedy pouze o určitou výseč kyberkriminality (nikdy např. nezachytí podvodné jednání falešného účtu se smyšlenou identitou). Z hlediska sociodemografických charakteristik jednání pravomocně odsouzená v roce 2019 relativně navazují na poznatky z roku 2015. Čas od času slyšíme poukazování na nárůst kyberkriminality demonstrovaný rostoucím počtem počítačových trestných činů v desítkách procent, konkrétní data však (co do počítačových trestných činů) nic tak výrazného neukazují. A to tehdy, když odebereme kategorii jednání spočívajících v neoprávněné manipulaci s tachografy, která představuje přinejmenším za rok 2019 plnou třetinu odsouzených počítačových trestných činů (kdežto v roce 2015 bylo takto souzeno pouze několik osob).

263 Nezbytnost věnovat se samostatně obětem různých jednání potvrzují i nejnovější probíhající zahraniční studie (van't Hoff-de Goede et al., 2023).

Naším zájmem bylo především rozšířit poznatkovou bázi relevantní pro české prostředí, a poskytnout tak podložená data jak pro orgány činné v trestním řízení, tak pro preventivní aktivity. Obě skupiny mohou nyní čerpat z informací nejen od obětí a pachatelů, na které se pochopitelně orientují především, ale vztažené na českou internetovou populaci vůbec, což může výrazně ovlivnit úhel pohledu (např. obrácení pozornosti od „neznámého hackera" k partnerovi).

Co se týče preventivních doporučení, je nezbytné odvíjet je od konkrétních oblastí a skupin uživatelů. Obecně lze říci, že v souvislosti s prevencí obvykle zmiňovaní senioři se zdají být relativně obezřetní, což podává dobré vysvědčení dosavadnímu preventivnímu úsilí ze strany řady organizací. Specifickou skupinu tradičně tvoří také naopak mladší osoby, v našem vzorku v kategorii 16–29 let. Vynikají orientací v kyberprostoru, z hlediska bezpečnostních návyků se ovšem zdají spíše lehkovážní (za zmínku stojí také jejich častější důvěra v policii). Muži vystupují sebevědoměji než ženy, v některých oblastech zřejmě oprávněně (např. odhalení phishingu).

Napříč širokou oblastí používání online účtů vidíme časté sdílení přihlašovacích údajů, včetně těch k e-bankingu. Dotýká se to zejména (nikoliv ovšem výlučně) nejbližších osob, které však zároveň patří k nejčastějším aktérům na obou stranách. To je poznatek, který dosud v preventivních aktivitách nezaznívá, přestože by mělo nesdílení přihlašovacích údajů (spolu s respektem vůči soukromí druhých, včetně nejbližších osob) patřit mezi základní návyky kyberhygieny. Podobně jako opatrnost spojená s fyzickým přístupem k zařízení používaným k přístupu na internet, ve kterých bývají přihlašovací údaje uložené nebo které slouží k autentizaci uživatele při přístupu do jinak nedostupných aplikací.

Prezentované dotazníkové šetření, potažmo získaná data mají samozřejmě své limity. Jejich velká výhoda spočívající v kombinaci viktimizačního a self-reportového šetření je zároveň i slabou stránkou. Usilovali jsme o co největší srovnatelnost otázek a odpovědí, nicméně některé self-reportové otázky jsme raději formulovali „mírněji", abychom respondenty neodradili od odpovědí. Např. při dotazech směřujících na motivaci měli respondenti coby oběti k dispozici širokou škálu možných odpovědí (včetně např. „*pomsta*", „*stalking*" atp.), kdežto možní pachatelé vybírali mezi penězi a zvědavostí, případně mohli uvést jakoukoliv vlastní odpověď. Podobně jsme používali u respondentů coby možných obětí formulaci „*neoprávněné použití účtu*", kdežto u možných pachatelů „*použití účtu bez výslovného souhlasu jeho majitele*". Rozhodnutí o oprávněnosti jednání jsme záměrně nechávali na posouzení samotných respondentů, neboť nám v tomto směru nešlo o objektivní zhodnocení protiprávnosti či trestnosti, ale o subjektivní dojem respondentů (zda sami vnímají zasažení, či nikoliv).

Jiné omezení vyplývá z využití metody CAWI (online dotazování). Námi preferovanou metodu CAPI nebylo možné realizovat vzhledem k omezením osobních kontaktů v období sběru dat v důsledku vládních opatření spojených s pandemií covid-19. Vzhledem k zaměření dotazníku na zkušenosti v online prostředí se však domníváme, že použití online formuláře je zcela namístě. Vyřazuje sice a priori z účasti osoby, které internet nepoužívají, ty by nicméně v případě jiné metody nepostoupily dále než k první otázce „*používáte internet?*" K dispozici jsou samozřejmě pouze data ohledně respondentů ochotných vyplnit celý dotazník (resp. jeho relevantní části), kteří byli v době sběru dat zařazeni do využitého

panelu možných respondentů. Velikost dostupného online panelu byla proto zohledněna při volbě realizátora šetření ve výběrovém řízení, abychom minimalizovali případný vliv složení daného panelu.

Výběr vzorku „internetové populace ČR" představoval určitý oříšek. Mohli jsme si ovšem dovolit kvótní výběr, protože „internetová" populace vcelku kopíruje dle údajů ČSÚ a SPIR složení obyvatel ČR, dílčí odlišnosti byly zohledněny při odhadu konkrétních kvót. Nadreprezentování některých kategorií způsobené dobíráním respondentů po vyřazení nedůvěryhodných dotazníků bylo jen mírné.

Určité zkreslení může vycházet ze specifik roku 2020*, kdy se v důsledku pandemie covid-19 začaly v online prostředí výrazněji pohybovat i osoby, které tak do té doby činily jen výjimečně, nebo se rozšířila škála jejich aktivit a doby strávené online. Mohly se zde objevit jak potenciální neznalé oběti, tak noví pachatelé. Také jsme při více incidentech zpravidla žádali respondenty, aby vypovídali ohledně toho, který sami považují za nejzávažnější, což mohlo ovlivnit prevalenci (některý z jevů mohl být např. výrazně častější, leč vnímaný jako méně závažný, a tudíž se nedostal do našeho výběru).

