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

BAKALÁŘSKÁ PRÁCE

VYBRANÉ KRIMINOLOGICKÉ A KRIMINALISTICKÉ ASPEKTY KYBERNETICKÉ KRIMINALITY PÁCHANÉ FORMOU PHISHINGU

Autor práce: Marek Naščák DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Milan Kocík MBA, LL.M

Katedra: Katedra právních oborů a bezpečnostních studií

2025

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Marek Naščák, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Vybrané kriminologické a kriminalistické aspekty kybernetické kriminality páchané formou phishingu

Název bakalářské práce v anglickém jazyce: Selected Criminological and Criminalistic Aspects of Cybercrime Perpetrated by Phishing

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Datum zadání bakalářské práce (měsíc, rok): listopad 2024

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je zhodnotit vybrané kriminologické a kriminalistické aspekty kybernetické kriminality realizované prostřednictvím phishingu, se zaměřením na motivaci pachatelů, typologii obětí a metody provádění těchto útoků. Vedlejším cílem je identifikovat klíčové faktory přispívající k úspěšnosti phishingových útoků, zhodnotit současné preventivní a vyšetřovací pokusy a navrhnout možná opatření pro zvýšení ochrany před tímto typem kyberkriminality.

Student: Marek Naščák, DiS.	20. 11. 2024 *datum*	*podpis*
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.	22. 11. 2024 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	2. 12. 2024 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9. 12. 2024 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10. 12. 2024 *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 vedoucímu bakalářské práce JUDr. Milanu Kocíkovi, MBA, LL.M za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

NAŠČÁK, M., *Vybrané kriminologické a kriminalistické aspekty kybernetické kriminality páchané formou phishingu: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 66 s. Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M

Klíčová slova: phishing, kybernetická kriminalita, prevence, internet

Tato bakalářská práce se zaměřuje na analýzu a výzkum kybernetické kriminality, konkrétně phishingových útoků. Práce řeší teoretické aspekty phishingu, včetně jeho definice, vývoje a právní úpravy v České republice. Dále pojednává o kriminologických a kriminalistických aspektech, jako jsou typy phishingu, profil oběti, motivace pachatelů a jejich modus operandi. Analyzuje rovněž postupy policejních orgánů při vyšetřování těchto útoků a zajišťování důkazních prostředků. Praktická část práce zkoumá konkrétní případy kybernetické kriminality spáchané prostřednictvím phishingu a shrnuje současné preventivní a vyšetřovací metody. Cílem práce je navrhnout opatření pro zvýšení ochrany uživatelů před tímto typem kyberkriminality.

ABSTRACT

NAŠČÁK, M. *Selected Criminological and Criminalistic Aspects of Cybercrime Perpetrated by Phishing: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2025. 66 pgs. Supervisor: JUDr. Milan Kocík, MBA, LL.M.

Key words: phishing, cybercrime, prevention, internet

This bachelor's thesis focuses on the analysis and research of cybercrime, specifically phishing attacks. The thesis addresses the theoretical aspects of phishing, including its definition, development, and legal regulation in the Czech Republic. It further discusses criminological and forensic aspects, such as types of phishing, victim profiles, offender motivations, and their modus operandi. It also analyzes the procedures used by law enforcement authorities in investigating these attacks and securing evidence. The practical part of the thesis examines specific cases of cybercrime committed through phishing and summarizes current preventive and investigative methods. The aim of the thesis is to propose measures to enhance the protection of users against this type of cybercrime.

Obsah

Úvod

Digitální technologie se v současné době staly neoddělitelnou součástí každodenního života a výrazně ovlivnily způsoby, jakými lidé komunikují, pracují, učí se a obchodují. Internet jako klíčový faktor těchto technologií umožňuje téměř okamžitý přístup k informacím a službám z celého světa. Přestože digitální technologie přináší řadu výhod, její rozmach je zároveň doprovázen rostoucím počtem kybernetických hrozeb, které ohrožují bezpečnost jednotlivců, organizací i veřejných institucí.

Jednou z nejrozšířenějších a nejnebezpečnějších forem kybernetické kriminality je phishing, který představuje sofistikovanou metodu zaměřenou na manipulaci uživatelů s cílem získat jejich citlivé údaje, jako jsou přihlašovací informace, finanční data či osobní identifikační údaje. Statistické údaje ukazují, že phishingové útoky mají dlouhodobě rostoucí trend, přičemž jejich úspěšnost spočívá nejen v technické propracovanosti, ale také ve využívání psychologických faktorů lidského chování. Vzhledem k neustálému rozvoji phishingových útoků je zásadní nejen identifikovat současné metody kybernetických útočníků, ale rovněž analyzovat motivaci pachatelů, profil obětí a faktory, které ovlivňují úspěšnost těchto útoků.

Problematika phishingu představuje nejen závažnou hrozbu pro kybernetickou bezpečnost, ale zároveň se jedná o druh trestné činnosti, se kterou se v rámci svého profesního zaměření setkávám při vyšetřování hospodářské kriminality. Nejčastěji se setkávám se specifickou formou phishingu, tzv. inzertními podvody, tedy podvody realizovanými prostřednictvím online tržišť a sociálních platforem, jako jsou Facebook Marketplace, Bazoš, Vinted a další platformy umožňující nákup a prodej zboží. Útočníci zde vystupují jako falešní kupující či prodávající a pomocí předem naplánovaných kroků přimějí oběti k poskytnutí citlivých údajů. Často využívají podvodné platební brány, phishingové e-maily či odkazy na falešné webové stránky, jejichž prostřednictvím získávají přístup k bankovním účtům či osobním údajům uživatelů.

Tento druh phishingu se mi jeví jako relevantní z hlediska kybernetické kriminality, zejména vzhledem k rostoucí popularitě internetových tržišť a inzertních portálů, proto považuji jeho analýzu za klíčovou nejen z hlediska teoretického poznání, ale také pro praktické využití výsledků této práce v oblasti prevence.

1 Cíl a metodika bakalářské práce

Hlavním cílem této bakalářské práce je zhodnotit vybrané kriminologické a kriminalistické aspekty kybernetické kriminality, která je páchaná formou phishingových útoků. Tato práce se zaměřuje především na různé druhy phishingových útoků, motivy pachatelů, profil obětí a metody, které pachatelé využívají k jejich provádění. Vedlejším cílem je identifikovat klíčové faktory, jež přispívají k úspěšnosti phishingových útoků a na základě toho navrhnout preventivní opatření, jež by mohly zvýšit ochranu uživatelů před tímto typem kyberkriminality.

Teoretická část práce bude vypracována prostřednictvím důkladné rešerše odborné literatury a dalších dostupných zdrojů. V této části budou nejprve definovány základní pojmy, jako je kyberprostor, kybernetická kriminalita, apod. Následně bude phishing analyzován z pohledu právní úpravy České republiky. Z kriminologického a kriminalistického hlediska bude definován phishing, budou podrobně rozpracovány typy phishingových útoků a jejích vývoj v ČR, pojem profil oběti, motivace pachatelů a jejich modus operandi. Součástí teoretické části bude rovněž popsán postup policejních orgánů při prověřování případů kybernetické kriminality vyhledávání a zajišťování důkazních prostředků.

Praktická část práce se zaměří na kazuistiku konkrétních případů kybernetické kriminality spáchané prostřednictvím phishingu. Na základě analýzy získaných dat budou identifikovány klíčové faktory, jež ovlivňují úspěšnost těchto útoků, a na jejich základě budou formulována preventivní opatření. Tato opatření by měla přispět ke zvýšení ochrany uživatelů před phishingovými útoky.

2 Charakteristika základních pojmů z dané oblasti

V následující kapitole budou vysvětleny konkrétní pojmy související s daným tématem. Mezi hlavní body, které budou definovány, se řadí kyberprostor, kybernetická bezpečnost, druhy kybernetických zločinů, internet a sociální sítě.

2.1 Kyberprostor

Pro pochopení konkrétních pojmů spojených s kybernetickou kriminalitou je nezbytné nejprve objasnit samotný základ této problematiky, kterým je kyberprostor.

Jelikož je tato problematika velice obsáhlá a dost složitá na pochopení, je nutné si kyberprostor představit zjednodušeně. V každé literatuře, která se zabývá tímto tématem, je uváděna odlišná definice, avšak základ zůstává všude stejný. Jedná se o prostor, ničím neohraničený. Nerespektuje dosavadní pravidla pro realitu. Dle § 2, odst. a) Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, je kyberprostor vymezen následovně:

„*Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*[1]“

Potenciální pachatelé nemají konkrétní podobu a únik dat vně, je neomezený. Samozřejmě, že technologie v minulých letech představovaly minimální hrozby pro reálný svět a vznikaly pro člověka velice užitečné nástroje, jako jsou internet, internetové domény, emaily, sociální sítě apod. Internet jako takový, je defacto jen další fáze, která je úzce propojena s celým kyberprostorem.

Avšak s postupem let, s vývojem těchto technologií se hrozby zvyšovaly a nyní se člověk nachází v době, kdy vystupuje z virtuálního světa jistá umělá inteligence, která začíná mít na reálný svět nepředstavitelný vliv. Každý si musí uvědomit, že jakmile jednou vloží do kyberprostoru nějaká data, je téměř nemožné je někdy zcela odstranit a budou již napořád uloženy na nějakém cloudu-úložišti dat.

[1] ČESKO. Zákon č. 181 ze dne 28. srpna 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In. *Sbírka zákonů Česká republiky*. 2014, částka 75, §2, odst. a). Dostupné také z WWW: < https://www.zakonyprolidi.cz/cs/2014-181>.

Kyberprostor lze definovat jako nehmotné prostředí bez jasně vymezených fyzických hranic, které propojuje celý svět. Uživatelům poskytuje možnost anonymity, což může mít jak pozitivní, tak negativní dopady. Na jedné straně umožňuje svobodné vyjadřování názorů bez obav z postihu, na druhé straně anonymita usnadňuje páchání kyberkriminality. Přestože se jedná o virtuální prostor, je úzce propojen s reálným světem. I když kyberprostor přinesl mnoho nových možností, zároveň vyvolává rostoucí obavy o bezpečnost a nejistotu ohledně jeho budoucího vývoje.

Kyberprostor lze rozlišit na tři vrstvy. Kde první povrchová vrstva – Surface Web, je prostor který je znám pro nás všechny, klasické webové stránky internetu, které jsou volně dostupné a přístup je pro všechny stejný a neomezený. Druhá vrstva, říká se jí hlubový web – Deep Web, je už složitější. Pouhý klasický uživatel se zde již nedostane. V této vrstvě dochází k určitým změnám, nastavením, opravám aj. Přístup zde, má jen určitá skupina lidí, která pro tento vstup do kyberprostoru má oprávnění. Poslední třetí vrstva tzv. Dark Web – temný web. Na tomto webu jsou již všechny aktivity nelegální. Uživatelé, kteří k tomuto webu mají přístup, jsou na speciálním prohlížeči. Dochází zde k nelegálním obchodům, kdy si uživatel za bitcoiny může koupit a obstarat snad cokoliv – drogy, zbraně, dětskou pornografii či dokonce si najmout vraždu.[2]

2.2 Kybernetická bezpečnost

Vzhledem k tomu, že se nacházíme v době, kdy je společnost prakticky závislá na informačních technologiích a většina každodenních provozních záležitostí se bez této činnosti neobejde, společnost se musí umět bránit. Každý z nás se během dne setká s různými aktivitami, a když se nad tím zamyslíme, vždy narazíme na propojení s informačními technologiemi. Stačí zmínit pouhé využití svého mobilního telefonu s neomezeným přístupem k internetu nebo bezkontaktní placení - ať už debetní či kreditní kartou, chytrým telefonem, hodinkami či prstenem.

