VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

Phishing jako forma kybernetické kriminality v České republice a možnosti jeho prevence

Autor práce: Radek Šír, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Radek Šír, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce Phishing jako forma kybernetické kriminality v České republice a možnosti jeho prevence

Název bakalářské práce v anglickém jazyce: Phishing as a Form of Cybercrime in the Czech Republic and Options for Its Prevention

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): prosinec 2025

Cíl bakalářské práce: Cílem bakalářské práce je zhodnotit současný stav phishingu jako formy kybernetické kriminality v České republice, posoudit účinnost existujících preventivních opatření a na základě zjištěných poznatků formulovat konkrétní návrhy a doporučení pro zlepšení prevence proti phishingu a zvýšení efektivity ochrany uživatelů i organizací před phishingovými útoky.

Student: Radek Šír, DiS.	8.12.2025 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	11.12.25 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.12.2025 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2025 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.12.2025 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

ŠÍR, R. *Phishing jako forma kybernetické kriminality v České republice a možnosti jeho prevence: bakalářská práce*. Příbram: Vysoká škola evropských a regionálních studií, 2026. 71 s. Vedoucí práce: RNDr. Růžena Ferebauerová.

Klíčová slova: CSIRT.CZ, Česká republika, kybernetická kriminalita, Národní centrála proti terorismu, extremismu a kybernetické kriminalitě, Národní úřad pro kybernetickou a informační bezpečnost, phishing, Policie ČR, prevence, Služba kriminální policie a vyšetřování, sociální inženýrství

Tato bakalářská práce se zabývá problematikou phishingu jako jedné z dominantních forem kybernetické kriminality v České republice. Cílem práce je zhodnotit současný stav této hrozby, posoudit účinnost existujících preventivních opatření a na základě zjištěných poznatků formulovat konkrétní návrhy pro zvýšení efektivity ochrany jednotlivců i soukromých a státních organizací.

Teoretická část práce definuje phishing, jeho specifické rysy a různorodé formy páchání. Zároveň poskytuje částečný přehled relevantní národní i mezinárodní legislativy a popisuje aktuální strategie ochrany. Praktická část analyzuje reálný stav phishingu v ČR s využitím datových podkladů Policie ČR, Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB"), národního bezpečnostního týmu CSIRT.CZ, Národní centrály proti terorismu, extremismu a kybernetické kriminalitě (dále jen „NCTEKK") a Služby kriminální policie a vyšetřování (dále jen „SKPV"). Důležitou součástí práce je kvalitativní výzkum realizovaný formou řízených rozhovorů s experty z těchto institucí, který odkrývá aktuální trendy, jako je vliv umělé inteligence, profesionalizace útočníků a přetrvávající zranitelnost lidského faktoru.

Závěrečná část práce popisuje získané poznatky a navrhuje opatření směřující k posílení meziorgánové a mezistátní spolupráce, zrychlení reakce na incidenty, zlepšení legislativy a zefektivnění vzdělávacích programů. Práce tak nabízí komplexní pohled na problematiku a praktická doporučení pro boj s touto dynamicky rozvíjející se hrozbou.

ABSTRACT

ŠÍR, R. *Phishing as a Form of Cybercrime in the Czech Republic and Options for Its Prevention: Bachelor's Thesis*. Příbram: College of European and Regional Studies, 2026. 71 p. Thesis Supervisor: RNDr. Růžena Ferebauerová.

Keywords: Criminal Police and Investigation Service, CSIRT.CZ, Cybercrime, Czech Republic, National Cyber and Information Security Agency, National Headquarters for Countering Terrorism, Extremism and Cybercrime, Phishing, Police of the Czech Republic, Prevention, Social engineering

This bachelor thesis addresses the issue of phishing as one of the dominant forms of cybercrime in the Czech Republic. The aim of the work is to evaluate the current state of this threat, assess the effectiveness of existing preventive measures, and, based on the findings, formulate specific proposals to increase the efficiency of protection for individuals as well as private and state organizations.

The theoretical part defines phishing, its specific features, and its various forms. It also provides an partial overview of relevant national and international legislation and describes current protection strategies. The practical part analyzes the actual state of phishing in the Czech Republic using data from the Police of the Czech Republic, the National Cyber and Information Security Agency (hereinafter „NÚKIB"), the national security team CSIRT.CZ, the National Headquarters for Countering Terrorism, Extremism, and Cybercrime (hereinafter „NCTEKK") and the Criminal Police and Investigation Service (hereinafter „SKPV"). A crucial component of the thesis is qualitative research conducted through structured interviews with experts from these institutions, revealing current trends such as the influence of artificial intelligence, the professionalization of attackers, and the persistent vulnerability of the human factor.

The concluding part of the thesis describes the findings and proposes measures aimed at strengthening inter-agency and international cooperation, accelerating incident response, improving legislation, and increasing the effectiveness of educational programs. The thesis thus offers a comprehensive perspective on the issue and practical recommendations for combating this dynamically evolving threat.

Obsah

Úvod

Žijeme v éře rychlého technologického rozmachu, kdy digitalizace prostupuje všemi sférami lidské činnosti, od státní správy a bankovnictví až po soukromou sféru a jednotlivce. Zatímco tento pokrok přináší nezpochybnitelné výhody v podobě efektivity, rychlosti a globální dostupnosti služeb, vytváří ale zároveň i nové aspekty zranitelnosti. Evoluce moderní společnosti je tak neoddělitelně spjata s evolucí kriminality, která se z fyzického prostoru masivně přesouvá do prostředí kybernetického. Kybernetická kriminalita se stala pevnou a alarmující součástí bezpečnosti České republiky, přičemž její podíl na celkové registrované kriminalitě vykazuje dlouhodobě vzestupnou tendenci, která nerespektuje státní hranice ani tradiční metody policejního vyšetřování.

Mezi nejrozšířenější a z hlediska dopadů nejkritičtější metody útoků patří phishing. Tato technika, založená na sofistikované manipulaci s lidskou psychikou a systematickém zneužívání důvěry, představuje úzkou provázanost mezi technickým a psychologickým selháním jednotlivce. Phishing již dávno nepředstavuje pouze nekvalitní a snadno rozpoznatelné podvody v podobě špatné češtiny v psaných e-mailech. Současné trendy, jako je integrace umělé inteligence do tvorby podvodného obsahu, profesionalizace mezinárodních útočných skupin a rozvoj hybridních forem útoků, staví před bezpečnostní složky i soukromý sektor zcela nové a komplexní výzvy. Paradoxem současné bezpečnosti zůstává fakt, že i přes neustálé zdokonalování technických bariér, šifrování a plošné zavádění vícefaktorového ověřování zůstává nejslabším a nejčastěji atakovaným článkem celého řetězce lidský faktor.

Tato bakalářská práce se zaměřuje na objektivní rozbor tohoto fenoménu v jeho aktuální podobě. Aktuálnost a společenskou naléhavost tématu podtrhuje skutečnost, že phishingové kampaně dnes necílí primárně pouze na finanční prostředky jednotlivců, ale stále častěji ohrožují stabilitu státních institucí, integritu dat v soukromém sektoru a v krajních případech i kritickou infrastrukturu státu. Efektivní obrana proti těmto hrozbám proto vyžaduje komplexní přístup, který kombinuje vysokou technologickou připravenost s úzkou meziorgánovou a mezistátní spoluprací a především kontinuálním a adaptivním vzděláváním společnosti, které se dokáže přizpůsobovat na měnící se způsob podvodů od útočníků.

Cílem práce je komplexně zhodnotit současný stav phishingu v České republice, podrobně analyzovat jeho nejmodernější formy a kriticky posoudit účinnost stávajících

preventivních i represivních opatření. Na základě syntézy statistických dat a strukturovaných expertních rozhovorů s odborníky z klíčových institucí, jako jsou Služba kriminální policie a vyšetřování (SKPV), Národní centrála proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK) či vládní a národní CERT týmy (CSIRT.CZ), se práce pokusí identifikovat strukturální slabiny současného systému ochrany. Výzkum je dále podložen analýzou výročních a kvartálních zpráv Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), což umožňuje konfrontovat zkušenosti z terénu s oficiálními datovými výstupy.

Práce je metodologicky rozdělena na část teoretickou a praktickou. Teoretická část poskytuje nezbytný terminologický, technologický a legislativní rámec, který definuje postavení phishingu v rámci českého právního řádu a kybernetické bezpečnosti. Praktická část následně přináší unikátní pohled do vyšetřovací a analytické praxe skrze kvalitativní šetření. Ambicí autora je předložit ucelený soubor poznatků, který nepopsal pouze aktuální hrozby, ale posloužil jako odborný základ pro formulaci efektivnější strategie v boji proti phishingovým útokům a přispěl k celkovému zvýšení kybernetické odolnosti v českém digitálním prostoru.

Teoretická část

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je komplexně zhodnotit současný stav phishingu jako specifické a dynamicky se rozvíjející formy kybernetické kriminality v kontextu České republiky. Práce usiluje o hlubší analýzu mechanismů, které útočníci využívají k oklamání obětí, a to s důrazem na aktuální technologický vývoj a sociální inženýrství. Dílčím cílem je posouzení efektivity stávajících preventivních opatření na národní úrovni a následná formulace konkrétních doporučení, která by vedla k posílení informační bezpečnosti jak u individuálních uživatelů, tak v rámci organizačních struktur.

V rámci naplnění stanovených cílů je v práci uplatněn kombinovaný metodologický přístup, který systematicky propojuje teoretická východiska s praktickým výzkumem. Teoretická část je založena na metodě literární rešerše a kritické deskripce odborných pramenů. Tato pasáž zahrnuje analýzu relevantní národní i částečně mezinárodní legislativy, odborných publikací a aktuálních bezpečnostních standardů. Cílem této části je vytvořit pevný terminologický a právní základ pro následné zkoumání problematiky v českém prostředí.

Praktická část práce je zpracována pomocí analýzy sekundárních dat, která jsou čerpána z oficiálních statistik a výročních zpráv klíčových institucí. Konkrétně se jedná o data poskytnutá Policií ČR, Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a národním CSIRT týmem České republiky (CSIRT.CZ). Tato data jsou podrobena kvantitativnímu zkoumání s cílem identifikovat vývojové trendy, četnost útoků a proměny v taktice útočníků v posledních letech. Tímto způsobem je zajištěna vysoká míra objektivity a aktuálnosti předkládaných zjištění.

Pro hlubší vhled do problematiky je kvantitativní analýza doplněna kvalitativním prvkem v podobě strukturovaných rozhovorů s experty z výše uvedených institucí. Tato metoda umožňuje zachytit praktické zkušenosti odborníků a lépe pochopit reálnou účinnost nastavených obranných mechanismů. V závěrečné fázi jsou získané poznatky podrobeny komparaci a syntéze. Výsledkem je kritické vyhodnocení současného stavu ochrany, na jehož základě jsou navržena vlastní opatření směřující ke zvýšení úrovně kybernetické bezpečnosti v celospolečenském měřítku.

2 Kybernetická kriminalita

Nejdříve je nutné definovat samotný pojem kriminalita. Ten je v rámci České republiky úzce spjat s obsahem zvláštní části trestního zákoníku (zákon č. 40/2009 Sb.), který definuje jednotlivé trestné činy.[1] Typickým příkladem v oblasti digitálních útoků jsou činy uvedené v hlavě páté směřující proti majetkovým hodnotám obětí. Jedná se například o trestné činy v případě vztahu k uloženým datům, které naplňují skutkovou podstatu v souvislosti s *neoprávněným přístupem k počítačovému systému a nosiči informací (§230)*, který postihuje samotné vniknutí do cizího digitálního prostoru nebo *opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§231)*, jenž umožňuje postihovat již samotnou přípravnou fázi útoku nebo *poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§232)*.[2,3] V kontextu phishingu je zcela zásadní také *§209 podvod*, neboť útočníci dosahují svého cíle tím, že oběť aktivně uvádějí v omyl skrze klamnou identitu a manipulativní obsah zprávy. Tímto jednáním je naplněna základní skutková podstata tohoto trestného činu[4] – *„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…“*.[5] Celkově je ale klíčem k trestní kvalifikaci důležité správné posouzení a zjištění motivu v souvislosti s jeho společenskou škodlivostí.[6]

S kybernetickou kriminalitou také přímo souvisí kyberprostor, neboli *„Digitální prostředí umožňující vznik, zpracování a výměnu digitálních dat a informací, tvořené informačními systémy a službami informační společnosti.“*[7] Hlavní jeho vlastností je decentralizovanost, není tedy řízen žádnou nadřazenou autoritou. Fungování do značné míry vychází z principu samoregulace, která je založena na dohodě mezi uživateli a správci systémů. Jedná se také o prostředí s velmi širokým využitím – jako komunikační

[1] GŘIVNA, Tomáš; SCHEINOST, M. a ZOUBKOVÁ, I., *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. str. 24. ISBN 978-80-7598-554-5.
[2] POLICIE ČR. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník*. Online. Dostupné z: https://policie.gov.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx. [cit. 2026-01-03].
[3] NĚMEC, Miroslav. *Teorie a metodologie kriminalistiky pro magisterské studium*. *II. díl, Aktuální problémy kriminalistické praxe*. Praha: Abook, 2019. str. 306-307. ISBN 978-80-906974-2-3.
[4] ŽILKOVÁ, Markéta. *Trestní a kriminologické aspekty phishingu*. Diplomová práce. Praha: Právnická fakulta UK. 2023. str. 42. Vedoucí práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.
[5] ČESKO. Zákon č. 40/2009 Sb. trestní zákoník ze dne 8. ledna 2009. In *Sbírka zákonů České republiky*. 2009. §209. Hlava pátá.
[6] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. vydání. Plzeň: Aleš Čeněk, 2019. str. 965. ISBN 978-80-7380-741-2.
[7] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. str. 149. ISBN 978-80-88168-31-7.

platforma, zdroj informací, ale může také poskytovat prostředí pro osoby páchající trestnou činnost.[8] Právě v tomto smyslu se kybernetický prostor stává nositelem transformačních procesů, které civilizaci směřují k neznámé budoucnosti s nevídanými příležitostmi, ale také s dosud nejasnými riziky.[9]

Samotná kyberkriminalita je vnímána jako trestná činnost, kterou pachatel páchá v prostředí informačních a komunikačních technologií (ICT), jež mohou představovat buď samotný cíl útoku, nebo sloužit jako prostředek k realizaci různorodých forem kriminálních aktivit.[10] Česká technická norma uvádí, že „*počítačový zločin je zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený*".[11] Nicméně rozsah kybernetické kriminality se neustále proměňuje v závislosti na rostoucí dostupnosti a sofistikovanosti ICT prostředků. Právě tato technologická variabilita je hlavním důvodem, proč v odborné literatuře doposud absentuje jednotná definice, která by dokázala vyčerpávajícím způsobem postihnout všechny aspekty a formy trestné činnosti páchané v kyberprostoru.[12] Pachatelé kybernetické kriminality prokazují při volbě svých metod značnou invenci. Některé postupy, využívané již desítky let, prošly kontinuálním vývojem a staly se pevnou součástí jejich kriminálního know-how. V mnoha případech dosahují tyto metody takové míry sofistikovanosti, že jsou pro orgány činné v trestním řízení těžce objasnitelné.[13]

V roce 2023 se konala konvence Rady Evropy v Budapešti ohledně kyberkriminality, která umožňuje odborníkům z daných zemí sdílet své zkušenosti, spolupracovat v rámci zlepšení ochrany před tímto druhem kriminality a uznává potřebu chránit legitimní zájmy při využívání a rozvoji informačních technologií. Česká republika byla součástí konvekce a spolu s dalšími 95 státy světa.[14] V souladu s Budapešťskou úmluvou z roku 2001 lze kyberkriminalitu rozdělit do čtyř skupin. První tvoří delikty proti důvěrnosti, integritě a dostupnosti počítačových systémů (např. phishing či

[8] ŽILKOVÁ, Markéta. *Trestní a kriminologické aspekty phishingu*. Diplomová práce. Praha: Právnická fakulta UK. 2023. str. 2. Vedoucí práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.
[9] SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. Praha: Petrklíč, 2018. str. 12. ISBN 978-80-7229-652-1
[10] POLICIE ČR. *Kyberkriminalita*. Online. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx. [cit. 2026-01-03].
[11] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. str. 33. ISBN 978-80-7380-849-5.
[12] KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. str. 33. ISBN 978-80-88168-18-8.
[13] KLIMEK, L., ZÁHORA, J., a HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer. 2016. str. 29. ISBN 978-80-8168-538-5.
[14] COUNCIL OF EUROPE. *Convention on Cybercrime (ETS No.185)*. Budapest. 2023

hacking), zatímco druhá se zaměřuje na činy s počítači přímo související, jako jsou podvody a falšování. Třetí kategorie postihuje závadný obsah, zejména pornografické materiály, a čtvrtá skupina je vyhrazena porušování autorských práv v digitálním prostředí. Součástí je také dodatkový protokol ohledně rasismu a xenofobního obsahu. Existuje i jiné členění, které kybernetickou kriminalitu rozlišuje na trestní činnost závislou, anebo pouze usnadněnou využitím informačních a komunikačních technologií. Závislou činnost lze realizovat výhradně prostřednictvím výpočetní techniky a síťové infrastruktury. Kriminalitu usnadněnou zahrnují delikty, které existují i v offline prostředí, avšak při využití informačních a komunikačních technologií nabývají zcela nového rozměru. Pokud jsou tyto činy páchány v kyberprostoru, šíří se velmi rychle a mezi velký počet osob.[15]

2.1 Phishing

Mechanismus phishingu je založen na zneužití důvěry uživatele skrze vizuální imitaci legitimních subjektů. Proces útoku začíná vytvořením sofistikované zprávy, která maskuje skutečnou identitu odesílatele a vyžaduje po uživateli poskytnutí autorizačních údajů. Následným zneužitím těchto dat dochází k neoprávněné manipulaci s bankovními konty či k narušení integrity soukromých dat.[16] Velmi důležitou součástí tohoto podvodu je psychologická manipulace s názvem sociální inženýrství. V odborné literatuře je definováno jako akt manipulace s jedinci za účelem přimět je k vykonání určité činnosti nebo k vyzrazení důvěrných informací. V kontextu kybernetické bezpečnosti se tento termín specificky vztahuje k využití lsti a klamu za účelem sběru dat, spáchání podvodu nebo získání neoprávněného přístupu k informačním systémům. Charakteristickým rysem moderního sociálního inženýrství je pak skutečnost, že ve většině případů nedochází k přímému osobnímu kontaktu mezi útočníkem a obětí.[17] Důležité je také zmínit, že nejúčinnější obranou proti kybernetickým hrozbám zůstává racionální přístup

[15] VLACH, J.; KUDRLOVÁ, K. a PALOUŠOVÁ, V., *Kyberkriminalita v kriminologické perspektivě*. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2020. str. 13-14. ISBN 978-80-7338-189-9.

