UNIVERZITA KARLOVA

Právnická fakulta

Markéta Žilková

Trestní a kriminologické aspekty phishingu

Diplomová práce

Vedoucí diplomové práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 26. června 2023

Čestné prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 147 725 znaků včetně mezer.

V Praze dne 26. dubna 2023

Markéta Žilková

Poděkování

Na tomto místě bych chtěla poděkovat zejména prof. JUDr. Bc. Tomáši Gřivnovi, Ph.D., za jeho ochotu a pomoc, kterou mi poskytl při vedení této diplomové práce. Ráda bych poděkovala i svým rodičům a partnerovi za trpělivost a podporu, kterou mi poskytli při studiu.

Obsah

Úvod

V dnešní digitální době se společnost stává stále závislejší na moderních technologiích a komunikaci prostřednictvím internetu. Tyto technologie přinesly vylepšení a zjednodušení každodenního života, avšak stejně tak, jako nám pomáhají, nám mohou škodit. Jednou z nejrozšířenějších forem kybernetické kriminality je phishing, který je charakterizován podvodnými praktikami zaměřenými na získání osobních nebo přihlašovacích údajů od uživatelů. Ať už jde o údaje k internetovému bankovnictví, ale také k e-mailovým schránkám, sociálním sítím, apod.

Ačkoliv je v zahraniční literatuře zpracování problematiky phishingu podrobnější, v České republice neexistuje žádná obsáhlá odborná práce, která by se phishingem z tohoto hlediska zabývala, a to i přesto, že se jedná o závažný problém, s nímž se uživatelé setkávají prostřednictvím médií poměrně často. V části kriminologické proto budou využity ve velké míře zahraniční zdroje a výzkumy, zejména zabývající se typickým profilem oběti phishingu. Naopak v části trestní budou použity zdroje převážně české s ohledem na zaměření se na českou právní úpravu trestního práva.

Při zpracování této práce bude využita deskriptivní metoda k obecnému definování phishingu, kdy bude zkoumáno nejenom, co je phishing a jak probíhá, ale také jeho historie a formy. Následně bude využita logická indukce pro zpracování dat získaných z českých i zahraničních zdrojů, které poslouží k analýze a vyhodnocení vývoje phishingu na základě dostupných statistik a trendů. Zároveň bude provedena analýza odborné literatury, právních předpisů a dostupné judikatury k získání uceleného pohledu na trestní i kriminologické hledisko phishingu.

Cílem této diplomové práce je provést analýzu trestního postihu pachatele phishingu a kriminologických aspektů phishingu. V části trestních aspektů bude kladen důraz zejména na právní úpravu České republiky. Dále je cílem zhodnotit vývoj počtu případů tohoto druhu kybernetické kriminality a identifikovat formy phishingu, které se postupem času vyvinuly. Vzhledem ke každodenní interakci uživatelů s elektronickou komunikací je předpokladem této práce stoupající trend spáchaných phishingových útoků.

Výsledky této práce by mohly sloužit jako ucelený přehled i zdroj informací pro odbornou a laickou veřejnost zabývající se problematikou phishingu. Mají potenciál přispět i k lepšímu porozumění phishingu z trestního a kriminologického pohledu, i s ohledem na jeho vývoj, a jako případný podklad pro další zkoumání.

1. Kyberprostor, kybernetická kriminalita a jejich vztah k phishingu

1.1. Kyberprostor

Před vlastní definicí phishingu je nutné popsat i další pojmy, které se k phishingu vztahují. Jedním z nich je kyberprostor, ve kterém se vlastně všechna kybernetická kriminalita odehrává. Kybernetický prostor neboli kyberprostor podle § 2 písm. a) zákona o kybernetické bezpečnosti je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Tento pojem zavedl do obecného povědomí John Perry Barlow, zakladatel neziskové organizace Electronic Frontier Foundation, která vydala v roce 1996 Deklaraci nezávislosti kyberprostoru (*A Declaration of the Independence of Cyberspace*). Kyberprostor existuje nezávisle na vůli jednotlivce 24 hodin a 7 dní v týdnu a každý okamžik dojde ke změně dat, která jsou v něm obsažená.[1]

Důležitou vlastností kyberprostoru je jeho decentralizovanost. Není zde žádná centrální autorita, která by mohla rozhodnout o jeho existenci či neexistenci nebo jej dokonce mohla jakkoliv řídit. Fungování spočívá v dohodě uživatelů a správců, kteří se svým jednáním přizpůsobují majoritní většině. Kyberprostor je tedy řízen pouze jeho uživateli. Další významnou vlastností kyberprostoru je deteritorializace aktivit na internetu. Kyberprostor je globálním prostředím, které nerozdělují hranice mezi státy nebo kontinenty, a aktivity v tomto prostoru, ať už jsou legální nebo nelegální. Velmi těžce se lokalizují na určité teritorium, na území pod stejnou státní správou nebo jurisdikcí.[2]

Kyberprostor zahrnuje celý virtuální prostor, především prostředí internetu, jiných sítí a mobilních technologií. Jedná se vlastně o paralelní svět, který má spoustu možností využití. Slouží například jako platforma komunikace (na základě e-mailů, sociálních sítí), jako zdroj mnoha informací, prostor informačních systémů různých institucí, a to včetně veřejné správy, datové úložiště, zábava atd. Na druhou stranu však poskytuje prostředí i pro škodlivé jednání, a to včetně páchání kriminality.[3] Prostředí kyberprostoru je objektivně velmi obtížně vnímatelné, dění

[1] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 388-390.
[2] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, str. 34-35.
[3] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 388.

můžeme pozorovat pouze prostřednictvím přístrojů, které nám přístup do kyberprostoru umožňují.[4]

1.2. Kybernetická kriminalita

1.2.1. Rozdíl mezi počítačovou a kybernetickou kriminalitou

Pojmy počítačové a kybernetické kriminality se občas zaměňují, proto je dále rozvedeno, jaký je mezi nimi rozdíl. Před vymezením pojmu počítačové a kybernetické kriminality je potřeba definovat samostatný pojem *kriminalita.* Tento pojem se kryje s obsahem zvláštní části trestního zákoníku – kriminalitu tvoří jen takové trestné činy, jejichž skutková podstata je upravena ve zvláštní části trestního zákoníku.[5]

Počítačová kriminalita je velice široký pojem, který se prosadil v 90. letech 20. století.[6] Je pod ním třeba chápat páchání trestné činnosti, ve které vystupuje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, či jenom některá z jeho částí, případně větší množství samostatných počítačů nebo propojených do počítačové sítě. Počítač může být buď jako předmět trestné činnosti (s výjimkou takové trestné činnosti, jejímž předmětem jsou výše popsaná zařízení jako věci movité)[7], nebo naopak jako nástroj pachatele.[8]

Jako synonymum k počítačové kriminalitě se uvádí kybernetická kriminalita. Je možné, že k tomu přispívá terminologická nejednotnost a různé chápání těchto pojmů, které je pravděpodobně způsobené interdisciplinárním přístupem k řešení dané problematiky. Tyto pojmy jsou tak různými autory v odborných článcích a i v právních dokumentech zaměňovány či vykládány jinak.[9]

Podle Kuchty[10] i Šámala[11] se však o synonymum nejedná, poněvadž kybernetická kriminalita je odvozena od pojmu *kyberprostor*. Počítačová kriminalita se odehrává i mimo kyberprostor, avšak kybernetická kriminalita nikoliv. V případě kybernetické kriminality jde tedy

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, str. 19.
[5] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 24.
[6] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 32.
[7] Jde o případ, kdy útok nesměřuje vůči počítači s ohledem na jeho specifické vlastnosti, ale stane se pouze předmětem trestného činu, například krádeže, zpronevěry, kdy si ho pachatel přisvojí.
[8] SMEJKAL, Vladimír. *Kybernetická kriminalita.* 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 33.
[9] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 31.
[10] KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 7.
[11] ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2302.

spíše o podmnožinu kriminality počítačové. Krupička[12] považuje pojem kyberkriminalita spíše jako moderní synonymum pro pojem počítačové kriminality. K různému pojmenování přispěla nejspíše i Úmluva o počítačové kriminalitě, která je prvním mezinárodním aktem v této oblasti. Úmluva je takto oficiálně označována v českém jazyce, avšak její anglické znění je *Convention on Cybercrime* (lze se proto setkat i s označením Úmluva o kybernetické kriminalitě).

V rámci českého prostředí se setkáváme nejprve s pojmem *počítačová kriminalita,* který je definován jako zneužití výpočetní techniky buď jako prostředku, nebo jako předmětu útoku. Avšak poté, co byla Česká republika v roce 1992 připojena do sítě internet se objevil nový rozměr kriminality související s výpočetní technikou, a to ve vztahu k počítačovým sítím. Toto se následně projevilo u pojmosloví. Začal se používat spíše pojem *kybernetická kriminalita,* kdy tento pojem právě zdůrazňuje kyberprostor oproti samostatným počítačům a informacím.[13]

Vzhledem k výše uvedenému má autorka za to, že lze oba pojmy považovat v určitém smyslu za synonyma, kdy pojem počítačová kriminalita se používal dříve a pojem kyberkriminalita se používá spíše v současné sobě. V následujícím textu bude používán již jen pojem *kyberkriminalita* či *kybernetická kriminalita*.

1.2.2. Kybernetická kriminalita

Spolu s růstem možností využívání informačních a komunikačních prostředků se zvyšuje i možnost jejich užívání, či spíše zneužívání, k páchání trestné činnosti. Díky tomu tak neexistuje univerzální, obecně přijímaná definice, která by rozsah i hloubku pojmu kybernetická kriminalita plně postihla. Tento pojem se pak nejčastěji užívá v mezinárodních úmluvách jako označení trestné činnosti, která je páchaná prostředky informačních technologií, a tak se pojem přenesl i do slovníku odborné veřejnosti.[14] Jednotná definice neexistuje v teorii ani v legislativě, proto je uvedeno několik možných výkladů kybernetické kriminality.

Kybernetická kriminalita je podle výkladového slovníku kybernetické bezpečnosti trestná činnost, kdy služby nebo aplikace jsou v kybernetickém prostoru buď nástrojem, anebo cílem útoku, případně jde o trestnou činnost, v rámci které je kyberprostor zdrojem, nástrojem, cílem

[12] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 478.
[13] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 389.
[14] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 33.

nebo místem trestného činu.[15] Jde o takové jednání, kterým je porušován zákon nebo které je v rozporu s morálními pravidly společnosti.[16]

Kybernetickou kriminalitu je možné členit dle úlohy kyberprostoru při páchání trestného činu. Může jít o kriminalitu, která existuje pouze v prostředí kyberprostoru, tedy není zde ekvivalentní jednání v reálném světě. Často jsou spjaty s počítačovými programy, které byly nelegálně vytvořeny pro tato jednání (typickým zástupcem je hacking či kybergrooming). Za druhé může jít o kriminalitu, která existuje i mimo kyberprostor, který je zde využíván pouze jako nástroj či místo kriminálních aktivit. K jejich stíhání je možné využít již existujících úprav trestných činů či jejich modifikací (jde například o internetové podvody – phishing).[17] Většina kyberkriminality v současné době probíhá prostřednictvím internetu a díky tomu, že je celosvětový, způsobuje potíže při postihu prostřednictvím tradičního trestního systému, který je založen na státní suverenitě.[18]

1.3. Definice phishingu

Phishing je druh kriminálního jednání spadající do kybernetické kriminality, který spočívá v podvodném jednání na internetu. Zjednodušenou definicí by mohlo být, že phishing je proces oklamání uživatele, aby provedl to, co po něm útočník požaduje.[19] Toto podvodné jednání vede k získání různých citlivých informací o uživateli, může se jednat například o heslo, číslo platební karty, jeho PIN apod., kdy se útočník vydává za důvěryhodnou osobu nebo organizaci.[20]

Pojem phishing vychází z anglického slova „fishing“, tedy v překladu rybaření. V češtině by se dal pojem přeložit jako „rhybaření“, avšak tento překlad se nepoužívá a spíše se užívá anglická verze. Tento název může být odvozen od toho, že útočník podává obětem návnadu na háčku, na kterou se je snaží chytit a získat od nich citlivé údaje. Podobné to je s tím, že ani rybář nepočítá, že chytí všechny ryby, ale snaží se ulovit alespoň nějakou. Díky elektronickým

[15] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary.* Páté doplněné a upravené vydání. Přeložil Karel Vavruška. Praha: Česká pobočka AFCEA, 2022, str. 98.
[16] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, str. 19.
[17] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 480.
[18] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 390.
[19] ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.* In: Frontiers in Computer Science, 2021, vol. 3, str. 2.
[20] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 246.

komunikacím může útočník naráz napadnout velké množství potenciálních obětí a je pak otázka, zda se některá na uvedenou „návnadu“ nachytá.[21]

Základní podoba phishingu se skládá ze dvou částí – důvěryhodně vypadající e-mailová (či i jiná) zpráva a falešné podvodné stránky. Útočník se zpravidla vydává za známou a spolehlivou společnost, bankovní instituci či úřad, které posílají zprávy svým klientům, resp. obecně uživatelům. Útočníci připojí ke zprávě odkaz na jimi vytvořené falešné webové stránky, které vypadají identicky (či alespoň podobně) jako stránky legitimní instituce. Jejich cílem je oklamat uživatele, aby na těchto stránkách vyplnil své osobní údaje, které tak získá útočník. Občas útočník také slibuje nějakou výhru nebo odměnu, ale opět pouze výměnou za to, že mu uživatel poskytne své údaje, které může útočník zneužít.[22]

V širším slova smyslu pod pojem phishing spadá jakékoli podvodné jednání, které má v uživateli vzbudit důvěru a případně snížit jeho ostražitost. V takovém případě není po uživateli požadováno, aby něco vyplnil, ale je mu doručena zpráva (někdy je i přímo přesměrován na stránku), která obsahuje malware[23], na základě něj pak útočník zjistí zadané údaje.[24]

Phishing se řadí pod spam. V obecném smyslu jde o hromadnou nevyžádanou poštu. S pojmem spam je nejspíše většina lidí obeznámená, protože se takové zprávy často objevují v jejich e-mailových schránkách. Tento pojem je možné popsat ze dvou různých rovin. V užším slova smyslu jde o hromadné šíření nevyžádaného sdělení, nejčastěji pomocí elektronické komunikace (zpravidla se jedná o reklamu). V širším slova smyslu jde o všechny nevyžádané zprávy, které jsou uživatelům doručovány. Zde půjde například i o zprávy, které v sobě obsahují viry, trojské koně apod.[25] Spam obsahující podvodný nebo jiný kriminální obsah je označován jako „scam“ (podvod, švindl). Účelem scamu je pomocí sociálního inženýrství v rámci spamového e-mailu získat důvěru uživatele a donutit jej vykonat určité úkony (např. otevření přílohy e-mailu

[21] KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi*. In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 58.
[22] MOHAMMAD, Rami, THABTAH, Fadi, MCCLUSKEY, Lee. *Tutorial and critical analysis of phishing websites methods*. In: Computer Science Review, 2015, vol. 17, str. 2-4.
[23] Pojem „malware“ vznikl spojením anglických slov „malicious“ (v překladu zákeřný, škodlivý) a „software“ a používá se pro programy, jejichž cílem je škodit. Pod tento pojem patří především počítačové viry, trojské koně, spyware apod., ale obecně sem lze zařadit každý program, který někomu způsobí škodu nebo jinému získá neoprávněný prospěch. Nepatří sem však programy, které mají legální cíle, avšak vykazují chyby. (Zdroj: SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 225-226).
[24] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 246.
[25] VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestně právní kvalifikace*. In: Trestní právo, 2010, roč. 14, č. 12, str. 6.

nebo navštívení uvedeného URL).[26] Jejich cílem je získání finančních prostředků pomocí oklamání uživatelů. Pod scam se řadí phishing, malware a scamy nigerijského typu.[27]

Pachatelé phishingu využívají metod sociálního inženýrství. Útoky pomocí sociálního inženýrství jsou velice časté a nebezpečné. Zneužívají totiž největší slabinu bezpečnosti počítačových systémů, a tou je přirozená důvěřivost člověka či tendence podřídit se autoritě. U těchto útoků nejde o prolomení antivirových programů, firewallů a jiných bezpečnostních systémů, ale cílem je tyto technologie obejít. Záměrem je vylákání informací od lidí, kteří k nim mají přístup. Tyto útoky patří mezi nejsilnější, poněvadž jim nelze technicky zabránit. Jedinou možností je důkladné školení a informování osob.[28] Útočníci prostřednictvím vzájemné interakce působí na oběť manipulativně, aby vyzradila důvěrné informace či porušila bezpečnostní postupy. Informace jsou pak buď použity ke konkrétnímu účelu, nebo prodány na černém trhu.[29]

Existují různé druhy útoků pomocí sociálního inženýrství, avšak všechny mají společný vzor obsahující podobné fáze. Tyto fáze jsou čtyři: (1) průzkum volných zdrojů informací, (2) budování vztahu a důvěry, (3) využití důvěry a získání informace, (4) zmizení. Pachatel se nejprve pokouší o zamýšlené oběti získat všechny dostupné informace (pomocí internetu, telefonickým hovorem, nebo osobně, kupříkladu i prohledáváním odpadu cílové organizace). Získané údaje využije při následném kontaktování oběti. Tu kontaktuje buď přímo, nebo prostřednictvím elektronické komunikace, kdy díky využití nabytých informací vzbudí u oběti důvěru. Poté prostřednictvím psychologické manipulace vytáhne z oběti informace nebo ji donutí k bezpečnostní chybě. Tyto informace nebo chybu zneužije k dalšímu útoku, či je zpeněží.[30]

Klasickým příkladem užití sociálního inženýrství je naléhavost zprávy, apelace na rychlé jednání. Útočník žádá, aby mu uživatel ihned poskytl své údaje, jinak přijde o své peníze, bude mu zrušen účet, či mu bude udělena pokuta z důvodu neuhrazení služby apod. Základní reakcí uživatele je okamžitě jednat, protože nemá čas na přemýšlení o nastalé situaci.[31]

---

[26] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 231-235.
[27] LANCE, James. *Phishing bez záhad.* Přeložil Lubomír Moudrý. Praha: Grada Publishing, 2007, str. 25-26.
[28] SCOTT, Applegate. *Social Engineering: Hacking the Wetware!.* In: Information Security Journal: A Global Perspective, 2009, vol. 18, no. 1, str. 40-42.
[29] SALAHDINE, Fatima, KAABOUCH, Naima. *Social Engineering Attacks: A Survey*. In: Future Internet, 2019, vol. 11, no. 4, str. 2.
[30] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, str. 197. Dále SALAHDINE, Fatima, KAABOUCH, Naima. *Social Engineering Attacks: A Survey*. In: Future Internet, 2019, vol. 11, no. 4, str. 2.
[31] MOHAMMAD, Rami, THABTAH, Fadi, MCCLUSKEY, Lee. *Tutorial and critical analysis of phishing websites methods*. In: Computer Science Review, 2015, vol. 17, str. 2-4.

E-mailové zprávy, ve kterých odesílatelé nabízejí peněžní odměnu, přímo požadují poskytnutí hesla, obsahují gramatické chyby nebo mají nedokonalý design, jsou adresáty snáze vyhodnoceny jako podezřelé, a proto jim nevěnují pozornost. Na druhou stranu zprávy, ve kterých jsou pouze „běžné“ informace (týkající se např. aktualizace zabezpečení nebo aktualizace údajů) budou vnímány uživateli jako bezpečné. Toto právě představuje nebezpečí, protože i takto „neškodný“ e-mail může obsahovat odkaz na phishingovou stránku.[32]

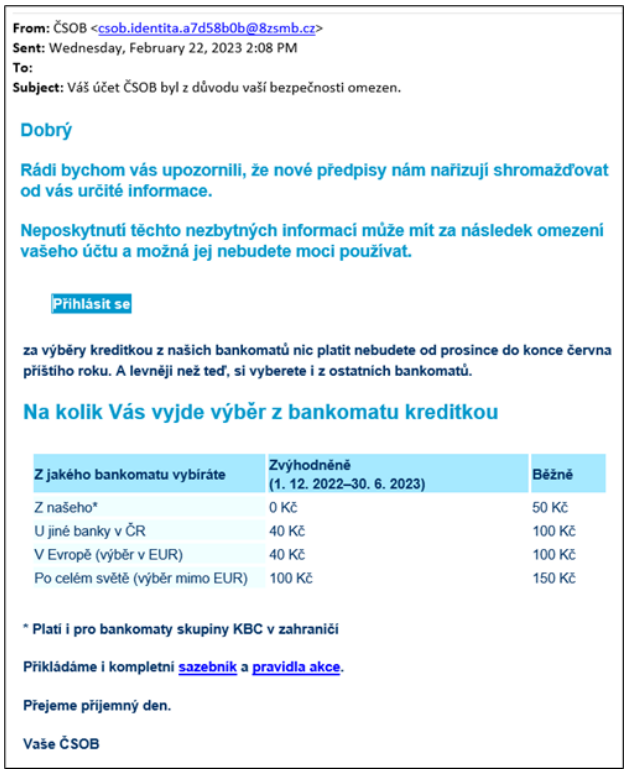
1.3.1. Ukázka phishingového útoku

Pro lepší představu, jak může konkrétně vypadat phishingový útok, jsou uvedeny následující příklady. Byly vybrány útoky, které útočníci uskutečnili na klienty ČSOB a zákazníky České pošty. Nakonec je pak uvedena část z rozhodnutí Krajského soudu v Praze, kde je názorně popsán postup pachatelů při phishingovém útoku.