Pro celou EU[3] vznikla v rámci této ochrany ENISA (European Network and Information Security Agency)[4]. Tato společnost klade na důraz právě ochranu společnosti před nebezpečím v rámci informačních sítích. [5] V České Republice vznikl 1. srpna 2017

[2] Národní centrum průmyslu 4.0. Kybernetická válka. *Ncp40.cz* [online]. © 2025 [cit. 2025-02-20]. Dostupné z WWW: <https://www.ncp40.cz/aktuality/kyberneticka-valka>.
[3] Evropská Unie.
[4] Evropská agentura pro informační a síťovou bezpečnost.
[5] JANSA, L.; OTEVŘEL, P.; ČERMÁK, J.; MALIŠ, P.; HOSTAŠ, P. et al. *Internetové právo*. Brno: Computer Press, 2016. s 416.

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) společně s novou přepracovanou verzí zákona pro kybernetickou bezpečnost - Zákon č. 205/2017 Sb., kterým se měnil zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Takto Českou Republiku chránila legislativa od roku 2015. Od srpna roku 2017 se tedy přidala k ochraně a také boji s kyberkriminalitou v České Republice společnost NÚKIB. Jedná se o hlavní orgán, který řeší bezpečnost před kybernetickou kriminalitou. Nyní v čele tohoto orgánu je Ing. Lukáš Kintr[6]. Jak sám uvádí ve své poslední zprávě statistik z kyberprostoru za rok 2023 – *„posláním NÚKIB je posilovat bezpečnost a odolnost České Republiky v kyberprostoru.[7]“*

Kyberprostor je stále více regulován zákony o kybernetické bezpečnosti, jako je GDPR či zákon o kybernetické bezpečnosti v ČR, a mezinárodními dohodami, kupříkladu Budapešťskou úmluvou o kyberkriminalitě. Státy a organizace, např. NATO, EU či OSN, se snaží nalézt rovnováhu mezi svobodou internetu a potřebou kybernetické bezpečnosti.

V posledních 50 letech jsme se posunuli od velkých sálových počítačů, přes minipočítače a osobní počítače, až k dnešnímu internetu a kyberprostoru. Dnes se útoky odehrávají v kyberprostoru, který je tvořen počítačovými sítěmi a jejich prvky, jako jsou další sítě, podsítě a zařízení s přidělenou IP adresou. To zahrnuje nejen počítače, ale i další zařízení schopná komunikovat pomocí protokolu TCP/IP, což je základní sada pravidel umožňující komunikaci v síti, jako je internet. Je tedy logické, že dnes hovoříme spíše o kybernetické kriminalitě než o kriminalitě počítačové - a v této souvislosti také o kybernetické bezpečnosti.[8]

Mimo konkrétní zákony, standardy a předpisy, které by přímo zabezpečovaly kyberprostor, je nutné, aby si každý člověk chránil své internetové prostředí co nejlépe. Každý kdo vlastní počítač, telefon, internetové bankovnictví, sociální sítě, emaily, apod., by měl dodržovat zásady bezpečného zacházení s těmito účty, pravidelně aktualizovat všechna zařízení, kontrolovat je proti virům a také často měnit svá přístupová hesla.

---

[6] Ředitel NÚKIB.

[7] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023*. [online] 17.07.2024. [cit. 2025-02-20]. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf>.

[8] SMEJKAL, V.; SOKOL, T.; KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. s 25.

Bezpečnost na internetu je v dnešní době opravdu důležitá. Jakým způsobem si chránit své soukromí a data sdílená na internetu, velice podrobně popisuje kniha – Bezpečný internet. Řeší se zde každá sekce zvlášť. Například samotný web Google má svou sekci „Centrum pro bezpečnost“, kde se můžeme setkat s pomocí jak svůj počítač/prohlížeč zabezpečit například pro svou rodinu a své děti.[9]

2.3 Internet

Dnes je přístup k internetu samozřejmostí v každé domácnosti. Využívat jej může prakticky každý, kdo vlastní i jen obyčejný mobilní telefon. Lidé jsou neustále připojeni, aniž by si uvědomovali, jak internet vlastně funguje a co přesně představuje.

Každý člověk má o internetu odlišnou představu, která je zpravidla ovlivněna jeho schopnostmi a konkrétními potřebami. Pro běžného uživatele je internet často spojený s vyhledávačem Google, kde může vyhledávat jakékoli informace, které ho zajímají. Dále si často vybaví sociální sítě jako Facebook, Instagram nebo TikTok, kde sleduje životy svých přátel, s nimiž může komunikovat, sdílet fotografie, nebo si prohlížet videa na YouTube a filmy na Netflixu. Díky internetu je možné nakupovat online, objednávat jídlo, poslouchat hudbu, hrát online hry s přáteli.

Internet je však mnohem komplexnější než jen nástroje pro zábavu a každodenní život. Lze ho definovat jako celosvětovou síť propojených počítačových systémů, které spolu komunikují podle stanovených pravidel, označovaných jako protokoly. Tato síť je tvořena mnoha menšími sítěmi, které spolu vzájemně komunikují a umožňují přenos dat mezi různými zařízeními.[10]

Ačkoli pro mnoho lidí internet představuje především nástroj zábavy, s postupujícím vývojem a novými technologiemi, včetně nástupu umělé inteligence, se očekává, že jeho vliv bude stále silnější a promění způsob, jakým žijeme.

2.3.1 Historie Internetu ve světě

Vznik samotného internetu se váže už k roku 1945, kdy se objevil článek v americkém časopise od slavného amerického politika Vannevara Bushe, ten zde zmiňoval počítače a jejich využití ke komunikaci. Tento fakt, dále vedl k vytvoření

[9] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Průvodce. Praha: Grada Publishing, 2015. s. 108.
[10] BURIAN, P. *Internet inteligentních aktivit*. Průvodce. Praha: Grada, 2014. s 336.

informační vědy jako takové. V následujících letech se v souvislosti s internetem nic zásadního nedělo. Hlavním podnětem pro vytvoření internetu, byl Sputnik 1 – první uměla družice ze Sovětského Svazu. Dne 4. října 1957, kdy byla družice vypuštěna do kosmu, dostali USA „studenou sprchu“ a uvědomili si, jak moc jsou s vývojem technologií pozadu. Tamní členové vlády, tedy začali co nejdříve řešit změny.

Vznikla agentura ARPA[11] zabývající se speciálním výzkumem. Později roku 1968 došlo k propojení čtyř počítačů amerických univerzit. Pro tuto počítačovou síť byl použit o rok později 1969 název ARPANET[12]. V této chvíli nikdo, z účastněných se na tomto projektu, neočekával tak rychlý pokrok dopředu. Bohužel se v těchto technologiích objevilo mnoho slabin a nedostatků, a tím se staly cílem pro vznik nelegálních aktivit. Všechny tyto nelegální aktivity probíhají právě přes tyto technologie a počítačové sítě.[13]

Faktem pro tato selhání je ten, že výpočetní technika a telekomunikace se stihly z jejich většiny posunout právě během druhé poloviny minulého století. Na tuto rychlost vývoje lidská společnost nemohla stačit a začala tak s odstupem času, za technologiemi bohužel zaostávat.

2.3.2 Historie Internetu v České Republice

Historie internetu pro Českou Republiku se váže k datu 13. února 1992, konkrétně tedy pro Československo. Vznikl projekt FESNET[14] a později po rozpadu Československa se název projektu změnil na CESNET. Začátky byly opravdu těžké a přenos dat byl velice pomalý.[15]

2.4 Kybernetický zločin a jeho druhy

Internetových zločinů existuje celá řada. Každý úkon má svůj název a často se liší i nepatrnými detaily. Pro představu jsou vysvětleny pouze některé z nich, zatímco několik dalších je zmíněno a přiblíženo jen okrajově.

- Obecná majetková kriminalita – zjednodušeně lze tento zločin popsat jako krádež věci movité. Pachatel spáchá zločin na poškozeném tak, že se

[11] Advanced Research Projects Agency.
[12] Advanced Research Projects Agency NETwork.
[13] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s 15.
[14] Federal Educational and Scientific Network.
[15] CZ.NIC. Jak na Internet. *Nic.cz* [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: < https://www.jaknainternet.cz/page/1205/historie-internetu/>.

dopustí neoprávněného užívání cizí věci, kdy se v tomto případě hovoří hlavně o internetovém připojení.

- Průmyslová špionáž – v tomto případě jde o zneužití dat, nabourání systému nebo celkovou krádež veškerých informací jistých podnikatelských subjektů, firem či státu. Může k tomu dojít skrz pracovníky, kteří systém a únik dat ze společnosti přímo ventilují vně nebo se může jednat o napadení zvenčí různými hackery. Důležité pro tento druh činu je právě to, že se jedná o cílený útok na systém nebo zneužití dat.

- Hacking – pro širokou veřejnost velice známý druh internetové kriminality. V tomto případě jde o proniknutí do systému jinou cestou, než tou legální. Dojde z většiny případů k překonání bezpečnostních opatření a ke krádeži dat uvnitř počítače.