Své limity má pochopitelně i analýza trestních spisů. Předně zahrnuje výlučně počítačové trestné činy (§ 230–232 TZ), a tedy zachycuje jen relativně specifickou výseč kyberkriminality, která zpravidla spočívá zjednodušeně v neoprávněném přístupu k informačnímu systému nebo v neoprávněné manipulaci s daty. Významnou část kyberkriminality, spočívající v různých formách podvodného jednání a/nebo páchání virtuálního násilí, však nemusí zachytit. Buď proto, že součástí jednání není onen neoprávněný přístup nebo manipulace s daty, anebo orgány činné v trestním řízení nepovažovaly za nutné subsumovat dané jednání pod skutkovou podstatu (mimo jiné) některého z počítačových trestných činů. Nemluvě samozřejmě o úbytku případů v postupu od zjištěných po objasněné, přes podání obžaloby až po pravomocné odsouzení.

Za zmínku pak stojí ještě i zde třetina trestních spisů vedených k neoprávněné manipulaci s tachografy, neboť může výrazně ovlivnit výsledný obrázek počítačových trestných činů, ačkoliv lze takové jednání jen obtížně řadit do kyberkriminality. Při práci s veřejně dostupnými statistickými údaji je proto nezbytné mít na paměti, že počítačové trestné činy zahrnují ve významné míře i tato jednání.

Předložené dotazníkové šetření spolu s analýzou trestních spisů jsou výzkumem kyberkriminality, který nemá v České republice obdoby a patří svým rozsahem mezi významná šetření i na mezinárodní úrovni. Obsáhl řadu jednání, z nichž každé by zasloužilo významnou pozornost samo o sobě. Představuje proto unikátní zdroj dat, ze kterých bude možné bohatě čerpat i v budoucnu, a která poskytují vynikající základ pro další výzkum.

V centru pozornosti se objeví nepochybně oběti kyberkriminality, tentokrát již ovšem specifikované v návaznosti na určitá jednání. Pozornost se v současnosti stále více zaměřuje i na fyzickou ochranu používaných zařízení. Pachatelé budou jistě v hledáčku výzkumníků i nadále, nicméně v jejich případě je více než jinde podstatné rozlišovat oblast jejich nelegálních aktivit. Co se týče konkrétních jednání, bylo by vhodné upřít pozornost zejména

na různé formy virtuálního násilí. Na jedné straně stojí (snad méně závažné) porušování soukromí (bez dalšího), na straně druhé pak vztahově orientované virtuální násilí, které se objevuje v hojné míře v trestních spisech i v dotazníkovém šetření.

Bez ohledu na to, kterým směrem se budoucí výzkum bude nakonec ubírat, význam kyberprostoru a potažmo kyberkriminality jistě nepoleví. Naopak se domníváme, že spolu s rostoucím provázáním kyberprostoru s každodenními činnostmi bude postupně klesat význam rozlišování virtuálních aktivit oproti těm ostatním, a úměrně tomu poroste zájem na jejich porozumění.

Resumé

Publikace předkládá výsledky výzkumného úkolu Institutu pro kriminologii a sociální prevenci „Posouzení trendů kyberkriminality", kterým se zabýval v letech 2020–2023 pod vedením odpovědné řešitelky Mgr. Kateřiny Kudrlové, Ph.D., tým sestávající z Mgr. Jiřího Vlacha a Mgr. Viktorie Paloušové (v počátcích projektu též Mgr. Lukáše Kutila). Projekt zahrnoval rozsáhlé dotazníkové šetření zaměřené na vybrané zkušenosti online a analýzu trestních spisů vedených o počítačových trestných činech. S výsledky seznamujeme širokou i odbornou veřejnost zejména prostřednictvím této publikace, dále prostřednictvím dílčích článků a konferenčních vystoupení.

Tematické okruhy dotazníku vycházejí z výsledků předchozí analýzy trestních spisů vedených o počítačových trestných činech v roce 2015 (zjednodušeno) a rešerše veřejně dostupných statistických údajů relevantních pro kyberkriminalitu. Zaměřují se jednak na oblasti, ve kterých je jen málo nebo nejsou žádná dostupná data k dispozici (např. sdílení přihlašovacích údajů k různým online účtům), jednak na zpřesnění a prohloubení jinak dostupných dat (např. rozlišení phishingu požadujícího peníze oproti žádostem o osobní údaje). Získaná data tak zahrnují zařízení používaná k aktivitám online a jejich ochranu, vybrané uživatelské schopnosti a zkušenosti s neoprávněným jednáním: ransomwarem, phishingem, zneužíváním online účtů (e-maily, profily na sociálních sítích, e-banking, herní účty), podvody při obchodování online a porušováním autorských práv. Respondenti odpovídali jak coby možné oběti, tak formou self-reportu coby možní pachatelé.

Sběr dat realizovala profesionální společnost metodou CAWI v listopadu roku 2020, přičemž drtivá většina údajů se vztahuje přibližně k roku 2020 („*uplynulých 12 měsíců*", dále jen „2020*"). Objemný výsledný vzorek 6 811 respondentů reprezentuje českou internetovou populaci ve věku 16–74 let (kvótní výběr respektující pohlaví, věk, vzdělání, kraj a velikost místa bydliště). Data byla zpracována s využitím softwaru SPSS.

Analýza trestních spisů zahrnula prakticky 100 % trestních řízení vedených o tzv. počítačových trestných činech (§ 230–232 TZ), jejichž pachatel byl pravomocně odsouzen v roce 2019. Sledováno bylo několik desítek znaků, od sociodemografických charakteristik přes modus operandi po vybrané okolnosti trestního řízení.

Nyní již několik slov k výsledkům samotným, nejprve z dotazníkového šetření. Respondenti používali nejčastěji mobily, další hojně zastoupené byly notebooky a o něco méně stolní počítače. Zdaleka nejvíce zařízení je soukromých, výrazně méně zaměstnaneckých, několik i podnikatelských (soukromá určená výlučně k pracovním aktivitám). Používají nejčastěji Android (mobily) a Windows (počítače) a bývají s výjimkou mobilních telefonů zabezpečena antivirem. Pečují o ně převážně uživatelé sami, případně s pomocí IT odborníků (zejména zaměstnanecká zařízení). Sdílena jsou zařízení nejčastěji s partnery a osobami z úzkého rodinného kruhu, zaměstnanecká i s kolegy. Část zařízení byla v roce 2020* napadena ransomwarem (nižší jednotky procent), útoky zasahují častěji počítače než mobily. Muži se častěji snaží vyřešit situaci vlastními silami, ženy a mladí respondenti se častěji obracejí na policii (řádově 15 % napadených).

Drtivá většina respondentů používala v roce 2020* e-mail. Pětina z nich se v té době setkala s phishingem požadujícím osobní údaje, 40 % pak s phishingem požadujícím poslání peněz, velmi zhruba polovina respondentů v každé skupině opakovaně. Oba typy

phishingu zřejmě lépe odhalují muži a vysokoškoláci, kdežto ženy jim častěji podléhají. Rozesílatelů phishingu nebylo v roce 2020* mnoho (zejména muži a osoby mladší 29 let), jednali však opakovaně.