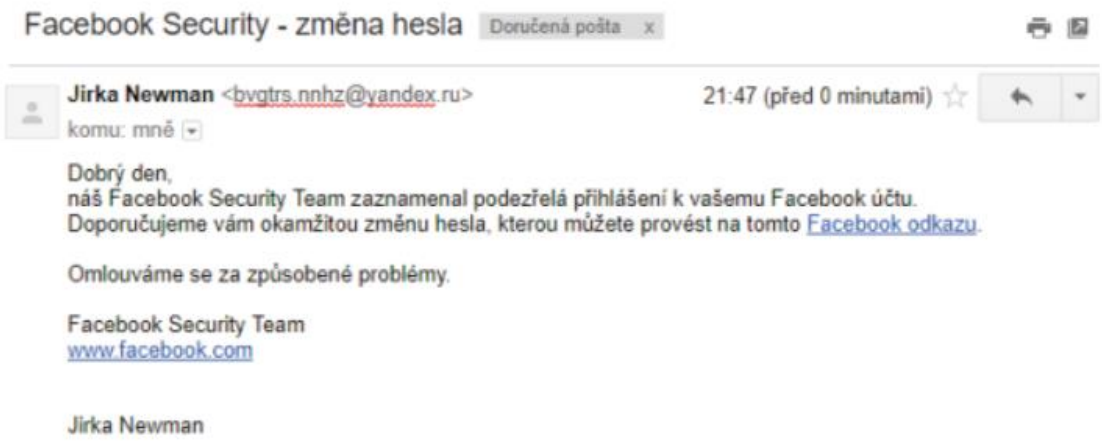
[16] JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Přeložil K. VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. str. 122. ISBN 978-80-908388-4-0.

[17] HADNAGY, Christopher. *Social engineering: the art of human hacking*. Indianapolis: Wiley Publishing, 2011. str. 32. ISBN 978-0-470-63953-5.

uživatele k elektronické komunikaci a jeho průběžné vzdělávání v aktuálních trendech kyberkriminality.[18]

U phishingu se v obecné rovině jedná o druh spamu, což lze vysvětlit jako nevyžádanou poštu, anebo SMS zprávu obsahující určitá masově zasílaná reklamní sdělení, skrz které jsou hromadně rozesílány škodlivé kódy a podvodné web stránky za účelem přimět osobu k určitému jednání, které má mít za následek zjištění citlivých údajů, bankovní identity a vylákání peněžních prostředků.[19,20] Úspěšnost phishingu je přímo úměrná míře nepozornosti uživatele. Jak už bylo popsáno výše, podvodníci se často snaží imitovat legitimní organizaci, a proto je důležité věnovat pozornost typografickým nesrovnalostem například v názvu e-mailové adresy a kriticky posuzovat validitu takové zprávy zejména při další interakci v podobě otevírání příloh a odkazů.[21]

Obr. 1: Ukázka phishingu – Facebook[22]



Z hlediska klasifikace se phishing pohybuje na pomezí přímé internetové kriminality a její nepřímé formy, která má své jasné paralely v nevirtuálním prostředí. Právě tento dvojí charakter phishingu představuje výzvu pro orgány činné v trestním řízení při stanovení správné skutkové podstaty. Potíže při právním hodnocení jsou často

[18] KOHOUT, R. a KLOZOVÁ, M., *Internetem bezpečně (nejen) pro seniory*. Vydání: první. Karlovy Vary: You connected, 2020. str. 21-22. ISBN 978-80-907852-0-5.

[19] taktéž str. 22-23.

[20] HOLT, Thomas J.; BOSSLER, Adam M. a SEIGFRIED-SPELLAR, Kathryn C. *Cybercrime and digital forensics: an introduction*. Third edition. London: Routledge, Taylor & Francis Group, 2022. str. 221. ISBN 9780367360061.

[21] MUNI. *PHISHING: Jak se nenechat ošálit v kyberprostoru?* Online. Dostupné z: https://security.muni.cz/kurzy/kyberkompas/phishing. [cit. 2026-01-14].

[22] taktéž

způsobeny komplexností tohoto deliktu a variabilitou způsobů jeho páchání, což vyžaduje důsledné pochopení technologických i psychologických aspektů útoku.[23]

Pojem phishing vznikl jazykovou modifikací anglického slova fishing neboli rybaření. Tato analogie vychází z povahy útoku, kdy útočník využívá klamavý obsah jako návnadu k oklamání oběti. Úspěšnost této metody je tedy podmíněna interakcí uživatele s podvodným prvkem, čímž dochází k pomyslnému chycení oběti a následné kompromitaci jejích dat. [24]

2.1.1 Historie a vývoj phishingu

Rozvoj phishingu je přímo navázaný na rozvoj internetu, který nastal ve druhé polovině devadesátých let minulého století. Předchůdci phishingu s ním sice nesdílí elektronický svět, ale spojuje je už dříve zmiňované sociální inženýrství. Jedním z prvních bylo podvodné jednání s názvem Španělský vězeň, které sahá až do druhé poloviny devatenáctého století. V tomto případě se jednalo o přesvědčení oběti, že velmi bohatý vězeň je ochoten se o bohatství podělit, pokud mu oběť přes prostředníka půjčí určitý obnos peněz na podplacení stráží. Avšak po zaplacení první částky se objeví komplikace a podvodník chce po oběti další a další peníze.[25]

V dnešní době je už toto jednoduché podvodné jednání pravděpodobně přežitkem, nicméně pouze lehkým pozměněním se dostáváme k dalšímu podobnému, ale značně rafinovanějšímu jednání známému jako Nigerijské listy, neboli 419 scam. Jak už název napovídá, tento druh phishingového podvodu má v prvopočátku souvislost s Nigérií, kdy i číslo 419 právě odkazuje na ustanovení trestního zákoníku v Nigérii odkazující na podvodné jednání. Později jsou k podvodu využívány i ostatní západoafrické země. Útočníci cíleně zneužívají nedostatečnou informovanost společnosti o konkrétních zemích a tamních politických či právních poměrech. Nestabilita těchto regionů pak slouží jako ideální prostředí. Tento typ kriminálního jednání staví na legendě o ohroženém majetku v politicky nestabilních oblastech. Pachatelé vystupují v roli majetných osob, které pod záminkou ochrany svých aktiv vyžadují součinnost oběti při jejich vyvedení ze země. Podstatou podvodu je vylákání finančních prostředků určených na administrativní náklady spojené s transakcí. Příslib vysoké odměny z celkového objemu fiktivního jmění

[23] KRUPIČKA, J. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012. str. 57. ISSN 0323-0619
[24] taktéž str. 57.
[25] taktéž str. 58-59.

slouží jako klíčový motiv k neuváženému jednání poškozeného. Podvodníci si jsou vědomi psychologického nátlaku na osoby, kdy po zaplacení první platby nechtějí ze své investice ustoupit a neustále platí dál.[26]

Na podobném principu, avšak s apelem na jiné lidské emoce, se posléze phishing vyvinul také v seznamkové podvody, kdy podstata útoku spočívá ve vytváření propracovaných fiktivních identit na online seznamkách. Útočníci cíleně vyhledávají osoby vykazující známky osamělosti či citové zranitelnosti. Za účelem zvýšení své kredibility si přisvojují identitu osob s vysokým společenským statusem či důvěryhodným povoláním, jako jsou lékaři v mezinárodních organizacích, armádní důstojníci na misích nebo pracovníci v humanitárním sektoru. Klíčovým mechanismem je intenzivní komunikace trvající i několik měsíců pro navázání silné citové závislosti. Následně útočník začne požadovat dárky, finance či údaje k platebním kartám.[27]

Současná podoba phishingu existuje přibližně třicet let. Poprvé se začal využívat v roce 1995 v USA, podvodníci se vydávali za administrátory společnosti America Online a po obětech chtěli jejich přihlašovací údaje k účtům z důvodu problémů s vyúčtováním, avšak s ohledem na dobu se tento podvod netýkal velkého počtu osob. První masový phishing útok proti finančním institucím byl oznámen v roce 2003. Mířil na čtyři americké společnosti – E-gold, E-loan, Wells Fargo a Citibank. Významný vývoj nastal v samotném objektu útoku. Navzdory rozsáhlým investicím do technické infrastruktury kybernetické bezpečnosti se zapomnělo na selhání lidského faktoru, které tvořilo kritické místo většiny zaznamenaných incidentů.[28] V České republice zasáhly první incidenty v roce 2006 finanční sektor, konkrétně českou pobočku Citibank a Českou spořitelnu.[29]

Phishingové útoky se i dnes stále vyvíjí. Dříve byla naprostá většina z nich rozpoznatelná díky gramatickým chybám a překlepům, když původní cizojazyčná zpráva byla nekvalitně automaticky překládána. V současnosti se překlady díky strojovému

[26] KRUPIČKA, J. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi.* In: Acta Universitatis Carolinae Iuridica, 2012. str. 59. ISSN 0323-0619
[27] KOHOUT, R. a KLOZOVÁ, M., *Internetem bezpečně (nejen) pro seniory*. Vydání: první. Karlovy Vary: You connected, 2020. str. 26-27. ISBN 978-80-907852-0-5.
[28] JAMES, Lance. *Phishing Exposed*. Syngress, 2005. str. 11. ISBN 978-0-080-48953-7.
[29] ŽILKOVÁ, Markéta. *Trestní a kriminologické aspekty phishingu*. Diplomová práce. Praha: Právnická fakulta UK. 2023. str. 12-13. Vedoucí práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.

učení a umělé inteligenci (AI*[30]) zlepšují a působí více autenticky a věrohodně.[31] Případů tak stále přibývá, v roce 2018 se společnost Proofpoint dotazovala 15 000 odborníků v oblasti bezpečnosti a více než 60 % uvedlo, že se s určitou formou phishingu v tomto roce setkali. V dnešní době stojí lidské chyby v této oblasti firmy miliony. Závažnost phishingových útoků a jejich ekonomické dopady lze ilustrovat na několika významných incidentech z poslední dekády. V roce 2017 čelila dánská logistická společnost Maersk rozsáhlému kybernetickému útoku, jehož celkové náklady byly vyčísleny na 300 milionů USD. Podobný scénář se opakoval v roce 2019 v Baltimoru, kde útok na městskou infrastrukturu způsobil škody ve výši 18 milionů USD. V českém prostředí byl v roce 2018 zaznamenán masový výskyt tzv. sextortion e-mailů, v nichž útočníci pod pohrůžkou zveřejnění kompromitujících materiálů získaných prostřednictvím webkamery vymáhali výkupné. Ve stejném období se terčem cíleného phishingu stalo také několik českých univerzit. Cílem těchto útoků bylo získání citlivých výzkumných dat, know-how a nepublikovaných výsledků, a to především v oborech lékařství a technických a humanitních věd. Se značným rozvojem sociálních sítí přešel trend phishingu ve větší míře taky sem. V období let 2017 až 2018 byl zaznamenán signifikantní nárůst kybernetických útoků tohoto typu, a to o více než 400 %. Trend zneužívání aktuálního společenského dění se potvrdil i během pandemie onemocnění COVID-19. Útočníci v rámci phishingových kampaní imitovali identitu významných institucí, jako je Světová zdravotnická organizace (WHO) či Americké centrum pro kontrolu a prevenci nemocí (CDC), s cílem využít zvýšené informační potřeby a obav veřejnosti.[32]

2.1.2 Typy phishingu

Vzhledem k neustálému zdokonalování technologických bezpečnostních mechanismů a zvyšování digitální gramotnosti uživatelů jsou útočníci nuceni kontinuálně transformovat své strategie a vyvíjet sofistikovanější metody sociálního inženýrství a

[30] POLČÁK, Radim. *Právo informačních technologií*. Právní monografie. Praha: Wolters Kluwer, 2018. str. 769-770. ISBN 978-80-7598-045-8.

[31] GOV.CZ. *Návod, jak poznat phishingové útoky*. Online. Dostupné z: https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky. [cit. 2026-01-04].

*"*Systémem AI se rozumí strojový systém navržený tak, aby fungoval s různými úrovněmi autonomie, který může po zavedení vykazovat adaptabilitu a který z obdržených vstupů odvozuje pro explicitní nebo implicitní cíle to, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzické nebo virtuální prostředí.*"

[32] NÚKIB. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit*. Online PDF. 2020. str. 2. [cit. 2026-01-14].

samotných podvodů. Phishing se tedy projevuje v celé řadě forem, jež lze rozdělit do následujících několika skupin.

2.1.2.1 Malware phishing

V současné době se jedná o jeden z nejrozšířenějších a nejvíce fatálních způsobů phishingu. Primárním cílem útočníka je v tomto případě přesvědčit uživatele k interakci s kompromitovaným obsahem, typicky prostřednictvím kliknutí na podvodný odkaz nebo stažení přiložené přílohy. Jakmile uživatel tuto akci provede, dochází k bezprostřední instalaci škodlivého kódu do operačního systému. Samotný malware lze přitom definovat jako programový kód vytvořený s jasně nekalým úmyslem, přičemž mezi jeho nejčastější formy patří počítačové viry, červi či trojské koně. Tyto entity jsou navrženy k destrukci systémových prostředků, neautorizované krádeži dat nebo skrytému monitorování aktivity uživatele.

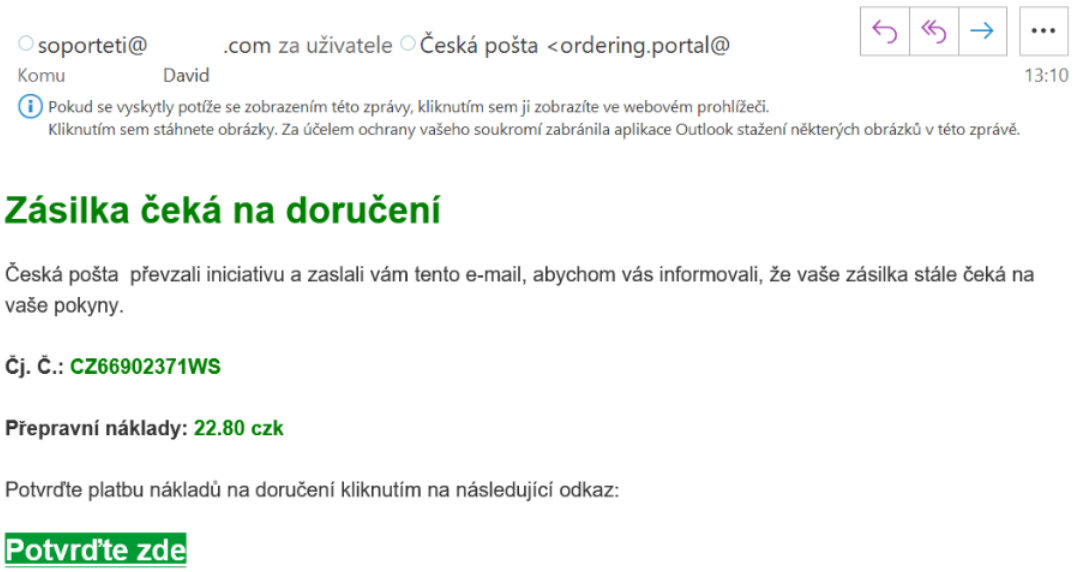
Charakteristickým rysem těchto podvodných kampaní je využití sofistikovaných metod sociálního inženýrství, které maskují skutečnou povahu přiloženého souboru. Často se jedná o dokumenty, které se při otevření jeví jako prázdné nebo nečitelné. Útočník následně uživatele vyzývá k povolení automatických a opakujících se úkolů pod záminkou správného zobrazení obsahu. V praxi se tyto útoky často opírají o scénáře vyvolávající urgentní potřebu řešení, jako je například oznámení o nedoručené poštovní zásilce, což výrazně snižuje pravděpodobnost, že uživatel pod tlakem okolností bezpečnostní varování ignoruje.

Účinnost této metody spočívá v její schopnosti kombinovat lidskou zvědavost s technickou zranitelností systému. Zatímco technické bariéry, jako jsou antivirové programy, se snaží tyto hrozby eliminovat, útočníci neustále vyvíjejí nové varianty malwaru, které jsou pro tradiční detekční nástroje v první fázi útoku neviditelné. Právě zneužití legitimních funkcí kancelářských aplikací představuje kritický bod, kdy se technologické zabezpečení stává neefektivním za předpokladu, že uživatel vědomě potvrdí spuštění škodlivého kódu.[33,34]

[33] JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Přeložil K. VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. str. 187. ISBN 978-80-908388-4-0.

[34] OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. str. 4. [cit. 2026-01-14].

Obr. 2: Malware phishing – Česká pošta[35]


soporteti@ .com za uživatele Česká pošta <ordering.portal@
Komu David 13:10
Pokud se vyskytly potíže se zobrazením této zprávy, kliknutím sem ji zobrazíte ve webovém prohlížeči.
Kliknutím sem stáhnete obrázky. Za účelem ochrany vašeho soukromí zabránila aplikace Outlook stažení některých obrázků v této zprávě.

Zásilka čeká na doručení

Česká pošta převzali iniciativu a zaslali vám tento e-mail, abychom vás informovali, že vaše zásilka stále čeká na vaše pokyny.