- Phishing – z doslovného anglického překladu můžeme mluvit o „rybaření" nicméně takto tento výraz nelze chápat, ani doslovně překládat. Jedná se o spojení dvou anglických slov a to „phreaking" a „fishing". Jedná se o velice úkladnou formu internetového zločinu, kdy se pachatel snaží vylákat z poškozeného co nejvíce informací, aniž by sám tušil, že se jedná o podvod.[16]

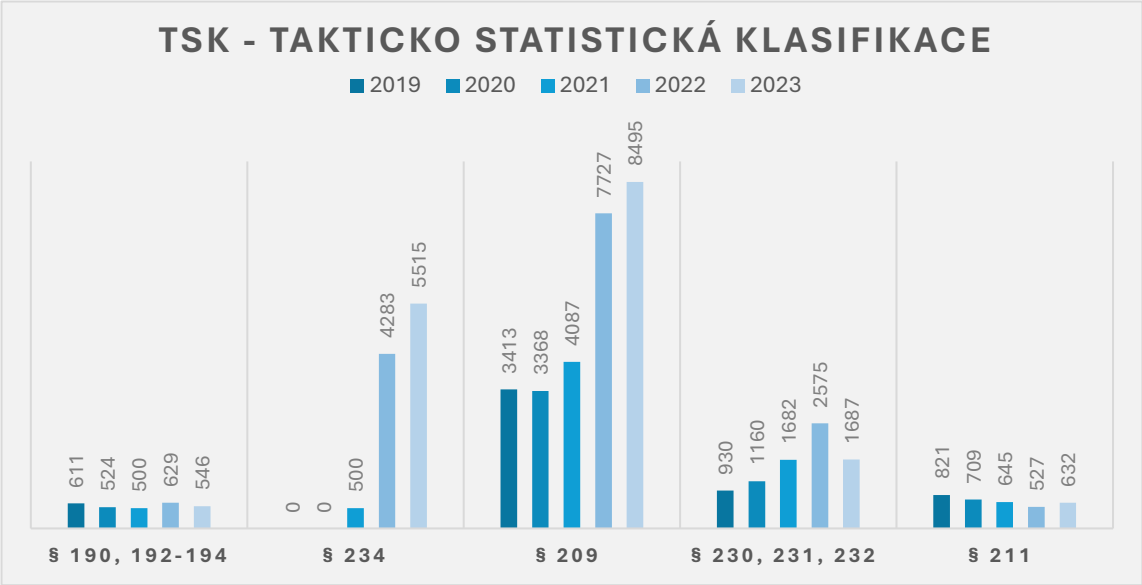
Další druhy můžeme označit jako Carding (zneužití kreditních karet na internetu), Skimming (zločiny páchané na bankomaty či platební terminály), Malware (tvorba a šíření škodlivého softwaru) a samozřejmě se najde spousta dalších.

Druhou skupinou jsou trestné činy prováděné s využitím počítačů a můžeme zařadit mezi ně tyto konkrétní případy – počítačové pirátství, podvody a zpronevěry, padělání, pomluvy, šíření pornografie, spamming (nevyžádané emailové zprávy), phreaking (zneužití telekomunikačních služeb), hoaxes (poplašené zprávy) a řadu dalších.[17]

[16] PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Tajemství. Liberec: Dialog, 2014. s 43-44.
[17] JANSA, L.; OTEVŘEL, P.; ČERMÁK, J.; MALIŠ, P.; HOSTAŠ, P. et al. *Internetové právo*. Brno: Computer Press, 2016. s 390-410.

Pro lepší orientaci v této problematice, je vždy nejlepším způsobem navštívit webové stránky Policie ČR. Zde může člověk najít opravdu veškeré detailní informace a statistické zprávy z každého roku. Díky těmto detailně zpracovaným statistikám byl mým zpracováním vytvořen níže uvedený graf, který má poukázat na pět nejčastějších případů trestné činnosti, ke kterým došlo za pomocí internetu nebo využití jiných sítích a jejich četnost v letech 2019 – 2023.

Graf 1 - Počet registrovaných případů spáchaných pomocí internetu nebo jiných sítí v ČR



Vlastní zpracování [18]

První skupinu tvoří ostatní mravnostní trestné činy a dětská pornografie a zneužití dítěte k ní (§ 190,192-194). Dalším zmíněným trestným činem je neoprávněné opatření, padělání a pozměnění platebního prostředku – platný od r. 2021 (§ 234). Nejvíce zastoupeným trestným činem ze strany využití internetu či jiné sítě, je podvod pod § 209. Trestný čin typický pro kybernetickou oblast a to neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla (§ 230, 231, 232). Posledním zmíněným a uvedeným skutkem je úvěrový podvod (§ 211).

Ve výše zmíněném grafu je použit výraz TSK nebo-li takticko-statistická klasifikace je systematické rozdělení trestné činnosti, které Policie ČR využívá v Evidenčně statistickém systému kriminality (ESSK) k evidenci a analýze kriminality.

[18] Kurzy cz. Kyberkriminalita a bezpečnost. *Zprávy.kurzy.cz.* [online]. © 2000 - 2025 [cit. 2025-02-10]. Dostupné z WWW: <https://zpravy.kurzy.cz/797436-kyberkriminalita-statistika-kriminality-na-uzemi-ceske-republiky-s-priznakem-kyberneticke/>.

2.5 Sociální sítě

Dříve neznámý pojem, později známý jen mladší generaci, a dnes již toto slovní spojení zná téměř opravdu každý bez ohledu na věk. Lze říci, že se jedná o novodobý fenomén, který je ve společnosti řešeným tématem číslo jedna.

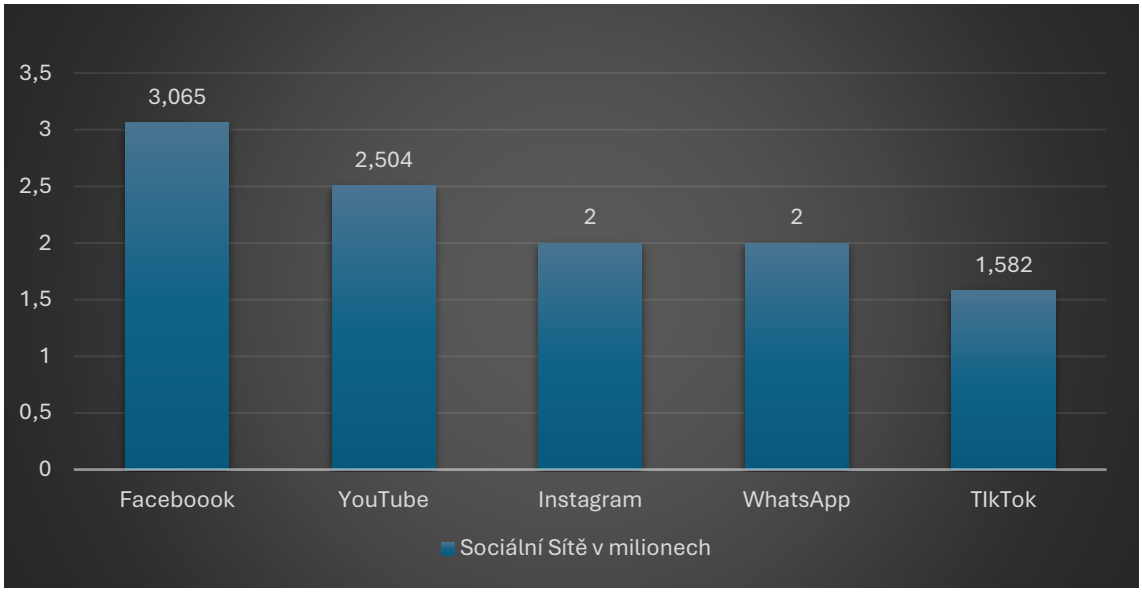
Pojem můžeme chápat jako službu, kterou můžeme provádět právě na internetu a společně s platnou registrací na konkrétních sítích umožňuje koncovému uživateli provádět jisté úkony. Mezi zmíněné úkony můžeme zmínit zakládání profilových sítí uživatelů, sdílení osobních fotografií či videí, možnost komunikace prostřednictvím chatu či jinou komunikaci mezi uživateli na konkrétních sítích. Typickou charakteristikou pro sociální síť je právě zmíněná komunikace. Nejedná se ve většině případů pouze o osobní komunikaci mezi dvěma uživateli, či uzavřenou skupinkou přátel. Základním pilířem je právě otevřenost a sdílnost mezi ostatními uživateli. Poslední dobou je tato vlastnost pro sociální síť opravdu zásadní a nejde si nevšimnout, jak se postupně tato sdílnost stává až do jisté míry nebezpečnou. Mnozí z nás, kteří takovým způsobem dávají najevo svůj nezájem a nesouhlas s druhou stranou, si neuvědomují, že stále jednají pod svou osobní identitou (tedy v některých případech) a mohou se i takto dopouštět trestných činů, i když to vypadá „že jen dávají najevo svůj názor“.[19]

Mezi nejznámější sociální sítě, které v dnešní době dominují, řadíme Facebook, Instagram, TikTok, Twitter, Linkedln nebo Youtube. Než se objevila světová síť Facebook, existovala pro Českou republiku spousta jiných sociálních sítí – Lidé.cz, Libimseti.cz, Xchat.cz aj. Pro filmové fanoušky existuje dále síť ČSFD.cz, která je lidmi navštěvována snad pokaždé, kdy se chtějí dozvědět zásadní informace k určitému filmu, seriálu či hercům.[20]

[19] JANSA, L.; OTEVŘEL, P.; ČERMÁK, J.; MALIŠ, P.; HOSTAŠ, P. et al. *Internetové právo*. Brno: Computer Press, 2016. s 351.
[20] KOŽÍŠEK, M. ; PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online*. Grada, 2016. s 24.

Níže ve zmíněném grafu lze vidět trend sociálních sítí mezi lidmi a jejich aktivní využití v roce 2024.

Graf 2 - Aktivní využití sociálních sítí v reálném čase



Vlastní zpracování [21]

Dle výše uvedených dat, lze vidět výsledek, že nejvíce používanou sociální sítí ve světě je stále Facebook. Sociální platforma, na které se lidí z celého světa mohou setkávat on-line. Pro mnohé z nás by při představě sociální sítě ani nenapadlo uvést stránky jako YouTube či aplikace jako WhatsApp.. Nicméně i tyto internetové kanály se řadí do skupiny sociálních sítí a jsou uváděny v grafu. WhatsApp je v poslední době velice oblíbeným komunikačním prostředkem mezi lidmi. Umožňuje posílání zpráv textových či hlasových, zasílání fotografií i videí a komunikace je chráněna koncovým šifrováním.

[21] Backlinko. Social Media Usage & Growth Statistics. *Backlinko.com*. [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: <https://backlinko.com/social-media-users?utm_source>.

3 Kybernetická kriminalita – kyberkriminalita

Kybernetická kriminalita má ve své podstatě mnoho různých slovních spojení a definicí. V jedné literatuře je pro toto protiprávní jednání nejvýstižnějším slovním spojením právě kyberkriminalita.[22] Dále se můžeme setkat s označením také jako kybernetická trestná činnost. Jedná se o převzetí názvu z anglického jazyka, kdy se vychází ze slova Cybercrime – překlad hovoří opět o jiném názvosloví a to Kyber zločin. Jak lze tedy vidět, označení je mnoho a konkrétní definice jednotlivých pojmů se může v detailech také mírně lišit. Dalším označením může být také internetová kriminalita, která má určitě svůj význam na pravém místě. Internet a informační technologie přinesly do společnosti a mezi populaci lidí obrovské pozitivum a vnímány byly zejména ty silné stránky. Zjednodušila se komunikace, obchody, celková informovanost a tím také vzdělanost a bohatství lidí jako takové. Jak ale už bylo výše zmíněno, s rychlostí vývoje informačních technologií se museli objevit ty slabé stránky a začaly se páchat konkrétní zločiny ve virtuálním světě.