První příklad je útok na klienty ČSOB.[33] Na obrázku č. 1 je vidět obsah této zprávy, která varuje klienty před nemožností používat jejich bankovní účet, pokud neposkytnou požadované údaje. Klienty by mohla na podvod upozornit adresa odesílatele této zprávy *csob.identita.a7d58b0b@8zsmb.cz*, která je na první pohled podezřelá – doména za zavináčem neobsahuje označení „csob“ a sled čísel a písmen ve jménu taktéž neodkazuje na důvěryhodného adresáta. Obsah zprávy je srozumitelný, i když by některé z frází klientům mohly připadat podezřelé.

Cílem útočníků je, aby klienti bankovní instituce rozkliknuli odkaz na falešnou stránku internetového bankovnictví, který je uveden ve zprávě, a vložili své přihlašovací údaje. Poté, co údaje zadají, se útočníci ihned přihlásí pomocí těchto údajů do skutečného internetového bankovnictví. Klientovi tak následně přijde ověřovací kód do SMS, případně žádost o potvrzení mobilním klíčem, kterou bez podezření potvrdí. Útočníci se tímto způsobem dostanou do internetového bankovnictví, kdy jim už pouze stačí, aby klient potvrdil zadaný převod peněz (opět pomocí SMS či mobilního klíče), který se maskuje například žádostí o nové ověření klienta.

[32] DE KIMPE, Lies et al. *You've got mail! Explaining individual differences in becoming a phishing target*. In: Telematics and Informatics, 2018, vol. 35, no. 5, str. 1278.
[33] *Upozorňujeme na další vlnu phishingových e-mailů, které cílí na klienty internetového bankovnictví*. ČSOB [online]. 2023 [cit. 2023-02-26]. Dostupné z: https://www.csob.cz/portal/-/s230222?redirect=%2Fportal%2Fbezpecnost%2Faktualni-hrozby.



From: ČSOB <csob.identita.a7d58b0b@8zsmb.cz>
Sent: Wednesday, February 22, 2023 2:08 PM
To:
Subject: Váš účet ČSOB byl z důvodu vaší bezpečnosti omezen.

Dobrý

Rádi bychom vás upozornili, že nové předpisy nám nařizují shromažďovat od vás určité informace.

Neposkytnutí těchto nezbytných informací může mít za následek omezení vašeho účtu a možná jej nebudete moci používat.

Přihlásit se

za výběry kreditkou z našich bankomatů nic platit nebudete od prosince do konce června příštího roku. A levněji než teď, si vyberete i z ostatních bankomatů.

Na kolik Vás vyjde výběr z bankomatu kreditkou

Z jakého bankomatu vybíráte	Zvýhodněně (1. 12. 2022–30. 6. 2023)	Běžně
Z našeho*	0 Kč	50 Kč
U jiné banky v ČR	40 Kč	100 Kč
V Evropě (výběr v EUR)	40 Kč	100 Kč
Po celém světě (výběr mimo EUR)	100 Kč	150 Kč

*** Platí i pro bankomaty skupiny KBC v zahraničí**

Přikládáme i kompletní sazebník a pravidla akce.

Přejeme příjemný den.

Vaše ČSOB

Obrázek 1 Ukázka phishingové e-mailové zprávy od ČSOB[34]

Na obrázku č. 2 je e-mailová zpráva údajně zaslaná od České pošty.[35] Příjemci této zprávy je sděleno, že na něj čeká balíček a musí zaplatit pouze 99 Kč, aby jej dostal. Pro zaplacení je přiložen odkaz, prostřednictvím kterého má příjemce zaplatit. V případě vyplnění platebních údajů je pravděpodobné, že tyto údaje získá útočník.

Odhalení podvodu je možné díky gramatickým chybám – „*Wděkujeme*“, „*českou poštu*“ uvedené s malým č. Taktéž e-mail odesílatele neodkazuje na Českou poštu a doména nejvyšší úrovně[36] *.in* může být u českého podniku přinejmenším podezřelá (Česká pošta používá *cpost.cz*). U lidí, kteří žádný balík neočekávají je pravděpodobné, že budou zprávu kontrolovat o trochu více, avšak u těch, kterým má být skutečně něco doručeno, je možné, že zprávě uvěří a poplatek se budou snažit zaplatit. Podle názoru autorky by však mohli příjemci zprávu ověřovat už kvůli dané částce 99 Kč, poněvadž většinou je poplatek za doručení již zaplacen předem nebo se platí až při převzetí balíku (v případě platby na dobírku).

[34] Tamtéž.
[35] *Aktuální podvodné e-maily a SMS: 14. 3. 2023 Bezpečnostní upozornění na podvodné e-maily.* Česká pošta [online]. 2023 [cit. 2023-03-15]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/aktualni-podvodne-e-maily.
[36] Domény nejvyšší úrovně, tzv. TLD, jsou například .eu, .com, .cz atd.

Od: Česká Pošta <support@gautampackersmover.in>

Datum: …

Předmět: Váš balíček na vás čeká.

Česká pošta

Vážený zákazníku.
Wděkujeme, že používáte českou poštu, váš balíček na vás čeká.
Musíte dokončit platbu ve výši (99,00 czk).
Co bych měl dělat?
Kliknutím na zabezpečený odkaz níže dokončíte platbu svých poplatků za dopravu
S pozdravem.

Péče o zákazníky České pošty.

Zaplat 'ted'

Obrázek 2 Ukázka phishingové e-mailové zprávy od České pošty[37]

Poslední ukázkou je jednání pachatelů, kteří se pomocí phishingu dokázali dostat jak na cizí facebookový profil, tak do internetového bankovnictví jiné osoby. Následně přesunuli peněžní prostředky na jiný účet nebo dokonce uzavřeli smlouvu o úvěru a tyto peníze pak převedli. Je zde vidět způsob, jak pachatelé mohou získat autorizační kód pro potvrzení platební transakce. Tento případ řešil Krajský soud v Praze, který rozsudkem odsoudil tři obviněné pro několik skutků spočívající v jednání podobném nebo stejném tomu uvedeném na obrázku č. 3. Na obrázku č. 3 je možné vidět postup obviněných vyplývající z výpovědi svědků.[38]

[37] Tamtéž.
[38] Rozsudek Krajského soudu v Praze ze dne 3. května 2017, sp. zn. 1 T 16/2017. Případ řešil i Nejvyšší soud, dovolání obviněného však bylo usnesením Nejvyššího soudu ze dne 31. října 2018, sp. zn. 6 Tdo 963/2018, odmítnuto.

K bodu 1) výroku rozsudku:

Svědek **J[redacted] Š[redacted]** (výpověď z přípravného řízení na č. l. 754 – 758přečtena dle § 211 odst. 1 tr. řádu), majitel zneužitého facebookového profilu, popsal, kterak se mu po přihlášení na facebook objevilo okno s konverzací, kde jej jeho spolužačka ze základní školy G[redacted] T[redacted] žádala, aby jí poslal hlas do soutěže o Apple iPhone. Žádosti vyhověl, přičemž se mu opět objevila tabulka pro nové přihlášení na facebook. Znovu tedy zadal své přihlašovací jméno a heslo. Pochvíli mu začali psát kamarádi, jestli nemá na facebooku nějaký vir, přičemž sám sledoval, jak někdo z jeho profilu píše dalším lidem, zda by mu nemohli poslat částku kolem 130 Kč. Celou věc se snažil zastavit, prostřednictvím svého bratra dával na facebook na „zeď" příspěvky, ať nikdo nereaguje, které však vzápětí někdo další mazal. Jediný, o kom ví, že na žádost o zaslání peněz reagoval, byla D[redacted] F[redacted].

Svědkyně **D[redacted] F[redacted]** (výpověď z přípravného řízení na č. l. 604 – 608 přečtena dle § 211 odst. 1 tr. řádu) vypověděla, že přes facebook komunikovala s J[redacted] Š[redacted], který ji požádal, aby mu půjčila 126 Kč, neboť potřebuje uskutečnit nějakou platbu. Chtěla mu vyhovět, takže jí poslal odkaz na stránku www.118129.w29.wedos.ws, ze které bylo možné platbu provést okamžitě. Na této stránce zadala přihlašovací údaje ke svému internetovému bankovnictví a dostala odpověď, že se momentálně nelze přihlásit pro odstávku systému. Když tuto informaci napsala J[redacted] Š[redacted], sdělil jí, že tedy zkusí poslat peníze, které má na účtu bez oněch 126 Kč a požádal ji, zda by si k ní nemohl poslat SMS zprávy – autorizační kódy od transakcí, protože mu to na mobilu nejde. Souhlasila a následně jí přišla SMS se jedná o nějakých 200.000 Kč. Věc blíže neřešila, kód opsala a popsala ho přes Facebook údajnému J[redacted] Š[redacted]. Následně ji volali z České spořitelny, a. s., zda si brala úvěr ve výši 200.000 Kč. Záležitost poté oznámila Policii ČR a s bankou se dohodla, že úvěr bude splácet dle dohody o narovnání, kterou s bankou uzavřela.

Obrázek 3 Ukázka phishingového útoku z rozsudku Krajského soudu v Praze[39]

[39] Rozsudek Krajského soudu v Praze ze dne 3. května 2017, sp. zn. 1 T 16/2017.

2. Kriminologické aspekty phishingu

Pro poznání kriminality je důležitý její popis, a to pomocí zjištění stavu, změn v rozsahu, intenzity a struktury kriminality během delšího časového období, ke kterému slouží analýza dat získaných ze statistik, ale i z jiných zdrojů. Dále je zapotřebí si klást otázky nejenom ohledně charakteristiky pachatele, ale též oběti trestného činu. Předmětem kriminologie je i kontrola kriminality, která se zabývá způsoby jak kriminalitu omezit a kontrolovat.[40]

2.1. Vývoj phishingu a jeho další druhy

2.1.1. Historie phishingu

Slovo „phishing" pochází z roku 1996, na původ názvu je více teorií. Použití písmen „ph" bylo nejspíše odvozeno od slova „phreaking", které vyjadřuje jednání, kdy se někdo snaží nezákonně získat výhodu v podobě levnějšího či zcela bezplatného uskutečňování telefonních hovorů, případně i odposlouchávat ostatní.[41] Další teorií je, že slovo phishing vzniklo jako zkratka výrazů „password harvesting fishing", tedy přeloženo doslovně „sběr hesel rybařením".[42]

První případ phishingu se objevil v Americe v roce 1995 nebo 1996[43] a týkal se společnosti America Online (AOL). Útočníci se vydávali za administrátory této společnosti, aby vylákali z uživatelů jejich přihlašovací údaje nebo nechali uživatele zadat přímo platební údaje. Jako důvod uvedli, že se vyskytl problém ohledně platby za vyúčtování služeb. V té době nemělo tolik lidí přístup k internetu, tyto případy tedy nebyly úplně časté, avšak na druhou stranu byly docela úspěšné, protože internet byl pro lidi novým a neznámým prostředím, nebyli proto tolik ostražití.[44]

V letech 2003 a 2004 došlo k velkému nárůstu počtu případů. Podle sdružení Anti-Phishing Working Group (založené v roce 2003) bylo v lednu 2004 zaznamenáno 176 případů, což bylo o 52 % více jak v prosinci 2003. Nejčastějším terčem byla internetová aukční síň eBay.[45] V České republice je prvním zaznamenaným případem v bankovním sektoru pokus phishingu, který se stal

[40] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 25.
[41] Tímto způsobem je možné získat i přístup k síti Internet a užívat jeho služeb v podstatě anonymně. Díky tomu se phreakingový útok využívá k provedení dalšího útoku z důvodu obtížného vypátrání pachatele díky jeho vstupu na síť. Vždy tedy dochází ke zneužívání telekomunikačních služeb poskytovatele, resp. zneužívání telefonních linek. (Zdroj: VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestně právní kvalifikace*. In: Trestní právo, 2010, roč. 14, č. 12, str. 12).
[42] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 224.
[43] Zdroje se ohledně konkrétního roku rozcházejí.
[44] LANCE, James. *Phishing bez záhad*. Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, str. 28.
[45] *Phishing Activity Trends Report*. Anti-Phishing Working Group [online]. 2004 [cit. 2022-11-15]. Dostupné z: https://docs.apwg.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.

v březnu 2006 a směřoval proti klientům Citibank. V létě 2006 pak následoval útok na klienty České spořitelny.[46]

Dříve byly phishingové zprávy poznatelné na první pohled díky své gramatice, překlepům a hůře provedené stylistice. V současnosti jsou e-maily napsané mnohem lépe, jsou přesvědčivější a obsahují potřebná loga a grafiku instituce, která zprávu měla údajně odeslat. Falešné webové stránky jsou identické s těmi pravými, poznat rozdíl je prakticky nemožné.[47]

V České republice máme výhodu jazykovou. Útočníkům se mnohdy nevyplatí shánět a platit překladatele, když mohou zaútočit pouze na „malý" kousek populace v rámci celého světa, proto většinou použijí internetové překladače, které už se sice také dostávají na kvalitní úroveň, ale s českým jazykem si ještě dokonale neporadí. Proto se na území České republiky uplatňují spíše útoky lokální, tedy jednání útočníků jako českých občanů, a tím se stávají tyto útoky nebezpečnější. Útočníci znají prostředí a i své potenciální oběti.[48]

Nedošlo pouze k vývoji podvodných e-mailů a jiných forem zpráv, ale také k vývoji falešných URL stránek. Webové stránky jsou vyhledatelné pod doménovým jménem, které se zobrazuje v panelu pro vyhledávání stránek. Útočníci využívají jednoduchou techniku tzv. *fuzzy domains* nebo také *look-alike domains*. V tomto případě jde pouze o oklamání uživatele, aby si nevšiml, že název webové stránky je odlišný od té skutečné.[49] Útočníci spoléhají na to, že uživatelé pravděpodobně nebudou kontrolovat pečlivě všechny znaky v názvu webové stránky a stanou se tak obětí. Studií Dhamija a kolektivu bylo zjištěno, že i malá změna může způsobit, že se nachytá velký počet uživatelů. V rámci výzkumu bylo pozměněno písmeno „w" v názvu stránky www.bankofthewest.com, kdy jej nahradilo dvakrát písmeno „v", tedy www.bankofthevvest.com. Tato změna obelstila 91 % účastníků výzkumu, kteří změnu nerozpoznali.[50]

Útočníci si proto často registrují falešnou doménu, která se podobá skutečné, ale je zde pozměněna skladba písmen, přívlastek je navíc nebo je jiná doména nejvyšší úrovně.[51] Jako příklad modifikace české stránky by mohla posloužit například webová stránka České spořitelny, jejíž URL adresa je www.csas.cz. S využitím techniky *fuzzy domains* by si mohli útočníci

[46] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, str. 113.
[47] SRIVASTAVA, Tushar. *Phishing and Pharming – The Deadly Duo*. SANS Institute, 2007, str. 6.
[48] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. [online]. Praha, 2012 [cit. 2022-12-14]. Disertační práce. Univerzita Karlova, Právnická fakulta, Katedra trestního práva. Vedoucí práce Jelínek, Jiří. str. 99.
[49] LANCE, James. *Phishing bez záhad.* Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, str. 30.
[50] DARWISH, Ali, ZARKA, Ahmed, ALOUL, Fadi. *Towards understanding phishing victims' profile*. International Conference on Computer Systems and Industrial Informatics, IEEE, 2012, str. 2.
[51] LANCE, James. *Phishing bez záhad*. Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, str. 30.

například registrovat doménu www.cssas.cz, www.cssa.cz nebo i www.csas.eu apod. Sofistikovanějším způsobem je případ, kdy útočníci použijí spyware, který nainstaluje do počítače falešný panel pro zadávání internetové adresy a doménové jméno falešné stránky pak vypadá stejně jako to originální.[52]

Rozšíření phishingu napomohla i oblíbenost sociálních sítí. Pokud útočník neoprávněně získá přístup k cizímu profilu na sociální síti, může z něho požádat ostatní uživatele, které má oběť „v přátelích", o zaslání menších finančních částek. Této žádosti oběti často vyhoví, protože pochází od člověka, kterého znají. Útočník ke zprávě připojí zpravidla i odkaz na falešné stránky internetového bankovnictví nebo platební bránu a tím zneužije platební údaje. Pokud získá i ověřovací kód, dokáže z účtu oběti odčerpat finanční prostředky.[53]

S rozvojem internetového bankovnictví, kdy většina lidí zadává své platební příkazy právě přes internet nebo přes internet platí platebními kartami, se finanční kriminalita částečně změnila z přímé na nepřímou. Útočníci již nevykrádají banky se zbraněmi, ale napadají účty klientů bank přes internet.[54]

Z výše uvedeného vyplývá, že techniky phishingu se stále vyvíjí a využívají všech nových trendů, aby oklamaly i takové uživatele, kteří dbají na svoji bezpečnost v kyberprostoru.

2.1.1.1. Nigerijské listy

Někdy se za předchůdce phishingu považují tzv. Nigerijské listy[55] (neboli podvod typu vymáhání zálohového poplatku) vzhledem k povaze podvodného jednání. V současné době se v literatuře občas řadí pod phishing, avšak podle názoru autorky jde o samostatnou kategorii spadající pod scam. Za phishing se proto nepovažují, ač využívají podobné metody. Tento názor zastává např. Lance[56], naopak podle Koloucha[57], vzhledem k povaze podvodného jednání, by bylo možné Nigerijské listy zařadit pod phishing. V této kapitole budou proto Nigerijské listy zjednodušeně popsány. Hlavním rozdílem mezi nimi a phishingem je, že se pachatel nevydává za

[52] HLAVÁČOVÁ, Kateřina. *Phishing a jeho postupná evoluce*. In: VOJÁČEK, Ladislav, TAUCHEN, Jaromír (ed.). Majetkové a hospodářské trestné činy včera a dnes. Sborník z konference. Brno: Masarykova univerzita, 2016, str. 271.
[53] Tamtéž, str. 273.
[54] LANCE, James. *Phishing bez záhad*. Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, str. 22.
[55] Známé také pod označením Scam 419, číslo 419 má vyjadřovat číslo ustanovení v nigerijském trestním zákoníku, který upravuje podvodné jednání. (Zdroj: KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 59).
[56] LANCE, James. *Phishing bez záhad*. Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, str. 31.
[57] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 239.

osobu či společnost, kterou uživatel zná, ale předmětem zprávy je většinou nějaký sentimentální příběh.

Počátek Nigerijských listů se odhaduje na začátek 80. let 20. století, jde tak o dobu, kdy internet v dnešní podobě ještě neexistoval.[58] Dříve byly pro Nigerijské listy využívány pouze klasické prostředky komunikace, například dopisy, které však mají pouze omezený rozsah. Až elektronická pošta z nich učinila celosvětovou hrozbu, protože poskytla možnost zasílání podvodných psaní neomezenému počtu adresátů.[59]

V případě Nigerijských listů útočníci využívali, že uživatelé neznali politickou situaci v západoafrických zemích. Slibovali jim převedení milionových částek z tzv. mrtvých kont, které měly zůstat po obětech anebo svržených diktátorech po proběhlé občanské válce v Nigerii nebo jiné africké zemi. Častý byl i příběh tamních podnikatelů či farmářů, že jsou ohroženi na životě, a proto musí emigrovat ze země, kde nechtějí zanechat svůj majetek. K převodu majetku však potřebovali pomoc od adresátů zpráv, za kterou slíbili podíl na daném majetku. Asistence spočívala většinou v různých poplatcích, např. za zřízení společnosti, přes kterou bude majetek vyveden, za převoz atd.[60]

Nigerijské listy obecně apelují na city adresáta, kdy útočník vymyslí dojemný příběh a požádá o zaslání peněžních prostředků nebo alespoň půjčky.[61] Další variantou je případ, kdy prostřednictvím elektronické pošty jsou příjemci těchto zpráv lákáni na nabídky vysokých finančních částek, kde na straně odesílatele stojí například vdova po bohatém podnikateli. Ta prosí o pomoc při převodu peněz ze země, kde žije, a za tuto pomoc slibuje vysokou odměnu. Podmínkou je zaplacení určité platby, která je však většinou oproti slíbené odměně nízká. Pokud příjemce příběhu uvěří a zašle požadovanou částku, je zpravidla opakovaně vyzýván k zaplacení dalších peněžních částek, které vznikají v souvislosti s převodem peněz.[62]

Touto taktikou spoléhají útočníci na základní fungování lidské psychiky, kdy oběť poté, co zaplatí prvotní požadovanou částku, se nechce své investice vzdát. Jak se postupně celková částka poskytnutá obětí zvyšuje, je pro oběť stále těžší ztrátu přijmout a naopak roste očekávání, že

[58] VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestně právní kvalifikace*. In: Trestní právo, 2010, roč. 14, č. 12, str. 11.
[59] KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi*. In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 59.
[60] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 490.
[61] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 401.
[62] VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestně právní kvalifikace*. In: Trestní právo, 2010, roč. 14, č. 12, str. 11.

poslední splátka už bude opravdu poslední a bude získána jen slíbená odměna. Což samozřejmě nenastane.[63]

2.1.2. Typy phishingu

Phishing získal postupně několik podob, které mohou pro útočníky znamenat mnohem vyšší výnosy. Podle formy a způsobu oklamání uživatelů jej lze rozdělit na následující typy.