Čj. Č.: CZ66902371WS

Přepravní náklady: 22.80 czk

Potvrďte platbu nákladů na doručení kliknutím na následující odkaz:

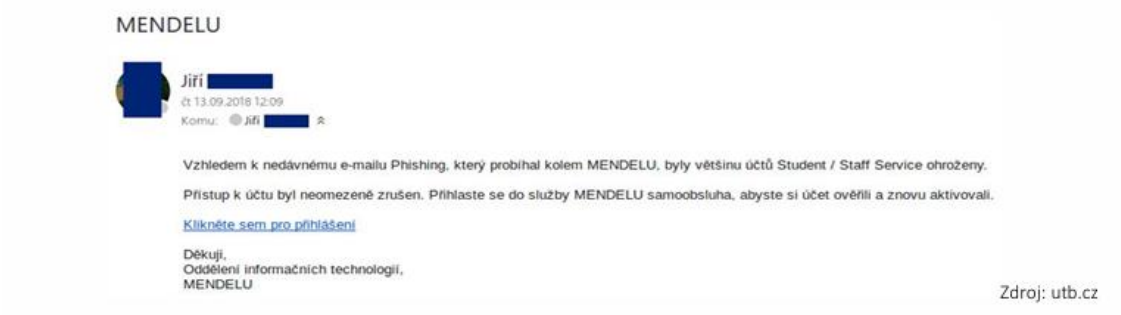
Potvrďte zde

2.1.2.2 Spear phishing

Tento druh představuje vysoce personalizovanou formu útoku, která je na rozdíl od plošných kampaní zaměřena na specifickou organizaci či konkrétního jednotlivce. Úspěšná realizace této techniky vyžaduje důkladnou přípravnou fázi, během níž útočník shromažďuje detailní informace o cíli, zejména o operační a organizační struktuře firmy. Společným rysem obětí bývá jejich profesní zařazení, například příslušnost k určitému firemnímu oddělení, což útočníkovi umožňuje vytvořit kontextuálně uvěřitelný a relevantní obsah zprávy.[36] Pokud je cíl významný v dané organizaci, označuje se tento druh někdy jako „whaling“, neboli lov velryb. V tomto případě se útočníci zaměřují například na generální ředitele společností, kdy je často značná část soukromých informací veřejně dohledatelná, což přispívá k věrohodnosti podvodu.[37]

[35] GOV.CZ. *Návod, jak poznat phishingové útoky*. Online. Dostupné z: https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky. [cit. 2026-01-14].
[36] MUNTODE R. A a PARWE S. S. *An Overview on Phishing – its types and Countermeasures*. International Journal of Engineering Research and Technology. ESRSA Publications Pvt. str. 546. ISSN 2278-0181.
[37] OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. str. 5. [cit. 2026-01-14].

Obr. 3: Spear phishing – MENDELU[38]



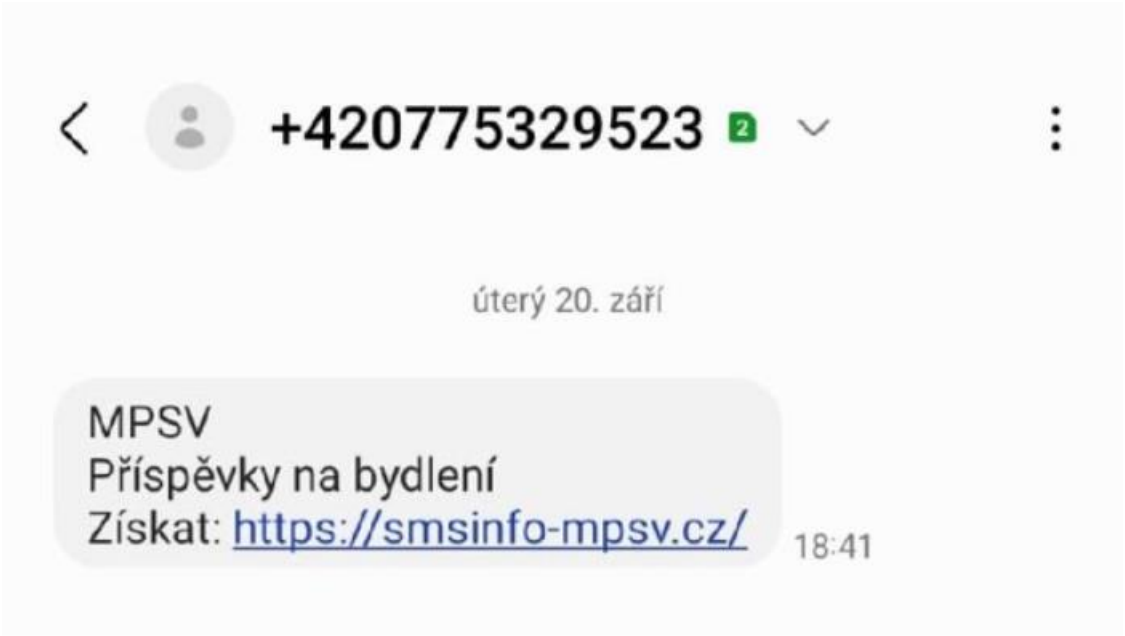
2.1.2.3 Smishing, vishing a spoofing

Kromě e-mailové komunikace využívají útočníci také mobilní sítě. Termín smishing vznikl spojením slov SMS a phishing, což označuje útoky, u nichž je využíváno textových zpráv. Na rozdíl od e-mailové komunikace umožňuje tento způsob útoku efektivně obcházet antispamové filtry e-mailových klientů. V důsledku toho dochází k doručení podvodného sdělení k širšímu spektru potenciálních obětí, aniž by byla zpráva automaticky detekována jako závadná. Podobný princip uplatňuje vishing, jenž využívá přímého hlasového kontaktu. Identifikace vishingu se stává s rostoucí sofistikovaností technologií čím dál náročnější. Původní schémata, využívající primitivní hlasové automaty, jsou nahrazována pokročilými systémy, které věrně simulují lidskou řeč. Toto postupné zdokonalování činí z vishingu mnohem hůře detekovatelný útok pro cílové subjekty, neboť klesá výskyt dříve typických indicií, jako byla nepřirozená intonace či strojový projev.[39] Obě techniky využívají specifického charakteru mobilní komunikace k navození pocitu bezprostřednosti a legitimity.[40] Při srovnání efektivity různých vektorů vykazuje smishing nadstandardní výsledky v oblasti uživatelské odezvy. Statistické údaje naznačují, že zatímco e-mailové kampaně dosahují přibližně 20 % míry otevření, u SMS zpráv je tato hodnota asi 98 %. Právě vysoká pravděpodobnost interakce oběti s doručenou zprávou činí ze smishingu jeden z nejvíce preferovaných nástrojů současné kyberkriminality.[41]

[38] NÚKIB. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit*. Online PDF. 2020. str. 4. [cit. 2026-01-14].
[39] OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. str. 8. [cit. 2026-01-14].
[40] GHAZI-TEHRANI, A. K. a PONTELL, H. N. *Phishing Evolves: Analyzing the Enduring Cybercrime.* Victims & Offenders. 2021, vol. 16, no. 3, str. 319. ISSN 1556-4886.
[41] OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. str. 6. [cit. 2026-01-14].

V rámci vishingu a smishingu se často paralelně využívá také spoofing, což představuje technickou metodu falšování identity. Podstata této techniky spočívá v manipulaci s identifikačními údaji tak, aby se útočník navenek jevil jako důvěryhodná organizace. V praxi může spoofing zahrnovat širokou škálu falšování, od e-mailových a IP adres přes telefonní čísla až po kompletní vizuální identitu webových stránek. Typickým příkladem je e-mailový spoofing, při kterém útočník modifikuje data odchozí zprávy. Cílem je, aby se příjemci zobrazil odesílatel pocházející z legitimního a prověřeného zdroje. Paralelně s tím se v prostředí mobilních sítí rozvíjí spoofing telefonního čísla, který je kritickým prvkem podvodných hovorů.[42]

Obr. 4: SMS phishing (smishing) - MPSV[43]



2.1.2.4 Pharming

Na rozdíl od standardních forem phishingu, pharming manipuluje se samotnou infrastrukturou internetu. Tato technika modifikuje proces překladu doménových jmen (DNS) na IP adresy. Funkci DNS lze přirovnat k telefonnímu seznamu. Hlavním jeho úkolem je transformovat řetězce čísel do jednodušších URL odkazů (například www.seznam.cz). Pokud útočník dokáže tento proces napadnout, může následně oběť nasměrovat na libovolné webové stránky bez jejího vědomí. [44] Podvržené stránky jsou navrženy tak, aby vizuálně přesně kopírovali stránky oficiální, což výrazně omezuje

[42] ESET. *Spoofing*. Online. Dostupné z: https://www.eset.com/cz/slovnik/spoofing/. [cit. 2026-03-18].
[43] GOV.CZ. *Návod, jak poznat phishingové útoky*. Online. Dostupné z: https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky. [cit. 2026-01-14].
[44] OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. str. 9. [cit. 2026-01-14].

pravděpodobnost odhalení běžným uživatelem, který následně do klamavého formuláře zadá své přihlašovací údaje. Tyto údaje jsou poté odeslány k útočníkovi za účelem infiltrace nebo instalace škodlivého softwaru.[45]

S pharmingem také souvisejí další specifické útoky, které také nemíří přímo na uživatele, ale na samotný proces:

- Watering hole phishing – Strategie zacílená na populární webové portály navštěvované specifickými skupinami uživatelů. Útočník zneužije zranitelnost legitimního webu k distribuci malwaru nebo k následnému přesměrování návštěvníků.

- Typosquatting – Metoda využívající nepozornosti uživatelů při manuálním zadávání adres do prohlížeče. Útočníci registrují domény s drobnými překlepy oproti originálu, čímž zachytávají provoz směřující k legitimním subjektům.

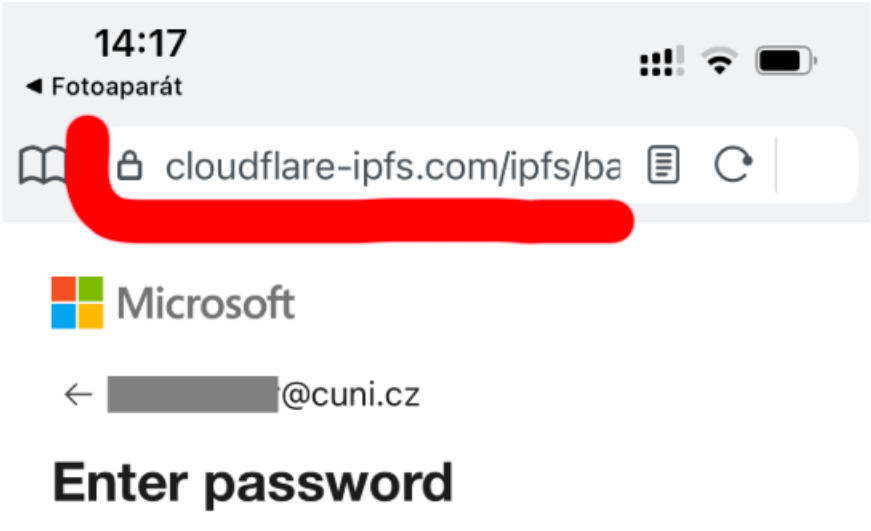
- Clickjacking – Technika zneužívající zranitelnosti uživatelského rozhraní webových stránek. Útočník do legitimního webu vloží neviditelné prvky, které zachytávají kliknutí nebo vstupy uživatele.

- Tabnabbing – Specifická forma útoku, při níž nečinná karta v prohlížeči automaticky změní svůj obsah na imitaci přihlašovací stránky známé služby. Uživatel se po návratu znovu přihlásí a předá tak své údaje útočníkovi.

- HTTPS phishing – Zneužití webového protokolu (HTTPS*[46]) k vytvoření klamného pocitu bezpečí. Přítomnost bezpečnostního certifikátu dnes již negarantuje legitimitu obsahu, ale pouze šifrování přenosu. Útočník tak sice šifruje spojení, aby zabránil odposlechu třetí stranou, ale data jsou zasílána přímo do jeho infrastruktury.[47]

[45] DVOŘÁK, Marek. *Phishing, pharming a jejich trestní postih*. Trestněprávní revue. 2018. roč. 17, č. 4. str. 86. ISSN 1213-5313.
[46] KOĎOUSKOVÁ, Barbora. *HTTPS v kostce: co to je, jak funguje a jak na něj přejít*. Online. Dostupné z: https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls#co-je-https. [cit. 2026-03-09].
[47] KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-03-09].

Obr. 5: Pharming – Microsoft[48]



2.1.2.5 Cryptocurrency phishing

Phishing se nevyhl ani této poměrně nové a moderní oblasti. Nejrizikovější kategorií jsou útoky zacílené přímo na držitele kryptoměnových peněženek. Namísto dlouhodobé a technicky náročné těžby volí tito útočníci metodu odcizení digitálních aktiv od legitimních uživatelů. Tato strategie opět využívá sociálního inženýrství k získání privátních klíčů nebo přístupových údajů, čímž dochází k okamžitému převodu finančních prostředků pod kontrolu útočníka.[49]

Také investiční podvody v oblasti kryptoměn jsou úzce spjaty s phishingovými technikami. Jedná se například o kryptoměnové podvody, kdy útočníci skrze dlouhodobou psychologickou manipulaci budují s obětí důvěrný vztah. Cílem této přípravné fáze je přesvědčit oběť k postupnému investování stále vyšších finančních částek do fiktivních investičních platforem, které jsou ve skutečnosti plně pod kontrolou kriminálních skupin. Veškeré vložené prostředky automaticky převádí v reálném čase na anonymní kryptoměnové adresy útočníků. Podvodné systémy jsou navrženy tak, aby

*„*HTTPS (Hypertext Transfer Protocol Secure) je novější verze protokolu zajišťující komunikaci mezi webovým serverem a prohlížečem. Na rozdíl od původního HTTP (Hypertext Transfer Protocol) přenášená data šifruje a snižuje tak riziko zneužití osobních údajů, záměny obsahu či odposlech online komunikace.“

[48] CSIRT-CUNI. *Příklady phishing e-mailů*. Online. Dostupné z: https://security.cuni.cz/cs/examples_phishing/. [cit. 2026-01-16].

[49] KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-03-09].

vizuálně simulovaly růst hodnoty investic, čímž motivují oběť k dalšímu vkládání kapitálu. Výsledkem je často totální ztráta investovaných prostředků.[50]

2.1.2.6 Quishing

Termín quishing představuje specifickou a v poslední době vysoce progresivní metodu phishingového kybernetického útoku, která vznikla spojením slov „QR kód“ a „phishing“. Tato technika zneužívá důvěryhodnosti a masového rozšíření QR kódů k oklamání uživatelů a následné krádeži jejich citlivých dat. Zatímco v běžném životě slouží tyto kódy k rychlému přístupu k webovým informacím, jídelním lístkům či platebním bránám, v rukou útočníka se stávají sofistikovaným nástrojem sociálního inženýrství, který efektivně maskuje škodlivý záměr pod vizuálně neutrální prvek.

Samotný mechanismus útoku spočívá ve vytvoření a následné distribuci modifikovaného QR kódu, který v sobě nese zakódovaný odkaz na podvodnou doménu nebo přímý pokyn ke stažení škodlivého softwaru do mobilního zařízení. Útočníci tyto kódy infiltrují do různých komunikačních kanálů, přičemž využívají jak digitální, tak fyzický prostor. V kyberprostoru se quishing objevuje především v e-mailové komunikaci, kde QR kód slouží k obejití bezpečnostních filtrů, které by jinak klasický textový odkaz identifikovaly jako rizikový. Ve fyzickém světě pak útočníci vylepují podvodné nálepky na veřejně dostupná místa.

Jakmile uživatel kód naskenuje pomocí svého chytrého telefonu, je zpravidla přesměrován na vizuálně věrnou kopii legitimní přihlašovací stránky, například internetového bankovnictví, kurýrní služby nebo e-mailového klienta. Zde je pod záminkou nutné autorizace nebo aktualizace údajů vyzván k zadání osobních informací, přístupových hesel či údajů o platební kartě.[51]

2.1.2.7 Evil Twin

Metoda Evil Twin (neboli “zlé dvojče”) představuje sofistikovanou formu kybernetického útoku. Zatímco klasické phishingové kampaně primárně zneužívají e-mailovou komunikaci, anebo SMS zprávy, k šíření malwaru nebo k neoprávněnému

[50] FBI. *Cryptocurrency Investment Fraud*. Online. Dostupné z: https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud. [cit. 2026-03-09].
[51] E-BEZPEČÍ. *Co je quishing?* Online. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/online-zavislosti/57-rizikove-jevy/4062-co-je-quishing. [cit. 2026-03-18].

přístupu k přihlašovacím údajům, Evil Twin se zaměřuje na prolomení bezpečnosti síťové infrastruktury prostřednictvím vytvoření podvodného přístupového bodu.