Policií ČR je kybernetická kriminalita, dříve nazývána jako informační kriminalita, definována „*jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí.*[23]*“*

Dle Završnika, jednotná definice pro kybernetickou kriminalitu neexistuje. Nelze tedy správně a jednoznačně charakterizovat kyberkriminalitu jak v teorii či v legislativě.[24]

V oblasti informačních a komunikačních technologií existuje značná rozmanitost v názvosloví, přestože v posledních letech probíhají snahy o jeho sjednocení a přizpůsobení českému prostředí.[25]

Samotný počátek kybernetické kriminality můžeme zařadit již do osmdesátých let, kdy se pro rozvoj elektroniky a mikroprocesorů zařadil osobní počítač. S ním totiž docházelo k jistému zneužití dat, a proto se začal používat pojem „počítačová kriminalita“. Toto slovní označení se však zdálo být nezvyklé a právní teorie navrhla

[22] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s 12.
[23] Policie ČR. Kyberkriminalita. *Policie.gov.cz* [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: <https://policie.gov.cz/clanek/kyberkriminalita.aspx>.
[24] ZAVRŠNIK, A. *Kyberkriminalita*. Právní monografie. Praha: Wolters Kluwer, 2017. s 3.
[25] SEDLÁK, P.; KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. s 12.

používat označení „kriminalita spojená s počítači“. Z názvu je patrné, že aby k takovému trestnému činu mohlo dojít, musí se tedy jednat o někoho, kdo se orientuje ve výpočetní technice a autoři navrhli označení „kriminalita v informatice“. Jelikož se informační a komunikační síť rozvíjeli a objevovalo se mnoho i nových zařízení, díky kterým mohlo k trestným činům docházet, došlo se k závěru, že aby nabylo k těmto trestným činům, stává se tak v prostředí internetu a proto „internetová kriminalita“ – e-kriminalita, virtuální kriminalita nebo kriminalita na počítačových sítích. Konečným označením celé této epizody názvů a historie, je pojem kyberkriminalita – spojení slov kybernetická kriminalita. Takto je tento čin definován v Úmluvě Rady Evropy o kyberkriminalitě z roku 2001. Pojem kybernetický prostor – kyberprostor, byl prvně vysvětlen v knize Wiliiama Gibsona. Vzhledem k povaze, že se jedná o trestný čin, se vedle slova kyber – vložilo označení kriminalita.[26]

Představme si dobu, kdy svět neznal internet, ani jiné technologie, kdy pachatelé vždy museli svůj čin provádět fyzicky, pod svou identitou, s rizikem rychlého dopadení a chycení za provedený zločin. V moderní době, je možné takové trestné činy provádět prakticky bez fyzické námahy, klidně z pohodlí domova u svého počítače. Proto bylo a je nutné, uchopit tuto kriminalitu z jiného úhlu a snažit se co nejlépe celou problematiku tohoto boje s internetovou dobou pochopit.

V základu je potřeba rozlišit dvě základní kategorie počítačové kriminality a to trestná činnost proti počítači a trestná činnost spáchaná s využitím počítačů.[27] Podrobnějšímu vysvětlení jednotlivých druhů internetové kriminality bude věnována další podkapitola.

3.1 Vývoj kybernetické kriminality v ČR

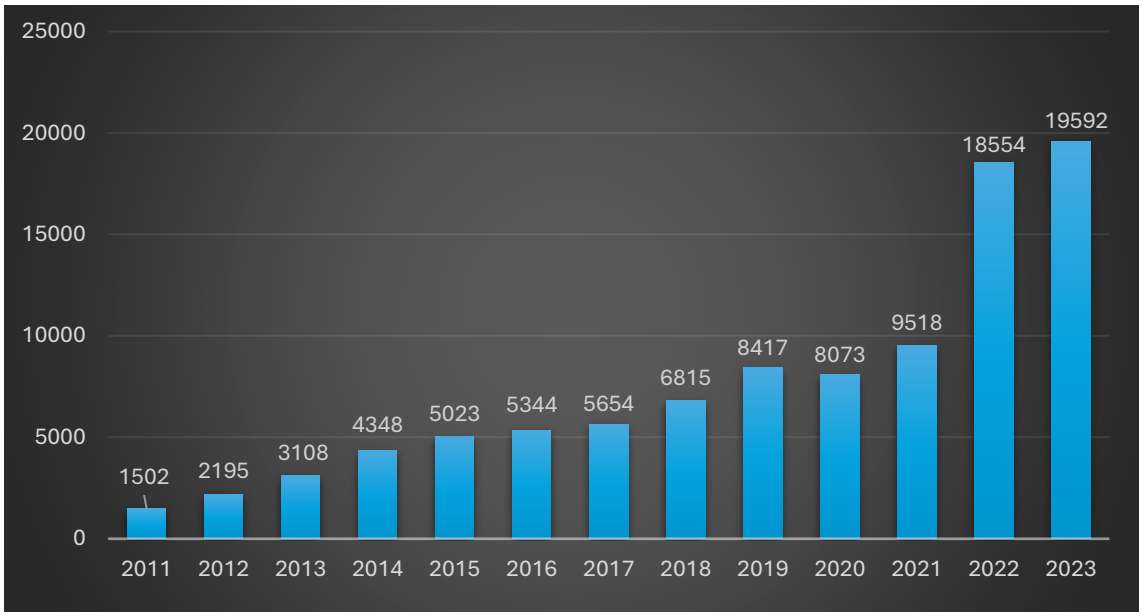
Jak lze očekávat, vývoj kyberkriminality s rozvojem technologií roste a jsou k tomu i dostupné statistiky a konkrétní čísla poukazující na fakt, že internet a trestná činnost uvnitř, je stále větší a silnější hrozbou pro reálný svět a je zapotřebí s tímto trendem udržet správný krok. V rámci této ochrany v České Republice vznikl již zmíněný NÚKIB. Jedná se o hlavní orgán pro ochranu před hrozbami v rámci kybernetické

[26] ZAVRŠNIK, A. *Kyberkriminalita*. Právní monografie. Praha: Wolters Kluwer, 2017. s 2-3.
[27] JANSA, L.; OTEVŘEL, P.; ČERMÁK, J.; MALIŠ, P.; HOSTAŠ, P. et al. *Internetové právo*. Brno: Computer Press, 2016. s 385.

kriminality a to včetně ochrany v rámci utajených zpráv v oblasti informačních, komunikačních systémů a také kryptografické ochrany.[28]

NÚKIB každoročně vydává zprávu o kybernetické bezpečnosti v České Republice s ohledem i na okolní svět. Níže uvedená tabulka znázorňuje vývoj kyberkriminality v konkrétních letech v České Republice. Policie ČR sleduje kybernetickou kriminalitu od roku 2011, kde se v České Republice objevovala jen zřídka.

Graf 3 - Vývoj kybernetické trestné činnosti v letech 2011 – 2023



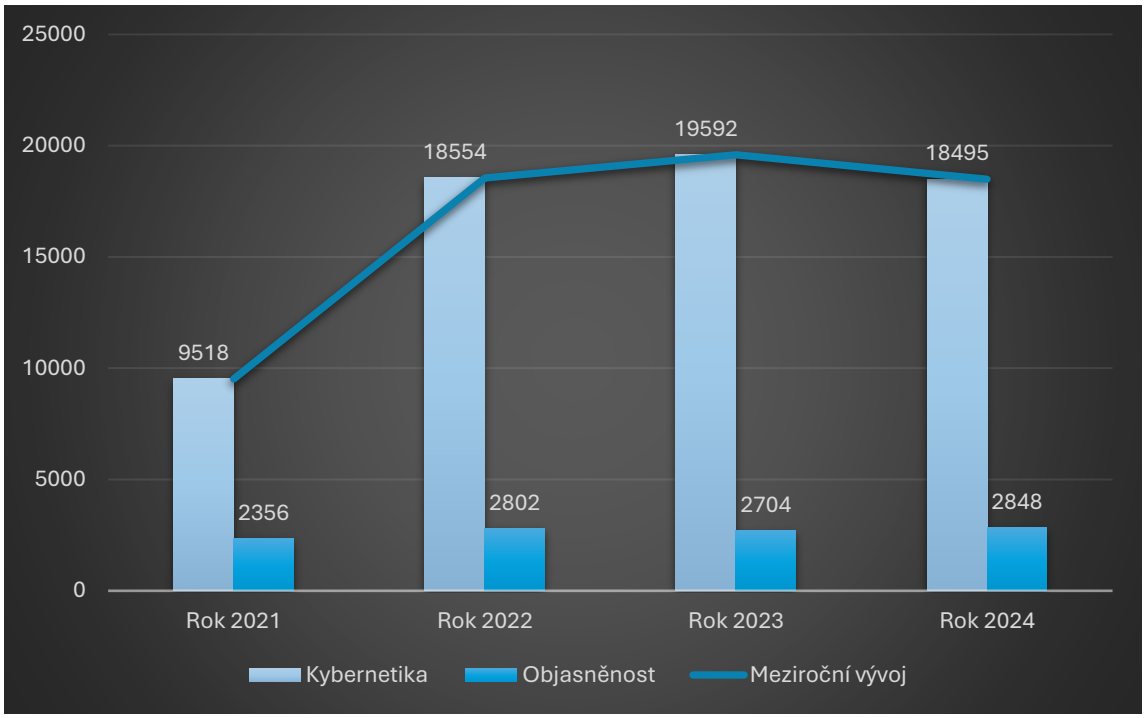
Vlastní zpracování [29]

Výše uvedená čísla slouží jako důkaz toho, že kybernetická trestná činnost ve skutečnosti neustále roste, a v posledních letech toto tempo nárůstu ještě zrychluje.

Nyní si víc přibližme poslední čtyři roky, tedy rok 2021 – 2024 s ohledem na objasněnou registrovanou kybernetickou kriminalitu a její meziroční nárust či pokles. K těmto datům může každý jedinec dojít sám, pokud navštíví oficiální webové stránky Policie ČR a bude se zajímat o vývoj registrované kriminality v konkrétních letech. Nás však zajímá pouze kriminalita v rovině kybernetické. Pro lepší přehled a orientaci, jsou zjištěné data znázorněny do grafů.

[28] Národní úřad pro kybernetickou a informační bezpečnost. O NÚKIB. *Nukib.gov.cz* [online]. [cit. 2025-02-10]. Dostupné z WWW: <https://nukib.gov.cz/cs/o-nukib/>.
[29] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023*. [online] 17.07.2024 [cit. 2025-02-20]. s. 27. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf>.

Graf 4 - Registrovaná kybernetická činnost v letech 2021 - 2024



Vlastní zpracování [30],[31]

Jak lze vidět z výše uvedeného grafu, kybernetická trestná činnost v posledních letech – zejména v letech 2021 a 2022 vzrostla o 94,9%. V dalších letech už docházelo k meziročnímu nárustu pomaleji. Mezi léty 2022 a 2023 došlo k vzestupu již pouze o 5,6% a v posledním mezidobí z roku 2023 a 2024 došlo dokonce k mírnému poklesu a to opět o cca 5,6%. Z grafu lze vidět, že vzhledem k celkovému počtu registrovaných trestných činů z oblasti kybernetiky, je stále objasněnost případů podstatně nižší a pohybuje se okolo 2-3 tis. skutků.