E-maily bývají zabezpečeny silnými hesly, respondenti je však často sdílejí s dalšími osobami, nejčastěji z úzkého rodinného kruhu a partnery. Část z těchto osob pak znalost hesla zneužije k získání neoprávněného přístupu k e-mailu, častým způsobem je také fyzický přístup ke konkrétnímu zařízení. Celkově se zkušenost s neoprávněným přístupem k e-mailu pohybuje v jednotkách procent aktérů na obou stranách. Oběti detekují zejména jednání zanechávající patrné stopy (změna hesla, smazání obsahu, převzetí identity v podobě komunikace jménem majitele e-mailu atp.), kdežto pachatelé znatelně častěji hovoří o pouhém prohlédnutí obsahu. Oběti často předpokládají neoprávněný přístup ze strany neznámého hackera, z pohledu pachatelů jde ovšem výrazně častěji o přístup na online účet jejich partnerů, případně osob z úzkého rodinného kruhu, motivovaný zvědavostí či žárlivostí.

Při sebeprezentaci vystupují sebevědomě především muži a osoby mladší 29 let. Respondenti hojně využívají sociální sítě, nejčastěji Facebook. Téměř polovina má nějakou představu o darkwebu, mladí uživatelé a muži mnohdy i osobní zkušenost s ním. I zde mají jednotky procent zkušenost s neoprávněným použitím profilu na sociální síti, o něco více osoby mladší 29 let. Poznatky se výrazně shodují se zjištěními v oblasti zneužívání e-mailů: k hlavním aktérům na obou stranách patří partneři a osoby z úzkého rodinného kruhu, docházelo ke zneužívání známého hesla a fyzického přístupu a detekované jednání oproti deklarovanému se výrazně odlišovalo. Oproti majetkovému zájmu převládalo virtuální násilí, předpokládaly ho zejména osoby mladší 29 let (muži častěji peníze). I zde převládaly zvědavost a/nebo žárlivost.

Respondenti také komunikovali a sami využívali falešné profily se smyšlenou nebo cizí identitou. Zhruba desetina z nich něco požadovala – falešné profily s cizí identitou vyhledávaly spíše finanční profit, profily se smyšlenou identitou častěji intimní komunikaci. Kontaktovaní respondenti častěji hovořili o falešném profilu se smyšlenou dívčí/ženskou identitou, sami respondenti však používali častěji naopak smyšlenou chlapeckou/mužskou identitu. Je možné, že smyšlená chlapecká/mužská identita je hůře odhalitelná, anebo jsou respondenti vůči dívčím/ženským profilům obezřetnější. Profily s cizí identitou se inspirovaly nejčastěji mediálně známými osobnostmi.

Zneužívání e-bankingu evokuje oproti sociálním sítím a e-mailům jednoznačně finanční motivaci, ve skutečnosti ovšem zaujímá z pohledu pachatelů významné místo pouhá zvědavost. I zde přichází ke slovu značný podíl neoprávněných aktivit umožněných sdílenými přihlašovacími údaji. Také z hlediska aktérů se zneužívání e-bankingu výrazně podobá zkušenostem s e-maily a sociálními sítěmi.

Celkově lze u online účtů shrnout, že patrně dochází k řadě nedetekovaných neoprávněných přístupů. Aktéry jsou stávající partneři pohánění zvědavostí a využívající dřívější znalosti hesla či sdílení zařízení s partnerem, případně fyzického přístupu ke konkrétnímu zařízení, přičemž jejich aktivita zůstává skryta, neboť si „pouze" prohlížejí jinak skrytý obsah.

Poněkud odlišný obrázek se ukazuje u herních účtů. I zde je sice patrná disproporce mezi výpověďmi respondentů na straně obětí a na straně pachatelů, převažující motivací je ovšem samotné hraní (vyjma hazardních her).

Většina respondentů (přes 90 %) nakupuje online na e-shopech, přičemž zhruba pětina z nich se v roce 2020* setkala s dodáním vadného zboží vinou e-shopu, většinou v hodnotě do 2 tis. Kč. Tři čtvrtiny z nich následně požadovaly po e-shopu nápravu a shodně zhruba tři čtvrtiny se nějaké nápravy skutečně domohly. Necelá polovina respondentů nakupuje na inzertních portálech, necelé pětině pak bylo dodáno v roce 2020* také vadné zboží (opět nejčastěji v hodnotě do 2 tis. Kč). I zde se zhruba tři čtvrtiny obrátily na prodejce, plné nápravy se však domohla pouze necelá polovina respondentů (další pětina pak alespoň částečné nápravy). Několik desítek respondentů samo zboží prodávalo přes e-shop a necelá třetina přes inzertní portály, nicméně většina z nich se vyvarovala dodání vadného zboží (tři čtvrtiny e-shopů a přes 90 % prodejců na inzertních portálech).

Zhruba dvě třetiny respondentů stahovaly v roce 2020* nějaký obsah, přičemž zhruba čtvrtina z nich uvedla nelegální hudbu nebo filmy a desetina software (např. počítačové hry). Část respondentů (méně než desetina) také sama v roce 2020* nelegální obsah zpřístupňovala ostatním. Převažující motivací byla příliš vysoká cena legálního přístupu, u softwaru pak přistupovalo téměř stejně často potěšení z vlastních schopností. Převažujícím věkem byla kategorie do 24 let, v souhrnu do 34 let (zhruba tři čtvrtiny).

Mezi zaměstnanci s přístupem do jinak neveřejného informačního systému se našlo několik desítek osob, které v roce 2020* zneužily svého přístupu nad rámec svých oprávnění nebo zneužily přístup kolegy. Mimoto zhruba pětina respondentů nalezla někdy cizí paměťový nosič, přičemž téměř polovina z nich ho použila, z toho téměř polovina bez jakékoliv předchozí kontroly případného ukrytého malwaru. Činili tak ovšem převážně v soukromých zařízeních.

Při sledování pachatelů a obětí jsme vytvořili index viktimizace a index páchání. Mezi pachateli se koncentrují mladší jedinci, nicméně výrazný vliv zde může mít digitální pirátství. K viktimizaci dochází nejčastěji na sociálních sítích a zneužitím soukromého e-mailu, obecně však nelze poukázat na nějaký konkrétní sociodemografický či jiný rys specifický pro oběti kyberkriminality. Zjištěné vztahy jsou spíše jen slabými náznaky. Ohroženější se zdají mladí lidé, ti však zároveň výrazně častěji s digitálními technologiemi běžně pracují. Míra vlastního zabezpečení nemá na viktimizaci větší vliv. Kromě toho detekované útoky (např. neoprávněné použití online účtu) mohou vypovídat více o schopnosti takové útoky detekovat než o samotné jejich prevalenci.