Z hlediska nebezpečnosti je tato technika srovnatelná s vysoce personalizovaným cíleným phishingem. Její kritický aspekt spočívá v absolutní transparentnosti pro koncového uživatele, ten se připojuje k bezdrátové síti, která se svými parametry jeví jako legitimní. Identifikace útoku je pro běžného uživatele takřka nemožná, neboť útočník plně kontroluje komunikační kanál a může podvrhnout libovolné autentizační rozhraní či přihlašovací portály, čímž dosahuje vysoké úspěšnosti při krádeži citlivých dat.[52]

Zajištění adekvátní úrovně ochrany uživatelů a podnikových dat před těmito útoky vyžaduje implementaci víceúrovňové bezpečnostní strategie, která kombinuje technická opatření s disciplinovaným přístupem uživatelů. Základním předpokladem je kritická verifikace síťové identity, neboť pouhý název sítě nelze považovat za dostatečný prvek pro ověření její legitimity. V prostředí veřejných Wi-Fi sítí je nezbytné omezit přenos citlivých informací a pro operace vyžadující autentizaci raději využívat mobilní datové připojení, které je mnohonásobně bezpečnější. Klíčovým technologickým pilířem ochrany je pak nasazení virtuální soukromé sítě, která veškerou komunikaci uzavře, čímž efektivně brání neoprávněnému odposlechu a manipulaci s daty i v případě připojení k nebezpečnému přístupovému bodu.[53]

2.1.3 Hlášení incidentů a počet případů

Hlášení kybernetických bezpečnostních incidentů je v České republice legislativně rozděleno mezi dva hlavní koordinační orgány v závislosti na charakteru subjektu. Poskytovatelé digitálních služeb a subjekty zajišťující významné sítě podávají hlášení národnímu bezpečnostnímu týmu CERT (CSIRT.CZ), jehož provozovatelem je sdružení CZ.NIC. Ostatní povinné subjekty definované zákonem o kybernetické bezpečnosti pak incidenty ohlašují vládnímu bezpečnostnímu týmu CERT (GovCERT.CZ), který spadá pod Národní centrum kybernetické bezpečnosti (NCKB) jakožto výkonnou sekci Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Při analýze četnosti kybernetických bezpečnostních incidentů v České republice lze například v období let 2016–2018 sledovat specifické trendy v hlášeních

[52] SPRÁVA SÍTĚ. *Co je Evil Twin*. Online. Dostupné z: https://www.sprava-site.eu/evil-twin/. [cit. 2026-03-09].
[53] FORTRA. *How to Detect and Attack Evil Twin WiFi Access Points*. Online. Dostupné z: https://www.tripwire.com/state-of-security/detect-attack-evil-twin-wifi-access-points. [cit. 2026-03-09].

adresovaných oběma hlavním bezpečnostním týmům. Národnímu týmu CSIRT.CZ, který přijímá hlášení od poskytovatelů digitálních služeb a provozovatelů významných sítí, bylo v roce 2018 oznámeno celkem 1079 incidentů, což představuje mírný pokles oproti 1121 incidentům z roku 2016, avšak nárůst ve srovnání s 1008 incidenty z roku 2017.[54] V dnešní době už je počet incidentů více jak dvojnásobný, kdy za rok 2024 eviduje CSIRT.CZ 2282 případů (1689 phishing) a v roce 2025 počet případů poprvé překonal hranici tří tisíc, konkrétně jich bylo 3005 (z toho 2004 phishing).[55]

Obr. 6: Statistika kyberkriminality a druhy - CSIRT.CZ[56]

	2022	2023	2024	2025	2026	sum
Sensor Network*	8815	8903	9682	6853	357	34610
Phishing	1485	2064	1689	2004	127	7369
Spam	220	352	260	483	26	1341
Malware	228	163	108	178	13	690
Information gathering	71	105	99	126	2	403
Intrusions	39	21	69	125	9	263
Other	24	35	53	84	5	201
DOS		12	4	5		21
sum	2067	2752	2282	3005	182	10288

Je však nezbytné zdůraznit, že hlášení postoupená týmu CSIRT.CZ zpravidla zahrnují komplexní incidenty s rozsáhlými důsledky na informační infrastrukturu ČR, případně problémy, které subjekty nedokázaly vyřešit vlastními prostředky, anebo u nichž je identifikace původce značně obtížná. Vládní bezpečnostní tým GovCERT.CZ zaznamenal v roce 2018 celkem 164 hlášení, což ve srovnání s pouhými 24 incidenty v roce 2017 představuje signifikantní meziroční nárůst. I v tomto případě počet případů narůstá. NÚKIB, v rámci GovCERT.cz, ve zprávě o stavu kybernetické bezpečnosti ČR za rok 2024 uvedl, že mu bylo nahlášeno rekordních 268 incidentů.[57] Tento nepoměr v

[54] KASL, F. *Kybernetický bezpečnostní incident a jeho ohlašování. v rámci zabezpečení osobních údajů v kontextu internetu věcí*. Časopis pro právní vědu a praxi. Masaryk University Press. 2020. roč. 28, č. 3. str. 434-436. ISSN 1210-9126.
[55] CSIRT.CZ. *Statistiky řešených incidentů*. Online. Dostupné z: https://www.cert-cr.cz/cs/o-nas/statistiky/. [cit. 2026-01-24].
[56] CSIRT.CZ. *Statistiky řešených incidentů*. Online. Dostupné z: https://www.cert-cr.cz/cs/o-nas/statistiky/. [cit. 2026-01-25].
[57] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Online PDF. str. 4 [cit. 2026-01-24].

počtu hlášení mezi oběma týmy odráží odlišnou povahu ohlašujících subjektů, kdy u týmu GovCERT.CZ dochází zejména k evidenci kritičtějších hrozeb směřujících proti státní administrativě a prvkům kritické informační infrastruktury. Také v květnu 2018 nabylo účinnosti obecné nařízení, které zavedlo plošnou ohlašovací povinnost pro všechny správce osobních údajů, kteří musí v případě narušení bezpečnosti vše ohlásit dozorovému úřadu.[58]

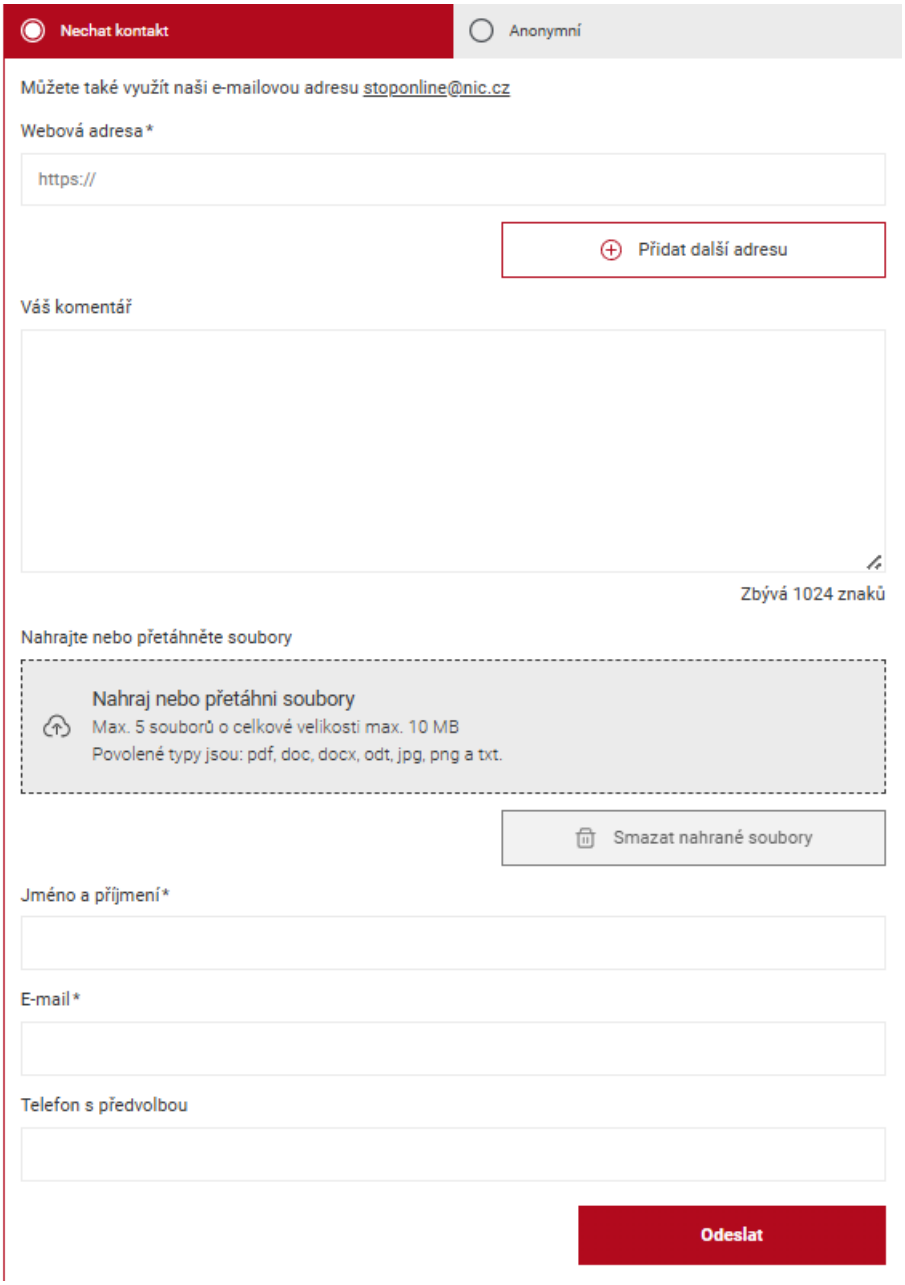
Subjekty, na které se nevztahuje zákonná ohlašovací povinnost, mohou podezření na spáchání kybernetické kriminality oznámit standardními procesními postupy v souladu s trestním řádem. Oznámení o skutečnostech nasvědčujících spáchání trestného činu lze učinit ústně do protokolu, písemně nebo elektronicky (opatřené zaručeným elektronickým podpisem či zaslané prostřednictvím datové schránky). Podání je možné adresovat kterémukoliv útvaru Policie ČR, státnímu zastupitelství, případně jej lze učinit ústně u soudu.[59] Specifický nástroj pro potírání kybernetické kriminality představuje platforma www.stoponline.cz, která slouží k hlášení nezákonného internetového obsahu. Na provozu tohoto portálu se aktivně podílí sdružení CZ.NIC spolu s národním bezpečnostním týmem CSIRT.CZ, přičemž klíčovým aspektem fungování je úzká kooperace s Policií České republiky. Právě díky úzké institucionální spolupráci lze v případech vysoké závažnosti bezodkladně zamezit dalšímu šíření a zobrazování nelegálního obsahu na internetu. Tento kooperační model umožňuje eliminaci závadného obsahu v minimální časové prodlevě od jeho nahlášení.[60]

[58] KASL, F. *Kybernetický bezpečnostní incident a jeho ohlašování. v rámci zabezpečení osobních údajů v kontextu internetu věcí*. Časopis pro právní vědu a praxi. Masaryk University Press. 2020. roč. 28, č. 3. str. 436. ISSN 1210-9126.

[59] POLICIE ČR. *Oznámení trestného činu*. Online. Dostupné z: https://policie.gov.cz/clanek/oznameni-trestnehocinu.aspx?_gl=1*62fnvo*_ga*ODc2MDIxMjQyLjE3NjI3MDIyNDU.*_ga_MGE9DCQJ5M*czE3NjkyNjI3NTkkbzckZzEkdDE3NjkyNjI5MzgkajU1JGwwJGgw. [cit. 2026-01-24].

[60] STOPONLINE. *O STOPonline*. Online. Dostupné z: https://www.stoponline.cz/cs/o-nas/o-stoponline/. [cit. 2026-01-24].

Obr. 7: Formulář STOPonline[61]

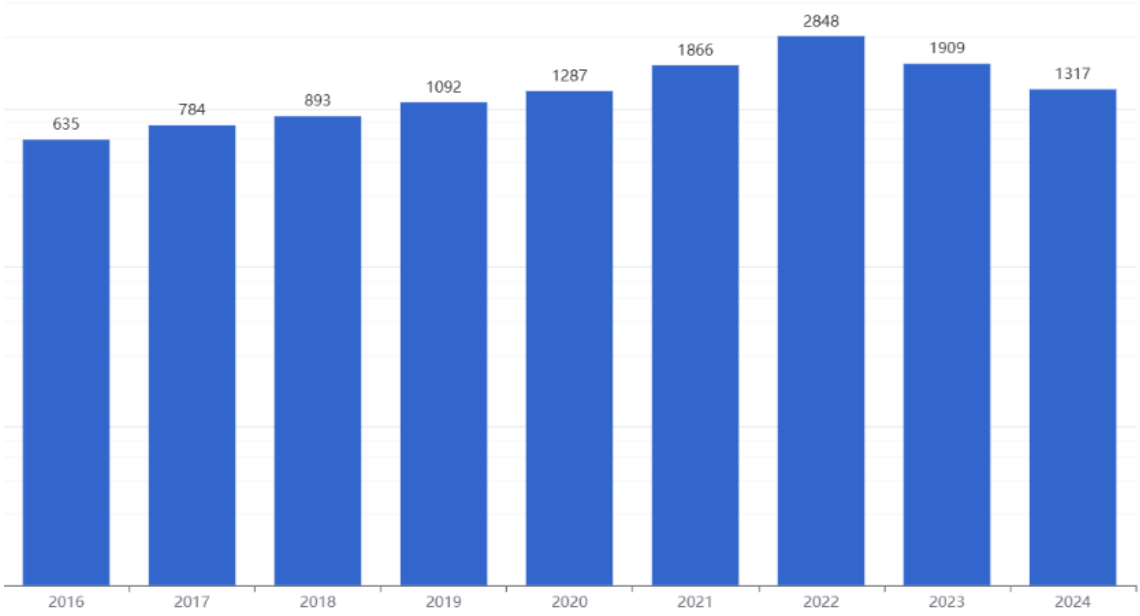


Statistiky Policie ČR v oblasti kybernetické kriminality nereflektují phishing jako samostatnou kategorii, nýbrž jej zahrnují do celkového objemu kybernetické kriminality. Tato oblast začala vykazovat vzestupnou tendenci již v letech 2016–2018. Zatímco v roce 2016 bylo registrováno 635 trestných činů spáchaných v kyberprostoru, v roce 2017 se jednalo o 784 případů a v roce 2018 tento počet vyrostl na 893 incidentů. Výrazný zlom v trendu nastal v roce 2022, kdy došlo k bezprecedentnímu nárůstu této trestné činnosti na celkem 2848 registrovaných případů. Naopak v roce 2024 byl zaznamenán

[61] STOPONLINE. *Kybernetické hrozby a útoky*. Online. Dostupné z: https://www.stoponline.cz/cs/kyberneticke-hrozby-a-utoky/. [cit. 2026-01-24].

signifikantní pokles, kdy počet evidovaných činů klesl na méně než polovinu hodnoty z roku 2022, konkrétně na 1 317 případů.[62]

Obr. 8: Statistika kyberkriminality – Policie ČR[63]



2.1.4 Red flags a prevence

Prevence phishingu se stala kritickou součástí kybernetické bezpečnosti. Ačkoliv se schopnost uživatelů identifikovat nevyžádanou poštu zvyšuje, tak vzhledem k vysoké pravděpodobnosti, že bude uživatel dříve či později vystaven pokusu o takový útok, se stává právě prevence klíčovým faktorem obranyschopnosti a důležitou součástí pro včasnou identifikaci varovných signálů, tzv. red flags.[64]

2.1.4.1 Příklady red flags

Klíčovým aspektem detekce phishingových útoků je schopnost uživatele identifikovat již zmiňované red flags. Jedná se o specifické indikátory a anomálie přítomné přímo v obsahu zprávy, v hlavičce odesílatele nebo v doprovodných datech a přílohách. Tyto varovné signály slouží jako základní diagnostický nástroj, který uživateli umožňuje v reálném čase rozpoznat nesrovnalosti oproti běžnému standardu legitimní

[62] RIS3.GOV.CZ. *G1 Kyberkriminalita – Celkové počty registrovaných trestných činů spáchaných v kyberprostoru.* Online. Dostupné z: https://ris3.gov.cz/monitoring/indikatory/m02c0208-celkove-pocty-registrovanych-trestnych-cinu-spachanych-v-kyberprostoru. [cit. 2026-01-24].
[63] taktéž
[64] KASPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-01-25].

komunikace. V podstatě jde o soubor rozpoznávacích znaků, které tvoří jednoduchou, ale účinnou příručku pro rychlé vyhodnocení kredibility doručené zprávy.

- Neočekávaný odesílatel – Fiktivní potvrzení o nákupu zboží, které uživatel ve skutečnosti nerealizoval, podvodné oznámení o stavu doručení neobjednaných zásilek atd.

- Podezřelá adresa odesílatele – Zejména použití modifikovaných e-mailových adres, které se pouze vizuálně podobají oficiálním doménám.

- Naléhavost a hrozby – Vyvolání časové tísně k vynucení okamžité reakce, stupňování nátlaku prostřednictvím hrozeb, které nejčastěji varují před okamžitým zablokováním uživatelského účtu nebo možným zahájením právních kroků, což má u oběti vyvolat strach a vést k neuváženému jednání.

- Gramatické a stylistické chyby – Výrazné gramatické a stylistické chyby, které svou četností a charakterem překračují rámec běžných překlepů. Takové nedostatky jsou u oficiální komunikace legitimních organizací nepřípustné a často signalizují automatizovaný překlad.

- Podezřelé odkazy a přílohy, přítomnost neobvyklých příloh – Přítomnost nevyžádaných příloh, které uživatel neočekával. Podezření vzbuzují zejména nestandardní typy souborů nebo jejich netypické názvy.

- Žádost o osobní informace – Přímé žádosti o poskytnutí citlivých osobních údajů prostřednictvím e-mailu či SMS, odkazy směřující na podvodné přihlašovací stránky, výzvy k aktualizaci údajů k uživatelskému účtu nebo požadavky na sdělení finančních a platebních informací.

- Nereálně výhodné nabídky – Příslib fiktivních výher z neexistujících soutěží, kterých se uživatel nikdy neúčastnil. Podezření vzbuzuje zejména požadavek na uhrazení poplatku pro získání ceny nebo nečekaná oznámení o dědictví po vzdálených příbuzných.[65]

[65] GOVERNMENT OF CANADA. *The 7 red flags of phishing*. Online. Dostupné z: https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing. [cit. 2026-01-24].

2.1.4.2 Principy prevence

Podoba phishingových útoků se neustále vyvíjí, přičemž kyberzločinci využívají stále sofistikovanější techniky k obcházení bezpečnostních opatření. Phishing zůstává jednou z nejrozšířenějších a nejvíce poškozujících hrozeb, kterým organizace po celém světě čelí, což potvrzují i data z posledního čtvrtletí roku 2024, kdy bylo zaznamenáno téměř milion útoků. Tento znepokojivý vzestupný trend, spolu s průměrnými náklady na únik dat dosahujícími téměř 5 milionů dolarů, podtrhuje naléhavou potřebu zavádění strategií prevence k ochraně digitálních aktiv a organizací.[66]

- Obezřetnost při interakci – Posouzení obsahu před každou interakcí, neotevírat nevyžádané přílohy a neklikat na vložené odkazy, i když zpráva vizuálně imituje legitimní instituci.

- Verifikace legitimity – Při obdržení urgentní žádosti o platbu nebo poskytnutí citlivých údajů je nezbytné provést ověření identity odesílatele prostřednictvím nezávislého komunikačního kanálu.

- Implementace vícefaktorové autentizace – Aktivace vícefaktorového ověření, které představuje důležitou vrstvu ochrany digitální identity. I v případě úspěšného odcizení hesla útočníkem zabraňuje neautorizovanému přístupu k účtu, čímž výrazně snižuje riziko zneužití citlivých dat.

- Pravidelná aktualizace softwaru – Aktualizace je klíčovým prvkem technické prevence, neboť značná část phishingových útoků cíleně zneužívá známé zranitelnosti v zastaralém programovém vybavení.

- Sebevzdělávání – Nezbytnou součástí komplexní strategie kybernetické obrany je neustálé vzdělávání uživatelů. Organizace by měly implementovat pravidelné programy na zvyšování bezpečnostního povědomí, které zaměstnancům umožní včas identifikovat phishing.[67]

- Anti-spam software – Tyto systémy jsou navrženy k aktivní ochraně e-mailových schránek před nevyžádanou poštou a phishingovými útoky.

[66] CYBER SECURITY NEWS. *Phishing Attack Prevention – Best Practices for 2025*. Online. Dostupné z: https://cybersecuritynews.com/phishing-attack-prevention/. [cit. 2026-01-25].
[67] GOVERNMENT OF CANADA. *Don't get hooked: understanding phishing and how to stay safe*. Online. Dostupné z: https://www.getcybersafe.gc.ca/en/blogs/dont-get-hooked-understanding-phishing-stay-safe. [cit. 2026-01-24].