2.1.2.1. Pharming

Jde o složení slov „phreaking“[64] a „farming“ (ve smyslu hospodaření, farmaření). Jedná se o sofistikovanější formu phishingu a velice nebezpečnou, protože uživatel se může podílet pouze minimálně a i tak je napaden. U tohoto typu není již tolik využíváno sociální inženýrství.[65]

V tomto případě jde o manipulaci provozu webových stránek, to následně vede ke krádeži citlivých informací. Může být spáchán dvěma způsoby. U první metody jde v podstatě o útok na server doménových jmen (zkratka DNS z anglického *Domain Name System*), pomocí něhož dochází k převodu adresy zadávané do webového prohlížeče na IP adresu.[66] U druhé metody jde pak o útok na jednotlivé počítače, kdy útočník umístí škodlivý program přímo do počítače uživatele. Přesměrování na falešnou webovou stránku je pak automatizované vlivem jednání útočníka.[67]

V případě, že se jeden z postupů útočníkovi podaří, tak poté, co uživatel zadá v internetovém prohlížeči správnou adresu, nedojde k propojení na příslušnou IP adresu originálního webového serveru, ale na podvrženou IP adresu. Doménové jméno v adresním řádku však zůstává stejné jako zadané.[68] Falešné webové stránky věrně imitují ty originální, uživatel většinou nepozná rozdíl a zadá své přihlašovací údaje, které následně získá útočník. Tyto falešné webové stránky mají za cíl buď zachytit osobní nebo přihlašovací údaje, nebo se pokoušejí do počítače nainstalovat škodlivý malware. Výsledek je tak stejný jako u phishingu.[69] Nejčastěji jde

[63] KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi*. In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 59.
[64] Viz kapitola 2.1.
[65] *What Is Pharming and How to Protect Yourself. Kaspersky* [online]. [cit. 2022-11-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming.
[66] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, str. 113.
[67] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017, str. 38.
[68] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 263.
[69] DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 86.

o stránky internetového bankovnictví, online platební platformy apod. Jakmile pachatel získá údaje oběti, může je sám použít k podvodnému jednání nebo je prodá jiné osobě na dark webu.[70]

Tyto útoky jsou méně časté, poněvadž vyžadují od útočníka více práce a počítačových znalostí, ale na druhou stranu jsou nebezpečnější, protože mohou postihnout velké množství uživatelů, aniž by o tom věděli.[71] Obrana před pharmingem je pro uživatele velice obtížná. U napadení DNS se oběť nemůže bránit žádným způsobem. Proti útoku na úrovni lokálního počítače je jediná ochrana, kterou by měl dodržovat každý uživatel, a to obecná ochrana před zavlečením škodlivého softwaru (užívání originálního softwaru a jeho pravidelná aktualizace, užívání antiviru a firewallu, neaktivování podezřelých odkazů atd.), která tento útok může minimalizovat.[72]

2.1.2.2. Spear-phishing

Spear-phishing je další formou phishingu, na rozdíl od základní podoby phishingu jde o útok cílený a nikoliv nahodilý. Cílem tohoto útoku je někdo konkrétní, ať už jde o jednotlivce, skupinu nebo organizaci.

Útočník jde po určitých datech či informacích konkrétního subjektu, např. organizace (může se jednat o duševní vlastnictví, finanční údaje, utajované informace apod.). Využije volně dostupné zdroje (s tím mu značně pomáhají sociální sítě), aby zjistil o cílovém příjemci co nejvíce informací a na základě toho vytvoří e-mail nebo jinou zprávu, která díky získaným znalostem působí věrohodně. Prostřednictvím těchto zpráv pak začne komunikovat s osobou zevnitř organizace jako s kolegou[73], kdy tato osoba komunikuje s útočníkem bez problému, protože jde o osobu jí známou, proto její zprávy často nijak neprověřuje. Útočník může oběť využít jako prostředek pro šíření dalších zpráv, které mohou být infikovány malwarem, v rámci organizace.[74]

Sofistikovanost útočníků se neustále zvyšuje, jsou přesvědčivější a dotýkají se aktuálních témat (v poslední době například pandemie koronaviru), pro uživatele je z toho důvodu složitější falešnou zprávu rozpoznat. Motivací útočníků v tomto případě může být finanční zisk, krádež dat nebo i vyřazení systémů (pro společnosti znamenají ztrátu pohybující se v řádech desítek až stovek

[70] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 263.
[71] *What Is Pharming and How to Protect Yourself. Kaspersky* [online]. [cit. 2022-11-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming.
[72] JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016, str. 396.
[73] Avšak zde už pouze použití netypického pozdravu, či vykání namísto tykání a naopak, zvyšuje pravděpodobnost, že uživatel podvod odhalí a útočníkovi nepodlehne.
[74] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 264.

milionů korun a také přerušení služeb pro jejich uživatele). Společnosti mohou taktéž čelit vysokým pokutám v případě, že útočníci získají osobní údaje zákazníků.[75]

Chyba jednoho zaměstnance může mít závažné důsledky pro společnost, stát i pro neziskové organizace. Díky získaným datům mohou pachatelé nabýt citlivé informace, ale i ovlivnit trh s akciemi či spáchat některé činy související se špionáží. Navíc se útokem může do počítačů dostat malware, čímž se tyto počítače dají zneužít na útok DoS (Denial of Service).[76] Konkrétním příkladem, který měl velmi závažné následky, byl případ na Ukrajině v roce 2016, kde otevření spear-phishingového e-mailu obsahujícího škodlivý malware BlackEnergy, znamenalo šestihodinový výpadek elektrické energie u 230 000 osob.[77]

Spear-phishing má i svoji fyzickou formu, která se nazývá „baiting". Může jít o případ, kdy útočník nechá někde v blízkosti svého cíle (například na parkovišti společnosti) pohozený USB disk, který obsahuje škodlivý kód. Zaměstnanec společnosti ho může vzít s cílem nalézt jeho vlastníka a zapojí ho do pracovního počítače, který je připojen k cílové síti. Škodlivý kód pak umožní útočníkovi přístup do sítě.[78]

2.1.2.2.1. Whaling attack

Whaling neboli lov velryb spadá pod formu spear-phishingu a cílí převážně na vysoce postavené osoby v rámci dané organizace. Útočníci se snaží o těchto osobách zjistit co nejvíce informací (například přes sociální sítě), aby pak mohli jejich jménem rozesílat ostatním členům organizace věrohodně vypadající zprávy. Je zde mnohem pravděpodobnější, že se útok povede, protože každý splní pokyn spíše od svého nadřízeného, než když ho pošle řadový zaměstnanec nebo někdo úplně cizí. Zaměstnanci se většinou zdráhají odmítnout žádost od někoho, koho považují za důležitého.[79]

Vcelku úspěšný útok se skoro povedl na hračkářskou společnost Mattel, když finanční ředitel obdržel e-mailovou zprávu se žádostí o převod finančních prostředků od útočníka, který se

[75] *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit.* Národní úřad pro kybernetickou a informační bezpečnost [online]. 2020 [cit. 2022-11-22]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/.
[76] *What is Spear Phishing?*. Kaspersky [online]. [cit. 2023-02-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/spear-phishing.
[77] *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit.* Národní úřad pro kybernetickou a informační bezpečnost [online]. 2020 [cit. 2022-11-22]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/.
[78] Tamtéž.
[79] *Whaling: how it works, and what your organisation can do about it.* National Cyber Security Centre [online]. [cit. 2022-11-22]. Dostupné z: https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it.

vydával za nového výkonného ředitele. To mu vyšlo, poněvadž společnost procházela zrovna personálními změnami. Společnost málem přišla o 3 miliony dolarů.[80] Nestalo se tak, protože převod peněz, které mířily do banky v Číně, pozdržel státní svátek, a díky včasnému zásahu čínské policie byl bankovní účet zmražen a peníze vráceny zpět společnosti Mattel. Útočník se však dodnes nezjistil.[81]

V České republice byl v prosinci 2022 zaznamenán případ, kdy společnost z Českých Budějovic přišla o zhruba 1,2 milionu korun. Údajný předseda představenstva společnosti měl poslat e-mailovou zprávu místopředsedovi představenstva, aby poslal částku okolo 1,2 milionu korun (částka byla uvedena v eurech) na zahraniční účet. Místopředseda představenstva si nezkontroloval e-mailovou adresu svého nadřízeného, která nebyla kopií existující e-mailové adresy, ale šlo o podezřelou adresu, a částku poslal.[82]

2.1.2.3. Vishing

Vishing jako další druh phishingu probíhá skrze telefonický hovor, jde o kombinaci slov „voice" a „phishing". Útočník se v tomto případě snaží pod falešnou identitou vylákat od uživatele např. přihlašovací údaje, údaje z platebních karet apod. Často se útočník vydává za zástupce banky či jiné známé instituce.[83] Útočníci využívají tzv. spoofingu[84] telefonního čísla, tím dokážou napodobit jakékoliv telefonní číslo, tedy i infolinku banky.[85]

Volající, který se představí například jako pracovník určité banky, upozorňuje uživatele, že jeho účet byl napaden a že je nutné, aby své peníze z účtu převedl na bankovní účet, který volající označí jako bezpečný. Má se prý jednat pouze o dočasné bezpečnostní opatření. Toto někdy bývá „potvrzeno" dalším hovorem, tentokrát od osoby vydávající se za policistu. Údajný policista potvrzuje informace z předchozího hovoru a upozorňuje na nezbytnost převedení peněžních prostředků na bezpečnější účet. Pak už volající požaduje pouze sdělení autorizační SMS

[80] *What is a Whaling Attack?*. Kaspersky [online]. [cit. 2022-11-11]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack.
[81] *Mattel vs. Chinese cyberthieves: It's no game*. CBS NEWS [online]. 2016 [cit. 2022-11-22]. Dostupné z: https://www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/.
[82] BARTOSZ, Jakub. *Člen vedení budějovické firmy poslal podvodníkovi přes milion*. [online]. 2022 [cit. 2022-12-29]. Dostupné z: https://www.novinky.cz/clanek/krimi-clen-vedeni-budejovicke-firmy-poslal-podvodnikovi-pres-milion-40417671#dop_ab_variant=0&dop_source_zone_name=novinky.sznhp.box&source=hp&seq_no=8&utm_campaign=abtest203_personalizovany_layout_varAA&utm_medium=z-boxiku&utm_source=www.seznam.cz.
[83] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 265.
[84] Za spoofing lze obecně považovat jakoukoliv situaci, kdy se útočník vydává za někoho jiného. Může jít o falešné telefonní číslo, e-mail nebo i IP adresu.
[85] *Vishing a spoofing*. Policejní prezidium ČR [online]. 2021 [cit. 2022-11-22]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx.

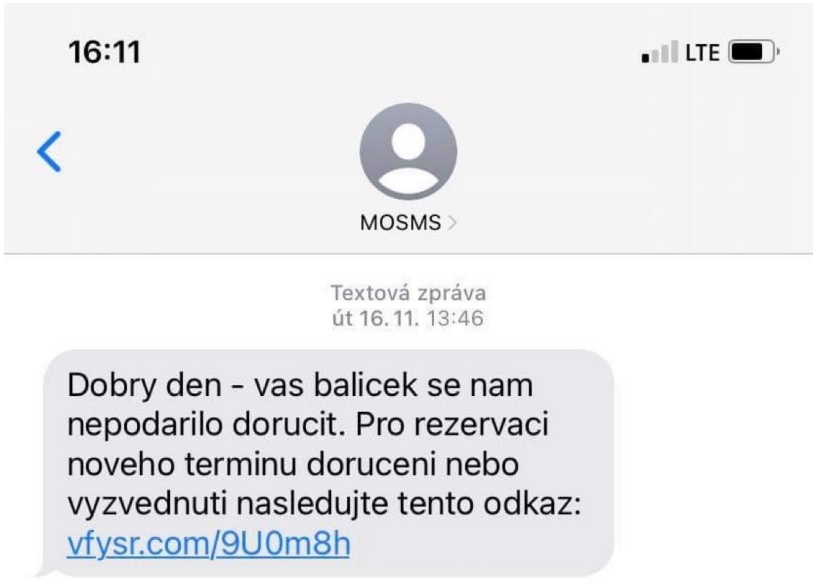
nebo jiné potvrzení platby, která má být tím bezpečnostním opatřením. Pokud oběť potvrdí i toto, o své finanční prostředky na účtu přijde.[86] Útočníci často volají v noci, kdy je uživatel rozespalý a zmatený a snáze se pak řídí pokyny útočníka, podle kterého je nutné jednat okamžitě.[87]

2.1.2.4. Smishing

Smishing, kombinace slov „SMS“ a „phishing“, je podvodné jednání probíhající skrze SMS zprávy. Cílem útočníků je buď vylákat z uživatele peníze (např. tím, že zavolá na placenou infolinku nebo pošle dárcovskou SMS), anebo donutit uživatele kliknout na podezřelé URL adresy. Po kliknutí na URL adresu může být uživatel přesměrován na falešnou stránku, která po něm vyžaduje zadání údajů nebo instaluje malware.[88] Také může aktivací odkazu dojít k ovládnutí mobilního telefonu či zneužití dat, které telefon obsahuje.[89]

Autorka této práce se setkala se smishingem v podobě SMS zprávy (viz obrázek č. 4), která jí přišla dne 16. listopadu 2022 a odkazovala na doručení balíčku, který si údajně autorka nepřevzala. Zde lze snadno odhalit, že se může jednat o podvod. Zpráva nepíše nic o tom, kdo zásilku přepravuje, o jakou zásilku jde (její číslo) a kdy ji doručovali. Ani uvedený odkaz nevypadá jako by byl od známého přepravce. Tyto SMS zprávy jsou často zasílány například před Vánoci, kdy se předpokládá, že lidé nakupují vánoční dárky z internetových obchodů a nemají dokonalý přehled o tom, co objednali a co už vyzvedli.

[86] Tamtéž.
[87] *Vishing: Jak ho rozeznat a vyhnout se mu?*. ESET [online]. 2021 [cit. 2022-11-22]. Dostupné z: https://digitalsecurityguide.eset.com/cz/vishing-jak-ho-rozeznat-a-vyhnout-se-mu.
[88] KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 266.
[89] JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016, str. 396.



Obrázek 4 SMS zpráva zaslaná na telefonní číslo autorky

2.2. Počet případů phishingu

Ačkoliv k phishingu dochází poměrně často, uživatelé jsou stále náchylní stát se obětí podvodných e-mailů a falešných webových stránek. Velký počet případů kybernetických útoků phishingu je dán mimo jiné i díky tomu, že těží z výhod, které mimo kybernetický svět neexistují. Takovou výhodou je například bezplatnost e-mailů a jejich snadné a okamžité rozšíření po celém světě z jednoho místa.[90]

Útočníci využívají i různých aktuálních témat. Kupříkladu během pandemie koronaviru se objevilo mnoho zpráv s touto tematikou, kdy útočníci chtěli zneužít strach lidí z této nemoci a s tím související vyhledávání informací o COVID-19. Útočníci například zasílali zprávy, ve kterých jménem nějaké instituce nabízeli uživatelům, že mohou zjistit, kdo konkrétně v jejich okolí je nakažen. Pokud se uživatelé nachytali a otevřeli přílohu, stáhli si do svého počítače malware nebo jiný počítačový virus.[91]

V České republice vede od roku 2011 Policie České republiky statistiku trestných činů, které spadají pod kybernetickou kriminalitu. Z ní je možné zjistit u každého trestného činu, kolik

[90] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. [online]. Praha, 2012 [cit. 2022-12-14]. Disertační práce. Univerzita Karlova, Právnická fakulta, Katedra trestního práva. Vedoucí práce Jelínek, Jiří. str. 92.
[91] ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. In: Frontiers in Computer Science, 2021, vol. 3, str. 3-4.

jich bylo spácháno v kyberprostoru.[92] Co se týče phishingu, je tedy možné zjistit počet spáchaných trestných činů podvodu v kyberprostoru a celkový počet spáchaných trestných činů podvodu, ale stále není zjistitelné, zda se jedná konkrétně o phishing. Statistika zahrnující trestné činy upravené v § 230-232 TrZ, které je možné zařadit prakticky pouze do kyberkriminality, je vedena i v rámci statistiky z oblasti justice Ministerstvem spravedlnosti České republiky.

Podle zprávy Policie České republiky o vývoji registrované kriminality v roce 2022 je v oblasti kybernetické kriminality dlouhodobě evidován poměrně stálý a vysoký růst této kriminality. Dále zpráva uvádí: „*Určitá část protiprávního jednání spočívá souběhově i v napadení emailových účtů, resp. jejich přístupových údajů, případně v napadení přístupových údajů sociálních sítí a v neposlední řadě taktéž např. přístupů do internetového bankovnictví.* […] *Dále stále zaznamenáváme případy tzv. reverzních inzertních podvodů a od srpna roku 2022 se setkáváme s podvodnými SMS zprávami, které se tváří jako odeslané od Ministerstva práce a sociálních věcí, kdy je cílem pachatele vylákat z oběti přístupové údaje do bankovnictví a ty následně zneužít. Již tradičně byl v prosinci zaznamenán nárůst tzv. „vánočního phishingu", tedy podvodných e-mailů a SMS zpráv s legendou o doplacení zásilky, opět s cílem zejména vylákat citlivé bankovní údaje a tyto zneužít".*[93]

V souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, bylo dotázáno Ministerstvo spravedlnosti České republiky a Policie České republiky: „*Kolik trestných činů podvodu podle § 209 TrZ bylo spácháno prostřednictvím internetu a jaký je celkový počet těchto trestných činů spáchaných v letech 2017-2023?".* Na žádost odpovědělo Ministerstvo spravedlnosti, které informovalo, že nevede statistiky trestných činů spáchaných prostřednictvím internetu, ale pouze statistiku obecnou. Policie České republiky poskytla statistiku týkající se trestného činu podvodu, spáchaného prostřednictvím internetu, která byla vložena do tabulky č. 1. Z tabulky lze usuzovat, že jde o vzrůstající počet podvodů spáchaných na internetu, ačkoliv stále není možné zjistit, jaká část z toho jsou phishingové útoky.

[92] VOKUŠ, Jiří. *Kybernetická kriminalita*. Policie České republiky [online]. 2019 [cit. 2023-03-28]. Dostupné z: https://www.policie.cz/clanek/kyberneticka-kriminalita.aspx.
[93] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022*. Policie České republiky [online]. 2023 [cit. 2023-04-28]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx.

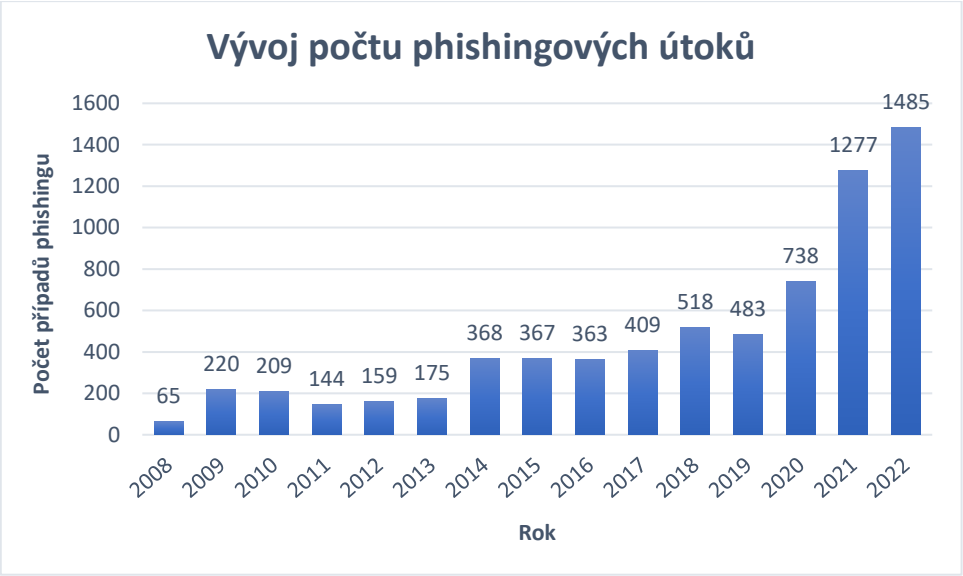
	Celkový počet registrovaných skutků podle § 209 TrZ	Z toho spáchané pomocí internetu
2017	8 752	2 416
2018	8 449	2 673
2019	9 179	3 829
2020	7 952	3 735
2021	8 471	4 373
2022	13 263	7 941
2023[94]	2 573	1 528

Tabulka 1 Statistika Policie České republiky 2017-2023 týkající se § 209 TrZ

V České republice vede statistiku ohledně kybernetických útoků také CSIRT.CZ, nebo-li Národní CSIRT tým České republiky, který provozuje sdružení CZ.NIC, a to na základě veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem. Od 1. srpna 2017 pak veřejnoprávní smlouva přešla pod Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem pro kybernetickou bezpečnost. CSIRT (*Computer Security Emergency Response Team*) je obecné označení týmu, který hledá bezpečnostní incidenty, jejich řešení a jak jim předcházet. Na webových stránkách CSIRT.cz je uvedena statistika řešených incidentů mezi nimiž se nachází i phishing. Tato statistika je tvořena incidenty, které nahlašují uživatelé prostřednictvím formuláře uvedeného na webových stránkách CSIRT, ale i incidenty nahlášenými od zahraničních či tuzemských partnerů.[95]

Pro větší přehlednost jsou údaje vloženy do grafu, aby bylo poznatelné, jak se počet incidentů vyvíjí v čase. Na grafu č. 1 je vidět zjevný stoupající trend počtu případů v rámci České republiky od roku 2008 do roku 2022. Ve statistice zveřejněné CSIRT.CZ je zaznamenán také počet případů za rok 2023, který na konci května přesahuje 900 případů, avšak do grafu uvedeného níže není tento údaj zahrnut, poněvadž by tento graf, zaznamenávající pouze roční přehledy, zkresloval. I tak ovšem jde o velké množství případů, které byly zaznamenané za pouhých pět měsíců.