Potvrdila se značná latence sledovaných jevů, celkově na úrovni zhruba desetiny jednání oznámených na policii. Tendenci nahlásit alespoň některý z útoků vykazují zejména polyviktimizovaní jedinci. Ti, kdo se na policii přesto obrátí, bývají s její prací spíše spokojeni.

Co se týče výsledků analýzy trestních spisů za rok 2019, navazují na předchozí zjištění z roku 2015. Mezi odsouzenými převažují muži, v polovině případů souzeni pro souběh počítačového a jiného trestného činu. Více než polovina byla prvopachateli. Věková struktura se oproti roku 2015 o něco změnila, když klesl celkový podíl mladších pachatelů.

Patrně se postupně stírá (a bude rozmělňovat i nadále) rozdíl mezi staršími generacemi a generacemi vyrůstajícími již v prostředí digitálních technologií. Výši uložených trestů ovlivňují z velké části sbíhající se trestné činy, zpravidla přísněji trestné. Ze 158 sledovaných případů se vyskytlo 50 věcí spočívajících v neoprávněné manipulaci s tachografy.

Poznatky z analýzy trestních spisů je však třeba brát s výhradou znění skutkových podstat počítačových trestných činů. Dle našeho názoru neodpovídá přiléhavě sociální realitě, vychází však z mezinárodních závazků. Přesto by zde mohl být určitý prostor k částečné dekriminalizaci. Ta je žádoucí především proto, aby hrozba trestněprávního postihu nedopadala na relativně běžné jednání s malou újmou způsobenou obětem, zatímco závažnější případy by byly i nadále postihnutelné.

Jako významné téma pro budoucí výzkum kyberkriminality v rámci Institutu pro kriminologii a sociální prevenci se jeví virtuální násilí, páchané zejména mezi partnery. Ti představují specifickou skupinu, která nečekaně vystoupila do popředí v souvislosti se zneužíváním online účtů motivovaným jinak než penězi.

Summary

Kudrlová, K., Paloušová, V. & Vlach, J. (2023). Cybercrime from the perspective of justice system and everyday users a IKSP.

The publication presents findings of the research conducted by the Institute for Criminology and Social Prevention „Assessment of cybercrime trends". Team led by Dr. Kateřina Kudrlova was working on it between 2020 and 2023. The project consisted of an extensive questionnaire survey focused on selected online experiences and analysis of criminal files on cybercrimes. Results are presented to the general and professional public mainly through this publication, as well as through several articles and conference presentations.

Topics of the questionnaire are based on results of the previous analysis of criminal files related to cybercrime in 2015 (in short) and on search of publicly available statistical data relevant to cybercrime. They focus both on areas where little or no data is available (e.g. sharing of login details for different online accounts) and on improving and deepening otherwise available data (e.g. distinguishing phishing requests for money versus requests for personal data). Data collected thus include devices used for online activities and their protection, selected user skills and experiences of unjustified behaviour: ransomware, phishing, online account misuse (emails, social media profiles, e-banking, gaming accounts), online trading fraud and copyright infringement. Respondents answered both as potential victims and self-reported as potential perpetrators.

The data collection was carried out by a professional company using the CAWI method in November 2020, with the vast majority of the data relating to approximately 2020 („the past 12 months", hereafter „2020*"). The resulting large sample of 6,811 respondents represents the Czech internet population aged 16–74 (quota sampling taking into account gender, age, education, region and size of place of residence). Data were analysed using SPSS software.

The analysis of criminal files included practically 100% of criminal proceedings on so-called computer crimes (Section 230–232 of the Czech Criminal Code), whose perpetrator was finally convicted in 2019. Dozens of features were monitored, from socio-demographic characteristics through modus operandi to selected circumstances of the criminal proceedings.

Now a few words about actual results, first with regard to the questionnaire survey. Respondents were most likely to use mobile phones, with laptops next in prevalence and desktop computers somewhat less so. By far the largest number of devices were private, with significantly fewer employee devices, and a few business devices (private devices dedicated exclusively to work related activities). Devices most commonly use Android (mobile phones) and Windows (computers) and tend to be secured with antivirus, with the exception of mobile phones. They are mostly maintained by users themselves or with the help of IT professionals (especially employee devices). Devices are most often shared with partners and close family members, while employee devices are also shared with colleagues. Some devices were attacked by ransomware in 2020* (lower percentage units),

with attacks affecting computers more often than mobile phones. Men are more likely to try to resolve the situation on their own, women and young respondents are more likely to turn to the police (about 15% of those attacked).

The vast majority of respondents used email in 2020*. A fifth of them had experienced phishing requesting personal information at that time, and 40% had experienced phishing requesting money, very roughly half of the respondents in each group repeatedly. Both types of phishing appear to be more easily detected by men and university students, whereas women are more likely to be victimised. There were not many phishing scammers in 2020* (especially men and those under 29), but they acted repeatedly.

Emails tend to be secured with strong passwords, but respondents often share these passwords with others, most often with close family members and partners. Some of these people then misuse their knowledge of the password to get unauthorised access to the email, and it is also common to physically access a particular device. Overall, the experience of unauthorised access to email is in units of percentages of actors on both sides. In particular, victims detect actions that leave noticeable traces (changing passwords, deleting content, assuming identity in the form of communication on behalf of the email owner, etc.), whereas perpetrators are noticeably more likely to report simply viewing content. Victims often assume unauthorised access by an unknown hacker, but perpetrators are significantly more likely to access the online accounts of their partners or close family members, motivated by curiosity or jealousy.

When it comes to self-presentation, it is mainly men and people under 29 years of age who are confident. Respondents make extensive use of social networks, most often Facebook. Almost half of them have some idea about the dark web, young users and men often have personal experience with it. Here too, units of percentage have experience of unauthorised use of a profile on a social network, slightly more so for those under 29. The findings are strongly consistent with those in the area of email misuse: the main actors on both sides include partners and people from the close family circle, there was misuse of known passwords and physical access, and the detected behaviour differed significantly from that reported. Compared to financial motivation, virtual violence was predominant, and was expected especially by persons under 29 years of age (men were more likely to expect money motivation). Here too, curiosity and/or jealousy were predominant.

Respondents also communicated with and used fake profiles with fictitious or someone else's identity. About a tenth of them asked for something – fake profiles with someone else's identity were more likely to seek financial gain, profiles with fictitious identities were more likely to seek intimate communication. Contacted respondents were more likely to report a fake profile with a fictitious girl/female identity, but the respondents themselves were more likely to use a fictitious boy/man identity. It is possible that the fictitious boy/male identity is harder to detect or that respondents are more cautious about girl/female profiles. Profiles with someone else's identity were most often inspired by media personalities.