Vedle využívání statických seznamů blokovaných domén, disponují také moderními algoritmy, které se v čase adaptují a učí identifikovat nové typy hrozeb.

- Anti-malware software – Technologie sloužící k eliminaci širokého spektra kybernetických hrozeb, které mohou do systému proniknout skrze phishingové kampaně. Tento software je navržen k detekci i vysoce sofistikovaných a skrytých forem škodlivého kódu. Díky pravidelným aktualizacím ze strany dodavatelů se schopnosti těchto systémů neustále zdokonalují.[68]

- Firewall – Funguje jako brána monitorující a regulující zakázanou aktivitu v rámci privátní sítě. V kontextu síťové bezpečnosti firewally vytvářejí kritické body, jimiž prochází veškerý provoz. Zde dochází k analýze datových paketů na základě předem definovaných parametrů a k následnému rozhodnutí o jejich propuštění či zablokování.[69]

V době rychlého a neustálého rozvoje sociálních sítí je také významným faktorem zvyšující vulnerabilitu uživatele nadměrné zveřejňování osobních údajů. Toto a přijímáním cizích osob do okruhu kontaktů, poskytuje útočníkům cenné a snadno získatelné informace, které lze jednoduše zneužít v jejich prospěch.[70]

2.1.5 Metodika eliminace identifikovaných phishingových hrozeb

V případě, že podvodná komunikace překoná automatizované antispamové filtry a pronikne přímo do doručené pošty, je nezbytné, aby uživatel aplikoval specifické obranné strategie k minimalizaci rizika napadení systému.

- Okamžité odstranění podezřelé komunikace – Základním bezpečnostním opatřením je odstranění e-mailu bez jeho předchozího otevření. Ačkoliv se většina škodlivých kódů aktivuje až interakcí s přílohou nebo odkazem, některé e-mailové klienty umožňují spouštění již při pouhém zobrazení

[68] KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-01-25].
[69] KACPERSKY. *What is a firewall? Definition and explanation*. Online. Dostupné z: https://www.kaspersky.com/resource-center/definitions/firewall. [cit. 2026-01-25].
[70] ŽILKOVÁ, Markéta. *Trestní a kriminologické aspekty phishingu*. Diplomová práce. Praha: Právnická fakulta UK. 2023. str. 34. Vedoucí práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.

zprávy. Úplná absence interakce s podezřelým obsahem je tedy nejspolehlivějším způsobem eliminace rizika.

- Manuální blokování domény odesílatele – Pro zvýšení kolektivní bezpečnosti se doporučuje manuální zařazení domény odesílatele na seznam blokovaných subjektů. Tento krok zabraňuje tomu, aby méně obezřetní uživatelé přišli do styku s legitimně vypadající zprávou. Aktivní správa blokovaných seznamů tak vytváří dodatečnou bariéru proti opakovaným útokům ze stejného zdroje.
- Implementace dalších bezpečnostních prvků – Kromě standardních nástrojů je důležité posílit ochranu i pořízením specializovaného antivirového softwaru, který v reálném čase monitoruje aktivitu v e-mailové schránce. Tyto nástroje slouží jako sekundární kontrolní mechanismus, který identifikuje hrozby i v momentě, kdy lidský faktor selže.[71]

[71] KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-03-09].

3 Konkluze k teoretické části

Teoretická část práce prokázala, že phishing nepředstavuje pouze statickou hrozbu, ale dynamickou a neustále se vyvíjející formu kybernetické kriminality. Jeho nebezpečí spočívá především v efektivní kombinaci pokročilých technických prostředků s propracovanými metodami sociálního inženýrství, které cíleně útočí na psychologii uživatele. Dosavadní analýza právního rámce a bezpečnostních mechanismů sice ukázala, že česká legislativa i technologické bariéry poskytují relativně kvalitní základ pro ochranu, zároveň však potvrdila, že rozhodujícím faktorem úspěšnosti útoku zůstává uživatelské chování a schopnost včasné identifikace varovných signálů v krizové situaci.

Pro pochopení skutečného rozsahu a reálného dopadu této hrozby v prostředí České republiky však nepostačuje pouze studium teoretických modelů a právních norem. Teorie často naráží na limity v podobě adaptability útočníků, kteří dokážou velmi rychle reagovat na nově zaváděná opatření. Je proto nezbytné podrobit analýze reálná data a zkušenosti z přímé vyšetřovací a analytické praxe. Pouze skrze konfrontaci teoretických předpokladů s faktickým stavem kriminality lze identifikovat systémové mezery a slabá místa, která útočníci v současnosti nejčastěji zneužívají. Následující kapitoly se proto zaměřují na ověření těchto teoretických předpokladů skrze přímou konfrontaci s aktuálními daty a poznatky od expertů z praxe.

Praktická část

Praktická část této práce se zaměřuje na hloubkovou analýzu aktuálního stavu phishingu v České republice a na kritické zhodnocení mechanismů, které slouží k jeho potírání. Cílem je propojit teoretická východiska s realitou kybernetického prostoru v tuzemském prostředí, přičemž práce kombinuje analýzu dostupných statistických dat s konkrétními zkušenostmi a názory odborníků z oboru.

4 Interpretace výsledků výzkumného šetření

Základní pilíř praktické části tvoří data poskytnutá klíčovými autoritami v oblasti kybernetické bezpečnosti – Službou kriminální policie a vyšetřování Policie ČR (dále jen „SKPV"), Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě (dále jen „NCTEKK"), Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") a národním CSIRT týmem (dále jen „CSIRT.CZ"), která jsou už také z části popsaná v teoretické části této práce. Empirická část vychází z vlastního šetření realizovaného v březnu 2026. Data byla získána prostřednictvím řízených rozhovorů online nebo telefonicky s experty z řad SKPV, NCTEKK a národního CSIRT týmu, což zajistilo vysokou odbornou úroveň a aktuálnost analyzovaných poznatků. Zástupci NÚKIB se z rozhovoru omluvili z časových a kapacitních důvodů, proto je jejich postoj v práci reflektován pouze skrze analýzu oficiálních výročních zpráv a publikovaných dat, čímž je zajištěna objektivita a zapojení všech státních organizací.

Respondenti z řad SKPV, NCTEKK a CSIRT.CZ zodpověděli otázky v rozsahu svých odborných kompetencí, čímž poskytli cenný vhled do operativní i preventivní praxe. U SKPV a NCTEKK jsou stanoviska spojena do jednotného výstupu. V případě týmu CSIRT.CZ byly otázky vypracovány odbornými analytiky nezávisle na sobě a jsou tak prezentovány odděleně. Na většinu otázek odpověděl primární respondent, zatímco specifické dotazy byly zodpovězeny nebo doplněny druhým specialistou v závislosti na jejich konkrétní odborné kompetenci. U některých dotazů respondenti z CSIRT.CZ vyjádření neposkytli, neboť daná témata nespadají do jejich přímé věcné působnosti.

Využití jednotného souboru 16 otázek pro všechny oslovené instituce umožnilo získat data vhodná k přímému srovnání. Tento metodický postup byl zvolen především proto, aby vedle komparace odborných názorů jasně vyplynulo vymezení kompetencí jednotlivých orgánů, což umožnilo zmapovat přesahy v činnostech těchto institucí a zhodnotit rozsah jejich pravomocí v rámci řešení phishingové hrozby.

Vzhledem k absenci výslovného souhlasu se zveřejněním konkrétních jmen zúčastněných, jsou proto jednotlivé osoby u přesného přepisu rozhovorů v příloze anonymně rozlišeny a byla jim přidělena i identifikační čísla (např. CSIRT1).

4.1 Vyhodnocení rozhovorů a dat

1. Jaký je současný trend v počtu evidovaných kybernetických incidentů v ČR a jak významnou část z nich tvoří právě phishing?

Dotázaní z řad SKPV i NCTEKK hodnotí tuto kriminalitu jako dlouhodobě rostoucí a velmi dynamickou, přičemž i přes mírný meziroční pokles v roce 2024, Policie ČR rok 2025 nebo 2026 v době psaní práce neuvádí, tvoří tyto delikty více než desetinu všech registrovaných trestných činů v zemi. Shoda panuje v tom, že ačkoliv phishing není v oficiálních policejních statistikách sledován jako samostatná kategorie (viz. obrázek 8), na rozdíl od statistik týmu CSIRT.CZ, v praxi představuje dominantní metodu útoků. Potvrzují, že phishing a jeho moderní varianty, jako jsou smishing, vishing či spoofing, tvoří stěžejní část útoků zaměřených na sociální inženýrství, jejichž primárním cílem je neoprávněné získání přístupových údajů, platebních dat s následnou manipulací s finančními prostředky obětí. Analytici národního týmu CSIRT.CZ se odkazují na jejich oficiálně publikované statistiky (viz. obrázek 6) ze kterých je také patrná rostoucí tendence.

Národní úřad pro kybernetickou a informační bezpečnost eviduje celkovou mírně klesající tendenci v oblasti kybernetické kriminality v roce 2025 oproti rekordnímu roku 2024. Zejména první polovina roku 2025 byla charakteristická podprůměrnými hodnotami. Ve druhé polovině roku incidentů přibylo, ale i tak se jedná o nižší čísla než v posledních letech. V celém období převažovaly útoky na dostupnost služeb a provozní výpadky, které byly klasifikovány jako méně významné. NÚKIB se v rámci svých čtvrtletních zpráv zmiňuje o spear-phishing jako o druhu phishingu, který je momentálně útočníky výrazněji využíván, ale přesná čísla jednotlivých druhů incidentů neuvádí.[72]

[72] NÚKIB. *Čtvrtletní přehled hrozeb pohledem NÚKIB Q1,Q2,Q3,Q4 2025*. Online PDF. str. 2 [cit. 2026-03-17].

2. Lze v posledních 2–3 letech pozorovat změnu v profilu pachatelů? Převažují spíše samostatní útočníci, nebo organizované skupiny se zázemím v ČR nebo zahraničí?

V profilech pachatelů kybernetických útoků v posledních dvou až třech letech lze pozorovat výrazný posun od izolovaných jednotlivců k profesionalizovaným a mezinárodně organizovaným skupinám dle respondentů. Podle vyjádření SKPV a NCTEKK dochází k rozmachu přeshraniční spolupráce, kde jsou role rozděleny mezi technické zajištění útoku, přímý kontakt s obětí a následnou legalizaci výnosů z trestné činnosti. Typicky s využíváním zahraničních call center a finančních mul pro převody prostředků, přičemž domácí pachatelé se v tomto řetězci uplatňují zejména v navazujících fázích při výběrech hotovosti či zprostředkování bankovních účtů. Ačkoliv analytický tým CSIRT.CZ nemá zákonnou pravomoc k vyšetřování konkrétních osob, čímž se právě ukazuje rozdíl v kompetencích jednotlivých státních organizaci, na základě sledovaných incidentů se přiklání také k názoru, že za většinou útoků stojí organizované skupiny. Celkovým trendem je dle odpovídajících tedy narůstající sofistikovanost a dělba práce, kdy skupiny fungují jako servisní organizace poskytující technické zázemí pro další pachatele, což zásadně mění charakter i efektivitu moderního phishingu a kybernetické kriminality jako celku.

NÚKIB poukazuje na zvýšení aktivity hacktivistických skupin, které se zaměřují na slabě zabezpečené systémy. Tento trend představuje riziko zejména pro průmysl a kritickou infrastrukturu.[73]

3. V čem spatřujete největší bariéry při vyšetřování a potírání phishingových kampaní?

Podle respondentů je lze rozdělit do tří klíčových rovin, a to legislativní, technickou a mezinárodní. Odborníci z CSIRT.CZ a SKPV poukazují na limity v legislativě a obtížnou prokazatelnost úmyslu, což komplikuje včasné odstraňování podvodných domén či e-shopů, i když vykazují jasné znaky kybernetické kriminality. NCTEKK vnímá jako zásadní překážku vysokou rychlost útoků, kdy mezi rozesláním kampaně a odčerpáním finančních prostředků často uplynou pouze hodiny, což značně stěžuje následné vyšetřování a možnosti represivních složek v zásahu. Dále také mezinárodní přesah, který představuje bariéru v komunikaci se zahraničními registrátory

[73] NÚKIB. *Zpráva o činnosti NÚKIB 2024*. Online PDF. str. 7 [cit. 2026-03-17].

a hostingy, kdy i přes intervenci policie bývá problémem rozdílná jurisdikce. Tento problém prohlubuje roztříštěnost a různou úroveň ochoty ke spolupráci v rámci mezinárodních organizací jako Europol či Interpol. V neposlední řadě vyšetřování ztěžuje vysoká míra anonymity u pachatelů, využívání šifrovaných platforem, kryptoměn a fakt, že oběti často incident nahlásí s velkým časovým prodlením.

4. Jaké formy phishingu vnímáte aktuálně v českém prostředí jako nejnebezpečnější?

Dotázaní kladou důraz na metody, které kombinují technickou sofistikovanost se značným psychologickým nátlakem. Respondenti z SKPV i týmu CSIRT.CZ se shodují, že z hlediska přímých finančních škod a úspěšnosti dominuje vishing, který je pro útočníky sice náročnější na realizaci, ale generuje nejvyšší zisky. NCTEKK doplňuje tento výčet o smishing a podvodné nabídky investic, přičemž upozorňuje na nastupující hrozbu v podobě quishingu. V korporátním a institucionálním sektoru je pak za nejrizikovější považován spear-phishing a útoky typu BEC/CEO podvod (například falešné emaily od vedení společnosti), které cílí na konkrétní osoby s přístupovými právy a hesly k důležitým systémům a účtům. Obecně lze shrnout, že nejvyšší nebezpečí představují útoky směřující k okamžitému převodu finančních prostředků nebo úplnému převzetí identity oběti, u nichž se technické napodobení důvěryhodných zdrojů a institucí pojí s vyvoláním pocitu časové tísně.

5. Pozorujete v praxi nárůst útoků v perfektní češtině nebo lépe cílených kampaní díky AI?

Experti se shodují na postupném zlepšování jazykové úrovně a sofistikovanosti útoků, byť s určitými výhradami k současné situaci. SKPV a NCTEKK potvrzují, že generativní AI slouží jako pomoc, která pachatelům umožňuje odstraňovat dřívější typické varovné znaky, jako byly gramatické chyby či nekvalitní strojové překlady. Podle NCTEKK jsou dnešní útoky stylově lépe přizpůsobeny cílovým skupinám a věrněji napodobují oficiální komunikaci institucí. Analytici týmu CSIRT.cz však upozorňují, že u nejrozšířenějších typů podvodů zatím masivní nasazení AI nepozorují. Zároveň dodávají, že současné generování za pomoci AI má tendenci nadužívat specifické grafické prvky, jako jsou například emotikony, které mohou v oficiálním styku působit neautenticky a pro pozorného uživatele zůstávají rozpoznatelným znakem nesrovnalostí.

Celkovým predikovaným trendem však zůstává nárůst přesvědčivosti kampaní v důsledku eliminace jazykových bariér pro zahraniční útočníky.

6. Které sektory jsou v současnosti nejčastějšími cíli?

Dle odpovědí nelze cíle přesně vymezit, jedná se o široký rozptyl zasahující soukromý i veřejný sektor, přičemž hlavním motivem zůstává finanční zisk a přístup k citlivým datům a informacím. Podle NCTEKK a SKPV jsou primárními terči klienti bankovních institucí, uživatelé online tržišť a zákazníci doručovacích služeb. Významné riziko je však spatřováno také v cílených útocích na zaměstnance soukromých firem a institucí s přístupem k platebním procesům. Ve veřejné sféře jsou pak kritickými cíli organizace státní správy a subjekty kritické infrastruktury, kde phishing neslouží pouze k přímému obohacení, ale často funguje jako počáteční vstupní bod pro hlubší zasažení systémů nebo získání strategických informací. Shoda mezi respondenty panuje v tom, že nejfrekventovanějšími typy incidentů v českém prostředí zůstávají bankovní, investiční a jiné online finanční podvody, které tvoří jádro současné kyberkriminality.

7. Jak hodnotíte úroveň povědomí běžných českých uživatelů o phishingu a jsou osvětové kampaně dostatečné?

Odpovědět na tuto otázku nelze dle respondentů z SKPV a NCTEKK jednoznačně a univerzálně. NCTEKK konstatuje, že ačkoliv se celková informovanost veřejnosti zlepšuje, není rovnoměrná a útočníci na tento vývoj reagují sofistikovanějším využíváním emocí a časového tlaku. Preventivní kampaně, jako je například projekt #nePINdej na kterém spolupracuje i Policie ČR, jsou považovány za smysluplné, avšak pouze za předpokladu, že jsou dlouhodobé a pravidelně obměňované o nové druhy podvodů. Zástupci SKPV doplňují tento pohled o sociologický rozměr, kdy úroveň odolnosti společnosti přímo souvisí s její vyspělostí a ochotou jednotlivců přijímat riziko. Dostatečnost a efektivitu osvěty je tak dle nich obtížné objektivně měřit, neboť technologický pokrok a digitalizace společnosti paradoxně vytvářejí stále nové příležitosti pro pachatele, kteří své metody přizpůsobují právě aktuální úrovni znalostí obětí. Celkově se tedy respondenti shodují, že jednorázová osvěta je neúčinná a klíč k vyšší bezpečnosti spočívá v kontinuálním vysvětlování konkrétních podvodných scénářů a dlouhodobých kampaních.