[94] Údaje za období od 1. ledna 2023 až 28. února 2023.
[95] *O týmu CSIRT.CZ*. CSIRT.CZ [online]. 2019 [cit. 2023-03-09]. Dostupné z: https://csirt.cz/cs/hlaseni-incidentu/faq/.



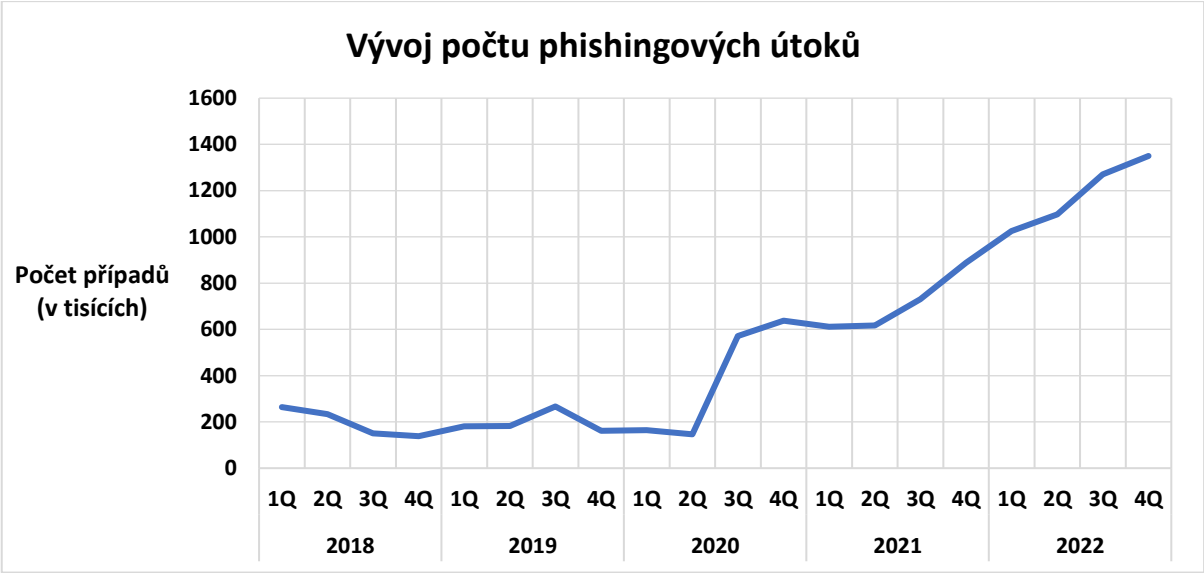
Graf 1 Statistika CSIRT.CZ[96]

Mezi nejčastěji zaznamenané podvodné aktivity v roce 2022, které byly řešeny ve spolupráci s Policií České republiky, patří phishingové kampaně, falešné e-shopy, falešné webové stránky, atd. Na zvýšený počet řešených incidentů může mít vliv například stále větší míra digitalizace, automatizace procesů a rozšiřující se využívání informačních systémů v různých oblastech.[97]

V rámci světových záznamů případů phishingu byla vybrána statistika neziskové asociace Anti-Phishing Working Group, která se zaměřuje na boj proti krádežím identity a podvodům. Sdružuje členy, kteří mohou být značně postihnuti phishingovými útoky. Členy se mohou stát bankovní instituce, online obchodníci, poskytovatelé internetových služeb a další. Nyní má okolo 2300 členů včetně Microsoft, McAfee, či PayPal.[98]

APWG zveřejňuje čtvrtletní záznamy vývoje počtu případů, a to již od roku 2004. Pro diplomovou práci byly použity záznamy pouze od roku 2018, poněvadž pro tuto práci není potřeba rozsáhlé časové období, aby bylo zřejmé, jak se trend vyvíjí. Údaje ze čtvrtletních zpráv jsou vzaty z kolonky *Unique phishing sites*, která je ve statistických zprávách brána jako základní měřítko počtu nahlášeného phishingu po celém světě. Tabulka s přesným počtem případů za každé čtvrtletí je uvedena v Příloze č. 1.

[96] *Statistiky řešených incidentů*. CSIRT.CZ [online]. 2022 [cit. 2023-05-22]. Dostupné z: https://csirt.cz/cs/o-nas/statistiky/.
[97] *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2022*. CSIRT.CZ [online]. 2023 [cit. 2023-03-28]. Dostupné z: https://csirt.cz/cs/o-nas/.
[98] *About The APWG*. Anti-Phishing Working Group [online]. 2023 [cit. 2023-03-09]. Dostupné z: https://apwg.org/about-us/.



Graf 2 Statistika APWG[99]

Ze zprávy APWG ze čtvrtého čtvrtletí roku 2022 vyplývá, že počet případů dosáhl dalšího maxima, za rok 2022 bylo přes 4,7 milionu případů phishingových útoků, které tato organizace zaznamenala. Celkový počet může být mnohem větší. Ve zprávě se uvádí, že od začátku roku 2019 je zaznamenán strmý nárůst počtu phishingových útoků, a to o více než 150 % ročně.

Na konci května 2023 bylo také možné najít na internetu aktivních více než 70 000 platných phishingových webových stránek. I to prokazuje, že phishing je stále aktuálním problémem.[100]

Závěrem lze uvést, že počet zaznamenaných případů phishingu v České republice i celkově ve světě má vzestupnou tendenci. Nic prozatím nenaznačuje, že by do budoucna měly tyto křivky postupně klesat. Vzhledem k přetrvávajícímu užívání výhod kyberprostoru se snížení počtu případů nepředpokládá. Hypotéza daná v úvodu této diplomové práce, že počet detekovaných případů phishingových útoků se stále zvyšuje, byla správná, což jasně ukazují dva výše uvedené grafy a tabulka.

2.3. Pachatel

Podle kriminologie není pachatelem jen osoba, která naplnila znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, ale i osoba, kterou orgány činné v trestním řízení trestně nestíhají. Kriminologie se zaměřuje i na osoby, které svým věkem (děti) nebo stavem

[99] *Phishing Activity Trends Reports*. Anti-Phishing Working Group [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://apwg.org/trendsreports/
[100] *Statistics about phishing activity.* PhishTank [online]. Cisco Talos Intelligence Group, 2023 [cit. 2023-05-25]. Dostupné z: https://www.phishtank.com/stats.php

vědomí (nepříčetnost) přesahují uvedený rámec, který vymezuje trestní právo. Zabývá se též jedinci, kteří si svůj trest za spáchaný trestný čin odpykali, ale i jedinci, kteří by mohli být potenciální pachatelé trestných činů apod.[101]

Tato část představuje některé charakteristiky pachatelů kybernetické kriminality obecně, přičemž následně se bude zabývat pouze pachateli phishingu a jejich znaky, ač je není možné zcela jednoznačně specifikovat.

2.3.1. Pachatel kyberkriminality

Se vznikem nového druhu trestné činnosti je obvykle spojeno i vytvoření nové kategorie pachatelů, kteří se této trestné činnosti dopouštějí. Kybernetická kriminalita však představuje velmi nesourodé spektrum nesourodých možností a způsobů spáchání, které jsou spojeny pouze objektem počítače.[102] Typologie pachatelů bude rozdílná u různých druhů kybernetické kriminality. Jiný pachatel bude v případě šíření dětské pornografie a jiný pachatel bude u phishingu.[103]

Pachatel se nachází v kyberprostoru jako globálním prostředí, může se v něm velmi rychle pohybovat, změnit identitu i zmizet, může vytvářet, předstírat nebo i realizovat různé hrozby. Výhodou pro něj je možnost využívat různost právních předpisů v různých jurisdikcích, jakož i nedostatků ve vyšetřovacích procesech.[104] Je mnoho znaků kyberprostoru, které mají vliv na dynamiku pachatelů kybernetických trestných činů. Kyberprostor je relativně anonymní[105], což vyvolává pocit vnímané undergroundové aktivity a na celý kyberprostor to vrhá pocit záhadnosti. Výhodou je, že místo a čas spáchání trestného činu si lze vybrat a lze jej také změnit. Škodlivý následek tak může být způsoben z jakékoliv lokace po celém světě. To umožňuje pachatelům jednat s minimálním rizikem.[106]

Počítače v současné době zasahují do všech sfér života, a to má vliv i na velké množství trestných činů souvisejících s počítačem. Pachatelem této trestné činnosti se tak může stát každý a nelze vytvořit přesně určený typ pachatele. Pro určení alespoň některých znaků pachatele, které

[101] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 95.
[102] VÁLKOVÁ, Helena, KUCHTA, Josef, HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019, str. 527.
[103] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 485.
[104] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, str. 19.
[105] Pachatel zanechává stopy, avšak v praxi při vyšetřování jeho jednání nemusí být tyto stopy vždy využitelné. (Zdroj: GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 390).
[106] GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 40.

je však třeba specifikovat podle dalších vlivů, lze vyjít z toho, že pachatel bývá často inteligentní, vzdělaný a ovládá potřebné počítačové dovednosti. Nezákonná činnost nebývá mnohdy prováděna jen pro zábavu, ale stále více za účelem získání finančního zisku, který je však získáván spíše po menších částkách.[107]

Asi základní podmínkou pro to, aby se někdo mohl stát pachatelem kybernetické kriminality je schopnost umět pracovat s počítačem nebo jiným zařízením sloužícím ke zpracování dat. Avšak nemusí se jednat pouze o prvotřídní počítačové odborníky. Pachatelé mohou pocházet z nejrůznějších vrstev, tříd nebo skupin a jejich počítačové vzdělání a dovednosti mohou být pouze základní.[108] Pachatele tak lze dělit na amatéry a profesionály. Amatéři většinou páchají tzv. tradiční kriminalitu v novém kabátě prostřednictvím kyberprostoru, která tolik nevyžaduje zvláštní počítačové schopnosti.[109]

Osobnost pachatele většinou nevykazuje zjevné patologické rysy, navenek se nijak neodlišuje od většiny společnosti, nepochází z nějaké určité vrstvy společnosti. Jednání pachatelů nezahrnuje prvky násilí a je vzdáleno tradičním hrubým formám jednání.[110] Trestnou činnost páchá spíše individuálně. Většinou se jedná o mladšího pachatele, nemá proto prozatím ani žádný záznam v trestním rejstříku. Věkové spektrum se však rozšiřuje, už se nejedná o převážně mladistvé a přechází se k pachatelům starším 40 let, kteří si s rozvojem počítačů své znalosti stále inovují.[111]

Pachatelé kyberkriminality ve většině případů nemají pocit viny a na svém jednání nespatřují nic špatného nebo škodlivého.[112] Páchání trestné činnosti za monitorem počítače, když poškozená osoba není současně přítomna, je pro pachatele mnohem snazší než páchání trestné činnosti v reálném světě. Nízký stupeň vnímání viktimizace a způsobeného následku znamená menší sociální tlak na pachatele, který by jej odradil od protiprávního jednání. Absence fyzického kontaktu odstraňuje zábrany, oběti nejsou schopny pozorovat varovné znaky jako řeč těla

[107] KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 13.
[108] VÁLKOVÁ, Helena, KUCHTA, Josef, HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019, str. 551.
[109] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 392.
[110] Toto je ovlivněno tím, že v kyberprostoru se téměř neobjevují trestné činy proti životu a zdraví, s výjimkou například kyberútoku na nemocnici apod., proto zde bude pouze málo násilnických typů pachatele. (Zdroj: JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 484).
[111] KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 13.
[112] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. vydání. Plzeň: Aleš Čeněk, 2021, str. 355.

a mimiku pachatele. Pachatel dokáže oběť snadněji oklamat předstíráním falešné identity nebo virtuální lásky s cílem vylákání peněz.[113]

Velkou většinu pachatelů tvoří muži, nižší procento žen může znamenat jejich nižší zájem o technické vzdělání, menší ambice a také se nechtějí zbytečně zaplést do problémů.[114] Avšak podle studie *Kyberkriminalita v kriminologické perspektivě* se posuzovaná skladba žen vymyká oproti běžným procentům (zhruba 22 % oproti běžným 12-15 %, kdy je pachatelkou trestného činu žena). Jde však pouze o malý vzorek. Důvodem zde uváděným je například to, že virtuální data jsou snadnější předmět útoku, jak z hlediska provedení útoku (pro ženu by mohlo být jednodušší smazat na dálku data než fyzicky napadnout jinou osobu), tak z hlediska psychického rozpoložení (stav napadené osoby může vyvolávat lítost, přičemž poškození dat, u kterých pachatel například ani neví komu patří, žádnou lítost vzbuzovat nebude).[115]

2.3.2. Pachatel phishingu

V rámci rešerše zdrojů nebyla nalezena žádná studie, která by se zabývala typickými znaky pachatele phishingu. Popsání konkrétních znaků pachatele proto přesahuje výzkum provedený v rámci této diplomové práce. Avšak neočekává se, že charakteristika pachatele phishingu bude rozdílná od pachatele kyberkriminality, proto výše uvedené lze použít i na pachatele phishingu.

Co se týče počítačových znalostí pachatele phishingu je zapotřebí, aby uměl zhotovit falešné webové stránky, ze kterých poté dokáže získat informace, které chce. Následné vytvoření e-mailové zprávy s logem společnosti a věrohodným příběhem už by pro něj nemělo být tolik složité. Pachatelem proto nemusí být jen profesionál. Avšak například pro spáchání pharmingu budou již vyžadovány specifické odborné počítačové znalosti pro nabourání cizího počítače či pro útok na DNS.

Odhalit pachatele phishingu je velice složité, při útoku je často používán tzv. spoofing, který umožní pachateli zakrýt identitu počítače, nebo pachatel využije počítač či identity (např. účtu na sociální síti nebo e-mailu) jiné nic netušící osoby. Dále může pachatel použít keylogger,

[113] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 5. vydání. Praha: Wolters Kluwer, 2019, str. 392.
[114] KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 13.
[115] VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ, Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020, str. 57.

tedy do počítače nainstalovaný program, který zaznamenává klávesovou aktivitu, a díky němu zjistit přístupové údaje k internetovému bankovnictví.[116]

Na území České republiky se většinou nevyskytovali přímo organizátoři phishingu, ale spíše tzv. bílí koně (např. osoby, které si založily účet za úplatu). Ti měli na svůj bankovní účet převzít peněžní prostředky, které byly neoprávněně odčerpány z účtu poškozeného a poslat je na jiný bankovní účet podle pokynů. Postupně se však na naše území přesunují i organizátoři phishingových útoků.[117]

2.3.3. Motivace a cíle pachatele

Motiv kybernetického trestného činu je důležitý pro posouzení společenské škodlivosti a pro trestní kvalifikaci jednání. U některých případů kybernetických trestných činů nelze škodu způsobenou takovým činem ani vyjádřit v penězích.[118]

Motivace pachatelů kybernetické trestné činnosti je různá, každý z nich sleduje jiný cíl. Zjišťování motivu je mnohdy důležité pro zjištění, kdo má nebo může mít z následků spáchaného činu prospěch. Obecně lze motivaci pachatelů kybernetických hrozeb dělit:

- účelem je získání finančního prospěchu,
- touha po získání moci nebo výsadního postavení (získání konkurenční převahy),
- snaha dokázat svoji intelektuální převahu a prokázání svých schopností (např. nad tvůrci ochranných programů),
- motivy vyplývající z konfliktů v mezilidských vztazích (např. msta, nenávist, závist apod.),
- snaha překonat subjektivní pocit nedocenění svých schopností (přáteli, nadřízenými atd.),[119]
- touha po dobrodružství, soutěživost (tato motivace se může vyskytovat u dobře situovaných jedinců).[120]

---

[116] JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016, str. 395.
[117] KUCHAŘÍK, Karel. *Aktuální trendy informační kriminality v rámci šetřených případů PČR.* In: KNÝ, Milan, SOUDKOVÁ, Šárka (ed.). Sborník Evropského měsíce kybernetické bezpečnosti 2014. Praha: Policejní akademie ČR, 2014, str. 6.
[118] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty.* 2. vydání. Plzeň: Aleš Čeněk, 2019, str. 965.
[119] KOLOUCH, Jan, BAŠTA, Pavel a kol. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2019, str. 78. Také PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. vydání. Plzeň: Aleš Čeněk, 2019, str. 965.
[120] VÁLKOVÁ, Helena, KUCHTA, Josef, HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019, str. 528.

Tyto motivy se mohou vyskytovat jak samostatně, tak v kombinacích. U phishingu nejvíce převažuje podle názoru autorky získání finančního prospěchu. Poté získání konkurenční převahy – tato motivace by mohla být například pro použití spear-phishingu, kdy útočník cílí na konkrétní subjekt, aby získal některé interní údaje. Tyto údaje by pak mohly být využity v rámci konkurenčního boje. U menšiny případů půjde o dokázání si svých schopností, případně převahu své moci, ač toto může být taktéž důvod, pro někoho nemusí být phishing natolik sofistikovaný, aby to bral za prokazování svých schopností. Avšak pokud by se jednalo například o pharming, tam už by takový motiv mohl existovat.

Dalším motivem může být také potěšení z pocitu beztrestnosti a vlastní neodhalitelnosti. U phishingu je stejně jako u ostatních činů kybernetické kriminality typická vysoká míra latence, kdy se ve většině případů pachatel nezjistí a případ je proto odložen z důvodu neznámého pachatele. Pachatelům se tato trestná činnost vyplatí, protože pravděpodobnost obohacení je vysoká a míra dopadení nízká. Organizace, které jsou napadeny, zejména finančního typu, často útoky ani nenahlašují, aby neztratily důvěru svých klientů a veřejnosti.[121]

Podle motivu lze tak hovořit o typech pachatelů – průnikáři (jejich cílem je prokázat vlastní schopnosti, aniž by očekávali osobní zisk), mstitelé a škodiči (jde jim převážně o způsobení škody, nikoliv o prolomení ochrany), profesionálové apod.[122]

2.4. Oběť

Oběť je definována v zákoně o obětech trestných činů v § 2 odst. 2: *„Obětí se rozumí fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena škoda nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil nebo měl obohatit.“* Osoba takto dotčená trestným činem se označuje jako oběť.[123]

2.4.1. Oběť kyberkriminality

Stejně jako v případě pachatele i typologie obětí se bude lišit na základě toho, o jaký kybernetický čin půjde.

[121] Tamtéž, str. 529-530.
[122] KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 13. Dále viz VÁLKOVÁ, Helena, KUCHTA, Josef, HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019, str. 528.
[123] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 120.

Často se obětí stane osoba, která je při používání počítače málo opatrná. Pravděpodobnou příčinou nedostatečné obezřetnosti při práci na počítači je nízká úroveň znalostí a zkušeností běžných uživatelů. Ti většinou zvládají na počítači pouze svoji práci, aniž by si uvědomovali další rizika spojená s používáním počítačů. V bezpečnosti na internetu se mohou utvrzovat díky falešnému pocitu, že se zatím nikdy nic nestalo. Tito uživatelé jsou mnohem více vystaveni možnému kybernetickému útoku.[124]

Oběti podceňují zabezpečení svého počítače, jsou nedbalé při poskytování svých údajů (nepřemýšlejí, kam údaje vkládají, kdo je vyžaduje a za jakým účelem) a otevírají přílohy e-mailových zpráv bez zhodnocení možného rizika s tím spojeného. Dalším problémem je také stále se opakující heslo, někdy i snadno odhalitelné, a to jak u nedůležitých účtů (kde by případné prolomení nic neznamenalo), tak i u účtů významných (e-mail, sociální sítě, internetové bankovnictví).[125]

Oběť kybernetického útoku mnohdy ani netuší, že byla napadena, protože neodhalí, že má ve svém zařízení spyware nebo neví, že jednání vůči ní je trestné. Oběť v některých případech ani nechce oznámit napadení svého zařízení orgánům činným v trestním řízení. Může se obávat, že při případné medializaci dojde ke ztrátě důvěry (většinou se jedná o veřejnou instituci, které záleží na důvěře klientů) anebo nechce, aby jí bylo zařízení dočasně odebráno kvůli zajištění důkazních prostředků. K vysoké latenci přispívá i to, že nejsou přímo vidět následky (např. oproti vloupání).[126]

V České republice je problematikou i legislativa, která reaguje velmi pomalu na rychlý rozvoj technologií. Mezi činitele ovlivňující legislativní proces lze zařadit vůli zákonodárce daný stav změnit, odpovídající vzdělání a schopnost porozumět problému. Nicméně na druhou stranu, díky rychle se měnícím způsobům kybernetických útoků, je velice obtížné na ně reagovat rychle. Po krátké chvíli se může přijatá norma stát nicotnou kvůli vyprázdnění pojmů v ní uvedených.[127]

[124] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, str. 31.
[125] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 485-486.
[126] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 391.
[127] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, str. 26.

2.4.2. Oběť phishingu

Oběť phishingu je podvodem vedena k určitému jednání, nejčastěji k zaslání peněz nebo zadání svých přihlašovacích údajů. Pravděpodobně ani není možné zjistit přesnou charakteristiku oběti phishingu vzhledem k pouze malému vzorku ze všech uživatelů, kteří s elektronickou komunikací pracují. Některé znaky však dokážeme zjistit pomocí různých studií a průzkumů.