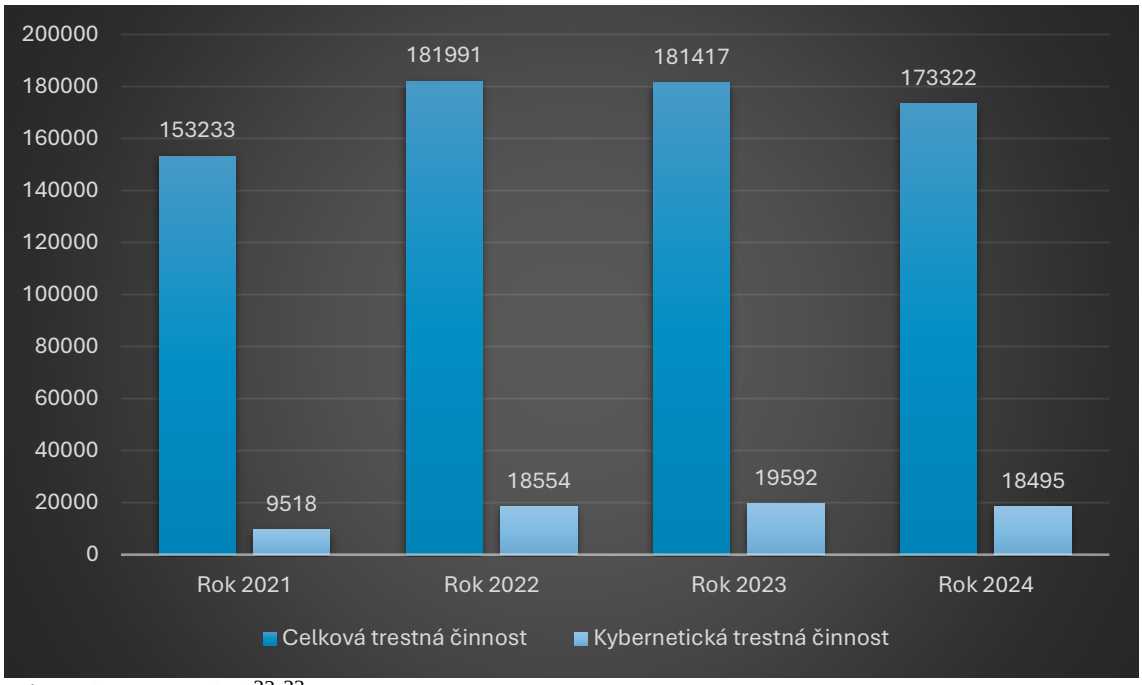
V dalším grafickém znázornění bude poukázán fakt, jak moc zasahuje kybernetická trestná činnost v posledních letech do celkové míry registrované trestné činnosti na území České Republiky. V procentuálním vyjádření to vypadalo v letech 2021 – 2024 následovně. V roce 2021 tvořila kybernetická trestná činnost 6,2% z celkové

[30] MORAVČÍK, O. *Vývoj registrované kriminality v roce 2021-2022*. [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

[31] MORAVČÍK, O., VINČÁLEK, J. Vývoj registrované kriminality v roce 2023-2024. [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>.

registrované kriminality, v roce 2022 pak 10,2%, v roce 2023 10,8% a pro rok 2024 to bylo konkrétně 10,7%.

Graf 5 - Kybernetická trestná činnost v rámci celkové kriminality na území ČR v letech 2021 - 2024



Vlastní zpracování [32],[33]

[32] MORAVČÍK, O. *Vývoj registrované kriminality v roce 2021-2022*. [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

[33] MORAVČÍK, O., VINČÁLEK, J. Vývoj registrované kriminality v roce 2023-2024. [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>.

4 Vymezení právní úpravy z pohledu trestního zákoníku

Phishing, jako forma kybernetické kriminality, není v českém trestním zákoníku výslovně definován. Nicméně, jednání spojená s phishingem lze postihovat prostřednictvím několika ustanovení trestního zákoníku. Za účelem řádného posouzení phishingu z hlediska trestního práva je nezbytné nejprve porozumět tomu, jakým způsobem a za jakých konkrétních okolností je spáchán.

Phishing může být v rámci českého trestního práva kvalifikován především podle § 209 trestního zákoníku, který upravuje trestný čin podvodu. Trestný čin podvodu v trestním zákoníku je definován v odst. 1 takto: „*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, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*[34]“

Tento paragraf je na phishing aplikovatelný poměrně jednoznačně, jelikož pachatel svým jednáním uvádí oběť v omyl s cílem získat neoprávněný finanční prospěch, nebo přístup k osobním údajům, což vede ke škodě na majetku oběti.

Dalším zákonným ustanovením použitelným v této souvislosti je § 234 trestního zákoníku, který se zabývá neoprávněným opatřením, padělání a pozměněním platebního prostředku. Tento trestný čin se skládá ze tří základních právních kvalifikací. První je naplněna, pokud pachatel bez souhlasu oprávněného uživatele obstará, zpřístupní, přijme nebo uchovává platební prostředek patřící jiné osobě. Druhá se týká případů, kdy pachatel obdobným způsobem nakládá s padělaným nebo pozměněným platebním prostředkem, bez ohledu na to, zda jedná ve svůj prospěch, či ve prospěch jiné osoby. Třetí právní kvalifikace, obsažená v odstavci třetím, vymezuje dvě samostatné roviny protiprávního jednání. V prvním případě pachatel padělá nebo pozmění platební prostředek s úmyslem užít jej jako pravý či platný. Ve druhém případě pak pachatel padělaný nebo pozměněný prostředek použije, jako by byl skutečně pravý.[35]

[34] ČESKO. Zákon č. 40 ze dne 9. února 2009 o trestním zákoníku (trestní zákoník). In. *Sbírka zákonů Česká republiky*. 2009, částka 11. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2009-40/zneni-20250211>.

[35] ČESKO. Zákon č. 40 ze dne 9. února 2009 o trestním zákoníku (trestní zákoník). In. *Sbírka zákonů Česká republiky*. 2009, částka 11. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2009-40/zneni-20250211>.

V souvislosti s phishingem dochází velmi často k neoprávněnému přístupu pachatele do internetového bankovnictví, kde následně provede platební transakci prostřednictvím příkazu k úhradě. V tomto případě jej můžeme kvalifikovat jako platební prostředek, neboť slouží k realizaci peněžního převodu. Přitom není podstatné, zda jde o fyzický platební doklad například papírový příkaz k úhradě nebo digitální platbu. Vzhledem k tomu, že právní ochrana se vztahuje i na listinné příkazy k zúčtování, nebylo by logické ani spravedlivé rozlišovat mezi různými formami téhož platebního prostředku a neposkytovat stejnou ochranu i jeho elektronické variantě. Právní systém proto musí reagovat na společenský a technologický vývoj a odpovídajícím způsobem přizpůsobovat svou regulaci.[36]

K naplnění právní kvalifikace podle ustanovení § 234 trestního zákoníku v souvislosti s phishingem dochází teprve tehdy, když pachatel na základě neoprávněně získaných údajů uskuteční platbu pomocí příslušného platebního prostředku. V rámci tohoto jednání se pachatel vydává za oprávněného uživatele, který má povolení disponovat finančními prostředky, čímž naplní znaky obsažené v odstavci třetím. V prostředí internetového bankovnictví nelze využít fyzický podpis ani pro přihlášení, ani pro autorizaci platebního příkazu. Místo něj dochází k identifikaci a schválení transakce prostřednictvím hesla a dalších autorizačních kódů, které banka zasílá majiteli účtu na mobilní telefon.

Jedním z klíčových prvků padělání v této souvislosti je využití správných přihlašovacích údajů a dalších potřebných dat bez vědomí skutečného klienta a banky, na jejichž základě dojde k vystavení platebního prostředku jinou než oprávněnou osobou. Tato situace je srovnatelná s padělám papírového příkazu k úhradě, v němž jsou veškeré náležitosti vyplněny správně, avšak podpis oprávněného držitele je dovedně nahrazen osobou, která čin padělání provádí, což vede k akceptaci příkazu bankou.[37]

Phishingové útoky využívající škodlivý software představují situaci, kdy je k phishingové zprávě připojena příloha obsahující malware. V takovém případě uživatel vědomě neposkytuje útočníkovi své citlivé údaje, neboť k jejich získání dochází prostřednictvím škodlivého softwaru, který se aktivuje po stažení či otevření přílohy.

[36] Rozsudek Nejvyššího soudu ze dne 16. května 2018, 4 Tdo 456/2018, nezveřejněný, ECLI:CZ:NS:2018. Dostupné také z WWW: <https://www.zakonyprolidi.cz/judikat/nscr/4-tdo-456-2018>.
[37] Rozsudek Nejvyššího soudu ze dne 16. května 2018, 4 Tdo 456/2018, nezveřejněný, ECLI:CZ:NS:2018. Dostupné také z WWW: <https://www.zakonyprolidi.cz/judikat/nscr/4-tdo-456-2018>.

Tento typ phishingu tak úzce souvisí s neoprávněným přístupem k počítačovému systému a nosiči informací, jak jej vymezuje § 230 trestního zákoníku. Pokud pachatel využívá malware v souvislosti s phishingem s cílem získání neoprávněného prospěchu, může být jeho jednání kvalifikováno zejména podle odstavce 3 uvedeného ustanovení.[38]

Z výše uvedeného vyplývá, že phishingové útoky v praxi nejčastěji spočívají v neoprávněném přihlášení pachatele do internetového bankovnictví, kde s využitím podvodně získaných údajů provede platební transakci, přičemž odstavec třetí § 234 trestního zákoníku, který upravuje neoprávněné opatření, padělání a pozměnění platebního prostředku představuje klíčovou právní úpravu, jejíž znaky jednání pachatele v případě phishingu naplňuje. Právě zde je podchyceno padělání či pozměnění platebního prostředku a jeho užití jako pravého, což nastává ve chvíli, kdy pachatel vystupuje jako oprávněný držitel a na základě zneužitých přihlašovacích údajů realizuje platbu. V případech, kdy je phishing provázán s malwarem, mohou být dotčena i ustanovení § 230 trestního zákoníku, neboť pachatel neoprávněně proniká do počítačového systému či nosiče informací s cílem dosáhnout majetkového prospěchu.

[38] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s 186.