E-banking misuse evokes a clearly financial motivation compared to social networks and emails, but in fact mere curiosity is a strong motivation for perpetrators. Here again,

a considerable amount of unauthorised activity enabled by shared login credentials comes into play. From the point of view of actors, e-banking misuse also bears a strong resemblance to experiences with emails and social networks.

Overall, the online accounts appear to be subject to a number of undetected unauthorised accesses. Actors are current partners, driven by curiosity and taking advantage of previous knowledge of a password or sharing a device with a partner, or physical access to a particular device, while their activity remains hidden as they ‚only' view otherwise hidden content.

The picture is somewhat different for gaming accounts. While there is also a disproportion between the respondents' answers on the victims' and the perpetrators' side, the predominant motivation is gaming itself (except for gambling).

The majority of respondents (over 90%) shop online on e-shops, and around a fifth of them have experienced a defective goods delivery in 2020* caused by the e-shop, mostly worth up to € 80. Three quarters of them have subsequently requested a correction from the e-shop, and about three quarters of them have actually obtained a remedy. Nearly half of the respondents shop on online marketplaces, while nearly a fifth also had defective goods delivered in 2020* (again, mostly in the value of up to € 80). Here too, about three quarters turned to the seller, but only less than half of the respondents obtained a full remedy (another fifth obtained at least a partial remedy). A few dozen respondents sold the goods themselves via e-shops and less than a third via advertising portals, but most of them avoided delivery of defective goods (three quarters of e-shops and over 90% of sellers on advertising portals).

Around two-thirds of respondents had downloaded some content in 2020*, with around a quarter reporting infringing music or films and a tenth reporting infringing software (e.g. computer games). Some respondents (less than a tenth) had also made infringing content available to others in 2020*. The prevailing motivation was excessively high cost of legal access, and for software, enjoyment of one's own skills was almost as common. The prevailing age category was under 24, and in total under 34 (roughly three quarters).

Among employees with access to an otherwise non-public information system, several dozen individuals were found to have misused their access beyond their authority or misused a colleague's access in 2020*. In addition, roughly one-fifth of respondents found an unknown storage medium and nearly half of them used it, including nearly half without any prior checking for possible hidden malware. However, they did so mostly on private devices.

While studying perpetrators and victims, we created a victimization index and a perpetration index. Younger individuals are concentrated among the perpetrators, however, digital piracy may have a significant impact. Victimization occurs most often on social media and through the misuse of private email, but in general it is not possible to point to any particular sociodemographic or other characteristics specific to victims of cybercrime. Rather, the relationships found are only weak indications. Young people appear to be more at risk, but they are also significantly more likely to use digital technologies on a regular

basis. The level of self security has no major impact on victimisation. In addition, detected attacks (e.g. unauthorised use of an online account) may say more about the ability to detect such attacks than about their prevalence.

It was confirmed that there is a substantial latency of the phenomena observed, overall at the level of about one tenth of the cases reported to the police. The tendency to report at least some of attacks is particularly evident among polyvictimized individuals. Those who do contact the police tend to be satisfied with their work.

As for the results of the analysis of criminal files for 2019, it follows previous findings from 2015. Among those convicted, men predominate, in half of the cases tried for the concurrence of a computer and another crime. More than half of those convicted were first-time offenders. The age structure has changed slightly from 2015, with a decrease in the overall proportion of younger offenders. The distinction between older generations and those already growing up in a digital environment is (and will continue to be) gradually blurring. The level of sentences imposed is largely influenced by the concurrency of offences, usually more severely punished. Of the 158 cases monitored, 50 involved the tampering with tachographs.

However, the findings from the analysis of the criminal files must be taken with reservation of the wording of the elements of computer crimes. In our opinion, it does not correspond adequately to social reality, but it is based on international obligations. Nevertheless, there could be some space for a limited decriminalisation. This is particularly desirable in order to ensure that the use of criminal sanctions does not apply to relatively common activities with little harm to the victim, while more serious cases would still be punishable.

Virtual violence, especially between intimate partners, appears to be an important topic for future research on cybercrime within the Institute for Criminology and Social Prevention. They represent a specific group that has unexpectedly come to the fore in the context of online account misuses motivated by motivations other than money.

Bibliografie

Blinka, L., Škařupová, K., Ševčíková, A., Licehammerová, Š. & Vondráčková, P. (2015). *Online závislosti*. Grada.

Bossler, A. M. (2021). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice*, 46, 911–934.

Brewer, R., Fox, S., & Miller, C. (2020). Applying the Techniques of Neutralization to the Study of Cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 547–565.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. doi:https://linkinghub.elsevier.com/retrieve/pii/S2214212618301455

Computerworld. (2020). *Potvrzeno. Nejslabším článkem kyberbezpečnosti je člověk*. https://www.computerworld.cz/clanky/potvrzeno-nejslabsim-clankem-kyberbezpecnosti-je--clovek/

Český statistický úřad. (2021a). *Informační společnost v číslech – 2021*. https://www.czso.cz/documents/10180/143060187/06100421.pdf/e115d5fc-ea3f-4c4e-a4fd--e789648e6615?version = 1.14

Český statistický úřad. (2021 b). *Studenti a absolventi vysokých škol v České republice (2001–2020)*. https://www.czso.cz/csu/czso/studenti-a-absolventi-vysokych-skol-v--ceske-republice-2020

Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007). Poly-victimization: A neglected component in child victimization. *Child abuse & neglect*, 31(1), 7–26. https://doi.org/10.1016/j.chiabu.2006. 06. 008

Finkelhor, D., Ormrod, R. K., Turner, H. A., & Hamby, S. L. (2005). Measuring poly--victimization using the Juvenile Victimization Questionnaire. *Child abuse & neglect*, 29(11), 1297–1312. https:// doi.org/10.1016/j.chiabu.2005. 06. 005

Gřivna, T. & Polčák, R. (2008). *Kyberkriminalita a právo*. Auditorium.

Guerra, C., & J. R. Ingram. (2020). Assessing the Relationship Between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, 43 (1), 44–60. https://doi.org/10.1080/01639625.2020.1774707

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, 33(4), 308–323.

Jansen, J. & Leukfeldt, R. Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, 10, 79–91.

Jelínek, J. & Ivor, J. (eds). *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015.

Jirovský, V. (2007). *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Grada.

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. In *2017 international conference on cyber situational awareness, data analytics and assessment* (cyber SA) (1–8).