Výběr těchto obětí se postupem času měnil, i když žádný způsob pravděpodobně úplně nevymizel. Klasický phishingový útok je založený na tom, že útočníci své oběti netipovali, jen zaslali náhodným uživatelům e-mail a čekali, zdali jsou tito uživatelé zákazníky instituce, kterou ve své zprávě použili, a zda se na zprávu nachytají. Postupem času se však vyvinul i spear-phishing, prostřednictvím něhož pachatelé už vyloženě začali cílit na specifickou skupinu osob.[128]

Na posouzení charakteristiky oběti phishingu bylo provedeno několik studií. Většina z nich je založena na metodě „hraní rolí“, kdy je uživatelům poskytnut dotazník, kde posuzují různé scénáře. Výzkumníci tak nemusí provádět skutečný phishingový experiment. Odpovědi uživatelů pak výzkumníci analyzují a vyvodí z nich závěry o potenciálních obětech phishingu. Některé studie však provádějí skutečný phishingový útok, který je „řízený“. Uživatelé dostanou phishingový e-mail, který je přesměruje na podvodnou webovou stránku, ta však neshromažďuje žádné citlivé údaje. Webová stránka eviduje pouze počet a nanejvýš uživatelské jméno oběti.[129]

Průzkum Shenga a jeho kolektivu[130] ukázal, že uživatelé podléhají phishingovému útoku z následujících důvodů – za prvé, posuzují webové stránky převážně podle toho, jak vypadají a jak na ně působí, to je však pro útočníky jednoduché napodobit. Za druhé, uživatelé nerozumí či nevěří bezpečnostním ukazatelům u webového prohlížeče, který by je mohl upozornit na nebezpečí. Za třetí, ačkoliv někteří uživatelé mají povědomí o existenci a fungování phishingu, neznamená to, že jsou před ním chráněni a že jej dokáží pokaždé rozpoznat. Ač si uvědomují závažnost následků útoku, není možné předpovědět jejich chování, pokud se takový útok opravdu stane.

V dostupných studiích bylo zjištěno, že mezi uživateli internetu, kteří jsou počítačově gramotní, bylo u starších uživatelů méně pravděpodobné, že se stanou obětí phishingu. Mladší uživatelé ve věku 18 až 25 let byli vůči útokům zranitelnější. Důvod, proč mladší lidé častěji

[128] HLAVÁČOVÁ, Kateřina. *Phishing a jeho postupná evoluce*. In: VOJÁČEK, Ladislav, TAUCHEN, Jaromír (ed.). Majetkové a hospodářské trestné činy včera a dnes. Sborník z konference. Brno: Masarykova univerzita, 2016, str. 271-272.
[129] DARWISH, Ali, ZARKA, Ahmed, ALOUL, Fadi. *Towards understanding phishing victims' profile*. International Conference on Computer Systems and Industrial Informatics, IEEE, 2012, str. 2-3.
[130] SHENG, Steve, LANYON, Mandy, KUMARAGURU, Ponnurangam, CRANOR, Lorrie, DOWNS, Julie. *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. Conference on Human Factors in Computing Systems – Proceedings, 2010, str. 1.

podlehnou útoku může být ten, že jsou důvěřivější ohledně online komunikace a více impulzivní, častěji klikají na nevyžádané e-maily bez delšího uvážení.[131]

Z průzkumů dále vyplynulo, že více podléhají útokům phishingu ženy než muži, i když některé průzkumy zaznamenaly, že v rámci pohlaví není žádný významný rozdíl a obě pohlaví podléhají phishingu stejně. Ženy mohou být náchylnější k tomu stát se obětí phishingu z důvodu, že mohou mít méně technických znalostí a dovedností, než mají muži. [132]

Dalšími vlastnostmi osob, u kterých se ukázalo, že jsou náchylnější podvolit se útoku, jsou například vyšší důvěra nebo tendence podřídit se autoritě. Také tendence ke spolehlivosti a pracovitosti zvyšuje pravděpodobnost, že daná osoba podlehne phishingu. Zatímco podezřívavost vůči ostatním lidem, kdy osoba dopředu předpokládá, že lidé nemají dobré úmysly, je spojena s nižší viktimizací.[133]

2.5. Kontrola

Kriminalita je negativní sociální jev. Nelze ji úplně odstranit, ale je možné a nutné ji omezovat a kontrolovat.[134] Základní prevence je klíčová k tomu, aby se uživatel nestal obětí některého z útoků. Je několik kroků, které by měly být dodrženy a které sníží šanci pachatele na úspěšný útok. Jde o opatření týkající se (1) vzdělání a vůbec povědomí zaměstnanců a obecně uživatelů, (2) technologie a (3) přijímání právních předpisů.

Co se týče prvního, tedy osob, které by mohly být cílem útočníků. Počet případů phishingu by mohl být nižší, pokud by tyto osoby byly schopny rozpoznat podvod, o který se útočníci pokoušejí. Každý uživatel by si měl dávat pozor na gramatiku, kvalitu grafiky, zkontrolovat odesílatele zprávy a také obsah zprávy. U webové stránky by si měl zkontrolovat, zda se na začátku adresy URL nachází „https“[135] a zda název webové stránky souhlasí s obsahem zprávy.[136] Ač podle některých odborníků vzdělávání uživatelů v oblasti ochrany proti phishingovým útokům nemá velký význam, průzkum Shenga a jeho kolektivu ukazuje spíše účinnost takových školení.

---

[131] DARWISH, Ali, ZARKA, Ahmed, ALOUL, Fadi. *Towards understanding phishing victims' profile*. International Conference on Computer Systems and Industrial Informatics, IEEE, 2012, str. 3. Viz také ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.* In: Frontiers in Computer Science, 2021, vol. 3, str. 8.

[132] DARWISH, Ali, ZARKA, Ahmed, ALOUL, Fadi. *Towards understanding phishing victims' profile*. International Conference on Computer Systems and Industrial Informatics, IEEE, 2012, str. 3.

[133] DE KIMPE, Lies et al. *You've got mail! Explaining individual differences in becoming a phishing target*. In: Telematics and Informatics, 2018, vol. 35, no. 5, str. 1279.

[134] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 23.

[135] HTTPS (*Hypertext Transfer Protocol Secure*) je protokol, který umožňuje zabezpečenou komunikaci v počítačové síti.

[136] SRIVASTAVA, Tushar. *Phishing and Pharming – The Deadly Duo*. SANS Institute, 2007, str. 22-23.

Pokud jsou správně vytvořené, mohou zvýšit schopnost uživatelů vyhnout se phishingovému útoku.[137]

Úplně nejdůležitější, zvláště u phishingu, je tedy vlastní obezřetnost uživatelů. Následkům jejich neopatrnosti nedokáže zabránit ani nejlepší ochranný software. Uživatelé by měli být opatrní zejména co se týče používání hesel, stahování obsahu, sdělování osobních či přihlašovacích údajů. Je však třeba zdůraznit i fyzickou ochranu jednotlivých zařízení, např. přístup k počítači, flash disku, zapsanému heslu někde na papíře atd.[138]

Techniky phishingu se postupem času zlepšují, avšak zároveň se zvyšuje i prevence, a tím povědomí uživatelů o možných rizicích a způsobech obrany. Základním pravidlem prevence je zejména zlaté pravidlo, že uživatel nemá uvádět své osobní, platební ani přístupové údaje pouze na základě výzvy uvedené v přijatém e-mailu či jiné zprávě nebo výzvy zveřejněné na webové stránce. Dalším pravidlem je, že k přístupu ke kritickým službám, jako je například internetové bankovnictví, se nevyužívají odkazy z e-mailů, ale vždy je potřeba zadat příslušnou stránku přímo do okna prohlížeče (i když ani to není záruka ochrany např. v případě pharmingového útoku popsaného výše).[139]

Dále také nadměrné zveřejňování osobních informací a přidávání cizích lidí na sociálních sítích do přátel zvyšuje riziko útoku. Toto sebeodhalování totiž znamená, že se tito uživatelé stávají viditelnějšími pro možné útočníky, kterým zároveň takto poskytují informace o své osobě, které lze zneužít. U osob, které užívají sociální sítě, je vyšší pravděpodobnost, že se stanou terčem útoku. Uživatelům je proto vždy doporučováno zabezpečit si určitým způsobem svůj profil, chránit si osobní informace a zbytečně je nezveřejňovat cizím lidem na internetu.[140]

Řada organizací zveřejňuje upozornění na konkrétní hrozby, případně informační materiály zahrnující různá doporučení k bezpečnému užívání internetu.[141] Například banky často zveřejňují na svých internetových stránkách (případně při přihlašování do

[137] SHENG, Steve, LANYON, Mandy, KUMARAGURU, Ponnurangam, CRANOR, Lorrie, DOWNS, Julie. *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. Conference on Human Factors in Computing Systems – Proceedings, 2010, str. 2.
[138] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 5. vydání. Praha: Wolters Kluwer, 2019, str. 406-407.
[139] JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016, str. 395.
[140] DE KIMPE, Lies et al. *You've got mail! Explaining individual differences in becoming a phishing target*. In: Telematics and Informatics, 2018, vol. 35, no. 5, str. 1280.
[141] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 407.

internetového bankovnictví) různá varování na nové hrozby, které se objevují, nebo je zasílají do e-mailových schránek a apelují na obezřetnost svých klientů.

Ohledně používání technologií jako prevence před phishingovými útoky (myšleno různé programy) je zapotřebí zdůraznit, že tyto nástroje ochrany nemohou být používány jako jediná ochrana. Vždy je nutné ji propojit s osvětou a obezřetností uživatelů. Uživatel by měl mít například vícefázové ověření pro přihlašování na e-mail, při placení prostřednictvím internetového bankovnictví, zablokované automatické vyskakování oken apod.[142] Každé zařízení vstupující do kyberprostoru by mělo mít ochranný software, tedy antivir, jehož součástí je často i firewall a antispyware. Uživatel by pak měl tento antivir pravidelně aktualizovat.[143]

Další kontrolou před útoky je přijímání právních předpisů[144], které upravují a snaží se omezit jak obecně kyberkriminalitu, tak phishing. Pachatelé phishingových útoků dokáží obětem způsobit závažnou újmu, převážně se to týká finanční ztráty, ale také například poškození dobrého jména a pověsti. Proto by orgány činné v trestním řízení měly tyto útoky co nejrychleji vystopovat a pachatele potrestat. Právní předpisy a trest z nich vyplývající tak mohou být jedním z represivních prvků zabraňujících provedení těchto útoků.[145] Tyto možné předpisy jsou uvedeny v následující kapitole.

Nelze spoléhat výhradně na počítačové programy, poněvadž i kvalitní software není vždy zárukou stoprocentní ochrany. S rychlým vývojem phishingu nemusí antivir útok poznat, protože nový typ v sobě ještě nemá definován. Vždy je proto třeba propojit obezřetnost uživatele s ochranným programem v počítači. Legislativní úprava a stanovení postihu těchto útoků je však neméně důležité.

[142] SRIVASTAVA, Tushar. *Phishing and Pharming – The Deadly Duo*. SANS Institute, 2007, str. 24-26.
[143] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer, 2019, str. 406.
[144] Pro zajímavost, první anti-phishingové zákony byly přijaty ve Spojených státech amerických už v roce 2004, kdy byly phishingové útoky přidány na seznam počítačových zločinů.
[145] ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. In: Frontiers in Computer Science, 2021, vol. 3, str. 18.

3. Trestněprávní úprava phishingu

V důsledku pokroku v oblasti techniky a vynalézavosti útočníků dochází v oblasti kyberkriminality k situacím, kdy určité jednání nenaplňuje žádnou ze skutkových podstat trestných činů, a to ani při použití extenzivního výkladu.[146] U některých jednání však není třeba jejich kybernetický aspekt nijak zvlášť reflektovat, jelikož k jejich postihu postačí použití stávajících skutkových podstat, které jsou v zákoně již upraveny. Toto platí například pro podvodná jednání typu phishing či Nigerijské listy. Avšak řada jednání, které mají určitou spojitost s kyberprostorem, nemá svůj odraz v reálném světě.[147]

Vzhledem k obtížnému definování kybernetického trestného činu, který nemá jasně dané meze, a také vzhledem k jeho obtížnému dokazování, dochází často k beztrestnosti zřejmě nelegitimního jednání pachatelů.[148] Problémem vymáhání práva vůči pachatelům phishingových útoků je zejména to, že pachatel může ihned zmizet v kyberprostoru a potom je nesnadné mu prokázat vinu a domoci se náhrady jakékoli újmy.[149]

U kybernetické kriminality pachatelé využívají rozdílnosti a komplikovanosti právních úprav a nepružného poskytování právní pomoci v trestních věcech ve snaze vyhnout se trestní odpovědnosti. Taktéž problematika obstarávání důkazů, které se zpravidla nacházejí na území jiného státu, zabraňuje efektivnímu dopadení pachatelů. Podstata problému spočívá v tom, že vnitrostátní právní normy mají vymezenou působnost územím státu, nicméně v prostředí internetu, kde neexistují žádné hranice, ztrácí princip teritoriality smysl.[150] Ačkoliv Rámcové rozhodnutí Rady o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy stanoví, že počítačová trestná činnost je zařazena mezi činy, u kterých byla v důsledku přijetí evropského zatýkacího rozkazu prolomena zásada oboustranné trestnosti.[151]

K efektivnímu postihu kybernetické kriminality je nutná harmonizace právních řádů jednotlivých států, a to cestou mezinárodněprávních nástrojů. Pro efektivní obranu proti této kriminalitě je proto zapotřebí určitá míra harmonizace trestněprávních norem, hmotných

[146] GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 82.
[147] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 499.
[148] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 25-26.
[149] ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. In: Frontiers in Computer Science, 2021, vol. 3, str. 19.
[150] GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 64.
[151] Seznam těchto trestných činů je uveden v čl. 2 odst. 2 Rámcového rozhodnutí Rady ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy. Jediným požadavkem u těchto činů je, aby trestný čin bylo možné ve vystavujícím členském státě potrestat trestem odnětí svobody nebo ochranným opatřením spojeným s odnětím osobní svobody s horní hranicí sazby v délce nejméně tři roky.

i procesních, a také usnadnění mezinárodní spolupráce ve stíhání společensky škodlivých jevů v kyberprostoru. V tomto pak hraje významnou roli Úmluva o počítačové kriminalitě, která je ve svém přístupu k dané problematice nejkomplexnější.[152] O této Úmluvě proto pojednává následující kapitola.

3.1. Úmluva Rady Evropy o počítačové kriminalitě

Úmluva Rady Evropy č. 185 o počítačové kriminalitě vstoupila v platnost 1. července 2004, Česká republika ji podepsala již v roce 2005, ale ratifikovala až 23. srpna 2013 s účinností od 1. prosince 2013, kdy byla vydána pod č. 104/2013 Sb. m. s.[153] Úmluva je první mezinárodní smlouvou, která se zabývá trestnými činy spáchanými prostřednictvím internetu a jiných počítačových sítí. Jde zejména o porušování autorských práv, počítačové podvody, dětskou pornografii a porušování bezpečnosti sítí, mimo to obsahuje také řadu pravomocí a postupů pro ochranu před kyberkriminalitou.[154]

Ačkoliv byla Úmluva ratifikována Českou republikou až v roce 2013, tedy Česká republika nebyla do té doby tímto dokumentem vázána, zákonodárce se již v důvodové zprávě k novému trestnímu zákoníku (účinnému od roku 2010) zmiňuje o záměru zavést trestněprávní úpravu kyberkriminality, která by byla s Úmluvou v souladu. Tím by došlo ke splnění případných závazků, které by v budoucnu měly vzniknout.[155] Podle důvodové zprávy jsou na základě Úmluvy v osnově upraveny skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 228) a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 229), kdy bylo třeba zapracovat zejména články 2 až 11 Úmluvy. Dále osnova na základě požadavků z praxe upravuje i trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 230.[156]

Úmluva neobsahuje definici kybernetické kriminality, ale popisuje souhrn aktivit, které by měly být ze strany smluvních stran postihovány jako trestné činy, a také upravuje procesní postupy, bez nichž by byla hmotněprávní úprava nedostatečná. Úmluva vychází z harmonizace, která spočívá v úpravě společného minimálního standardu vybraných trestných činů, avšak to

[152] GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 83.
[153] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019, str. 38.
[154] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 646.
[155] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019, str. 38.
[156] Důvodová zpráva k § 228–230 (dnes § 230–232) k zákonu č. 40/2009 Sb., trestní zákoník, č. 40/2009 Dz.

neznamená, že státy budou mít totožnou právní úpravu. Transformace Úmluvy do vnitrostátního práva a následná aplikace může být v jednotlivých státech rozdílná, poněvadž každý stát má rozdílnou právní kulturu, různá specifika legislativního procesu atd.[157]

Úmluva se skládá z 48 článků a vedle preambule se dělí do čtyř kapitol. Kapitola I vymezuje základní pojmy, kapitola II obsahuje závazky státu na úrovni hmotného a procesního práva včetně působnosti vnitrostátních norem, v kapitole III je upravena mezinárodní spolupráce a v kapitole IV jsou závěrečná ustanovení. Pro účely této práce je relevantní úprava trestního práva hmotného v kapitole II, skutkové podstaty se v části 1 této kapitoly rozdělují do oddílů:

- Tresné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů,
- trestné činy související s počítačem,
- trestné činy související s obsahem,
- trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Tyto trestné činy by měly být součástí vnitrostátního práva. Kromě deliktů, které se týkají počítačových systémů a počítačových dat, se do této kategorie podle Úmluvy řadí i delikty páchané díky počítačům snadněji, tedy pravděpodobně s vyšší společenskou nebezpečností (jde nejčastěji o trestné činy související s dětskou pornografií nebo porušování autorského práva).[158]

K phishingu se vztahuje konkrétně čl. 8 Úmluvy, který patří do trestných činů souvisejících s počítačem. Upravuje Počítačový podvod jako speciální druh podvodu, tedy podvod spáchaný zvláštním, specifickým způsobem, prostřednictvím zásahu do počítačových dat nebo do funkcí počítačového systému. Tento článek stanoví: „*Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejich vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně a neoprávněně, způsobení ztráty na majetku jinému: (a) jakýmkoliv vkládáním, pozměňováním, vymazáním nebo potlačením počítačových dat, (b) jakýmkoliv zásahem do fungování počítačového systému; s podvodným nebo nečestným úmyslem neoprávněně získat majetkový prospěch pro sebe nebo pro jiného*.“

Pod tento článek se bude řadit převážně internetový podvod ve všech svých podobách – typicky phishing, pharming, spear-phishing. Avšak patří sem i kombinace těchto útoků, kdy je

[157] GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 83-84.
[158] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019, str. 38.

phishing využit pro instalaci malwaru do počítačového systému a s jeho pomocí následně dojde k odčerpání peněžních prostředků.[159]

Relevantní pro phishing je i čl. 7 Úmluvy, který smluvním stranám stanoví povinnost, aby *„podle jejích vnitrostátních právních předpisů byly trestnými činy, pokud jsou spáchány úmyslně a neoprávněně, vkládání, pozměnění, vymazání nebo potlačení počítačových dat, které povede k nepravosti dat, a to s úmyslem, aby tato data byla považována za pravá nebo aby podle nich bylo pro právní účely jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná či nikoli. Strana může stanovit, že k založení trestní odpovědnosti je nezbytný úmysl podvést nebo podobný nečestný úmysl.“* Toto by se mohlo vztahovat zejména k vytváření falešných webových stránek, které mají vypadat jako pravé, čímž se snaží zmást uživatele, kteří s domněním, že jsou na pravé stránce zadají své údaje.

Na základě této Úmluvy, jak již bylo uvedeno výše, jsou formulovány trestné činy v současném trestním zákoníku, konkrétně § 230 a § 231 TrZ. Nad rámec Úmluvy byla do zvláštní části trestního zákoníku zařazena skutková podstata nedbalostního trestného činu podle § 232 TrZ.[160]

3.2. Směrnice o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání

Směrnice jsou legislativním aktem Evropské unie. Zavazují členské státy, aby implementovaly jejich obsah do právního řádu, avšak to, jakým způsobem to provedou, je ponecháno na členských státech. Státy především musejí dosáhnout cílů stanovených směrnicí.

Směrnice Evropského parlamentu a Rady (EU) ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání, tzv. non-cash směrnice, má za cíl odrážet vývoj v oblasti bezhotovostních platebních prostředků a modernizovat stávající pravidla jejich ochrany, aby se postupně zefektivnil boj proti podvodům v této oblasti. Ochrana proti podvodům dopadá nejenom na platební karty, ale nově i na virtuální peněženky (pokud slouží k placení) umožňující převod virtuálních aktiv. V oblasti trestněprávní je jejím cílem posílení

[159] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 362-363.
[160] DRAŠTÍK, Antonín, DURDÍK, Tomáš, FREMR, Robert, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander a kol. *Trestní zákoník. Komentář. I. díl.* Praha: Wolters Kluwer ČR, 2015, str. 1476.

schopnosti donucovacích orgánů bojovat proti kybernetické kriminalitě a odstranit překážky operativní povahy, které brání efektivnímu vyšetřování a stíhání trestných činů.[161]

Důvodem přijetí této směrnice je zaujmout jednotný přístup v oblasti trestního práva ohledně znaků skutkových podstat trestných činů, které přispívají k podvodnému používání bezhotovostních platebních prostředků nebo k němu vytvářejí podmínky. Proto by jednání spočívající v nabývání a přechovávání platebních prostředků s úmyslem spáchat podvod, například prostřednictvím podvodného získávání údajů nebo směrování či přesměrování uživatele platební služby na falešné webové stránky, mělo být považováno za trestnou činnost, aniž by bylo zapotřebí skutečné podvodné použití bezhotovostních platebních prostředků.[162]

Non-cash směrnice proto zavádí definice skutkových podstat trestných činů, které zahrnují podvodné použití bezhotovostních platebních prostředků nebo s tím souvisejí, a to i pokud jsou spáchány online (tedy například případy phishingu). Mimo to harmonizuje i skutkové podstaty podvodů souvisejících s informačními systémy spočívající v provedení nebo způsobení převodu peněz, peněžní hodnoty či virtuální měny (jedná se převážně o hackerské útoky na počítače s cílem získat neoprávněný přístup do internetového bankovnictví). Dále definuje jednání týkající se neoprávněného zacházení s nástroji či zařízeními, které byly vytvořeny či přizpůsobeny pro spáchání výše uvedených trestných činů (výroba a náčiní pro padělání platebních karet).