8. Při analýze úspěšných útoků – co bývá častějším důvodem selhání: technické zabezpečení, nebo lidský faktor?

Mezi respondenty z NCTEKK a SKPV panuje opět shoda, že dominantní příčinou selhání je lidský faktor, které v začátku umožní útočníkům vniknout do sytému. Podle expertů z NCTEKK je nejčastějším spouštěčem aktivní spolupráce oběti, která v důvěře v legitimitu komunikace klikne na podvodný odkaz, vyplní citlivé údaje nebo potvrdí finanční transakci, čímž vlastně obchází existující technické bariéry a zabezpečení daného systému. Zástupci SKPV k tomu dodávají, že lidský faktor hraje klíčovou roli i v širším kontextu, neboť je to právě člověk, kdo rozhoduje o nastavení a samotném využívání technického zabezpečení. Analytici týmu CSIRT.CZ tento pohled dále rozvíjejí a specifikují, že k selhání jednotlivce přispívá především kombinace nepozornosti, neznalosti a psychologické manipulace. Útočníci efektivně využívají vyvolaný strach s vidinou snadného zisku. Zásadním problémem je dle nich také digitální negramotnost, kdy uživatelé nedokážou rozlišit legitimní doménu od podvodné. Z technického hlediska také upozorňují, že útočníci se dnes často nepotřebují složitě prolamovat do cizích systémů, ale raději investují do nákupu vlastních domén, které využívají ke sdílení falešného obsahu. Přestože je lidské pochybení primární příčinou, všichni respondenti zdůrazňují, že dopady útoků jsou citelnější tam, kde chybí vícevrstvá ochrana, jako je kvalitní filtrování obsahu nebo detekce anomálií, která by mohla následky individuálního selhání uživatele minimalizovat, čímž se také podrobněji zabývá otázka číslo 10.

9. Jak efektivní je současná spolupráce mezi státními orgány a soukromým sektorem při včasném varování před phishingem?

Respondenti shodně klasifikují stávající kooperaci mezi orgány veřejné moci a soukromým sektorem jako zcela klíčový element v boji proti kybernetické kriminalitě. Její efektivita má dle SKPV rostoucí tendenci, což je podloženo zejména dobrou úrovní kooperace s bankovním sektorem. NCTEKK v této souvislosti vyzdvihuje formální partnerství Policie ČR s Českou bankovní asociací, které umožňuje operativně a neodkladně reagovat na aktuální vlny kybernetických podvodů v oblasti bankovnictví. Přestože je stávající interakce se správci domén a poskytovateli hostingů vnímána jako funkční, experti z NCTEKK identifikují prostor pro další zlepšení, zejména v oblasti zrychlení a standardizace procesů. Za klíčové pro budoucí posun považují především zefektivnění sdílení indikátorů kompromitace, urychlení blokace škodlivých domén a

nastavení mechanismů pro okamžité pozastavení podezřelých finančních převodů, kde je rychlost reakce rozhodujícím faktorem pro minimalizaci škod.

10. Do jaké míry považujete zavedení povinného vícefaktorového ověřování za účinné?

Interpretace odpovědí potvrzuje, že povinná implementace vícefaktorového ověřování (zkratka MFA, anglicky Multi-Factor Authentication) je experty vnímána jako klíčový nástroj kybernetické bezpečnosti. Ačkoliv MFA signifikantně zvyšuje ochranu citlivých dat, respondenti jednohlasně upozorňují na jeho limity v konfrontaci s metodami sociálního inženýrství, a tak nemůže být vnímáno jako definitivní řešení problému. Podle expertů z NCTEKK sice MFA efektivně eliminuje riziko prostého odcizení hesla, ale selhává v momentech, kdy je oběť zmanipulována k přímému schválení transakce, potvrzení notifikace nebo transakce. Zástupci SKPV v této souvislosti upozorňují, že právě existence MFA nutí pachatele k mnohem intenzivnější přímé interakci s poškozeným, což potvrzují i analytici z týmu CSIRT.cz. Ti dodávají, že zatímco „menším rybám" může MFA značně ztížit fungování, profesionální organizované gangy se na tento prvek již adaptovaly pomocí pokročilého sociálního inženýrství. Účinnost vícefaktorového ověřování je tedy vysoká z hlediska technického zvýšení nákladů na útok, ale její reálný dopad je limitován schopností útočníků manipulovat s lidským faktorem, což vyžaduje doplňující opatření v podobě detekce anomálií a neustálé osvěty.

11. Jakým způsobem probíhá sdílení informací o nových phishingových doménách a existuje v ČR něco jako národní blacklist?

Dotazovaní z NCTEKK a SKPV popisují existující systém jako víceúrovňovou kooperaci mezi orgány činnými v trestním řízení, bankovním sektorem a dalšími partnery. Výměna dat probíhá primárně skrze sdílení tzv. indikátorů kompromitace, které zahrnují seznamy škodlivých URL adres, IP adres, podvodných domén či telefonních čísel využívaných k podvodům. Tyto informace jsou následně integrovány do preventivních kampaní. Analytik CSIRT.CZ v této souvislosti poukazuje na konkrétní technický nástroj v podobě služby „Deny listy", kterou provozuje sdružení CZ.NIC. Tato platforma centralizuje data z činnosti národního CSIRT týmu a umožňuje poskytovatelům internetového připojení a správcům sítí automatizovaně blokovat přístup k doménám, které vykazují znaky podvodné či nezákonné činnosti. Z výpovědí vyplývá, že ačkoliv v České republice neexistuje univerzální státní blacklist, v praxi funguje efektivní

ekosystém sdílených databází a technologických řešení, který pomáhá k rychlejší reakci na nově vznikající phishingové kampaně.

12. Pokud by bylo možné změnit jeden prvek v českém systému kybernetické bezpečnosti, co by nejvíce pomohlo snížit úspěšnost phishingu?

U dvanácté otázky zdůrazňuje NCTEKK nutnost výrazného zrychlení koordinované reakce mezi klíčovými subjekty. Hlavním faktorem je podle nich co nejkratší časový úsek mezi detekcí podvodné kampaně a jejím technickým omezením. Rychlá blokace škodlivých domén, eliminace falešné infrastruktury a včasné zadržení podezřelých transakcí jsou vnímány jako faktory, které dokážou zásadním způsobem snížit efektivitu a výnosnost útoků. Zástupci SKPV k této otázce dodávají, že kybernetická bezpečnost představuje natolik provázaný a komplexní systém, že nelze poukázat pouze na jeden jediný prvek, jehož změna by byla natolik univerzálně zásadní, že by ve větší míře snížila úspěšnost phishingu.

13. Jsou současné vzdělávací programy ve školách a firmách dostatečné?

Zástupci z NCTEKK i SKPV jsou názoru, že stávající osvěta sice přispívá k postupnému zvyšování informovanosti, avšak ve své současné podobě není považována za dostatečnou. Za největší slabinu označují především jejich jednorázový a formální charakter, často realizovaný pouze formou statického e-learningu, který je odtržen od reálných hrozeb. NCTEKK zdůrazňuje, že pro skutečné zvýšení odolnosti je nezbytná pravidelná a praktická výuka postavená na modelových situacích a simulovaných útocích. U školského systému je zásadní potřeba budování dlouhodobé digitální gramotnosti a schopnosti rozpoznat snahu o podvodnou manipulaci, zatímco u firemního sektoru je doporučováno cílené školení zaměstnanců v rizikových rolích, jako mohou být například pracovníci finančních oddělení. Respondenti z SKPV k tomu dodávají, že nedostatečnost jednorázových školení se projevuje i ve státním sektoru, a potvrzují tak nutnost přechodu k praktičtějším a delším formám vzdělávání.

Zatímco výše zmínění respondenti volají po interaktivních simulacích, NÚKIB ve své strategii stále prosazuje spíše standardizované e-learningové moduly jako primární prostředek osvěty u jednotlivců a v institucích. Tato snaha je doplňována prezenčním vzděláváním v akademickém prostředí na vybraných školách a využíváním sociálních sítí

pro šíření krátkých informačních kampaní, které slouží k plošnému zvyšování digitální gramotnosti.[74]

14. Jak by se měla vyvíjet legislativa v oblasti odpovědnosti za škodu vzniklou phishingem? Má nést větší odpovědnost banka, nebo uživatel?

U NCTEKK i SKPV panuje shoda ohledně nutnosti vyváženého a individuálního přístupu bez přenesení viny na pouze jeden subjekt. Podle NCTEKK by legislativa měla motivovat obě strany k aktivní prevenci, ať už u bank a poskytovatelů služeb, kteří by měli nést odpovědnost za implementaci moderních technických opatření a monitorování podezřelých transakcí, tak i u uživatelů, kteří by měli postupovat s náležitou obezřetností při nakládání s autorizačními prvky. Klíčem k efektivní právní úpravě je podle nich jasné definování hranice mezi běžnou chybou a hrubou nedbalostí, stejně jako stanovení odpovědnosti za zjevná selhání bezpečnostních mechanismů na straně institucí. Zástupci SKPV tento postoj potvrzují s tím, že vzhledem ke komplexnosti kybernetických útoků, kde se prolíná technické zabezpečení s lidským rozhodováním, není možné a ani spravedlivé přenést plnou odpovědnost pouze na banku, či výhradně na uživatele.

15. Jakou roli by v budoucnu mělo hrát zapojení ISP do blokování phishingových stránek na síťové úrovni?

Všichni odpovídající jsou toho názoru, že zapojení ISP představuje velmi důležitý a účinný nástroj, jehož efektivita však závisí na rychlosti a centralizaci dat. NCTEKK vnímá síťové blokování jako užitečný doplněk k ostatním bezpečnostním prvkům, který má smysl zejména při včasné detekci větších kampaní. Zástupci SKPV však upozorňují na praktické překážky, jako jsou legislativní limity, sídla poskytovatelů mimo jurisdikci ČR a extrémní rychlost, s jakou pachatelé mění svou infrastrukturu. Analytici týmu CSIRT.cz v této souvislosti navrhují ideální model, ve kterém by všichni tuzemští ISP implementovali a aktivně doplňovali sdílené „Deny listy“. Taková centralizace a automatizace by umožnila zneškodnit phishingovou kampaň v řádu minut po jejím prvním výskytu, což by útočníky nutilo k neustálým a nákladným investicím do nových domén. Ačkoliv je tento přístup experty vnímán jako technicky žádoucí, zůstávají otázkou ekonomické náklady na straně ISP a potřeba jednotné a přesné legislativy, která by zajistila právní základ pro zásahy do síťového provozu.

[74] NÚKIB. *Zpráva o činnosti NÚKIB 2024*. Online PDF. str. 14 [cit. 2026-03-17].

16. Co byste vzkázali studentům a budoucím odborníkům?

Poslední otázka uzavírá rozhovory vzkazem pro nastupující generaci odborníků a studentů, přičemž všichni respondenti vyzdvihují rostoucí význam tohoto oboru a jeho přesah do fungování společnosti. Podle NCTEKK již phishing nelze vnímat jako okrajovou záležitost, nýbrž jako komplexní disciplínu na pomezí techniky, psychologie a organizovaného zločinu. Budoucí experti by proto měli disponovat nejen technickými znalostmi, ale i schopností porozumět chování obětí a ekonomickým motivacím útočníků. Největší společenský přínos budou mít ti odborníci, kteří dokážou spojit analytické myšlení s dovedností srozumitelně komunikovat rizika veřejnosti a prosazovat preventivní návyky v celé společnosti. Zástupci SKPV k tomu dodávají, že téma kybernetické bezpečnosti bude v čase dále nabývat na síle, což vyžaduje úzkou součinnost specialistů napříč různými odvětvími, zdaleka se neomezující pouze na IT. Analytik týmu CSIRT.cz pak doplňuje tento výhled o geopolitický rozměr a zdůrazňuje potřebu budování odolnosti vůči dezinformačním kampaním, zejména z Ruska a Číny.

NÚKIB v rámci své zprávy o stavu bezpečnosti z roku konce 2024 varuje do budoucna před rozmachem kvantových počítačů, které mají potenciál způsobit revoluci v mnoha odvětvích a mohou v příštích letech znamenat kritickou hrozbu pro stabilitu aktuálně využívaných standardů. S technologickým pokrokem také zůstává rizikovým faktorem aktivita hacktivistických skupin, kdy se očekává jejich zvýšená aktivita také v dalších letech a existuje reálná šance, že se činnost těchto skupin stane novým normálem nezávislým na trvání válečného konfliktu na Ukrajině.[75]

4.2 Diskuze výsledků rozhovorů a dat

Hlavním cílem předloženého výzkumu bylo komplexně zhodnotit aktuální stav a vývojové trendy v oblasti kybernetické kriminality se specifickým zaměřením na fenomén phishingu v prostředí České republiky. Vzhledem k vysoké dynamice této formy trestné činnosti bylo záměrem práce identifikovat nejen nejčastěji využívané druhy phishingových útoků, ale také prozkoumat další aspekty, které útočníci využívají k manipulaci s koncovými uživateli.

Prezentované výsledky poukazují na velmi dynamickou oblast kriminality, která i přes občasné výkyvy vykazuje vzestupnou tendenci. Útočníci často mají rychlejší

[75] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Online PDF. str. 49-50 [cit. 2026-03-17].

technický pokrok a disponují vysokou adaptibilitou, orgány následně musí pouze reagovat na vzniklé události, nikoliv se připravit dopředu. Zlepšení bezpečnostní situace brání také pomalá koordinace a spolupráce mezi klíčovými subjekty, složitá a nesourodá legislativa a nedostatečná kvalita vzdělávání společnosti, která uživatele prakticky nepřipraví na psychická nátlak a časovou tíseň. Efektivní obranu tak v současnosti brzdí nejen technické limity, ale i digitální negramotnost a zdlouhavé procesy sdílení informací.

Z rozhovorů je patrné, že dochází ke značnému nárustu kvality na straně útočníků, kteří jsou schopni využívat nové technologie ke svému prospěchu. Role AI v posledních letech slouží především k eliminaci jazykových bariér, ale vzhledem k jejímu rozmachu může v budoucnu útočníkům pomáhat i v jiných oblastech, stejně jako u NÚKIBu očekávaný rozkvět kvantových počítačů. Klíčovým poznatkem je změna od jednotlivců k mezinárodním organizovaným skupinám, kdy tato struktura tvoří phishing vysoce efektivním způsobem podvodu. Pomalá státní byrokracie, omezená národní jurisdikce a stávající represivní opatření umožňují orgánům reagovat pouze v omezené míře. Shoda mezi respondenty panuje také v tom, že přetrvávající slabinou je lidský faktor na který útočníci efektivně útočí za pomocí technik sociálního inženýrství a jsou schopni se následně takto dostat i přes systémy chráněné vícefaktorovou autorizací.

Účinnost stávajících opatření je dle respondentů momentálně poměrně dostačující, avšak prostor pro značné zlepšení uvádějí v rámci meziorgánové spolupráce v ČR a mezinárodní spolupráce mezi státy. Dále jsou zřejmé limity ve vzdělávání, kdy se experti přiklánění spíše ke kontinuálnímu vzdělávání uživatelů a zmiňují legislativní bariéry, které neumožňují okamžitý zásah proti útočníkům.

Hlavním doporučením pro zlepšení efektivity a celkové bezpečnosti je centralizace a vzájemné sdílení „Deny listů“ mezi poskytovateli internetového připojení, což by ve spojení s pokročilou a automatickou detekcí anomálií umožnilo eliminovat hrozby v krátkém čase a omezilo i dopad selhání lidského faktoru. Nezbytné jsou také legislativní změny, které by jasně vymezili rozdíl mezi pochybením a nedbalostí uživatele a posun od pouhého formálního technického zabezpečení k aktivní obraně, která dokáže identifikovat a zastavit manipulativní techniky sociálního inženýrství již v průběhu jejich realizace, například povinnost sledovat chování klienta, kdy transakce, která je u klienta vysoce neobvyklá, by byla neprodleně zablokována. Nicméně tento přístup by mohl u některých osob vyvolat vlnu nevole, avšak autor se domnívá, že v některých případech se jedná o jedinou možnost včasného zastavení podvodu. V neposlední řadě je nutné

stávající neefektivní a krátkodobou osvětu nahradit interaktivní prevencí a simulací kybernetických útoků, což by uživatele připravilo na psychologické techniky. Kampaně v oblasti kybernetické bezpečnosti musí být kontinuální a dynamicky orientované, aby včas odrážely momentální trendy a situaci.

Závěr

Předložená bakalářská práce se věnovala rozboru phishingu jako jedné z nejprogresivnějších forem kybernetické kriminality v České republice. Cílem provedeného výzkumu bylo zhodnotit momentální situaci v rámci této oblasti a následně formulovat doporučení, která by napomohla k efektivnější ochraně proti těmto útokům. Prezentované výsledky poukazují na velmi dynamickou sféru kriminality, která i přes občasné výkyvy vykazuje dlouhodobě vzestupnou tendenci. Útočníci v současnosti disponují vysokou adaptabilitou a technickým náskokem, což nutí státní orgány často pouze reaktivně odpovídat na vzniklé události namísto toho, aby se na ně mohly připravit s předstihem.

Z provedených rozhovorů s experty z SKPV, NCTEKK a CSIRT.CZ je patrný značný nárůst kvality na straně útočníků, kteří se transformovali z izolovaných jednotlivců do strukturovaných mezinárodních organizovaných skupin. Tato změna činí z phishingu vysoce efektivní a výnosný způsob podvodu. Role umělé inteligence v posledních letech slouží především k eliminaci jazykových bariér, čímž útoky získávají na věrohodnosti, avšak v budoucnu lze očekávat její využití i v dalších sofistikovaných oblastech. Klíčovým poznatkem zůstává skutečnost, že přetrvávající nejslabší stránkou bezpečnosti je lidský faktor. Útočníci pomocí technik sociálního inženýrství efektivně manipulují s psychikou obětí a jsou schopni překonat i systémy chráněné vícefaktorovou autorizací.

Efektivní obranu v současnosti brzdí nejen technické limity a digitální negramotnost, ale také zdlouhavé procesy sdílení informací a pomalá koordinace mezi klíčovými subjekty. Stávající represivní opatření a omezená národní jurisdikce v kombinaci s byrokracií umožňují státním orgánům reagovat pouze v omezené míře. Shoda mezi respondenty panuje v tom, že stávající vzdělávání ve formě jednorázových e-learningů je neefektivní, neboť uživatele prakticky nepřipraví na psychický nátlak a časovou tíseň, které jsou pro phishingové útoky typické. Ačkoliv je účinnost stávajících opatření považována za relativně dostačující, experti vidí značný prostor pro zlepšení zejména v oblasti meziorgánové a mezinárodní spolupráce.

Hlavním doporučením pro zvýšení celkové bezpečnosti je centralizace a vzájemné sdílení „Deny listů“ mezi poskytovateli internetového připojení. Toto opatření by ve spojení s automatickou detekcí anomálií umožnilo eliminovat hrozby ve značně kratším čase. Nezbytný je rovněž posun k aktivní obraně, například zavedením povinnosti

bankovních institucí sledovat nezvyklé chování klienta a neprodleně blokovat neobvyklé transakce. Přestože by takový přístup mohl vyvolat nevoli u části veřejnosti, autor se domnívá, že v mnoha případech jde o jedinou možnost, jak včas podvodu předejít a zastavit ho. V neposlední řadě je nutné pasivní formu vzdělávání nahradit kontinuální interaktivní prevencí a simulacemi útoků, které by uživatele reálně připravily na manipulační techniky útočníků.