Klapal, V. (2005). Svolení poškozeného jako okolnost vylučující protiprávnost. *Trestněprávní revue*. (10), 259.

Kolouch, J. (2016). *CyberCrime*. CZ.NIC. https://knihy.nic.cz/files/edice/cybercrime.pdf

Krulichová, E. & Buriánek, J. (Eds.). (2020). *Obavy ze zločinu: mýty a realita*. Charles University in Prague, Karolinum Press.

Kudrlová, K. (2018). Kybernetická kriminalita – dílčí poznatky z výzkumu. *II. Kriminologické dny 2018* (s. 148–157). Iuridicum Olomoucense.

Kudrlová, K. (2019). *Kriminalita spojená s využíváním nových médií dětmi*. [Dizertační práce, Univerzita Karlova]. Digitální repozitář UK. https://dspace.cuni.cz/handle/20.500.11956/111603

Kudrlová, K. (2022). Kyberkriminalita a covid. In K. Večerka (Ed.) *Sociální patologie za časů covidu* (s. 39–48). Česká sociologická společnost.

Kudrlová, K. (2023). Partner a soukromí online. In K. Večerka (Ed.) *Dopady a výzvy nových společenských situací* (s. 11–18). Česká sociologická společnost.

Kudrlová, K., & Vlach, J. (2023). Neoprávněný přístup na online účty (internetové bankovnictví, sociální sítě) a dekriminalizace jednoho z počítačových trestných činů. *Právník* (10), 926–943.

Kudrlová, K., Kutil, L., & Vlach, J. (2022). Výzkumné šetření IKSP „Zkušenosti obyvatel České republiky s vybranými jevy v online prostředí". *Kriminalistika*, (2), 139–152.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, 4(5), 26–32.

Leukfeldt, E. R., & M. Yar. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior* 37 (3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lukášová, M. (2019). Institut svolení poškozeného a jeho uplatnění nejen v judikatuře. *Trestněprávní revue*, 3, 60.

Markham, A. N. (2003). *Metaphors reflecting and shaping the reality of the Internet: Tool, place, way of being*. https://annettemarkham.com/writing/MarkhamTPW.pdf

Ministerstvo vnitra. (2021, květen). *Tisková zpráva ze zasedání Republikového výboru pro prevenci kriminality*. https://www.mvcr.cz/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci-kriminality-713175.aspx

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126, 106984.

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, 1–19.

Ngo, F. T., Piquero, A. R., LaPrade, J. & Duong, B. (2020). Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? *Criminal Justice Review*, 45(4), 430–451. https://doi.org/10.1177/ 0734016820934175

Novák, P. (2022, 7. září). *Phishing – odpovídá za ztrátu banka nebo majitel účtu?* https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu

Pospíšilová, H. P. (2023. 30. červen). International comparative study of COVID-19 leisure in the Czech Republic and Slovak Republic. *World Leisure Journal*. doi:10.1080/16078055.2023.2227608

Roberts, J. A. (2020). The Social Media Party: Fear of Missing Out (FoMO), Social Media Intensity, Connection, and Well-Being. *International Journal of Human–Computer Interaction*, 36(4). doi:doi.org/10.1080/10447318.2019.1646517

Roubalová, M., Holas, J., Martinková, M. & Paloušová, V. (2023). *Obyvatelé ČR a viktimizace: Nové poznatky z výzkumu*. Institut pro kriminologii a sociální prevenci.

Smejkal, V. (2015, 20. července). *Kybernetická kriminalita – fenomén dneška*. https://www.pravniprostor.cz/clanky/ostatni-pravo/kyberneticka-kriminalita-fenomen-dneska

Smejkal, V. (2022). *Kybernetická kriminalita*. 3. vydání. Aleš Čeněk.

Sykes, G., & Matza, D. (1957). Techniques of neutralization. *American Sociological Review*, 22, 664–670.

Šámal, P. (ed). (2012). *Trestní zákoník. Komentář*. 2. vydání. C. H. Beck.

Šámal, P., Novotný, O., Gřivna, T., Herczeg, J., Vanduchová, M., Vokoun, R. (ed). (2016). *Trestní právo hmotné*. 8. vyd. Wolters Kluwer ČR.

Švestka, J. D. (2014). *Občanský zákoník komentář*, svazek 1. Wolters Kluwer.

Telec, I. & Tůma, P. (2007). *Autorský zákon. Komentář*. C. H. Beck.

Tomášek, J. (2013). *Self-reportové studie kriminálního chování*. IKSP.

van de Weijer, S. G. A., and E. R. Leukfeldt. 2017. "Big Five Personality Traits of Cybercrime Victims." *Cyberpsychology, Behavior, and Social Networking* 20 (7): 407–412. https://doi.org/10.1089/cyber.2017.0028

van't Hoff-de Goede, M. S., van de Weijer, S., & Leukfeldt, R. (2023). Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization?. *Journal of Crime and Justice*, 1–20. DOI: 10.1080/0735648X.2023.2222719

Vláda ČR. (2008). *Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník*.

Vlach, J., Kudrlová, K., & Paloušová, V. (2020). *Kyberkriminalita v kriminologické perspektivě*. Institut pro kriminologii a sociální prevenci.

Volevecký, P. (2013). Několik poznámek k trestně právní ochraně bezhotovostních platebních prostředků. *Trestní právo*, 17(4), 30–35.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107–124. https://doi:10.1057/sj.2012.1

Wolfendale, J. (2007). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology* (2), 111–119.

World Economic Forum. (2022). *The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment*. https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf

Zkratky a slovníček pojmů

2020*	Období od prosince roku 2019 do listopadu roku 2020
BTC	Zkratka používaná pro kryptoměnu bitcoin
CSLAV	Centrální statistické listy a výkaznictví. Informační systém MSp
ČSÚ	Český statistický úřad
Darkweb	Jinak též dark web, darknet, dark net atp. Součást internetu (deepwebu) s vlastním obsahem, dostupná pouze prostřednictvím speciálního prohlížeče Tor
ICT	Informační a komunikační technologie
Malware	Škodlivý software
MSp	Ministerstvo spravedlnosti
MV	Ministerstvo vnitra
NB	Notebook
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Stolní počítač
Phishing	E-mail ze zdánlivě důvěryhodného zdroje usilující nejčastěji o přihlašovací údaje adresáta (např. přihlašovací údaje k účtu na sociální síti) nebo jiné osobní údaje (např. číslo bankovního účtu)
Ransomware	Zablokování (obvykle zašifrování) celého nebo části zařízení spojené zpravidla s požadavkem platby výměnou za jeho odblokování
SD	Směrodatná odchylka (standard deviation)
SNS	Sociální sítě
TČ	Trestný čin
TŘ	Zákon číslo 141/1961 Sb., trestní řád
TZ	Zákon číslo 40/2009 Sb., trestní zákoník
VN	Virtuální násilí
MZ	Majetkový zájem