Článek 17 non-cash směrnice ukládá členským státům povinnost k přijetí opatření, a to i prostřednictvím internetu, díky kterému se bude zvyšovat informovanost o podvodných metodách. Například o podvodném získávání platebních údajů pomocí phishingových útoků či o neoprávněném kopírování elektronických údajů pomocí skimmingu. Toto by mělo vést ke snížení rizika stát se obětí podvodu a tedy k celkovému snížení počtu spáchání těchto podvodů.[163]

Non-cash směrnice se tak snaží bojovat proti phishingu, a to nejenom tím, že stanoví úpravu právního řádu, aby bylo možné pachatele phishingového útoku postihnout, ale také je jejím cílem osvěta v této oblasti, aby uživatelé byli informováni o nebezpečí a byli obezřetní při poskytování svých údajů.

[161] Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.
[162] Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV, bod 13.
[163] Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

Tato směrnice byla implementovaná do českého trestního práva prostřednictvím zákona č. 130/2022 Sb.[164], který nabyl účinnosti dne 28. června 2022. V rámci trestního zákoníku zavedla tato novela nové výkladové ustanovení *Počítačový systém* v § 136a TrZ a upravila například §§ 182, 230, 231, 234 a další, aby byly v souladu s předpisy Evropské unie.[165]

3.3. Trestní zákoník

Zákon č. 40/2009 Sb., trestní zákoník, který nabyl účinnosti 1. ledna 2010, je základem české vnitrostátní úpravy v oblasti trestního práva. Tento zákon měl napravit některé nedostatky původního zákona č. 140/1961 Sb., trestního zákona, a harmonizovat vnitrostátní právo s mezinárodními závazky v oblasti kybernetické kriminality, kdy se mělo vycházet zejména z Úmluvy o počítačové kriminalitě.[166] Vlivem různorodosti jednotlivých kybernetických trestných činů se trestněprávní regulace rozpadá do různých skutkových podstat trestných činů v rámci mnoha hlav trestního zákoníku.[167]

Aby určité jednání mohlo být postihnuto podle trestního zákoníku a bylo považováno za trestný čin, je zapotřebí naplnit znaky podle § 13 odst. 1 TrZ. Podle tohoto ustanovení je trestným činem takový protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.

V průběhu popisu následujících trestných činů je často zmíněn pojem *počítačový systém*. Ten je zaveden v důsledku směrnice o útocích na informační systémy[168], avšak v trestním zákoníku je vymezen stejně jako je v této směrnici v čl. 2 písm. a) vymezen pojem informační systém. Počítačový systém je upraven ve výkladových ustanovení v § 136a TrZ, podle kterého je počítačový systém jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených

[164] Tímto zákonem však není implementována pouze non-cash směrnice, ale český právní řád reaguje i na jiné předpisy Evropské unie. Konkrétně zákon reaguje na (mimo non-cash směrnice) nařízení Evropského parlamentu a Rady (EU) 2019/816, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů, kterým se mění nařízení (EU) 2018/1726, a směrnice Evropského parlamentu a Rady (EU) 2019/884, kterou se mění rámcové rozhodnutí Rady 2009/315/SVV, pokud jde o výměnu informací o státních příslušnících třetích zemí a o Evropský informační systém rejstříků trestů (ECRIS), a nahrazuje rozhodnutí Rady 2009/316/SVV. Také přichází se zvýšením úrovně implementace směrnice Evropského parlamentu a Rady (EU) 2013/40 ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.

[165] Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

[166] KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 70.

[167] JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, str. 499.

[168] Směrnice Evropského parlamentu a Rady (EU) 2013/40 ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.

přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových údajů, jakož i počítačové údaje uložené, zpracované, opětovně vyhledané nebo přenesené tímto přístrojem či skupinou přístrojů za účelem jeho či jejich provozu, použití, ochrany a údržby.[169]

Český trestní zákoník nemá skutkovou podstatu, která by postihovala přímo phishing, proto je zapotřebí vyhledat skutkové podstaty, pod které lze jednání pachatelů phishingu podřadit, ačkoliv tyto nemusí přímo souviset s kyberkriminalitou. Phishing je možné kvalifikovat v závislosti na okolnostech a způsobu spáchání různě, avšak hlavním zde bude trestný čin podvodu podle § 209 TrZ, protože podstatou spáchání phishingu je uvedení uživatele v omyl.

3.3.1. Podvod (§ 209 TrZ)

V případě klasicky provedeného phishingového útoku se takové jednání bude stíhat jako trestný čin podvodu podle § 209 TrZ. Takový útok spočívá v přesměrování uživatele (po kliknutí na přiložený odkaz ve zprávě) na falešné webové stránky, kde uživatel uvedený v omyl zadá dobrovolně své údaje, čímž je poskytne pachateli a ten je zneužije k obohacení.[170]

Trestného činu podvodu podle § 209 odst. 1 TrZ se dopustí ten „*kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou*.“ Takový pachatel bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

Objektem tohoto trestného činu je cizí majetek, tedy majetek, který alespoň zčásti patří třetí osobě. Objektivní stránka trestného činu podvodu spočívá v podvodném jednání pachatele, které může představovat uvedení někoho v omyl, využití něčího omylu, nebo zamlčení podstatných skutečností. Pachatel se může tohoto jednání dopustit jak vůči poškozenému, tak i vůči třetí osobě. Následkem je pak vznik škody nikoli nepatrné na cizím majetku a obohacení pachatele nebo jiné osoby.[171] Předpokladem trestní odpovědnosti je úmyslné zavinění pachatele. Tento úmysl se musí vztahovat nejenom k uvedení jiné osoby v omyl, ale také k obohacení

[169] ŠČERBA, F. a kol. *Trestní zákoník. Komentář.* § 136a. 1. vydání (2. aktualizace). Beck-online [online právní informační systém]. Nakladatelství C. H. Beck, 2022, marg. č. 2 [cit. 2023-04-19]. Dostupné z: https://www-beck-online-cz.
[170] DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 87.
[171] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1687.

pachatele nebo jiné osoby a ke způsobení škody na cizím majetku, jakož i k příčinné souvislosti mezi těmito. Pachatelem může být kdokoliv, fyzická i právnická osoba.[172]

Trestný čin podvodu je dokonán v okamžiku, kdy se pachatel nebo jiná osoba obohatí. V případě, kdy pachatel například vytvoří pouze imitaci originální webové stránky, napíše e-mail, který by měl uvést uživatele v omyl anebo získá přihlašovací údaje, případně údaje k platební kartě, nepůjde ještě o dokonaný trestný čin podvodu. Mohlo by však jít o vývojové stádium tohoto trestného činu.[173] V případě vývojových stádií může jít buď o přípravu podle § 20 TrZ, ta je u trestného činu podvodu trestná (viz § 209 odst. 6 TrZ), pokud dojde k naplnění kvalifikované skutkové podstaty podle § 209 odst. 5 TrZ, kde je stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně deset let. Nebo podle § 21 TrZ může jít o pokus trestného činu. Přípravou nebo pokusem by mohlo být vytvoření falešné webové stránky a prostřednictvím ní získání přihlašovacích údajů a hesel.[174]

U trestného činu podvodu je nezbytné definovat také pojem *omyl*. Omyl lze definovat jako rozpor mezi subjektivní a objektivní realitou, tedy rozpor mezi představou a skutečností. Tento rozpor může mít podobu kvantitativní, kdy osoba, která je podváděná, nemá o rozhodné skutečnosti vůbec představu, anebo ji sice má, ale pouze o její části. Nebo může mít podobu kvalitativní, kdy podváděná osoba má představu o rozhodné skutečnosti, ale v důsledku jednání pachatele jí přikládá jiný význam. Omyl se může týkat i okolností, které mají teprve nastat. Pachatel však musí o omylu jiného vědět v okamžiku, kdy dochází k jeho obohacení či k obohacení jiné osoby.[175]

Z § 120 TrZ[176] vyplývá, že podvodného jednání se lze dopustit i pomocí technického zařízení ve smyslu tohoto ustanovení. Například provedením zásahu do dat uložených v počítačovém systému nebo na nosiči informací, či zásahem do programového vybavení počítače. Pachatel neuvádí v omyl technické zařízení, ale osobu, která nainstalovala zařízení tak, aby plnilo určité automatizované funkce. Zásah do zařízení je pouze prostředkem k uvedení nebo využití omylu osoby, která spoléhá na neovlivněné fungování technického zařízení.[177] Pachatel bude proto

[172] Tamtéž, str. 1697-1698.
[173] VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestněprávní kvalifikace*. In: Trestní právo, 2011, roč. 15, č. 1, str. 15.
[174] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 262.
[175] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1687-1688.
[176] § 120 TrZ stanoví: *„Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do dat uložených v počítačovém systému nebo na nosiči informací, zásahu do programového nebo technického vybavení počítačového systému nebo provedením jiné operace v počítačovém systému, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným."*
[177] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 229.

trestně odpovědný, ačkoliv počítačový systém (nebo jiné technické zařízení) provádí následně určitou operaci automaticky, bez aktivní činnosti člověka, pokud do něj předtím pachatel zasáhl s cílem obohatit se.[178]

Dle tohoto zvláštního ustanovení § 120 TrZ lze tedy uvést v omyl i zásahem do dat či programového nebo technického vybavení počítačového systému nebo provedením jiné obdobné operace, proto míří právě na způsobení škody phishingovými či jinými obdobnými útoky.[179] Například v případě pharmingového útoku pachatel napadne systém doménových jmen, díky čemuž následně dojde k nesprávnému spárování konkrétní IP adresy a uživatel se tak při zadání adresy webové stránky dostane na webovou stránku falešnou. Toto jednání pachatele by bylo možné kvalifikovat jako podvod pomocí výkladového ustanovení § 120 TrZ. Protože pachatel zasáhl do automatického procesu párování IP adres s originálním doménovým jménem, uvedl uživatele v omyl, aniž by při zadání této adresy uživatelem již cokoliv aktivně konal. Pachatel jedná s cílem obohatit se, pokud půjde například o stránky internetového bankovnictví nebo stránky platební brány, kdy lze přepokládat jeho úmysl získat finanční prostředky z účtu uživatele.

Cílem pachatele phishingu je uvedení osoby, která je oprávněna nakládat například s internetovým bankovním účtem, v omyl a získat tím přístup k účtu, nebo získat číslo platební karty či PIN k platební kartě (může jít však i o jiné webové stránky, kam uživatel zadá své údaje, které pachatel následně zneužije). Díky získání těchto údajů pak pachatel převede peněžní prostředky, které se na účtu nebo platební kartě nacházejí, čímž způsobí škodu, a on či jiná osoba se tím obohatí.[180] Pokud pachatel způsobí škodu nikoli nepatrnou, tedy škodu, která dosahuje částky nejméně 10 000 Kč podle § 138 odst. 1 písm. a) TrZ, naplňuje pak všechny znaky základní skutkové podstaty podvodu.

Na trestném činu podvodu může být zainteresováno až pět osob, kterými jsou: pachatel, osoba uváděná pachatelem v omyl a jednající v omylu, osoba provádějící v omylu majetkovou dispozici, osoba poškozená a osoba obohacená. Hovoří se pak o dotčené osobě, kterou může být osoba, jíž pachatel uvedl v omyl, ale která neprovádí majetkovou dispozici; osoba, kterou pachatel uvedl v omyl a která v omylu provádí příslušnou majetkovou dispozici a osoba, kterou pachatel neuvedl v omyl, ale která v důsledku omylu jiné osoby provádí majetkovou dispozici.[181] Pro

[178] DRAŠTÍK, Antonín, DURDÍK, Tomáš, FREMR, Robert, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander a kol. *Trestní zákoník. Komentář. I. díl.* Praha: Wolters Kluwer ČR, 2015, str. 777.
[179] JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016, str. 396.
[180] VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestněprávní kvalifikace*. In: Trestní právo, 2011, roč. 15, č. 1, str. 15.
[181] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1687.

posouzení otázky, komu vznikla jednáním pachatele škoda, je nutné zohlednit judikaturu Nejvyššího soudu. Nejvyšší soud konstatuje, že vklady na účtech a vkladních knížkách přecházejí do majetku banky, která s nimi může volně disponovat a využít je ke svému podnikání. Mezi vkladatelem a bankou pak vzniká závazkový právní vztah, kdy vkladatel má vůči bance pohledávku. Peněžní prostředky na účtu vedeném bankovním ústavem na základě smlouvy o běžném účtu nejsou tedy v majetku majitele účtu, v jehož prospěch byl tento účet zřízen, nýbrž v majetku banky.[182]

V omyl proto nebude uveden pouze uživatel. V případě, že pachatel získá od uživatele přihlašovací údaje, které pak použije a zadá platební příkaz k úhradě, uvede v omyl banku, která předpokládá, že příkaz k úhradě zadal oprávněný klient a transakci zrealizuje.[183] Dochází zde k dobrovolnému vydání peněžních prostředků ze strany banky, která je poškozenou, poté, co pachatel předstírá oprávnění nakládat s finančními prostředky na bankovním účtu.[184]

Při podvodném jednání pachatel neodjímá věc proti vůli poškozeného, ale poškozený mu věc sám vydá nebo mu dovolí, aby věc vzal. Cílem podvodu tedy je, aby osoba jednající v omylu vydala věc dobrovolně. Protiprávní jednání spočívá pak v tom, že „dobrovolné“ odevzdání věci poškozeným se děje na základě aktivního jednání pachatele, který uvede v omyl, využije omylu nebo zamlčí podstatné skutečnosti.[185] U phishingu může proto dojít ke dvojitému uvedení v omyl. Nejdříve uživatele, který v omylu poskytne pachateli své údaje k internetovému bankovnictví nebo platební kartě, a následně banky, která předpokládá, že příkaz k úhradě zadal její klient a přesune peněžní prostředky z jeho účtu na jiný. Jednáním pachatele je způsobena škoda bankovnímu ústavu jako majiteli peněžních prostředků na účtu.[186]

Kvalifikované skutkové podstaty postihují recidivistu, pachatele, který byl za takový čin v posledních třech letech odsouzen nebo potrestán (odst. 2), způsobení větší škody (odst. 3). Dále pokud pachatel spáchá tento trestný čin jako člen organizované skupiny, nebo jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného, spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, či způsobí-li značnou škodu (odst. 4). Případně pokud způsobí škodu velkého rozsahu, nebo spáchá-li takový čin v úmyslu umožnit nebo usnadnit

[182] Usnesení Nejvyššího soudu ze dne 30. ledna 2004, sp. zn. 11 Tdo 40/2004, publikované pod č. 14/2006 Sbírky soudních rozhodnutí a stanovisek.
[183] Usnesení Nejvyššího soudu ze dne 16. května 2018, sp. zn. 4 Tdo 456/2018, publikované pod č. 8/2019 Sbírky soudních rozhodnutí a stanovisek.
[184] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1689.
[185] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 228.
[186] Více viz kapitola 4.4.

spáchání teroristického trestného činu, trestného činu financování terorismu nebo vyhrožování teroristickým trestným činem (odst. 5). V případě phishingu si lze představit možnost spáchání všech těchto kvalifikovaných skutkových podstat.

Na závěr je nutné poznamenat, že pokaždé nemusí mít útočník v úmyslu získat neoprávněný prospěch, proto nedojde vždy k naplnění skutkové podstaty trestného činu podvodu. Útočník může pouze z hackerského zájmu získat potřebné údaje od uživatelů prostřednictvím phishingu, které však následně neužije a ani nemá v úmyslu užít k přístupu do systému nebo získání prospěchu. V tomto případě se nedopouští trestného činu podvodu, ale ani trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 1 TrZ (nepřekoná bezpečnostní opatření a nedojde k poruchovému následku). Nedochází ani ke spáchání trestných činů proti právům na ochranu osobnosti, soukromí a listovní tajemství. Z toho vyplývá, že takové jednání by nebylo postihnutelné podle trestního zákoníku.[187]

3.3.2. Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací (§ 230 TrZ)

Tento trestný čin se skládá ze dvou skutkových podstat, přičemž způsobení škody (případně úmysl vztahující se ke způsobení škody) je vyžadováno až u kvalifikovaných skutkových podstat. Pachatel nemusí mít žádnou speciální vlastnost, postavení nebo způsobilost, proto jím může být kterákoli fyzická nebo právnická osoba. V případě obou základních skutkových podstat je vyžadováno úmyslné zavinění pachatele.[188]

Objektem první základní skutkové podstaty je primárně důvěrnost počítačových dat a počítačového systému, až sekundárně jsou chráněny integrita a dostupnost.[189] Důvěrností lze rozumět zajištění toho, aby informace byla dostupná pouze osobám oprávněným k přístupu; integritou pak zabezpečení správnosti a kompletnosti informací a metod zpracování; a nakonec dostupností se rozumí zajištění, aby informace a s nimi spjatá aktiva byly přístupné autorizovaným uživatelům dle jejich potřeby.[190] Objektivní stránka spočívá v překonání bezpečnostního opatření a získání neoprávněného přístupu k počítačovému systému nebo k jeho části.[191]

[187] DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 87.
[188] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1881, 1887.
[189] ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2304.
[190] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 663.
[191] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1882.

Zákonodárce u tohoto ustanovení nestanovil podmínku, aby k naplnění znaků trestného činu došlo teprve tehdy, pokud bude pachatelovým úmyslem získat počítačová data či jiný nečestný úmysl (např. způsobit jinému škodu či získat prospěch). Trestné je proto již samotné získání přístupu překonáním bezpečnostního opatření.[192] Bezpečnostním opatřením je opatření, které slouží k ochraně před neoprávněným přístupem do počítačového systému nebo k jeho části (typicky jde o heslo, firewall, přenosné médium s přístupovým klíčem atd.).[193]

K překonání bezpečnostního opatření může dojít různými softwarovými či hardwarovými nástroji, útoky typu malware nebo hacking, ale taktéž i uhodnutím hesla (ať díky znalosti daného uživatele nebo v případě jednoduchého hesla). Úroveň zabezpečení není rozhodující, stačí, že pachatel musí překonat nějakou překážku. Překonání proto nemusí být pro pachatele nic složitého, uživatel však již samotným stanovením bezpečnostního opatření vyjadřuje svůj nesouhlas, aby do počítačového systému pronikl kdokoliv cizí. V případě proniknutí do počítačového systému je narušeno soukromí uživatele, protože v počítači se často nacházejí osobní data. Proto by trestné mělo být prolomení i těch nejjednodušších bezpečnostních opatření, pokud nejsou oprávněné.[194]

V případě phishingu však nejde o překonání bezpečnostního opatření, neboť přihlašovací údaje jsou od uživatele získané přímo a dobrovolně. Pachatel tedy nemusí překonávat žádnou překážku, z čehož vyplývá, že nemůže naplnit znaky trestného činu podle § 230 odst. 1 TrZ.[195]

Objektem druhé základní skutkové podstaty je především integrita a dostupnost počítačových dat a systémů, které jsou chráněny před neoprávněnými zásahy, jež mohou ovlivnit existenci, kvalitu či správnost dat, a také chrání před neoprávněným užíváním uložených počítačových dat.[196] Jedná se o trestný čin úmyslný. Objektivní stránka je naplněna v případě, že pachatel učiní neoprávněný zásah jedním ze způsobů, které jsou alternativně uvedeny pod písm. a) až d). Od novely trestního zákoníku účinné od 28. června 2022 lze nově neoprávněně zasáhnout do počítačového systému i bez získání přístupu do něj, tedy aniž by pachatel musel překonat bezpečnostní opatření.[197]

---

[192] DRAŠTÍK, Antonín, DURDÍK, Tomáš, FREMR, Robert, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander a kol. *Trestní zákoník. Komentář. I. díl.* Praha: Wolters Kluwer ČR, 2015, str. 1477.
[193] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1882.
[194] ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2305-2306. Dále viz ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1882-1883.
[195] KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 71.
[196] ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2304.
[197] ŠČERBA, F. a kol. *Trestní zákoník. Komentář.* § 230. 1. vydání (2. aktualizace). Beck-online [online právní informační systém]. Nakladatelství C. H. Beck, 2022, marg. č. 13 a 16 [cit. 2022-05-20]. Dostupné z: https://www-beck-online-cz.