5 Kybernetický zločin – Phishing

Jazykový původ k termínu phishing lze nalézt v anglickém slově „fishing“, což doslova znamená rybaření. Tato metafora je zřejmá, neboť útočník při phishingu využívá lest, tedy návnadu, kterou nabízí svým obětem s cílem je „chytnout“. Podobnost s rybolovem doplňuje skutečnost, že stejně jako rybář předpokládá, že na jeho návnadu nezareagují všechny ryby v rybníku, tak i pachatel phishingu počítá s tím, že pouze část potenciálních obětí podlehne jeho vlivu. Pro obě strany je dostačující, když alespoň některá cílová skupina zareaguje, což útočníkovi umožní dosáhnout zamýšleného finančního zisku.[39]

Základ phishingu spočívá v takzvaném sociálním inženýrství, jež využívá různé psychologické postupy k navázání důvěry oběti, která pak dobrovolně vyzradí své citlivé údaje nebo další vyžadované informace.[40]

Tento typ útoku spočívá v tom, že útočník vytváří falešné webové stránky, které se vizuálně i funkčně podobají stránkám internetového bankovnictví nebo online obchodů, přičemž hlavním cílem je neoprávněný přístup k citlivým informacím oběti.[41]

Mezi citlivé informace, na které se podvodníci zaměřují, patří zejména přístupové údaje k různým online platformám, jako jsou e-mailové služby, sociální sítě, internetové bankovnictví či e-shopy. Tyto údaje zahrnují zejména uživatelská jména a hesla, která umožňují přihlášení k osobním i firemním účtům. Dále se jedná o finanční údaje spojené s platebními kartami, jako je jejich číslo, jméno držitele, bezpečnostní CVV kód nebo PIN, jež mohou být zneužity k neoprávněným transakcím. Kromě toho se útočníci snaží získat i osobní identifikační informace, mezi které patří například celé jméno, datum narození, rodné číslo, adresa trvalého bydliště nebo čísla občanských průkazů a dalších dokladů totožnosti. Uvedené údaje mohou být zneužity k podvodnému získání identity oběti, což umožňuje útočníkům jednat jejím jménem, například uzavírat smlouvy, podávat žádosti o úvěry nebo provádět finanční podvody. Dalším častým důvodem je

[39] KRUPIČKA, J. Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi. *AUC IURIDICA.* 2012, č. 58, s. 58.
[40] JELÍNEK, J a kolektiv. *Kriminologie*. Praha: Leges, 2021. s 489.
[41] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s 246.

jejich prodej na černém trhu, kde jsou zvláště ceněné kompletní osobní údaje, které mohou být použity k dalším podvodům a trestné činnosti.

Běžný scénář phishingového útoku spočívá v tom, že oběť obdrží e-mail nebo zprávu prostřednictvím sociální sítě, která se na první pohled tváří jako oznámení od známého poskytovatele služeb, s nímž uživatel skutečně přichází do styku nebo jeho služby využívá. V textu této zprávy je adresát vyzván, aby klikl na odkaz uvedený přímo ve zprávě, který ho přesměruje na určitou internetovou stránku, kde má vyplnit požadované údaje, například k ověření totožnosti nebo potvrzení nastavení. Ve skutečnosti však tento odkaz nemá s původním poskytovatelem nic společného, pouze vzhled nebo rozložení stránky napodobuje oficiální web. Jakmile oběť na falešnou stránku vstoupí a zadá své osobní údaje, tyto se okamžitě dostanou do rukou útočníka, který je může zneužít.[42]

5.1 Vývoj Phishingu

Historické kořeny dnešního phishingu sahají do 19. století, kdy se objevily první podvodné praktiky. Autor Arthur Train v povídce z roku 1910 detailně popsal jeden z prvních příkladů podvodného jednání tohoto typu, známý jako „španělský vězeň“. V této povídce byla oběť přesvědčena o existenci mimořádně bohatého vězně, jenž byl ochoten se podělit o své bohatství. Základním prvkem celého postupu bylo zapojení prostředníka, který oběti předložil požadavek o úhradu specifikované finanční částky. Tato částka měla údajně sloužit k podplacení stráží, jež držely vězně ve vazbě. Po uskutečnění platby však oběť čelila sledu neočekávaných komplikací, kdy byly vyžadovány další finanční prostředky, což postupně vedlo ke kompletnímu vyčerpání jejích finančních zdrojů. Tento postup, založený na postupném a manipulativním získávání peněz, lze považovat za raný předobraz dnešních phishingových útoků.[43]

Jedním z prvních zaznamenaných phishingových útoků se stal případ zneužívání služby America Online (AOL) v 90. letech. V době, kdy byla AOL největším poskytovatelem internetového připojení, přihlašovaly se do její sítě miliony uživatelů denně. Její obrovská popularita však zároveň přitahovala jednotlivce se záměrem zneužít důvěřivost uživatelů a získat přístup k jejich osobním údajům. Mezi nejaktivnější patřili

[42] JELÍNEK, J a kolektiv. *Kriminologie*. Praha: Leges, 2021. s 490.
[43] KRUPIČKA, J. Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi. *AUC IURIDICA*. 2012, č. 58, s. 58-59.

členové warez komunit, kteří AOL využívali nejen k distribuci pirátského softwaru, ale také k prvním pokusům o podvodné získávání přístupových údajů.

Zpočátku se útočníci zaměřovali na krádež uživatelských hesel a používali generátory náhodných čísel kreditních karet, které jim umožňovaly zakládat falešné účty AOL. Tyto účty následně sloužily k rozesílání spamu a dalším podvodným aktivitám. Proces byl zefektivněn softwarem AOHell, který automatizoval phishingové útoky a umožňoval útočníkům snadněji manipulovat s účty uživatelů.[44]

V roce 1995 AOL na tento problém zareagovala zavedením bezpečnostních opatření, která zabránila zakládání účtů pomocí náhodně generovaných kreditních karet. Tím však phishingové útoky neskončily. Útočníci přešli na sofistikovanější metody sociálního inženýrství, kdy prostřednictvím falešných e-mailů a zpráv v AOL Instant Messengeru (AIM) oslovovali uživatele, vydávali se za zaměstnance AOL a žádali o ověření přihlašovacích údajů či platebních informací. Jelikož se jednalo o nový typ podvodu, mnoho uživatelů nepoznalo nebezpečí a na podvodné zprávy reagovalo, čímž útočníkům umožnilo přístup k citlivým údajům.[45]

Tento raný phishingový útok ukázal, jak mohou být uživatelé snadno manipulováni pomocí důvěryhodně vypadajících zpráv. Situace se zhoršila, když si podvodníci začali zakládat účty AIM přes internet, čímž se vyhnuli jednoduchému blokování ze strany AOL. V důsledku rostoucího rizika byla společnost nucena implementovat bezpečnostní varování do svých e-mailových služeb a komunikačních nástrojů, aby uživatele upozornila na možné nebezpečí. Tento případ je považován za jeden z prvních phishingových útoků, který položil základy moderním metodám kybernetických podvodů.[46]

Phishing v dnešní podobě se vyvinul z těchto prvotních podvodných technik a stal se vysoce propracovanou formou kybernetické kriminality, kde útočníci cíleně oslovují uživatele za účelem získání citlivých a následného dosažení finančního zisku. Tato postupná změna dokládá, jak se základní principy podvodného jednání dokázaly

[44] Phishing.org. History of Phishing. *Phishing.org*. [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.phishing.org/history-of-phishing>.
[45] Phishing.org. History of Phishing. *Phishing.org*. [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.phishing.org/history-of-phishing>.
[46] Phishing.org. History of Phishing. *Phishing.org*. [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.phishing.org/history-of-phishing>.

adaptovat a integrovat do nových technologií a komunikačních sítí, přičemž současné útoky jsou často zaměřeny právě na elektronické bankovnictví.

5.2 Typy phishingu

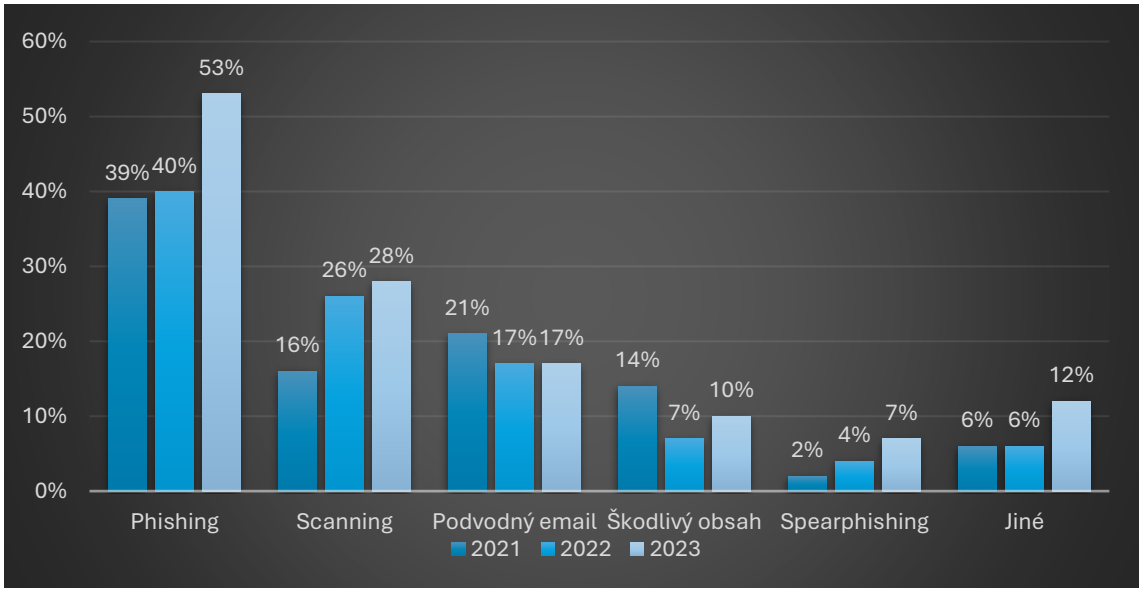
Phishing, lze klasifikovat do několika kategorií na základě použité metody útoku a specifické cílové skupiny. Různé varianty tohoto podvodu se liší způsobem, jakým útočníci oslovují oběti a jaké komunikační kanály k útoku používají, navíc útočníci své metody neustále inovují a adaptují na moderní bezpečnostní opatření a technologické pokroky.

Dle poslední zprávy vydané od NÚKIBu za rok 2023, se Česká republika setkává i s dalšími novými typy phishingu. Ve zprávě se uvádí, že v tomto směru kybernetického zločinu se jedná dlouhodobě o nejrozšířenější techniku útočníků v kybernetickém prostředí. Kvalita prováděných phishingových útoků se neustále zlepšuje a zdokonaluje. Je stále horší a těžší útoky v brzkém čase odhalit a zabezpečit tak jejich dalšímu šíření. Mezi nově se vyskytující typy phishingových útoků se uvádí vishing, smishing či quishing. Z níže uvedeného grafu lze vidět zřetelný přírůstek v této skupině útoků. Hodnoty jsou uvedeny opět ze zprávy o kybernetické činnosti z NÚKIBu pro rok 2023, kde bylo vyzváno celkem 423 respondentů jak z řad regulovaného i neregulovaného finančního trhu. [47]

Phishing jako takový, v posledních letech dominuje a nebude tomu nejspíše jinak i pro následující roky. Obecně phishing tvoří již více než 50% celkových kybernetických útoků, což jde poznat na níže uvedeném grafu. Samozřejmě, že žádné statistiky nejsou nikdy úplně věrohodné a neodpovídají skutečnosti na 100%. Ale dle něčeho se společnost musí řídit a musí konat jisté obranné kroky. Proto tyhle statistiky vyhodnocené z NÚKIBu jsou brány jako nejrelevantnější a s nimi se pak i dále pracuje.

[47] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023*. [online] 17.07.2024 [cit. 2025-02-20]. s. 6, 25. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf>.