Přehled titulů vydaných v edici Institutu pro kriminologii a sociální prevenci od roku 2012

Ediční řada Studie:

2023

475 Hulmáková, J., Biedermanová, E., Tomášek, J., Vlach, J. & Voldřichová, I. *Násilná kriminalita dětí mladších patnácti let.*

476 Roubalová, M., Holas, J., Martinková, M. & Paloušová, V. *Obyvatelé ČR a viktimizace. Nové poznatky z výzkumu.*

477 Zhřívalová, P., Raszková, T., Háková, L. & Novák, P. *Diferenciace odsouzených ve věznici s ostrahou.*

2022

472 Holas, J. (ed.) *Research on Crime and Criminal Justice in the Czech Republic (selected results of research activities of IKSP in the years 2016–2019).*

474 Scheinost, M., Biedermanová, E., Blatníková, Š., Diblíková, S., Hulmáková, J., Večerka K. & Zeman, P. *Analýza trendů kriminality v České republice v roce 2021.*

2021

465 Háková, L. *Zločin a trest v kriminálním zpravodajství.*

468 Blatníková, Š., Novopacká, M., Přesličková, H. & Zeman, P. *Kriminální historie pachatelů závažného násilí v ČR.*

469 Diblíková, S., Špejra, M. & Vlach, J. *Vyhodnocení procesu spuštění elektronického monitorovacího systému (EMS) v ČR.*

470 Scheinost, M., Diblíková, S., Frydrych, J., Háková, L., Holas, J., Hulmáková, J., Kasal, Z., Kudrlová, K., Kutil, L., Šereda, P., Štěpánek, Z., Večerka, K. & Vlach, J. *Analýza trendů kriminality v ČR v roce 2020.*

2020

462 Scheinost, M., Barbořík, M., Čáp, J., Diblíková, S., Frydrych, J., Holas, J., Hulmáková, J., Karban, M., Linhartová, H., Martinková, M., Raszková, T., Večerka, K. & Zhřívalová, P. *Analýza trendů kriminality v České republice v roce 2019.*

463 Vlach, J., Kudrlová, K. & Paloušová, V. *Kyberkriminalita v kriminologické perspektivě.*

464 Rozum, J., Háková, L., Hulmáková, J., Špejra, M. & Zhřívalová, P. *Zprávy PMS pro účely rozhodnutí v trestním řízení: kvalita, význam, efektivita.*

2019

449 Roubalová, M., Holas, J., Kostelníková, Z. & Pešková, M. *Oběti kriminality. Poznatky z viktimizační studie.*

452 Tomášek, J., Diblíková, S., Hamplová, N. & Rozum, J. *Rodinné skupinové konference.*

453 Zeman, P., Blatníková, Š., Grohmannová, K., Koňák, T., Novák, P., Roubalová, M. & Trávníčková, I. *Uživatelé drog ve vězení – hodnocení účinnosti terapeutických programů.*

454 Diblíková, S., Cejp, M., Hulmáková, J., Raszková, T., Roubalová, M., Scheinost, M., Večerka, K. & Zhřívalová, P. *Analýza trendů kriminality v České republice v roce 2018.*

455 Roubalová, M., Grohmannová, K., Trávníčková, I. & Zeman, P. *Možnosti zjišťování míry a struktury sekundární drogové kriminality v podmínkách České republiky.*

456 Blatníková, Š. & Zeman, P. *Evidence dat o ochranném léčení a zabezpečovací detenci v ČR – nedostatky a možná řešení.*

457 Martinková, M. & Biedermanová, E. *Senioři v České republice jako oběti i pachatelé kriminálních deliktů.*

458 Večerka, K., Hulmáková, J. & Štěchová, M. *Mladiství v procesu poruchové socializace.*

459 Holas, J. *Bezpečí, kriminalita a prevence.*

460 Tomášek, J., Háková, L. & Kostelníková, Z. *Probace a její efektivita pohledem pachatelů, veřejnosti a médií.*

2018

447 Diblíková, S., Cejp, M., Hulmáková, J., Pešková, M., Scheinost, M. & Večerka, K. *Analýza trendů kriminality v České republice v roce 2017.*

446 Scheinost, M., Cejp, Diviák, T. & Pojman, P. *Trendy vývoje organizovaného zločinu a jeho vybraných forem.*

2017

440 Zeman, P. (ed.) *Research on Crime and Criminal Justice in the Czech Republic (selected results of research activities of IKSP in the years 2012-2015).*

441 Tomášek, J., Faridová, P., Kostelníková, Z., Přesličková, H., Rozum, J. & Zhřívalová, P. *Zaměstnání jako faktor desistence.*

443 Karabec, Z., Diblíková, S., Hulmáková, J., Vlach, & Zeman, P. *Criminal Justice System in the Czech Republic. 3rd amended and revised edition.*

444 Budka, I. *Využití právních nástrojů pro potírání organizovaného zločinu.*

445 Diblíková, S., Hulmáková, J., Karban, M., Martinková, M., Scheinost, M. & Večerka, K. *Analýza trendů kriminality v České republice v roce 2016.*

2016

431 Blatníková, Š., Faridová, P., Vranka, M. *Kriminální styly myšlení: Inventář PICT-cz.*

432 Marešová, A., Biedermanová, E., Rozum, J., Tamchyna, M. & Zhřívalová, P. *Výkon nepodmíněného trestu odnětí svobody – kriminologická analýza.*

433 Blatníková, Š. *Nebezpečnost a násilí ve vězeňském prostředí.*

435 Holas, J., Háková, L., Krulichová, E. & Scheinost, M. *Regionální kriminalita a její odraz v kvalitě života obyvatel.*

437 Diblíková, S., Cejp, M., Martinková, M., Smejkal, V. & Štefunková, M. *Analýza trendů kriminality v České republice v roce 2015.*

438 Tomášek, J., Diblíková, S. & Scheinost, M. *Probace jako efektivní nástroj snižování recidivy.*

439 Rozum, J., Háková, L., Tomášek, J., & Vlach, J. *Efektivita trestní politiky z pohledu recidivy.*

2015

423 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Trestní sankce – jejich uplatňování, vliv na recidivu a mediální obraz v televizním zpravodajství. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí III.).*

424 Marešová, A., Havel, R., Martinková, M. & Tamchyna, M. *Násilná kriminalita v nejisté době.*

425 Marešová, A., Biedermanová, E., Diblíková, S., Požár, J. & Martinková, M. *Analýza trendů kriminality v ČR v roce 2014.*