Seznam zdrojů

Literární zdroje

1) GŘIVNA, T.; SCHEINOST, M. a ZOUBKOVÁ, I., *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 588 str. ISBN 978-80-7598-554-5.
2) HADNAGY, Ch. *Social engineering: the art of human hacking*. Indianapolis: Wiley Publishing, 2011. 477 str. ISBN 978-0-470-63953-5.
3) HOLT, T. J.; BOSSLER, A. M. a SEIGFRIED-SPELLAR, Kathryn C. *Cybercrime and digital forensics: an introduction*. Third edition. London: Routledge, Taylor & Francis Group, 2022. 754 str. ISBN 9780367360061.
4) JAMES, L. *Phishing Exposed*. Syngress, 2005. 450 str. ISBN 978-0-080-48953-7.
5) JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Přeložil K. VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. 396 str. ISBN 978-80-908388-4-0.
6) KLIMEK, L., ZÁHORA, J., a HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer. 2016. 448 str. ISBN 978-80-8168-538-5.
7) KOHOUT, R. a KLOZOVÁ, M., *Internetem bezpečně (nejen) pro seniory*. Vydání: první. Karlovy Vary: You connected, 2020. 55 str. ISBN 978-80-907852-0-5.
8) KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. 82 str. ISBN 978-80-88168-18-8.
9) KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. 556 str. ISBN 978-80-88168-31-7.
10) NĚMEC, M. *Teorie a metodologie kriminalistiky pro magisterské studium. II. díl, Aktuální problémy kriminalistické praxe*. Praha: Abook, 2019. 491 str. ISBN 978-80-906974-2-3.
11) POLČÁK, R. *Právo informačních technologií*. Právní monografie. Praha: Wolters Kluwer, 2018. 988 str. ISBN 978-80-7598-045-8.
12) PORADA, V. a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. vydání. Plzeň: Aleš Čeněk, 2019. 1205 str. ISBN 978-80-7380-741-2.

13) SAK, P. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. Praha: Petrklíč, 2018. 272 str. ISBN 978-80-7229-652-1.
14) SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1168 str. ISBN 978-80-7380-849-5.
15) VLACH, J.; KUDRLOVÁ, K. a PALOUŠOVÁ, V. *Kyberkriminalita v kriminologické perspektivě*. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2020. 143 str. ISBN 978-80-7338-189-9.

Elektronické zdroje

1) CSIRT.CZ. *Statistiky řešených incidentů*. Online. Dostupné z: https://www.cert-cr.cz/cs/o-nas/statistiky/. [cit. 2026-01-24].
2) CSIRT.CZ. *Statistiky řešených incidentů*. Online. Dostupné z: https://www.cert-cr.cz/cs/o-nas/statistiky/. [cit. 2026-01-25].
3) CSIRT-CUNI. *Příklady phishing e-mailů*. Online. Dostupné z: https://security.cuni.cz/cs/examples_phishing/. [cit. 2026-01-16].
4) CYBER SECURITY NEWS. *Phishing Attack Prevention – Best Practices for 2025*. Online. Dostupné z: https://cybersecuritynews.com/phishing-attack-prevention/. [cit. 2026-01-25].
5) E-BEZPEČÍ. *Co je quishing?* Online. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/online-zavislosti/57-rizikove-jevy/4062-co-je-quishing. [cit. 2026-03-18].
6) ESET. *Spoofing*. Online. Dostupné z: https://www.eset.com/cz/slovnik/spoofing/. [cit. 2026-03-18].
7) FBI. *Cryptocurrency Investment Fraud*. Online. Dostupné z: https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud. [cit. 2026-03-09].
8) FORTRA. *How to Detect and Attack Evil Twin WiFi Access Points*. Online. Dostupné z: https://www.tripwire.com/state-of-security/detect-attack-evil-twin-wifi-access-points. [cit. 2026-03-09].
9) GOV.CZ. *Návod, jak poznat phishingové útoky*. Online. Dostupné z: https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky. [cit. 2026-01-04].

10) GOV.CZ. *Návod, jak poznat phishingové útoky*. Online. Dostupné z: https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky. [cit. 2026-01-14].
11) GOVERNMENT OF CANADA. *Don't get hooked: understanding phishing and how to stay safe*. Online. Dostupné z: https://www.getcybersafe.gc.ca/en/blogs/dont-get-hooked-understanding-phishing-stay-safe. [cit. 2026-01-24].
12) GOVERNMENT OF CANADA. *The 7 red flags of phishing*. Online. Dostupné z: https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing. [cit. 2026-01-24].
13) KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-01-25].
14) KACPERSKY. *All About Phishing Scams & Prevention: What You Need to Know*. Online. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips. [cit. 2026-03-09].
15) KACPERSKY. *What is a firewall? Definition and explanation*. Online. Dostupné z: https://www.kaspersky.com/resource-center/definitions/firewall. [cit. 2026-01-25].
16) KOĎOUSKOVÁ, B. *HTTPS v kostce: co to je, jak funguje a jak na něj přejít*. Online. Dostupné z: https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls#co-je-https. [cit. 2026-03-09].
17) MUNI. *PHISHING: Jak se nenechat ošálit v kyberprostoru*? Online. Dostupné z: https://security.muni.cz/kurzy/kyberkompas/phishing. [cit. 2026-01-14].
18) NÚKIB. *Čtvrtletní přehled hrozeb pohledem NÚKIB Q1,Q2,Q3,Q4 2025*. Online PDF. [cit. 2026-03-17].
19) NÚKIB. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit*. Online PDF. 2020. [cit. 2026-01-14].
20) NÚKIB. *Zpráva o činnosti NÚKIB 2024*. Online PDF. [cit. 2026-03-17].
21) NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Online PDF. [cit. 2026-01-24].
22) NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Online PDF. [cit. 2026-03-17].
23) OPENTEXT. *Types of Phishing Attacks You Need to Know to Stay Safe*. Online PDF. [cit. 2026-01-14].

24) POLICIE ČR. *Kyberkriminalita*. Online. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx. [cit. 2026-01-03].
25) POLICIE ČR. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník*. Online. Dostupné z: https://policie.gov.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx. [cit. 2026-01-03].
26) POLICIE ČR. *Oznámení trestného činu*. Online. Dostupné z: https://policie.gov.cz/clanek/oznameni-trestnehocinu.aspx?_gl=1*62fnvo*_ga*ODc2MDIxMjQyLjE3NjI3MDIyNDU.*_ga_MGE9DCQJ5M*czE3NjkyNjI3NTkkbzckZzEkdDE3NjkyNjI5MzgkajU1JGwwJGgw. [cit. 2026-01-24].
27) RIS3.GOV.CZ. *G1 Kyberkriminalita – Celkové počty registrovaných trestných činů spáchaných v kyberprostoru*. Online. Dostupné z: https://ris3.gov.cz/monitoring/indikatory/m02c0208-celkove-pocty-registrovanych-trestnych-cinu-spachanych-v-kyberprostoru. [cit. 2026-01-24].
28) SPRÁVA SÍTĚ. *Co je Evil Twin*. Online. Dostupné z: https://www.sprava-site.eu/evil-twin/. [cit. 2026-03-09].
29) STOPONLINE. *Kybernetické hrozby a útoky*. Online. Dostupné z: https://www.stoponline.cz/cs/kyberneticke-hrozby-a-utoky/. [cit. 2026-01-24].
30) STOPONLINE. *O STOPonline*. Online. Dostupné z: https://www.stoponline.cz/cs/o-nas/o-stoponline/. [cit. 2026-01-24].

Ostatní zdroje

1) COUNCIL OF EUROPE. *Convention on Cybercrime (ETS No.185)*. Budapest. 2023
2) ČESKO. Zákon č. 40/2009 Sb. trestní zákoník ze dne 8. ledna 2009. In Sbírka zákonů České republiky. 2009. §209. Hlava pátá.
3) DVOŘÁK, M. *Phishing, pharming a jejich trestní postih*. Trestněprávní revue. 2018. roč. 17, č. ISSN 1213-5313.
4) GHAZI-TEHRANI, A. K. a PONTELL, H. N. *Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders*. 2021. vol. 16, no. 3. ISSN 1556-4886.
5) KASL, F. *Kybernetický bezpečnostní incident a jeho ohlašování. v rámci zabezpečení osobních údajů v kontextu internetu věcí*. Časopis pro právní vědu a praxi. Masaryk University Press. 2020. roč. 28, č. 3. ISSN 1210-9126.

6) KRUPIČKA, J. *Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi*. Acta Universitatis Carolinae Iuridica. 2012. ISSN 0323-0619
7) MUNTODE R. A a PARWE S. S. *An Overview on Phishing – its types and Countermeasures*. International Journal of Engineering Research and Technology. ESRSA Publications Pvt. ISSN 2278-0181.
8) ŽILKOVÁ, M. *Trestní a kriminologické aspekty phishingu*. Diplomová práce. Praha: Právnická fakulta UK. 2023. Vedoucí práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D.

Seznam zkratek

SKPV – Služba kriminální policie a vyšetřování

NCTEKK – Národní centrála proti terorismu, extrémismu a kybernetické kriminalitě

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

ICT – Informační a komunikační technologie

AI – Umělá inteligence

WHO – Světová zdravotnická organizace

CDC – Středisko pro kontrolu a prevenci nemocí v USA

IP – Internetový protokol

DNS – Systém doménových jmen

URL – Jednotný lokátor zdroje (také webová adresa)

HTTPS – Zabezpečený protokol pro přenos dat na internetu

QR – Rychlá odezva (QR kód – dvourozměrný čárový kód)

CSIRT – Bezpečnostní pohotovostní tým pro počítačové incidenty (také CERT)

NCKB – Národní centrum kybernetické bezpečnosti

MFA – Vícefaktorové ověřování nebo autentizace

ISP – Poskytovatel internetového připojení

IT – Informační technologie

Seznam obrázků

Seznam příloh

Příloha I. – seznam otázek k rozhovoru

1. Jaký je současný trend v počtu evidovaných kybernetických incidentů v ČR a jak významnou část z nich tvoří právě phishing?
2. Lze v posledních 2–3 letech pozorovat změnu v profilu pachatelů? Převažují spíše samostatní útočníci, nebo organizované skupiny se zázemím v ČR nebo zahraničí?
3. V čem spatřujete největší bariéry při vyšetřování a potírání phishingových kampaní?
4. Jaké formy phishingu vnímáte aktuálně v českém prostředí jako nejnebezpečnější?
5. Pozorujete v praxi nárůst útoků v perfektní češtině nebo lépe cílených kampaní díky AI?
6. Které sektory jsou v současnosti nejčastějšími cíli?
7. Jak hodnotíte úroveň povědomí běžných českých uživatelů o phishingu a jsou osvětové kampaně dostatečné?
8. Při analýze úspěšných útoků – co bývá častějším důvodem selhání: technické zabezpečení, nebo lidský faktor?
9. Jak efektivní je současná spolupráce mezi státními orgány a soukromým sektorem při včasném varování před phishingem?
10. Do jaké míry považujete zavedení povinného vícefaktorového ověřování za účinné?
11. Jakým způsobem probíhá sdílení informací o nových phishingových doménách a existuje v ČR něco jako národní blacklist?
12. Pokud by bylo možné změnit jeden prvek v českém systému kybernetické bezpečnosti, co by nejvíce pomohlo snížit úspěšnost phishingu?
13. Jsou současné vzdělávací programy ve školách a firmách dostatečné?
14. Jak by se měla vyvíjet legislativa v oblasti odpovědnosti za škodu vzniklou phishingem? Má nést větší odpovědnost banka, nebo uživatel?
15. Jakou roli by v budoucnu mělo hrát zapojení ISP do blokování phishingových stránek na síťové úrovni?
16. Co byste vzkázali studentům a budoucím odborníkům?

Příloha II. – odpovědi NCTEKK

1. **Jaký je současný trend v počtu evidovaných kybernetických incidentů v ČR a jak významnou část z nich tvoří právě phishing?**

   Z pohledu Policie ČR i NCTEKK je zřejmé, že kybernetická kriminalita patří dlouhodobě k nejdynamičtěji rostoucím formám kriminality. I když v roce 2024 došlo v celkovém součtu k mírnému meziročnímu poklesu, stále jde o velmi významný segment kriminality, který tvoří více než desetinu všech registrovaných trestných činů v České republice. U phishingu je třeba říct, že veřejně dostupné policejní statistiky jej většinou neoddělují jako samostatnou kategorii. Z praxe ale vyplývá, že phishing a jeho varianty, zejména smishing, vishing a spoofing, tvoří významnou část útoků zaměřených na získání přístupových údajů, platebních dat nebo převodu finančních prostředků.

2. **Lze v posledních 2–3 letech pozorovat změnu v profilu pachatelů? Převažují spíše samostatní útočníci, nebo organizované skupiny se zázemím v ČR nebo zahraničí?**

   V posledních letech sledujeme posun od jednotlivců k volně propojeným nebo přímo organizovaným skupinám, které fungují mezinárodně a dělí si role mezi technické zajištění, kontakt s obětí, výběr prostředků a jejich legalizaci. Řada phishingových kampaní dnes nevzniká izolovaně, ale jako součást širšího podvodného ekosystému. Typické je zapojení zahraničních call center, překupníků účtů, osob využívaných jako tzv. money mule a technicky připravených skupin, které fungují jako služba pro další pachatele. Domácí pachatelé se často uplatňují v navazujících fázích, zejména při výběru prostředků nebo zprostředkování účtů. Tento trend odpovídá i širším poznatkům Policie ČR o profesionalizaci kybernetické kriminality.

3. **V čem spatřujete největší bariéry při vyšetřování a potírání phishingových kampaní?**

   Největší bariéry spatřujeme ve třech rovinách. První je vysoká rychlost útoku: od rozeslání kampaně po odčerpání prostředků často uplynou jen hodiny. Druhou je přeshraničnost, kdy infrastruktura útoku, pachatelé, účty i hosting bývají v různých jurisdikcích. Třetí je anonymizace a využívání služeb třetích stran, například zahraničních poskytovatelů hostingu, dočasných domén, šifrovaných

komunikačních platforem nebo kryptoměnových nástrojů. Bariérou je i to, že lidská chyba nebo pozdní oznámení často nastupují dříve, než může represivní složka efektivně zasáhnout.

4. **Jaké formy phishingu vnímáte aktuálně v českém prostředí jako nejnebezpečnější?**

Za nejnebezpečnější považujeme ty formy, které kombinují technické napodobení důvěryhodné instituce s psychologickým tlakem na oběť. V českém prostředí jde zejména o smishing a vishing navázaný na bankovní sektor, falešné investiční nabídky, podvodné odkazy na dopravce nebo doručovací služby a nově také quishing, tedy zneužívání QR kódů. Vysoce rizikový je také spear phishing, pokud míří na zaměstnance institucí, firem nebo osob s přístupem do důležitých systémů. Závažnost se zvyšuje tehdy, pokud útok nesměřuje jen ke krádeži dat, ale k okamžitému převodu f inančních prostředků nebo převzetí identity oběti.

5. **Pozorujete v praxi nárůst útoků v perfektní češtině nebo lépe cílených kampaní díky AI?**

Ano, v praxi je patrné, že jazyková úroveň podvodných kampaní se zlepšuje. Dříve byly typickým varovným znakem gramatické chyby, nepřesvědčivé formulace nebo nekvalitní překlady. Dnes se stále častěji setkáváme s texty, které působí přirozeněji, jsou stylově přizpůsobené cílové skupině a lépe napodobují komunikaci bank, úřadů či známých služeb. Nástroje založené na generativní AI tento trend pravděpodobně dále urychlují, protože snižují jazykovou bariéru pro pachatele a usnadňují personalizaci útoku. Z pohledu NCTEKK tak očekáváme další růst kvality a přesvědčivosti phishingových kampaní v budoucnu.

6. **Které sektory jsou v současnosti nejčastějšími cíli?**

Mezi nejčastější cíle patří bankovní klienti, uživatelé online tržišť a bazarových platforem, zákazníci dopravních a doručovacích služeb a dále zaměstnanci firem a institucí, kteří mají přístup k platebním procesům nebo interním systémům. Vedle finanční sféry je rizikový také veřejný sektor a organizace kritické infrastruktury, kde phishing může sloužit jako vstupní bod pro další kompromitaci systémů. V preventivních materiálech Policie ČR a MV se můžete dočíst, že se

jedná zejména o bankovní podvody, investiční podvody a další online finanční podvody.

7. **Jak hodnotíte úroveň povědomí běžných českých uživatelů o phishingu a jsou osvětové kampaně dostatečné?**

   Povědomí veřejnosti se zlepšuje, ale stále není rovnoměrné. Část populace již základní znaky podvodu rozpozná, nicméně útočníci tomu přizpůsobují své metody a cílí na důvěru, časový tlak a emoce. Z pohledu NCTEKK mají preventivní kampaně smysl, zejména pokud jsou dlouhodobé, praktické a srozumitelné. Samotná jednorázová osvěta však nestačí. Je třeba opakovaně vysvětlovat konkrétní scénáře útoků a reagovat na aktuální modus operandi pachatelů. Tomu odpovídá i zapojení Policie ČR do kampaní jako #nePINdej či do širší osvětové činnosti k internetovým podvodům.

8. **Při analýze úspěšných útoků – co bývá častějším důvodem selhání: technické zabezpečení, nebo lidský faktor?**

   Ve většině případů je rozhodující kombinace obou faktorů, ale nejčastějším spouštěčem bývá lidský faktor. Oběť klikne na odkaz, vyplní údaje, potvrdí transakci nebo sdělí autorizační prvek v domnění, že komunikuje s legitimní institucí. Technické zabezpečení může riziko výrazně snížit, ale pokud je uživatel přesvědčen k aktivní spolupráci s pachatelem, část obrany se obchází. Zároveň platí, že tam, kde chybí vícevrstvá ochrana, například detekce anomálií, omezení transakčních limitů nebo kvalitní filtrování, bývá dopad útoku vyšší.