Graf 6 - Nejčastější typy kybernetických útoků v letech 2021 - 2023



Vlastní zpracování [48]

Dle jednoho z velice používaného programu proti virům v PC, ale také i v jiných zařízeních – antivirus Eset, je níže uvedena typologie aktuální podoby phishingu.

- *E-mail phishing* – většinou se jedná o phishingový útok adresovaný větší skupině lidí a adresátů. Nejedná se nikdy o jeden konkrétní cíl, ale o mnoho adres, kde pro všechny je společné, najít slabého jedince, který se na zprávu chytí a začne s nimi spolupracovat. Může se také označovat jako bulk phishing.

- *Spear phishing* – Tady už se řeší kybernetický útok prakticky vedený „na míru“ kdy si útočník před útokem zjistí co největší množství informací o dané skupině nebo přímo o konkrétním uživateli a vede pak útok na přímo.

- *Whaling* – druh phishingových útoků, kteří se zaměřují na tzv. velké ryby, tím se myslí vysoce postavené osoby firem, manažeři, ředitelé či majitelé firem.

- *CEO fraud* – přesný opak od útoků Whalingu. Tyto útoky jsou vedeny proti všem zaměstnancům, klientům a jiným řadoým členům firem, kde původ podvodných zpráv se jeví, jako oficiální vyjádření od jejich nadřízených, hlavním partnerům a jiných.

[48] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023*. [online] 17.07.2024 [cit. 2025-02-20]. s. 15. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf>.

- *Vishing* – jednoduchým překladem lze hovořit o podvodné volání. Útočník může používat předem nahrané a namluvené zprávy. Začínal se rozšiřovat od roku 2020 kdy se tento útok začal objevovat velice často. Jedná se podvod prováděný na základně telefonického hovoru. Nejčastěji docházelo k hovorům z bank a jiných podobných institucí, kdy koncový uživatel neměl šanci rozeznat dotyčného volajícího za podvodníka. Osobně jsem se s jedním hovorem setkal. Dokážu si představit, kdy takových hovorů bylo spousty a obdržely jej starší generace – v tomto případě není šance, aby člověk reagoval racionálně a mohl si v danou chvíli uvědomit, že může jít o podvod a ihned hovor zavěsit. K tomuto typu útoku pak bez prostředně patří i pojem spoofing, kdy se jedná o napodobení jakéhokoliv telefonního čísla organizace, ze které podvodný hovor pochází.[49]

- *Smishing* – velice často v poslední době používán druh phishingového útoku i u nás. Jedná se o zasílání sms zpráv s přiloženým odkazem, kde se po otevření oběť dostává již na fiktivní podvodné stránky, kde pachatelé požadují zadat veškeré osobní údaje oběti.

- *Page hijacking* – v tomto případě se zamění originální webová stránka za falešnou. Než se tato skutečnost oznámí a řeší se celoplošně její náprava, dochází tak k vymáhání citlivých údajů přes falešné webové stránky.

- *Catfishing* – pachatel si zde zakládá smyšlený osobní profil, za účelem získání nových přátel, údajů od nich a další informace z okolí. Slouží tak k možnosti provádět kyberšikanu, podvod skrz finanční stránku či za účelem navázání kontaktů a zajišťovat pak kompromitující důkazy.[50]

5.3 Hlavní charakteristiky phishingu

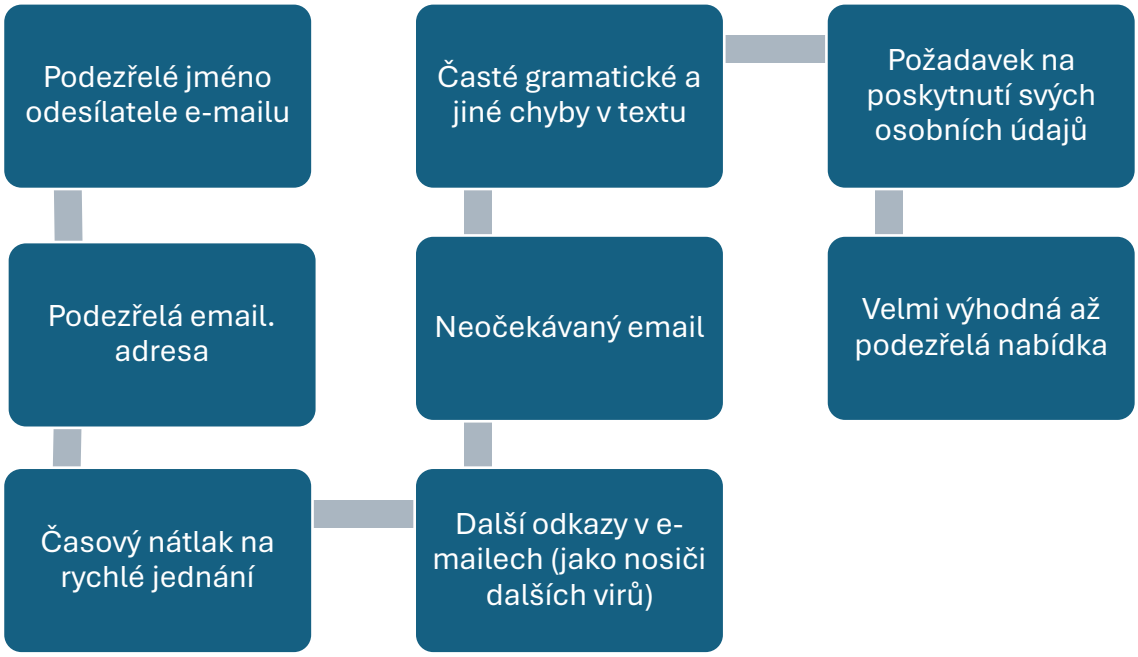
V mnoha odborných publikacích se může setkat s výkladem pojmu phishing, jeho základními typy, charakteristikou možných útoků apod.

Zkusme se zamyslet nad skutečností. V oblasti kyberprostoru a jeho bezpečnosti se dnes člověk pohybuje po velmi tenkém ledě. Aby se vyhnul podvodům a nepřišel o značné finanční prostředky, musí se neustále v této oblasti vzdělávat.

[49] Policie České republiky. Prevence. *Policie.gov.cz.* [online]. © 2025 [cit. 2025-02-28]. Dostupné z WWW: < https://policie.gov.cz/clanek/vishing-a-spoofing.aspx>.
[50] Eset. Slovník pojmů. *Eset.cz.* [online]. © 1992-2025 [cit. 2025-02-28]. Dostupné z WWW: <https://www.eset.com/cz/phishing/>.

Níže uvedené schéma, popisuje základní charakteristiku pro phishingový útok a reálně ukazuje, na co si člověk při setkání s jakýmkoliv bodem uvedeným níže, by měl dát pozor.

Obrázek 1 - Základní charakteristika pro phishingový útok



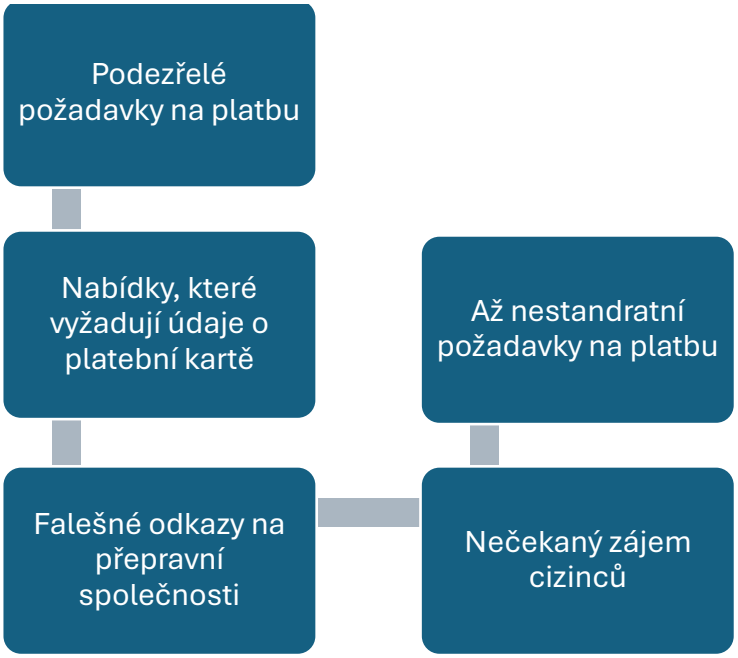
Vlastní zpracování [51],[52]

Jedním z nejčastějších phishingových útoků posledních let je tzv. bazarový podvod. Tyto útoky sdílejí společné charakteristiky, ale kvůli jejich vysoké četnosti se dále dělí na různé typy. Bazarový, neboli inzertní podvod, je velmi rozšířený a stále se ve velké míře mezi kybernetickými hrozbami pravidelně objevuje. Přestože jde vždy o tentýž scénář, jednotlivé případy se od sebe nijak výrazně neliší. Typickým znakem je podobný způsob komunikace, přičemž podvodníci vždy kladou důraz na rychlé uzavření obchodu.

[51] Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-02-28]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily>.

[52] Eset. Slovník pojmů. *Eset.cz*. [online]. © 1992-2025 [cit. 2025-02-28]. Dostupné z WWW: <https://www.eset.com/cz/phishing/>.

Obrázek 2 - Základní charakteristika pro inzertní útok



Vlastní zpracování [53]

Obě výše uvedená schémata, mají lépe upozornit na skutečnosti, se kterými se každý z nás může kdykoliv dostat do kontaktu. Pokud se jeden ze zmíněných bodů objeví, měl by člověk být na pozoru a opravdu začít přemýšlet nad reálnou hrozbou phishingového útoku.

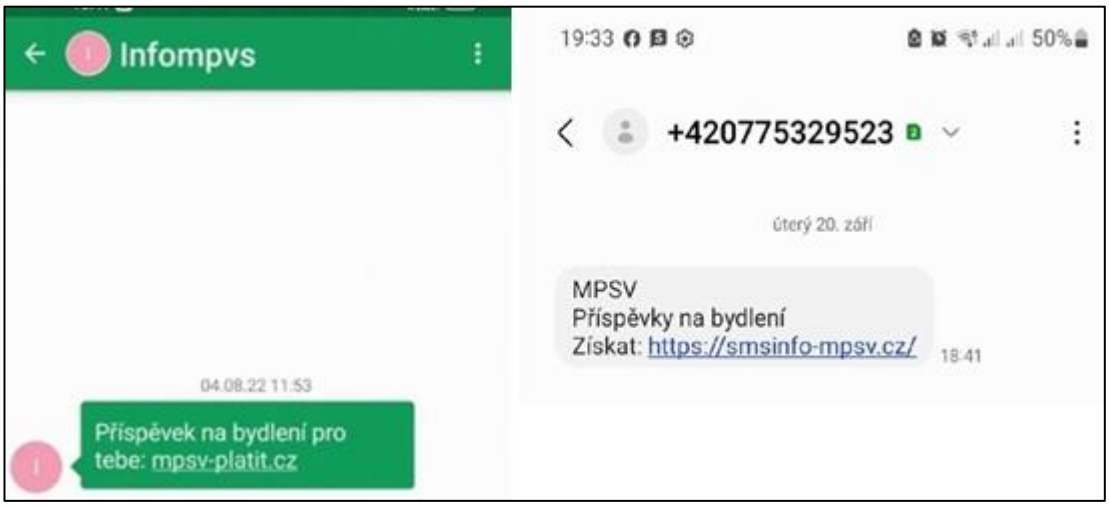
[53] Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody>.