426 Zeman, P., Štefunková, M. & Trávníčková, I. *Drogová kriminalita a trestní zákoník.*

427 Večerka, K. & Štěchová, M. *Preventivní praxe po novelizaci zákona o sociálně-právní ochraně dětí.*

428 Blatníková, Š., Faridová, P. & Zeman, P. *Znásilnění v ČR – trestné činy a odsouzení pachatelé.*

429 Scheinost, M., Válková, H., (eds.) *Sankční politika a její uplatňování. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí IV.).*

430 Cejp, M., Blatníková, Š., Háková, L., Holas, J., Trávníčková, I. & Vlach, J. *Společenské zdroje vývoje organizovaného zločinu.*

422 Škvain, P. *Zabezpečovací detence z pohledu vybraných zahraničních právních úprav.*

2014

414 Martinková, M., Slavětínský, V. & Vlach, J. *Vybrané problémy z oblasti domácího násilí v ČR.*

415 Štěchová, M. & Večerka, K. *Systémový přístup k prevenci kriminality mládeže.*

417 Marešová, A., Cejp, M., Holas, J., Martinková, M. & Rozum, J. *Analýza trendů kriminality v roce 2013.*

418 Blatníková, Š., Faridová, P. & Zeman, P. *Násilná sexuální kriminalita – téma pro experty i veřejnost.*

419 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Sankční politika pohledem praxe. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí II.).*

2013

403 Košťál, J. V*ybrané metody vícerozměrné statistiky.* (Vybrané metody kriminologického výzkumu - svazek 4).

404 Pojman, P. *Ruský a ukrajinský organizovaný zločin.*

405 Tomášek, J. *Self-reportové studie kriminálního chování.* (Vybrané metody kriminologického výzkumu - svazek 5).

406 Holas, J. *Politický radikalismus a mládež.*

408 Zeman, P., Diblíková, S., Slavětínský, V. & Štefunková, M. *Zkrácené formy trestního řízení – možnosti a limity.*

410 Scheinost, M., a kol. *Trestní sankce a jejich odraz v praxi, tisku a v názorech veřejnosti. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí I.).*

411 Marešová, A., Cejp, M., Holas, J., Kuchařík, K., Martinková, M. & Scheinost, M. *Analýza trendů kriminality v roce 2012.*

412 Holas, J. & Večerka, K. *Stát a občan v prevenci kriminality.*

2012

397 Cejp, M. (ed.) *Selected Results of Research Activities of ICSP in the Years 2008–2011.*

398 Marešová, A., Cejp, M., Martinková, M., Tomášek, J., Vlach, J. & Zeman, P. *Crime in the Czech Republic in 2010.*

399 Večerka, K. *Mládež o kriminalitě a etice každodennosti.*

402 Marešová, A., Biedermanová, E., Cejp, M., Holas, J., Martinková, M. & Tomášek, J. *Analýza trendů kriminality v roce 2011.*

Ediční řada Prameny:

2022

471 *14. Kongres OSN o prevenci kriminality a trestní justici. Kjóto, Japonsko, 7.–12. března 2021.*

473 Montanari, L., Royuela, L., Hasselberg, I., Vandam, L. *Vězeňství a drogy v Evropě. Aktuální a budoucí výzvy.*

2021

466 *Dokumenty OSN k dopadům pandemie Covid-19 na kriminalitu.*

467 *Zabezpečovací detence a trest odnětí svobody (Empirický výzkum výkonu zabezpečovací detence a trestu odnětí svobody předcházejícího zabezpečovací detenci).*

2020

461 *Globální studie o pašování migrantů 2018.*

2019

448 Heiskanen, M. & Lietonen, A. *Kriminalita a gender. Studie zaměřená na zastoupení mužů a žen v mezinárodní statistice kriminality.*

450 *Škody působené kybernetickou kriminalitou. Zpráva shrnující hlavní poznatky Pracovní skupiny k nákladům kyberkriminality.*

451 *Příručka k evaluaci. Pokyny k navrhování, provádění a používání nezávislé evaluace v UNODC.*

2017

442 UNODC: *Mezinárodní klasifikace trestných činů pro statistické účely.*

2016

434 Heiskanen, M., Aebi, M. E., van der Brugge, W., Jehle, J.-M. *Evidence alternativních trestů a zjišťování míry atrice. Metodologická studie komparativních dat v Evropě.*

436 *13. kongres OSN o prevenci kriminality a trestní justici. Dauhá, Katar, 12.–19. dubna 2015.*

2015

420 Francis, B., Humphreys, L., Kirby, S. & Soothill, K. *Kriminální kariéra v organizovaném zločinu.*

421 Mendel, R. A. *Mládeži nepřístupno. Argumenty pro snižování počtu odnětí svobody u mladistvých.*

2014

416 Benes, M. & Astbury, B. (eds.) *Problémy trestního soudnictví: evaluace programů, prevence kriminality, strach z kriminality a recidiva – pohledem australských kriminologů.*

2013

407 United Nations Office on Drugs and Crime *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu.*

409 United Nations Office on Drugs and Crime *Světová zpráva o obchodování s lidmi 2012.*

413 European Forum for Urban Security *Pouliční násilí v EU: Skupiny mladistvých a násilí na veřejnosti.*

2012

395 Cejp, M. (ed.) *Britské strategické dokumenty k prevenci a potírání závažné trestné činnosti.*

396 Goodey, J. & Aromaa, K. (eds.) *Trestné činy z nenávisti (příspěvky ze Stockholmského kriminologického sympozia 2006 a 2007).*

400 Marešová, A. (ed.) *Trendy kriminality ve světě a nové problémy a reakce v oblasti prevence kriminality a trestní justice.*

401 Diblíková, S. (ed.) *Rada Evropy a International Juvenile Justice Observatory k soudnictví nad mládeží.*

Plné texty všech titulů, publikovaných v edici Institutu pro kriminologii a sociální prevenci od roku 2000, jsou volně dostupné na webu IKSP www.iksp.cz v sekci Publikace.

Kyberkriminalita z pohledu justiční praxe a každodenních uživatelů

Autoři:	Kateřina Kudrlová
	Viktorie Paloušová
	Jiří Vlach
Vydavatel:	Institut pro kriminologii a sociální prevenci
	Nám. 14. října 12, 150 00 Praha 5
Určeno:	pro odbornou veřejnost
Design:	addnoise.org
Sazba:	Lukáš Pracný, sazbaknih.cz
Tisk:	Reprocentrum, a. s., Blansko
Vydání:	první, prosinec 2023
Náklad:	200 ks

www.iksp.cz

ISBN 978-80-7338-204-9