9. **Jak efektivní je současná spolupráce mezi státními orgány a soukromým sektorem při včasném varování před phishingem?**

   Spolupráci hodnotíme jako nezbytnou a v řadě oblastí jako funkční, ale stále je prostor pro zrychlení a větší standardizaci. Zásadní roli hrají banky, operátoři, poskytovatelé e-mailových a hostingových služeb, bezpečnostní týmy a také správci domén. Důležitým signálem je i formální spolupráce Policie ČR s Českou bankovní asociací, která reaguje právě na vishing, smishing a související podvody. Pro další posun by bylo vhodné ještě více zrychlit předávání indikátorů kompromitace, postupy pro blokaci škodlivých domén a mechanismy pro okamžité pozastavení podezřelých převodů.

10. **Do jaké míry považujete zavedení povinného vícefaktorového ověřování za účinné?**

    Vícefaktorové ověřování považujeme za velmi důležitý bezpečnostní prvek, ale nikoli za samospasitelný nástroj. MFA významně zvyšuje odolnost proti útokům zaměřeným na prosté odcizení hesla, nicméně neochrání plně v situaci, kdy útočník oběť zmanipuluje tak, aby sama schválila přihlášení nebo transakci. Pachatelé dnes běžně necílí jen na přihlašovací údaje, ale i na autorizační kódy, push notifikace nebo přímé potvrzení operace v mobilní aplikaci. Účinnost MFA je proto vysoká pouze v kombinaci s osvětou, detekcí anomálií a bezpečným nastavením procesů na straně poskytovatele služby.

11. **Jakým způsobem probíhá sdílení informací o nových phishingových doménách a existuje v ČR něco jako národní blacklist?**

    Sdílení informací probíhá mezi více aktéry, a to jak na úrovni orgánů činných v trestním řízení, tak v rámci bezpečnostní komunity, bankovního sektoru a dalších partnerů. V praxi se pracuje s indikátory kompromitace, seznamy škodlivých domén, URL adres, IP adres nebo telefonních čísel. Tyto informace se využívají i v rámci preventivních kampaní. Obecně lze říct, že v České republice existují různé dílčí mechanismy blokace a sdílení rizikových indikátorů.

12. **Pokud by bylo možné změnit jeden prvek v českém systému kybernetické bezpečnosti, co by nejvíce pomohlo snížit úspěšnost phishingu?**

    Za nejúčinnější systémovou změnu bychom považovali výrazné zrychlení koordinované reakce mezi bankami, telekomunikačními operátory, správci domén, poskytovateli hostingu a státem. Jinými slovy: co nejkratší čas mezi detekcí kampaně a jejím technickým omezením. Pokud se podaří během velmi krátké doby zablokovat škodlivou doménu, zadržet podezřelou transakci nebo vyřadit z provozu falešnou infrastrukturu, úspěšnost kampaně klesá zásadním způsobem.

13. **Jsou současné vzdělávací programy ve školách a firmách dostatečné?**

    Současné programy jsou užitečné, ale samy o sobě nejsou dostatečné. Největší slabinou bývá, že školení bývá jednorázové, formální nebo odtržené od reálných scénářů. Efektivní je naopak pravidelná a praktická výuka, doplněná modelovými

situacemi, simulovanými útoky a jednoduchými pravidly pro každodenní praxi. U škol je důležitá dlouhodobá digitální gramotnost a schopnost rozpoznat manipulaci. U firem pak zejména trénink zaměstnanců v rizikových rolích, například ve financích a administraci systémů.

14. Jak by se měla vyvíjet legislativa v oblasti odpovědnosti za škodu vzniklou phishingem? Má nést větší odpovědnost banka, nebo uživatel?

Za NCTEKK bychom doporučili vyvážený přístup. Odpovědnost by neměla být posuzována mechanicky, ale podle konkrétních okolností. Poskytovatel služby má mít povinnost zavádět přiměřená technická a procesní opatření, sledovat anomálie a reagovat na zjevně rizikové transakce. Uživatel má současně postupovat s náležitou obezřetností a nesdělovat údaje či autorizační prvky. Legislativa by měla motivovat obě strany k prevenci a současně vytvářet jasnější pravidla pro případy hrubé nedbalosti nebo naopak zjevného selhání bezpečnostních mechanismů.

15. Jakou roli by v budoucnu mělo hrát zapojení ISP do blokování phishingových stránek na síťové úrovni?

Zapojení poskytovatelů internetového připojení může být užitečným doplňkovým nástrojem, zejména u masových kampaní. Nemělo by však být jediným opatřením, protože pachatelé infrastrukturu rychle mění a přecházejí na nové domény nebo platformy. Smysl má zejména rychlé a právně předvídatelné blokování zjevně škodlivých zdrojů na základě ověřených indikátorů, a to v kombinaci s blokací na úrovni domén, hostingu, e-mailové ochrany a finančních toků. Klíčová je opět rychlost a koordinace.

16. Co byste vzkázali studentům a budoucím odborníkům?

Phishing dnes není okrajový problém, ale stabilní součást kybernetické kriminality, která stojí na propojení techniky, psychologie, organizovaného zločinu a finanční motivace. Budoucí odborníci by proto měli chápat nejen technickou stránku útoku, ale i chování obětí, ekonomiku podvodu a význam mezioborové spolupráce. Největší přínos mají lidé, kteří dokážou spojit analytické myšlení, praktické bezpečnostní návyky, orientaci v digitálním prostředí a schopnost srozumitelně vysvětlovat rizika veřejnosti. Právě prevence a rychlá reakce totiž dnes rozhodují o tom, zda phishingová kampaň uspěje, nebo selže.

Příloha III. – odpovědi SKPV

1. **Jaký je současný trend v počtu evidovaných kybernetických incidentů v ČR a jak významnou část z nich tvoří právě phishing?**

   Kybernetická kriminalita je jednou z forem kriminality, která vykazuje rostoucí trend a vývoj, nicméně phishing není samostatně sledovanou kategorií. Phishing ve všech svých formách je významnou částí útoků zaměřených na získání přístupových údajů, platebních dat nebo převodu finančních prostředků.

2. **Lze v posledních 2–3 letech pozorovat změnu v profilu pachatelů? Převažují spíše samostatní útočníci, nebo organizované skupiny se zázemím v ČR nebo zahraničí?**

   Ano, lze pozorovat změny z hlediska pachatelů této trestné činnosti. Stále více se na této formě podílí ve spolupachatelství organizované skupiny s různou rolí zapojení. Přeshraniční spolupráce pachatelů je na vzestupu a některé skupiny se organizují operativně, kdy určitá část využívá druhých k plnění jednotlivých i třeba méně sofistikovaných rolí na daném teritoriu.

3. **V čem spatřujete největší bariéry při vyšetřování a potírání phishingových kampaní?**

   Mezinárodní přesah a s tím spojené formy policejní spolupráce, resp. orgánů činných v trestním řízení, Europol x Interpol, další bilaterální či multilaterální smlouvy upravující tuto oblast, popř. zcela neexistují možnost této spolupráce. Dále také poskytovatelé webhostingu a finančních účtů.

4. **Jaké formy phishingu vnímáte aktuálně v českém prostředí jako nejnebezpečnější?**

   V českém prostředí se vyskytují víceméně všechny formy phishingu – plošné e-maily, spear fishing, smishing, vishing a BEC / CEO = „Business e-mail compromise“. Nejvíce oznámení na tuto trestnou činnost je učiněno při převodu finančních prostředků. Otázkou je, zdali je proto tato forma „nejnebezpečnější“.

5. **Pozorujete v praxi nárůst útoků v perfektní češtině nebo lépe cílených kampaní díky AI?**

   Útoky v oblasti kybernetické kriminality jsou stále sofistikovanější a zlepšuje se i jazyková vybavenost. Vývoj umělé inteligence má samozřejmě i své negativní externality.

6. **Které sektory jsou v současnosti nejčastějšími cíli?**

   Veřejný sektor – „citlivé" informace, narušení kritické infrastruktury i soukromý sektor – bankovní sektor, on-line shopy, soukromé firmy, občané.

7. **Jak hodnotíte úroveň povědomí běžných českých uživatelů o phishingu a jsou osvětové kampaně dostatečné?**

   Dostatečnost osvětové kampaně v oblasti kyberkriminality jako i v jiných oblastech bude vždy záviset na míře ochoty přijetí rizika a možnosti předcházet tomuto riziku. Vyspělost společnosti určuje míru přijatelného rizika, odolnost společnosti proti kyberkriminalitě, ale zároveň může představovat příležitost pro pachatele. I z tohoto pohledu lze úroveň povědomí a míru dostatečnosti osvětové kampaně těžko hodnotit.

8. **Při analýze úspěšných útoků – co bývá častějším důvodem selhání: technické zabezpečení, nebo lidský faktor?**

   Ve většině případů jde o lidský faktor, a to i z pohledu, že tento mnohdy rozhoduje o technickém zabezpečení nebo jeho využívání.

9. **Jak efektivní je současná spolupráce mezi státními orgány a soukromým sektorem při včasném varování před phishingem?**

   Spolupráce je naprosto nezbytná a její efektivita se zvyšuje. Míra efektivity je dána vzájemnou ochotou této spolupráce. Spolupráce s bankovním sektorem je na dobré úrovni.

10. **Do jaké míry považujete zavedení povinného vícefaktorového ověřování za účinné?**

    Jeden z důležitých bezpečnostních prvků, na který navazují další bezpečnostní prvky, např. dotaz, zdali uživatel provedl transakci apod. Proto jsou pachatelé často v přímé interakci s klientem, poškozeným.

11. **Jakým způsobem probíhá sdílení informací o nových phishingových doménách a existuje v ČR něco jako národní blacklist?**

    Jiný způsob sdílení informací probíhá v konkrétní věci (např. dle trestního řádu), obecně pak na různých úrovních a mezi různými aktéry. Informace se využívají i v rámci preventivních kampaní, kde se mimo jiné uvádí seznamy podezřelých IP či URL adres, domén.

12. **Pokud by bylo možné změnit jeden prvek v českém systému kybernetické bezpečnosti, co by nejvíce pomohlo snížit úspěšnost phishingu?**

    Jde o provázaný systém, neumím odpovědět.

13. **Jsou současné vzdělávací programy ve školách a firmách dostatečné?**

    Nemohu posoudit tyto sektory. Obecně se vědomosti v této oblasti zlepšují. I ve státním sektoru jde mnohdy jen o jednorázové školení např. formou e-learningu. Toto nepovažuji za dostatečné.

14. **Jak by se měla vyvíjet legislativa v oblasti odpovědnosti za škodu vzniklou phishingem? Má nést větší odpovědnost banka, nebo uživatel?**

    Vzhledem k shora uvedenému není možné přenést odpovědnost pouze na jeden subjekt.

15. **Jakou roli by v budoucnu mělo hrát zapojení ISP do blokování phishingových stránek na síťové úrovni?**

    ISP nebo IAP zde mohou sehrát velmi důležitou roli. Ale položme si otázky: co je prvořadým cílem poskytovatelů internetových stránek; kde sídlí, jaká pravidla např. legislativní jim můžeme nastavit např. i k provedení blokace phishingových

stránek; jak často a rychle pachatelé mění, mohou změnit doménu, poskytovatele sítě atd.

16. Co byste vzkázali studentům a budoucím odborníkům?

Phishing, ale obecně téma kyberbezpečnost bude v čase sílit a bude nutná spolupráce odborníků z jednotlivých odvětví, nejen z IT. Vzdělávání v oboru může být i příležitost pro ty, kteří chtějí chránit nejen sebe, ale i společnost.

Příloha IV. – odpovědi CSIRT.CZ

1. **Jaký je současný trend v počtu evidovaných kybernetický incidentů v ČR a jak významnou část z nich tvoří právě phishing?**

   CSIRT1 – (Respondent odkázal na statistiky: https://csirt.cz/cs/o-nas/statistiky/.)

2. **Lze v posledních 2–3 letech pozorovat změnu v profilu pachatelů? Převažují spíše samostatní útočníci, nebo organizované skupiny se zázemím v ČR nebo zahraničí?**

   CSIRT1 – Nejsme policie, jsme státní neziskovka, nemáme právo vyšetřovat, nemáme tedy profily pachatelů. Domníváme se, že se spíše jedná o organizované skupiny.

3. **V čem spatřujete největší bariéry při vyšetřování a potírání phishingových kampaní (např. legislativa, technické limity, mezinárodní spolupráce)?**

   CSIRT1 – Pravděpodobně legislativa.

   CSIRT2 – Někdy nemůžeme definitivně prokázat, že se jedná o phishing, i když je jasné, třeba na 90 %, že doména je používána pouze pro nekalé účely. Mám na mysli zejména falešné e-shopy, které mají tunu negativních recenzi, žádnou pozitivní, všichni tvrdí, že byli okradeni, ale my ji stejně nemůžeme odstranit. Nebo silně amorální, ale legální přeprodej dálničních známek. Potom taky je problém, když se snažíme nechat odstranit doménu u zahraničního registrátora nebo u hostingu. Pokud je text v češtině, oni jsou potom v podobné situaci a také nemohou jen tak obsah odstranit. Phishing z jejich pohledu není zřejmí, hlavně u takových těch dezinformačních webů, které propagují falešné investiční platformy. I s přiloženou a přeloženou výzvou od Policie ČR to je někdy marná snaha a pošlou nám odpověď, že to není průkazné a nemůžou to odstranit. Občas ale mile překvapí.

4. **Jaké formy phishingu (vishing, smishing, spear-phishing) vnímáte aktuálně v českém prostředí jako nejnebezpečnější?**

   CSIRT1 – Pro firmy spear-phishing, u běžných občanů falešné hovory vishing. Zase, nemáme data, ale tipl bych, že vishing zabere útočníkům víc práce, ale mají z něj více peněz.

CSIRT2 – Z hlediska napáchaných škod to asi bude vishing, viz falešný policista/bankéř.

5. **Pozorujete v praxi nárůst útoků v perfektní češtině nebo lépe cílených kampaní díky AI?**

   CSIRT1 – Ne. Nejčastější jsou falešné linky na bazarech, tam zatím AI nevidím.

   CSIRT2 – AI dělá phishing realističtější, ale zároveň do zpráv neustále přidává smajlíky a podobné blbiny, které AI podle mě dost prozradí a zpráva nevypadá autenticky. Lidi prostě nepoužívají při komunikaci smajlíky typu obálka, mapa, auto apod, protože nikdo ani neví, jaký to má na klávesnici kód nebo jak to napsat. Aspoň jsem se s tím nesetkal. U netechnicky zaměřených lidí to ale pravděpodobně unikne pozornosti.

6. **Které sektory (státní správa, bankovnictví, kritická infrastruktura) jsou v současnosti nejčastějšími cíli?**

   CSIRT1 i CSIRT2 – Bez odpovědi.

7. **Jak hodnotíte úroveň povědomí běžných českých uživatelů phishingu? Jsou osvětové kampaně (např. Nebuď oběť, Kybertest) podle vás dostatečně efektivní?**

   CSIRT1 i CSIRT2 – Bez odpovědi.

8. **Při analýze úspěšných útoků – co bývá častějším důvodem selhání: technické zabezpečení (např. propuštěný e-mail filtrem) nebo selhání lidského faktoru?**

   CSIRT1 – Lidský faktor a přehlédnutí. Další vyvolaný stres a snadný zisk. Další je neznalost, lidé neumí zjistit, na které doméně se nacházejí, myslí si, že jsou na stránkách novin, ale je to falešný článek na doméně, která s danými novinami nemá nic společného. Technické zabezpečení není pro případy, co se setkáváme, tolik problém. Útočníci si kupují své domény, ne že se prolamují do cizích.

   CSIRT2 – Lidský faktor je a bude vždycky největší zádrhel. Emailové filtry vznikají v reakci na již proběhlé útoky a útočníci mají spoustu možností emaily vytunit, aby filtrem prolezly. Tohle je ale samozřejmě stojí více úsilí a energie a menší výdělek.

9. **Jak efektivní je současná spolupráce mezi státními orgány (NÚKIB, Policie) a soukromým sektorem (banky, operátoři) při včasném varování před phishingem?**

   CSIRT1 i CSIRT2 – Bez odpovědi.

10. **Do jaké míry považujete zavedení povinného vícefaktorového ověřování (MFA) proti phishingu za účinné, nebo už útočníci tuto bariéru běžně obcházejí?**

    CSIRT1 – Určitě jim přidělává práci a zvyšuje finanční náročnost.

    CSIRT2 – Ostřílené gangy jsou schopné se adaptovat skrz sociální inženýrství a znovu zmiňuji falešného policistu. Menší ryby to ale asi dost omezí v působnosti.

11. **Jakým způsobem probíhá sdílení informací o nových phishingových doménách mezi vašimi institucemi? Existuje v ČR něco jako „národní blacklist“ podvodných stránek?**

    CSIRT2 – (Respondent odkázal na blog: https://blog.nic.cz/2025/02/20/sluzba-deny-listy-aneb-jak-data-z-prace-narodniho-csirtu-pomahaji-chranit-uzivatele/.)

12. **Pokud byste měli možnost změnit jeden prvek v českém systému kybernetické bezpečnosti, co by to bylo pro radikální snížení úspěšnosti phishingu?**

    CSIRT1 i CSIRT2 – Bez odpovědi.

13. **Jsou současné vzdělávací programy ve školách a firmách dostatečné, nebo by se metodika školení měla radikálně změnit (např. povinné simulace útoků)?**

    CSIRT1 i CSIRT2 – Bez odpovědi.

14. **Jak by se měla vyvíjet legislativa v oblasti odpovědnosti za škodu vzniklou phishingem? Má nést větší odpovědnost banka, anebo uživatel?**

    CSIRT1 i CSIRT2 – Bez odpovědi.

15. **Jakou roli by v budoucnu mělo hrát zapojení poskytovatelů internetového připojení (ISP) v aktivním blokování phishingových stránek na síťové úrovni?**

    CSIRT2 – Asi ideální by bylo, samozřejmě i pro nás, kdyby všichni ISP implementovali naše DL a samy do nich přispívali. První výskyt by se hned rozšířil mezi ostatní poskytovatele a v řádu minut by celá phishingová kampaň byla na českém internetu nedostupná. Pro scammery by to znamenalo nutnost koupit novou doménu, ale nevím, jak je to technicky dosažitelné, co tomu brání, ani kolik to vlastně stojí firmu, která DL odebírá a jestli to pro ně nejsou neopodstatněné výdaje. Někteří mají asi i svoje blacklisty, ale určitě by bylo dobré to nějak centralizovat a udržovat aktuální.

16. **Co byste vzkázali studentům a budoucím odborníkům: v čem bude spočívat největší výzva v ochraně uživatelů v příštích pěti letech?**

    CSIRT1 – Odolnost proti ruským a čínským dezinformacím.