Pro možnou právní kvalifikaci phishingu je v druhém odstavci nejpodstatnější písm. c), tedy padělání nebo pozměnění dat, aby byla považovaná za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná. Pachatelův úmysl spočívá ve vyvolání dojmu pravosti vytvořených dat. Předstíraná pravost dat se může týkat jak jejich původce (pachatel zastírá svoji identitu identitou jiného subjektu), tak obsahu (např. podvodné webové stránky, na něž je uživatel ve zprávě odkázán). Právě u phishingu s cílem vylákat údaje např. k internetovému bankovnictví nebo i k jinému účtu (e-mail, sociální sítě apod.), jsou používány e-mailové zprávy, které mají vypadat jako pravé, z důvodu, že se pachatel vydává za oprávněný subjekt.[198]

Podle Smejkala[199] by na phishing měla dopadat právní kvalifikace podle § 230 odst. 2 písm. c) TrZ (toto však více nerozvádí) a další jednání (spočívající v uvedení uživatele v omyl a způsobení škody) pak naplňuje znaky skutkové podstaty trestného činu podvodu podle § 209 TrZ s odkazem na § 120 TrZ. Trestný čin podle § 230 odst. 2 TrZ není speciální vůči trestnému činu podvodu podle § 209 TrZ a je možné jej spáchat v jednočinném souběhu. Může tak jít o případy, kdy pachatel prostřednictvím neoprávněné manipulace s daty uloženými v počítačovém systému nebo na nosiči informací jedná podvodně ve smyslu § 209 TrZ, k čemuž často využívá phishing, vishing, malware atd.[200]

Autorka této práce zastává názor, že by phishing mohl naplňovat právní kvalifikaci podle § 230 odst. 2 písm. c) TrZ. Zejména tehdy, kdy pachatel vytvoří falešné webové stránky, kopírující existující a známý subjekt (např. některé banky, platební brány atd.), které působí jako pravé a jejichž cílem je oklamat uživatele, aby na nich vyplnil své přihlašovací údaje. Jak bylo uvedeno, novelou trestního zákoníku byl zrušen znak *získání přístupu*. Nezáleží tedy na tom, že uživatel potřebné informace sám dobrovolně sdělí pachateli, proto je možné naplnit skutkovou podstatu tohoto ustanovení podle odst. 2 i v případě phishingu.[201]

Dvořák[202] přináší ve svém článku ohledně trestného činu podle § 230 TrZ ještě další pohled. Za situace, že pachatel použije v rámci phishingového útoku zároveň i malware (řadí se sem i ransomware, viry, trojské koně atd.) za účelem narušení běžné činnosti systému, půjde

[198] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1885.
[199] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022, str. 649.
[200] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1890.
[201] Krupička zastával ve svém článku názor, že není možné, aby ustanovení § 230 odst. 2 TrZ dopadalo na phishing právě z důvodu nutnosti naplnění znaku překonání bezpečnostního opatření pachatelem, jak upravovalo starší znění zákona, za jehož trvání článek vyšel (KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 71).
[202] DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 87.

o kombinovanou formu phishingu. Jednání pak lze posoudit jako jednočinný souběh trestného činu podvodu podle § 209 TrZ s trestným činem neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 2 písm. a), b), d) TrZ. Konkrétní kvalifikace bude záležet na škodlivých účincích daného typu malwaru. Přičemž je nutné poznamenat, že pokud oním škodlivým softwarem bude ransomware (pachatel požaduje po oběti výkupné za obnovení přístupu k jeho datům), může k právní kvalifikaci přibýt v nejzávažnějších případech i trestný čin vydírání podle § 175 TrZ.

Co se týče způsobení škody, jiné újmy nebo získání neoprávněného prospěchu, tak to je upraveno až v rámci kvalifikovaných skutkových podstat. Pro dokonání kvalifikované skutkové podstaty podle § 230 odst. 3 písm. a) TrZ nemusí dojít k uskutečnění úmyslu způsobit jinému újmu, postačí pouze existence takového úmyslu. V tomto ustanovení není určena minimální výše škody, omezeno je to až odstavcem 4, kde je stanovena škoda značná (tedy minimálně 1 000 000 Kč), která již musí být způsobena.[203]

3.3.3. Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TrZ)

Trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku upravený v § 234 TrZ[204] se skládá ze tří základních skutkových podstat. První z nich naplní pachatel, který opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného bez souhlasu oprávněného uživatele. Druhou naplní pachatel, který opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek, nehledě na to, jestli tak činí na svůj účet nebo na účet druhého. Třetí základní skutková podstata, upravená v odstavci tři, obsahuje dvě varianty. První spočívá v tom, že pachatel padělá nebo pozmění platební prostředek v úmyslu použít takový prostředek jako pravý nebo platný (alinea první), a druhá v tom, že pachatel použije jako pravý nebo platný padělaný nebo pozměněný platební prostředek (alinea druhá).

Objektem trestného činu podle § 234 TrZ je ochrana jednotlivých platebních prostředků, ochrana základních funkcí platebních prostředků a prostřednictvím toho zajištění řádného platebního styku. Nejde však o ochranu majetkových zájmů dotčených účastníků platebního

[203] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1887.
[204] Ustanovení § 234 TrZ bylo vloženo do trestního zákoníku na základě Rámcového rozhodnutí Rady ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků (2001/413/SVV). (Zdroj: VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestněprávní kvalifikace*. In: Trestní právo, 2011, roč. 15, č. 1, str. 15).

styku.[205] Subjektivní stránka je charakterizována úmyslem pachatele pokrýt všechny znaky objektivní stránky, to platí pro všechny tři základní skutkové podstaty tohoto trestného činu. Pachatelem může být jakákoli trestně odpovědná fyzická osoba. Trestní odpovědnost právnických osob není vyloučena.[206]

Peněžními prostředky jsou podle § 2 odst. 1 písm. c) zákona o platebním styku bankovky, mince, bezhotovostní peněžní prostředky a elektronické peníze. Peněžními prostředky však nejsou kryptoměny (například Bitcoin, Ethereum, apod.), protože nejsou podle zákona platidlem žádného státu ani nadstátní organizace. Avšak novelou trestního zákoníku provedenou zákonem č. 130/2022 (účinnost 28. června 2022) je ochrana kryptoměn a virtuálních měn zahrnuta pod ochranu v § 234 TrZ.[207]

Dvořák[208] se ve svém článku zabýval otázkou, zda se může pachatel dopustit také trestného činu podle § 234 TrZ, pokud phishingovým útokem získá neoprávněný přístup k cizí elektronické peněžence s virtuální měnou a užije v ní uložených prostředků ve svůj prospěch. Dospěl k závěru, že takové jednání směřující k neoprávněnému zpřístupnění virtuální měny ve vlastnictví jiné osoby nelze postihnout jako trestný čin podle § 234 TrZ, protože toto ustanovení nedopadá na kryptoměny. V době vydání článku ještě nebyla v § 234 TrZ poskytnuta ochrana virtuální měně, avšak v současné době se virtuální měna již řadí mezi platební prostředky, proto by výše uvedené jednání podle autorky této práce v současné době mohlo být postihnuto jako trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 TrZ.

Ustanovení § 234 TrZ neupravuje, co se rozumí platebními prostředky. Podle § 2 odst. 1 písm. d) zákona o platebním styku se platebními prostředky rozumí *„zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz“.* Platebními prostředky jsou tak prostředky sloužící k platebnímu styku, tj. zejména uložení, výběr nebo převod peněžních prostředků a prostředků, které vykonávají funkci platidel.[209]

V souvislosti s phishingem jde velmi často o vniknutí pachatele do internetového bankovnictví, kde zadá příkaz k úhradě. Příkaz k zúčtování (prováděn prostřednictvím příkazu

[205] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1912.
[206] Tamtéž, str. 1921-1922.
[207] ŠČERBA, F. a kol. *Trestní zákoník. Komentář.* § 234. 1. vydání (2. aktualizace). Beck-online [online právní informační systém]. Nakladatelství C. H. Beck, 2022, marg. č. 8 [cit. 2022-05-14]. Dostupné z: https://www-beck-online-cz.
[208] DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 88.
[209] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1913.

k úhradě nebo příkazu k inkasu) je považován za platební prostředek, neboť na jeho základě dochází k realizaci peněžní transakce. Nezáleží na tom, zda je v listinné podobě (formuláře a tiskopisy k úhradě nebo k inkasu), nebo v podobě elektronické (internetové bankovnictví, telefon, platební karta). Protože je-li poskytována ochrana příkazům k zúčtování v podobě listinné, bylo by zcela nelogické činit rozdíl mezi různými formami téhož platebního prostředku a neposkytovat ochranu i elektronické podobě (zejména s ohledem na společenský vývoj a technický pokrok, na které právo musí také reagovat).[210]

Ve vztahu k phishingu, co se týče ustanovení § 234 TrZ, není možné, aby pachatel naplnil trestný čin podle § 234 odst. 1 TrZ již samotným vylákáním přihlašovacích údajů od uživatele. Přístupové údaje k internetovému bankovnictví ani údaje platební karty totiž nenaplňují uvedenou definici platebního prostředku podle zákona o platebním styku, čili nejde o platební prostředek.[211] K naplnění skutkové podstaty trestného činu upraveného v ustanovení § 234 TrZ v souvislosti s phishingovým útokem dojde až tehdy, kdy pachatel na základě podvodně získaných údajů realizuje platbu prostřednictvím platebního prostředku. Vydává se tedy za oprávněného uživatele, který má oprávnění s peněžními prostředky nakládat, čímž naplní znaky odstavce 3. Proto bude tato kapitola zaměřena už pouze na § 234 odst. 3 TrZ.

Za padělání platebního prostředku podle § 234 odst. 3 TrZ se považuje jeho neoprávněné vyrobení či vyhotovení tak, že obsahuje zdánlivě správné, avšak ve skutečnosti falešné údaje, s cílem provést jeho prostřednictvím platební styk. Dále je paděláním vyplnění či vyhotovení platebního prostředku bez oprávnění.[212] Padělání se musí projevit v tom, že pachatel užije správných přihlašovacích a dalších potřebných údajů, bez vědomí klienta a banky, v důsledku čehož je platební prostředek vydán jinou než oprávněnou osobou. To je prakticky shodné s paděláním příkazu k úhradě v papírové podobě, kde by byly uvedeny správně všechny údaje, avšak podpis oprávněné osoby je zdařile nahrazen padělatelem, což vede k tomu, že je takový příkaz bankou akceptován.[213]

U internetového bankovnictví není možné pro přístup do něj, popřípadě pro schválení příkazu k úhradě aplikovat něčí podpis, při uskutečnění transakcí je proto podpis disponenta účtu nahrazen heslem a dalšími potvrzovacími (autorizačními) kódy, které jsou zasílány bankovním

[210] Usnesení Nejvyššího soudu ze dne 16. května 2018, sp. zn. 4 Tdo 456/2018, publikované pod č. 8/2019 Sbírky soudních rozhodnutí a stanovisek.
[211] Více viz KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 71-72.
[212] ŠČERBA, Filip. a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, str. 1921.
[213] Usnesení Nejvyššího soudu ze dne 18. ledna 2012, sp. zn. 6 Tdo 1677/2011.

ústavem na mobilní telefon disponenta účtu. Podpis příkazce je nahrazen právě použitím ověřovacích metod a jejich neoprávněné překonání odpovídá zfalšování podpisu příkazce.

Pokud pachatel bez oprávnění vyplní po překonání bezpečnostních prvků formulář platebního příkazu k převodu peněz, který odešle, vytvoří tak padělaný platební prostředek (vztahuje se i na použití platební karty) a jeho jednání naplňuje znaky skutkové podstaty trestného činu podle § 234 odst. 3 alinea první TrZ.[214] Za tento trestný čin hrozí trest odnětí svobody tři až osm let.

3.3.4. Závěr o právní kvalifikaci phishingového útoku

V případě stanovení právní kvalifikace dopadající na pachatele phishingového útoku přichází do úvahy několik možných situací.

Trestného činu podvodu podle § 209 TrZ se pachatel nejčastěji dopustí vůči uživateli, ze kterého vyláká podvodem (vydávající se za důvěryhodnou osobu nebo instituci) přihlašovací údaje k nějakému účtu (může jít o účet internetového bankovnictví, k sociální síti, k e-mailu apod.). Nebo vůči další osobě, se kterou komunikuje jako ta osoba, od které dříve získal přihlašovací údaje, případně vůči bance, která považuje pachatele za svého klienta. Podmínkou zde však je způsobení škody nikoli nepatrné.

Naplnění znaků skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 2 písm. c) TrZ se pachatel dopustí, pokud se vydává za oprávněný subjekt a zpráva pak má vzbuzovat dojem pravosti, nebo pokud vytvoří padělané internetové stránky, které mají vypadat jako stránky originální, a odkaz na ně pošle uživateli.

Jestliže pachatel použije podvodně získané přihlašovací údaje k internetovému bankovnictví jiné osoby (případně údaje platební karty) a vytvoří padělaný platební prostředek k bezhotovostní platbě, který odešle, čímž způsobí škodu nikoli nepatrnou na cizím majetku, je nutné jeho jednání posoudit nikoliv pouze jako trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 odst. 3 TrZ, ale také jako trestný čin podvodu podle § 209 odst. 1 TrZ, přičemž jde o trestné činy spáchané v jednočinném souběhu. Faktická konzumpce je zde vyloučena. Vzhledem ke skutkovým okolnostem spáchaného trestného činu podvodu jej zpravidla nelze považovat za vedlejší, málo významný produkt základního trestného

[214] Usnesení Nejvyššího soudu ze dne 16. května 2018, sp. zn. 4 Tdo 456/2018, publikované pod č. 8/2019 Sbírky soudních rozhodnutí a stanovisek.

činu vzhledem k různosti objektů obou trestných činů a k tomu, že trestný čin podle § 234 odst. 3 TrZ nevyžaduje obohacení pachatele nebo jiné osoby a ani způsobení škody.[215]

Případně pokud by se navíc uvažovalo o tom, že pachatel připojil k falešné zprávě malware, a uživatel si jej v omylu stáhne, bylo by možné takové jednání kvalifikovat podle některé z alternativ upravené v § 230 odst. 2 písm. a) až d) TrZ v závislosti na účincích malwaru a jednání pachatele.

3.4. Odpovědnost bank za škodu způsobenou phishingem

Podle judikatury Nejvyššího soudu[216] je vlastníkem peněžních prostředků na bankovním účtu banka, zatímco klient banky má vůči bance pohledávku, na základě které má nárok na výplatu peněžních prostředků ve výši vedené na tomto účtu. Pokud byly prostřednictvím phishingu neoprávněně odvedeny z bankovního účtu peníze, je to banka, které vzniká škoda, protože se jedná o její peněžní prostředky.[217]

V případě zneužití přístupových údajů jiného se pachatel vydává za oprávněného uživatele, za kterého zadá elektronický příkaz k úhradě, jenž potvrdí dohodnutým způsobem mezi bankou a klientem. K odčerpání peněžních prostředků proto dojde za plné kontroly poskytovatele účtu a služby přímého bankovnictví nad napadeným bankovním účtem. V takovém případě banka zcela dobrovolně přesune peněžní prostředky z jednoho bankovního účtu na jiný, protože předpokládá, že příkaz k úhradě zadává klient, který má jako jediný k dispozici nezbytné údaje pro vstup do internetového bankovnictví a pro odeslání potvrzení příkazu k úhradě. Pachatel se tedy vydává fakticky za disponenta účtu a neoprávněně autorizuje jeho podpis, přičemž banka jako poskytovatel účtu nemá žádný důvod předpokládat, že příkaz k úhradě nezadal klient. Banka je uvedena pachatelem v omyl, díky němuž dojde k přesunu peněžních prostředků z účtu klienta.[218]

Jestliže došlo k provedení platební transakce pachatelem, aniž by ji majitel účtu autorizoval, tedy bez jeho souhlasu, jedná se o tzv. neautorizovanou platební transakci. Tuto transakci pak může majitel účtu reklamovat u své banky z důvodu, že k ní nedal souhlas. Pokud

[215] Usnesení Nejvyššího soudu ze dne 27. srpna 2013, sp. zn. 4 Tdo 812/2013, publikované pod č. 27/2014 Sbírky soudních rozhodnutí a stanovisek.
[216] Usnesení Nejvyššího soudu ze dne 30. ledna 2004, sp. zn. 11 Tdo 40/2004, publikované pod č. 14/2006 Sbírky soudních rozhodnutí a stanovisek, usnesení Nejvyššího soudu ze dne 27. srpna 2013, sp. zn. 4 Tdo 812/2013, publikované pod č. 27/2014 Sbírky soudních rozhodnutí a stanovisek.
[217] NOVÁK, Patrik. *Phishing – odpovídá za ztrátu banka nebo majitel účtu?*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-27]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu.
[218] Usnesení Nejvyššího soudu ze dne 16. května 2018, sp. zn. 4 Tdo 456/2018, publikované pod č. 8/2019 Sbírky soudních rozhodnutí a stanovisek.

banka neuzná reklamaci, musí odůvodnit z jakých právních důvodů a na základě jakých skutečností tak rozhodla a dále doložit důkazy, jakým způsobem byly podvodně provedené transakce autorizovány.[219]

Podle § 182 odst. 1 písm. b) zákona o platebním styku nese plátce[220] ztrátu z neautorizovaných platebních transakcí *„v plném rozsahu, způsobil-li tuto ztrátu svým podvodným jednáním nebo tím, že úmyslně nebo z hrubé nedbalosti porušil některou ze svých povinností stanovených v § 165.“* V § 165 zákona o platebním styku jsou stanoveny povinnosti uživatele spočívající v ochraně osobních bezpečnostních prvků a nahlášení ztráty, odcizení, zneužití nebo neoprávněného použití platebního prostředku bez zbytečného odkladu bance. Častou argumentací bank proto je, že provedení podvodu umožnil klient, jelikož nedodržel pravidla bezpečnosti[221] a z hrubé nedbalosti ztrátu způsobil. Ztrátu by tedy v takovém případě měl nést klient sám.[222]

Co se týče hrubé nedbalosti, jde o vyšší míru nedbalosti ve smyslu její intenzity a míří se tím především na lehkomyslnost až bezohlednost škůdce, s jakou přistupuje k plnění své právní povinnosti. Dochází k porušení náležité míry opatrnosti takovým způsobem, který se výrazně vymyká tomu, co je běžně akceptovatelné. Hrubě nedbale jedná ten, komu lze vytknout mimořádně výraznou míru neopatrnosti nebo lehkomyslnosti.[223] Hrubé nedbalosti se tedy uživatel může dopustit tím, pokud poskytne své údaje a navíc potvrdí transakci pachatele pomocí stanovených ověřovacích metod. Hrubou nedbalost však musí klientovi prokázat banka a doložit, čím svoje povinnosti porušil.

U phishingu je problematické určit, kdy klient banky jedná v hrubé nedbalosti, protože phishingový útok bývá často velmi sofistikovaný a činí velký problém jej odhalit. Tedy i pokud klient jedná s běžnou opatrností, může se stát obětí phishingu. Díky tomu není možné jednoznačně stanovit, že poskytnutí přihlašovacích údajů a další kroky vedoucí ke ztrátě peněžních prostředků

[219] NOVÁK, Patrik. *Phishing – odpovídá za ztrátu banka nebo majitel účtu?*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-27]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu.

[220] Podle § 2 odst. 3 písm. a) zákona o platebním styku je plátcem uživatel, z jehož platebního účtu mají být odepsány peněžní prostředky k provedení platební transakce nebo který dává k dispozici peněžní prostředky k provedení platební transakce.

[221] Smluvní dokumentace bank zpravidla obsahuje ustanovení, která klienty upozorňuje na poskytování svých bezpečnostních prvků, zejména přihlašovací údaje a často také přímo upozorňují na riziko útoků a podvodných e-mailů.

[222] NOVÁK, Patrik. *Phishing – odpovídá za ztrátu banka nebo majitel účtu?*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-27]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu.

[223] PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. *Občanský zákoník. Komentář*. 2. vydání. Praha: C. H. Beck, 2019, str. 3006.

znamenají automaticky hrubou nedbalost. Banka tak musí posoudit všechny okolnosti případu, zejména jakou podobu měl phishingový útok a jak klient jednal, a odůvodnit, že klient jednal v hrubé nedbalosti.[224]

Avšak ohledně neautorizované platební transakce existují výjimky z § 182 odst. 1 zákona o platebním styku, kdy se tento odstavec nepoužije, pokud ztráta vznikla poté, co klient oznámil ztrátu, odcizení nebo zneužití platebního prostředku; banka nezajistila, aby klientovi byly k dispozici vhodné prostředky umožňující kdykoli oznámit ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku; nebo banka nepožadovala silné ověření klienta v případech podle § 223 odst. 1 nebo 6 zákona o platebním styku. Pokud by klient nahlásil phishingový útok bance a ta by včas nezareagovala a nezabránila takovému převodu, nebo klient nemohl útok nahlásit kvůli vině na straně banky, je odpovědnost za způsobenou ztrátu na straně banky.[225]

Silné ověření uživatele je pak upraveno v § 223 zákona o platebním styku. Od 1. ledna 2021 by banky neměly vyžadovat ověření plateb pouze přes SMS kód. Kvůli dosažení vyšší bezpečnosti plateb a ochrany klientů před podvody bylo zavedeno silné, minimálně dvoufaktorové ověření uživatele. To je vyžadováno při přístupu do internetového bankovnictví, při zadání elektronické platební transakce nebo při jiném úkonu prostřednictvím prostředků komunikace na dálku, které by mohlo vést k podvodnému jednání nebo ke zneužití, a také při požadování informací o platebním účtu. Jde o kombinaci prvků z kategorie držení nebo vlastnictví (něčeho, co klient má, například mobilní telefon), kategorie znalosti (něčeho, co klient zná, např. heslo či PIN) a kategorie jedinečnosti či biometrie (něčeho, co klient je, to klient potvrzuje např. otiskem prstu či prostřednictvím rozpoznání obličeje).[226] Pokud autorizace platební transakce neproběhne podle pravidel silného ověření, ponese banka odpovědnost za neautorizovanou platební transakci, která byla způsobena phishingovým útokem.

V případě, že reklamace klienta bude bankou zamítnuta a banka odmítne nahradit ztrátu způsobenou phishingovým útokem, zpravidla může klient bance podat podnět k opětovnému posouzení reklamace, které provádí jiný výše postavený pracovník banky. Jestliže není klient ani

[224] NOVÁK, Patrik. *Phishing – odpovídá za ztrátu banka nebo majitel účtu?*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-27]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu.

[225] NOVÁK, Patrik. *Phishing – odpovědnost banky a silné ověření*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-28]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovednost-banky-a-silne-overeni.

[226] *Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021.* Česká národní banka [online]. 2021 [cit. 2023-05-28]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/.

s takovým přezkumem spokojen, může podat žalobu k civilnímu soudu a domáhat se náhrady v rámci soudního řízení nebo se obrátit na finančního arbitra, který slouží k mimosoudnímu řešení sporů mezi spotřebiteli a finančními institucemi. Rozhodnutí finančního arbitra je přezkoumatelné na návrh neúspěšné strany soudem. Klient banky má i po jeho rozhodnutí stále možnost obrátit se na civilní soud.[227]

Z výše uvedeného tedy plyne, že i pokud uživatel podlehne phishingovému útoku a pachatel (nebo jiná osoba) se v důsledku toho obohatí, neznamená to automaticky, že o své peněžní prostředky přijde.

[227] NOVÁK, Patrik. *Phishing – odpovědnost banky a silné ověření*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-28]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovednost-banky-a-silne-overeni.

Závěr

Cílem této diplomové práce bylo poskytnout celkové zhodnocení trestních a kriminologických aspektů phishingu. Závěry ukazují, že phishing se neustále vyvíjí a mění svou podobu, čímž vytváří nové výzvy pro oblast trestního práva a kriminologie. I přes rostoucí povědomí o phishingu a kybernetické kriminalitě obecně a o jejich dopadech na jednotlivce i společnost, vzrůstá počet případů těchto útoků.

Výsledky diplomové práce ukazují, že phishing je sofistikovaným druhem kybernetické kriminality a neustále se zdokonaluje. Útočníci využívají metod sociálního inženýrství a technologie k manipulaci uživatelů s cílem získat od nich osobní nebo přístupové údaje. Phishing se proto řadí mezi nejrozšířenější druhy kybernetické kriminality. Na základě získaných dat popisujících dynamiku phishingu bylo potvrzeno, že phishing je každoročně stále rozšířenějším, a to globálně, proto vyžaduje neustálou pozornost a kontrolu.

Hypotéza přijatá v úvodu diplomové práce týkající se stoupajícího trendu počtu případů phishingu byla potvrzena. Vzhledem k rostoucímu počtu uživatelů internetu a zvyšující se závislosti na internetu lze očekávat, že počet případů phishingu bude i nadále stoupat a představovat tak významnou hrozbu.

V části práce popisující pachatele bylo zjištěno, že neexistují relevantní zdroje pro podrobné popsání znaků pachatele phishingu. Výzkumy v této oblasti jsou nedostatečné, a to nejenom v české literatuře, ale i v zahraniční. Z toho důvodu bylo v této části práce nutné vztáhnout znalosti týkající se pachatele kyberkriminality i na pachatele phishingu. Při popisu oběti phishingu byla použita převážně zahraniční literatura, kde bylo nalezeno množství studií zabývajících se tímto tématem. Pro úplnost porovnání byly taktéž popsány znaky oběti kyberkriminality.

U právní kvalifikace se zcela jistě nepodařilo zachytit všechna možná jednání, kterých by se pachatel mohl dopustit a která by se dala kvalifikovat jako trestný čin. Avšak z odborné literatury i judikatury vyplývá, že pachatel phishingu může naplňovat především trestné činy podvodu podle § 209 TrZ, neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 TrZ a neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 TrZ. Je nezbytné však poznamenat, že právní úprava není dostatečná, protože ač jednání naplňuje znaky phishingu nelze jej vždy postihnout prostředky trestního práva.

Závěry této práce jsou podpořeny odbornou literaturou, judikaturou a dalšími relevantními zdroji, které přispívají k celkovému pochopení problematiky a umožňují vyvodit závěry týkající se trestního stíhání a kriminologických aspektů phishingu. Zhodnocení vývoje počtu případů phishingu a proces jeho zdokonalení by mohly napomoci k lepšímu pochopení phishingu a navrhnutí účinnějších strategií pro boj proti němu. Je nezbytné posilovat právní rámec a trestněprávní postupy v boji proti phishingu, aby pachatelé mohli být efektivněji stíháni a potrestáni.

Seznam zkratek

APWG	Anti-Phishing Working Group
ČSOB	Československá obchodní banka, a.s.
Non-cash směrnice	Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
TrZ, trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník
Úmluva	Úmluva Rady Evropy č. 185 o počítačové kriminalitě
Zákon č. 130/2022 Sb.	Zákon č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony
Zákon o kybernetické bezpečnosti	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
Zákon o obětech trestných činů	Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů
Zákon o platebním styku	Zákon č. 370/2017 Sb., o platebním styku

Seznam použitých zdrojů

1. Knižní publikace

DRAŠTÍK, Antonín, DURDÍK, Tomáš, FREMR, Robert, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander a kol. *Trestní zákoník. Komentář*. *I. díl.* Praha: Wolters Kluwer ČR, 2015. 1568 s. ISBN 978-80-7478-790-4.

GŘIVNA, Tomáš, POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 5. vydání. Praha: Wolters Kluwer, 2019, 588 s. ISBN 978-80-7598-554-5.

JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

JELÍNEK, Jiří a kol. *Kriminologie*. Praha: Leges, 2021, 631 s. ISBN 978-80-7502-499-2.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007, 288 s. ISBN 978-80-247-1561-2.

KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016. 522 s. ISBN 978-80-88168-15-7.

KOLOUCH, Jan, BAŠTA, Pavel a kol. *CyberSecurity.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2019, 556 s. ISBN 978-80-88168-31-7.

KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. vydání. Plzeň: Aleš Čeněk, 2021, 417 s. ISBN 978-80-7380-859-4.

LANCE, James. *Phishing bez záhad.* Přeložil Lubomír Moudrý. Praha: Grada Publishing, a.s., 2007, 281 s. ISBN 978-80-247-1766-1.

PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. *Občanský zákoník. Komentář*. 2. vydání. Praha: C. H. Beck, 2019. ISBN 978-80-7400-747-7.

PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. vydání. Plzeň: Aleš Čeněk, 2019, 1205 s. ISBN 978-80-7380-741-2.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.

SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019, 378 s. ISBN 978-80-7380-765-8.

ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. 2. vydání. Praha: C. H. Beck, 2012, 3614 s. ISBN 978-80-7400-428-5.

ŠČERBA, Filip a kol. *Trestní zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2020, 3331 s. ISBN 978-80-7400-807-8.

VÁLKOVÁ, Helena, KUCHTA, Josef, HULMÁKOVÁ, Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019, 616 s. ISBN 978-80-7400-732-3.

VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ, Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020. ISBN 978-80-7338-189-9.

ZAVRŠNIK, Aleš. *Kyberkriminalita.* Praha: Wolters Kluwer ČR, 2017, 148 s. ISBN 978-80-7552-758-5.

2. Odborné články

ALKHALIL, Zainab, HEWAGE, Chaminda, NAWAF, Liqaa, KHAN, Imtiaz. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.* In: Frontiers in Computer Science, 2021, vol. 3, 23 s. ISSN 2624-9898.

DARWISH, Ali, ZARKA, Ahmed, ALOUL, Fadi. *Towards understanding phishing victims' profile*. International Conference on Computer Systems and Industrial Informatics, IEEE, 2012.

DE KIMPE, Lies et al. *You've got mail! Explaining individual differences in becoming a phishing target*. In: Telematics and Informatics, 2018, vol. 35, no. 5, str. 1277–1287. ISSN 0736-5853.

DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. In: Trestněprávní revue, 2018, roč. 17, č. 4, str. 84–89.

HLAVÁČOVÁ, Kateřina. *Phishing a jeho postupná evoluce*. In: VOJÁČEK, Ladislav, TAUCHEN, Jaromír (ed.). Majetkové a hospodářské trestné činy včera a dnes. Sborník z konference. Brno: Masarykova univerzita, 2016, str. 268-279. ISBN 978-80-210-8332-5.

JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary.* Páté doplněné a upravené vydání. Přeložil Karel Vavruška. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.

KRUPIČKA, Jiří. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012, č. 4, str. 57-73. ISSN 0323-0619.

KUCHAŘÍK, Karel. *Aktuální trendy informační kriminality v rámci šetřených případů PČR*. In: KNÝ, Milan, SOUDKOVÁ, Šárka (ed.). Sborník Evropského měsíce kybernetické bezpečnosti 2014. Praha: Policejní akademie ČR, 2014, str. 5-8.

KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence*. In: Časopis pro právní vědu a praxi. Brno: Právnická fakulta Masarykovy univerzity, 2016, roč. 24, č. 1, str. 5-19. ISSN 1210-9126.

MOHAMMAD, Rami, THABTAH, Fadi, MCCLUSKEY, Lee. *Tutorial and critical analysis of phishing websites methods*. In: Computer Science Review, 2015, vol. 17, str. 1-24. ISSN 1574-0137.

SALAHDINE, Fatima, KAABOUCH, Naima. *Social Engineering Attacks: A Survey*. In: Future Internet. 2019, vol. 11, no. 4, str. 1-17.

SCOTT, Applegate. *Social Engineering: Hacking the Wetware!.* In: Information Security Journal: A Global Perspective, 2009, vol. 18, no. 1, str. 40-46.

SHENG, Steve, LANYON, Mandy, KUMARAGURU, Ponnurangam, CRANOR, Lorrie, DOWNS, Julie. *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. Conference on Human Factors in Computing Systems – Proceedings, 2010, 10 s.

SRIVASTAVA, Tushar. *Phishing and Pharming – The Deadly Duo*. SANS Institute, 2007, 35 s.

VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestně právní kvalifikace*. In: Trestní právo, 2010, roč. 14, č. 12, str. 5-13.

VOLEVECKÝ, Petr. *Kybernetické hrozby a jejich trestněprávní kvalifikace*. In: Trestní právo, 2011, roč. 15, č. 1, str. 11-23.

3. Seznam jiných závěrečných prací

KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. [online]. Praha, 2012 [cit. 2022-12-14]. Disertační práce. Univerzita Karlova, Právnická fakulta, Katedra trestního práva. Vedoucí práce Jelínek, Jiří. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/41665/140021339.pdf?sequence=1&isAllowed=y.

4. Seznam použité judikatury

Usnesení Nejvyššího soudu ze dne 30. ledna 2004, sp. zn. 11 Tdo 40/2004, publikované pod č. 14/2006 Sbírky soudních rozhodnutí a stanovisek.

Usnesení Nejvyššího soudu ze dne 18. ledna 2012, sp. zn. 6 Tdo 1677/2011.

Usnesení Nejvyššího soudu ze dne 27. srpna 2013, sp. zn. 4 Tdo 812/2013, publikované pod č. 27/2014 Sbírky soudních rozhodnutí a stanovisek.

Usnesení Nejvyššího soudu ze dne 16. května 2018, sp. zn. 4 Tdo 456/2018, publikované pod č. 8/2019 Sbírky soudních rozhodnutí a stanovisek.

5. Seznam použitých právních předpisů

Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy.

Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV.

Směrnice Evropského parlamentu a Rady (EU) 2013/40 ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.

Úmluva Rady Evropy č. 185 o počítačové kriminalitě.

Zákon, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů.

Zákon č. 370/2017 Sb., o platebním styku.

Zákon č. 40/2009 Sb., trestní zákoník.

6. Seznam použitých internetových zdrojů

About The APWG. Anti-Phishing Working Group [online]. 2023 [cit. 2023-03-09]. Dostupné z: https://apwg.org/about-us/.

Aktuální podvodné e-maily a SMS: 14. 3. 2023 Bezpečnostní upozornění na podvodné e-maily. Česká pošta [online]. 2023 [cit. 2023-03-15]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/aktualni-podvodne-e-maily.

BARTOSZ, Jakub. *Člen vedení budějovické firmy poslal podvodníkovi přes milion*. [online]. 2022 [cit. 2022-12-29]. Dostupné z: https://www.novinky.cz/clanek/krimi-clen-vedeni-budejovicke-firmy-poslal-podvodnikovi-pres-milion-40417671#dop_ab_variant=0&dop_source_zone_name=novinky.sznhp.box&source=hp&seq_no=8&utm_campaign=abtest203_personalizovany_layout_varAA&utm_medium=z-boxiku&utm_source=www.seznam.cz.

Mattel vs. Chinese cyberthieves: It's no game. CBS NEWS [online]. 2016 [cit. 2022-11-22]. Dostupné z: https://www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/.

MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022*. Policie České republiky [online]. 2023 [cit. 2023-04-28]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx.

NOVÁK, Patrik. *Phishing – odpovídá za ztrátu banka nebo majitel účtu?*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-27]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu.

NOVÁK, Patrik. *Phishing – odpovědnost banky a silné ověření*. Kropáček Legal, Advokátní kancelář [online]. 2022 [cit. 2023-05-28]. Dostupné z: https://www.pravopropodnikatele.cz/phishing-odpovednost-banky-a-silne-overeni.

O týmu CSIRT.CZ. CSIRT.CZ [online]. 2019 [cit. 2023-03-09]. Dostupné z: https://csirt.cz/cs/hlaseni-incidentu/faq/.

Phishing Activity Trends Report. Anti-Phishing Working Group [online]. 2004 [cit. 2022-11-15]. Dostupné z: https://docs.apwg.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.

Phishing Activity Trends Reports. Anti-phishing Working Group [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://apwg.org/trendsreports/.

Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit. Národní úřad pro kybernetickou a informační bezpečnost [online]. 2020 [cit. 2022-11-22]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/.

Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. Česká národní banka [online]. 2021 [cit. 2023-05-28]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/.

Statistics about phishing activity. PhishTank [online]. Cisco Talos Intelligence Group, 2023 [cit. 2023-05-25]. Dostupné z: https://www.phishtank.com/stats.php.

Statistiky řešených incidentů. CSIRT.CZ [online]. 2022 [cit. 2023-05-22]. Dostupné z: https://csirt.cz/cs/o-nas/statistiky/.

ŠČERBA, F. a kol. *Trestní zákoník. Komentář.* 1. vydání (2. aktualizace). Beck-online [online právní informační systém]. Nakladatelství C. H. Beck, 2022. Dostupné z: https://www-beck-online-cz.

Upozorňujeme na další vlnu phishingových e-mailů, které cílí na klienty internetového bankovnictví. ČSOB [online]. 2023 [cit. 2023-02-26]. Dostupné z: https://www.csob.cz/portal/-/s230222?redirect=%2Fportal%2Fbezpecnost%2Faktualni-hrozby.

Vishing: Jak ho rozeznat a vyhnout se mu?. ESET [online]. 2021 [cit. 2022-11-22]. Dostupné z: https://digitalsecurityguide.eset.com/cz/vishing-jak-ho-rozeznat-a-vyhnout-se-mu.

Vishing a spoofing. Policejní prezidium ČR [online]. 2021 [cit. 2022-11-22]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx.

VOKUŠ, Jiří. *Kybernetická kriminalita*. Policie České republiky [online]. 2019 [cit. 2023-03-28]. Dostupné z: https://www.policie.cz/clanek/kyberneticka-kriminalita.aspx.

Whaling: how it works, and what your organisation can do about it. National Cyber Security Centre [online]. [cit. 2022-11-22]. Dostupné z: https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it.

What Is Pharming and How to Protect Yourself. Kaspersky [online]. [cit. 2022-11-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming.

What is Spear Phishing?. Kaspersky [online]. [cit. 2023-02-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/spear-phishing.

What is a Whaling Attack?. Kaspersky [online]. [cit. 2022-11-11]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack.

Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2022. CSIRT.CZ [online]. 2023 [cit. 2023-03-28]. Dostupné z: https://csirt.cz/cs/o-nas/.

7. Ostatní zdroje

Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník, č. 40/2009 Dz.

Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

Přílohy

Příloha č. 1: Tabulka s počtem případů podle APWG za každé čtvrtletí v letech 2018-2022

Čtvrtletí/rok	Počet případů
1Q/2018	263 538
2Q/2018	233 040
3Q/2018	151 014
4Q/2018	138 328
1Q/2019	180 768
2Q/2019	182 465
3Q/2019	266 378
4Q/2019	162 155
1Q/2020	164 772
2Q/2020	146 994
3Q/2020	571 764
4Q/2020	637 302
1Q/2021	611 877
2Q/2021	616 939
3Q/2021	730 372
4Q/2021	888 585
1Q/2022	1 025 968
2Q/2022	1 097 811
3Q/2022	1 270 883
4Q/2022	1 350 037

Trestní a kriminologické aspekty phishingu

Abstrakt

Diplomová práce se zaměřuje na analýzu trestních a kriminologických aspektů phishingu. Při shromažďování literárních zdrojů byl zjištěn nedostatek odborných prací, které by se systematicky zabývaly phishingem, i přestože se jedná o jeden z nejrozšířenějších druhů kybernetické kriminality, který pro uživatele kyberprostoru představuje velkou hrozbu. V česky psané literatuře je markantní zejména absence kriminologicky zaměřených studií.

Práce je rozdělena na část kriminologickou a trestněprávní. Práce poskytuje komplexní pohled na phishing a rozebírá jeho vývoj a proces zdokonalení. Nejdříve je tedy vymezeno, co je phishing a jak může vypadat a následně je práce zaměřena na jeho historii a druhy, které se postupem času vyvinuly. Cílem této práce je zhodnotit vývoj počtu phishingových útoků, zda je meziroční trend stoupající, klesající či zůstává přibližně stejný. Vzhledem k množství lidské interakce v kyberprostoru je předpokladem rostoucí trend počtu případů phishingu. Dále se zaměřuje na znaky pachatele a jeho motivaci, znaky oběti a možnosti prevence před phishingovými útoky. Zde jsou využívány, vzhledem k absenci české literatury zabývající se touto problematikou, především zahraniční zdroje a studie.

V části trestní je zmíněna evropská úprava, ale především se práce zaměřuje na český právní řád, konkrétně trestní zákoník, a zabývá se otázkou, jaká právní kvalifikace by mohla dopadat na pachatele phishingového útoku. V úvahu připadají trestné činy podvodu podle § 209 TrZ, neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací podle § 230 TrZ a neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 TrZ.

V práci jsou využívány deskriptivní metody k obecnému definování phishingu a logická indukce pro analýzu dat ze statistik vývoje a závěry odborné literatury. Výsledky této práce poskytují vhled do problematiky phishingu, práce může poskytnout základní rámec pro další studie v této oblasti a mohla by být inspirací pro další výzkumy, které pomohou zvýšit povědomí o phishingu jako závažné kybernetické kriminalitě a podpoří ochranu uživatelů před jeho škodlivými důsledky.

Závěry práce přinášejí doporučení pro posilování právního rámce a trestněprávních postupů, neboť phishing je přetrvávajícím a potenciálně se prohlubujícím problémem společnosti. Cílem práce je přispět k efektivní ochraně proti phishingu a zvýšit povědomí o jeho závažnosti v kybernetickém světě 21. století.

Klíčová slova:

phishing, kybernetická kriminalita, vývoj phishingu, pachatel a oběť phishingu, trestní postih

Criminal and criminological aspects of the phishing

Abstract

Present thesis is aimed on analysis of criminal and criminological aspects of phishing. While gathering the literature resources lack of studies systematically describing the problematic of phishing was discovered even though phishing is one of the most common cybernetical crimes and represents a significant thread for users of cyberspace. Czech literature is especially lacking studies concerning criminological aspects of phishing.

This thesis is divided to two parts - criminological and criminal. This thesis presents complex description of phishing including its evolution and process of refinement. In the first part phishing as a phenomenon and also its history and types evolving with time are described. The aim of this thesis is to evaluate the trend of number of phishing attacks and to determine whether its increasing, decreasing or level. Given the human interactions in cyberspace increasing trend is expected. In the next part characteristics and motivation of offender, characteristics of the victim and possibilities of prevention are discussed. In this part mostly international sources are being used given the absence of Czech sources.

In the criminal part European legislative is briefly mentioned. Nevertheless, this thesis is written in the environment of Czech law hence for mostly the Czech Penal Code is used to determine the legal qualification of the offender of phishing attacks. Given the nature of the phishing following sections of the Penal Code should be considered: Section 209 Fraud, Section 230 Unauthorised access to computer systems and unauthorised and interference with the computer system or information medium, Section 234 Unauthorised obtaining, forgery and alteration of means of payment.

In present thesis mostly descriptive methods for common definition of phishing, logical induction for data analysis using statistics of development of phishing and conclusions of literature sources were used. Results of this thesis bring insight to the problematics of phishing and may also bring a foundation for another phishing studies. Author hopes this thesis may also inspire other authors to conduct more research which would raise the public awareness of phishing as serious cybercrime and support protection of users of cyberspace from its negative influence.

Results of this work also brings suggestions which should help to strengthen the legal framework since the phishing is lasting and potentially increasing problem for the society. The aim of the thesis is to contribute to effective protection against phishing and to raise awareness of its seriousness in the cyber world of the 21st century.

Keywords:

phishing, cybercrime, development of phishing, offender and victim of phishing, criminal sanctions