5.4 Konkrétní příklady ve společnosti

Jak bylo zmíněno v minulé kapitole, typů phishingů je celá řada a stále se zlepšují, mění a rozšiřují. Pro lepší orientaci, aby si člověk mohl phishing jako takový představit a ve svých očích promítnout, bude níže použito pár obrázků z praxe, jak takový kybernetický útok může ve skutečnosti vypadat.

Jako první příklad si můžeme uvést velice častý typ phishingového útoku a to sms zprávou. Konkrétně se podvodné zprávy vydávaly za mpsv.cz a posílali informativní zprávy o příspěvcích na bydlení.

Obrázek 3 - Phishingový útok sms zprávou MPSV.cz

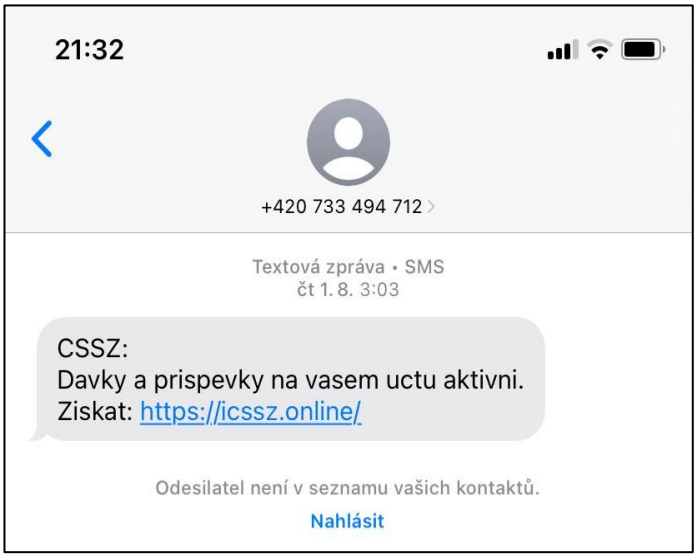


Zdroj [54]

V neposlední řadě uvedu konkrétní příklad založený na vlastní zkušenosti, kdy mi byla doručena SMS zpráva typu phishingového útoku. Viz další obrázek si lze všimnout, že po rozkliknutí daného odkazu zaslaného do sms zprávy, se konkrétnímu uživateli již zobrazí informace o phishingovém útoku. Konkrétní sms zpráva je z 1. srpna roku 2024, takže si lze všimnout, že s odstupem času, se společnost brání a snaží se veškeré nebezpečné odkazy a stránky uzavírat a širokou veřejnost poté o falešném odkazu co nejlépe informovat.

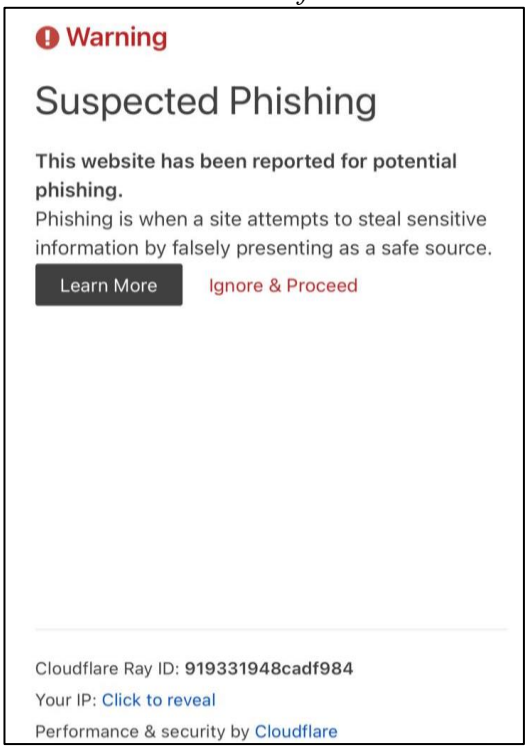
[54] Gov.cz. Český eGovernment. *Portal.gov.cz.* [online]. © 2025 [cit. 2025-02-26]. Dostupné z WWW: <https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky>.

Obrázek 4 - Phishingový útok sms zprávou CSSZ



Vlastní zpracování

Obrázek 5 - Aktuální informace na zobrazeném odkazu podvodné sms zprávy



Vlastní zpracování

Záleží také, kde si dotyčný uživatel tento již nahlášený odkaz otevře. Výše uvedený obrázek je screen z mobilního telefonu, konkrétně iPhone. Například na počítači, kde si klient platí antivirový program konkrétně ESET, dostane informativní hlášení podobné, jen s hlavičkou ESET antivirového programu, který si klade za cíl právě svého zákazníka co nejlépe od těchto útoků a případných virů ochránit.

Obrázek 6 - Příklad inzertní komunikace při podvodu

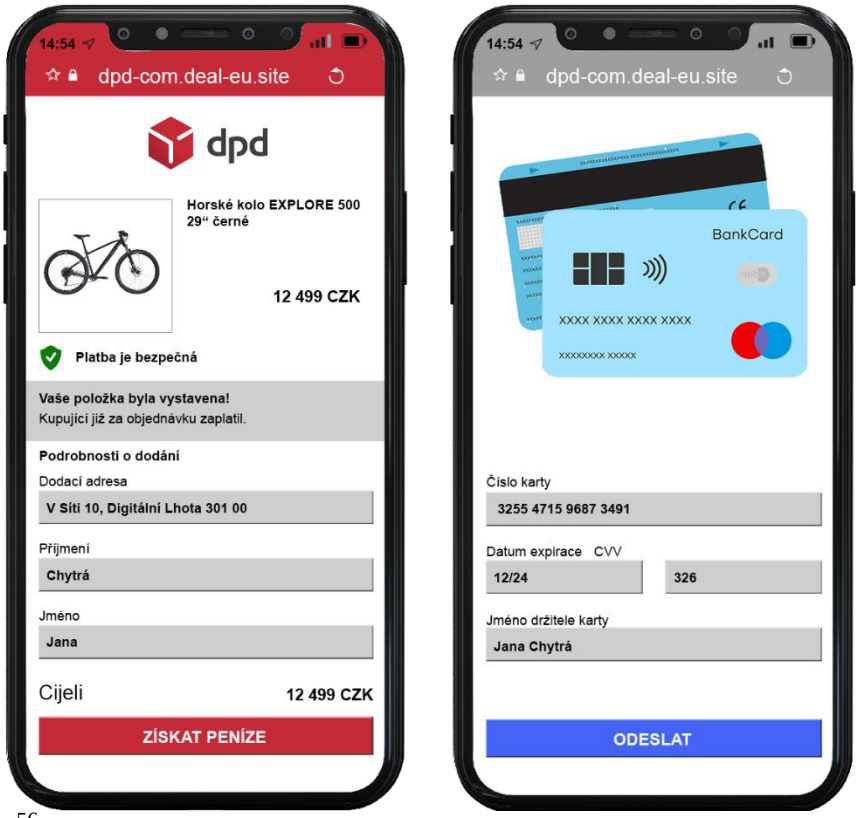
Zdroj [55]

Z přiloženého obrázku lze vidět celou komunikaci s osobou, která se dopouští kybernetického útoku. Tento typ podvodu byl a stále je velmi rozšířený. Přestože je již poměrně známý, stále existuje mnoho lidí, kteří se nechají oklamat, následují pokyny údajného kupujícího a nakonec přijdou o své finanční úspory.

Dalším příkladem je falešná webová stránka vydávající se za přepravní společnost. Odkazy na tyto stránky zasílají sami podvodníci, kteří tvrdí, že vše již bylo zaplaceno a stačí pouze zadat údaje o platební kartě pro převod peněz za zboží. Ve skutečnosti jde však o podvod, stránky jsou jen zdařilé napodobeniny.

[55] Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody>.

Obrázek 7- Příklad podvodného odkazu přepravní společnosti



Zdroj [56]

5.5 Pachatel

Na pachatele z pohledu kriminologie je nahlíženo z hlediska jeho osobnostních charakteristik, sociálního prostředí, motivace a dalších faktorů, které mohou utvářet jeho kriminální chování.

Definici pachatele podle trestního zákoníku lze formulovat na základě § 22 odst. 1 trestního zákoníku, který stanoví, že pachatelem trestného činu je osoba, jež tento čin spáchala buď samostatně, nebo ve spolupráci s další osobou. Tento právní pojem vymezuje pachatele jako subjekt, jenž naplnil skutkovou podstatu trestného činu.[57]

Avšak typologie pachatelů se značně odlišuje v závislosti na konkrétním druhu trestné činnosti. Lze předpokládat, že pachatelé phishingových podvodů budou

[56] Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody>.

[57] ČESKO. Zákon č. 40 ze dne 9. února 2009 o trestním zákoníku (trestní zákoník). In. *Sbírka zákonů Česká republiky*. 2009, částka 11. § 22, odst. 1). Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2009-40/zneni-20250211>.

disponovat odlišnými motivacemi, dovednostmi a způsoby jednání, než ti, kteří se dopouštějí šíření nelegálního obsahu, například dětské pornografie.[58]

Pachatelé phishingových podvodů, známí též jako phisheři, se vydávají za důvěryhodné subjekty s cílem přesvědčit uživatele k poskytnutí přístupu k jejich zákaznickým účtům nebo ke sdílení citlivých údajů.[59]

Výhodou je jejich schopnost se pohybovat v kyberprostoru, kde mohou snadno zůstat anonymní, měnit svou identitu nebo se vydávat za jinou osobu, což výrazně komplikuje jejich odhalení a dopadení.[60]

Jejich výhoda plyne z využívání různých anonymizačních nástrojů, například VPN (virtuální privátní sítě), které jim umožňují skrýt svou skutečnou IP adresu a tím i polohu. Zároveň je pro ně velmi snadné vytvářet falešné profily či e-mailové účty, což jim umožňuje vydávat se za někoho jiného nebo dokonce zneužívat identity reálných osob. Tato Anonymita jim navíc umožňuje jednat s pocitem bezpečí a bez přímého kontaktu s obětí. Páchání trestné činnosti prostřednictvím počítače nebo jiného zařízení určeného ke zpracování dat je pro pachatele výrazně jednodušší než v reálném světě. Na rozdíl od fyzického prostředí zde neexistuje přímý dohled ani možnost, že by byl pachatel „chycen při činu“. Nikdo jej nemůže přímo konfrontovat nebo zastavit v okamžiku spáchání trestného činu. Zároveň pachatel nevidí bezprostřední reakci oběti, což může vést k menším zábranám.

V rámci dostupných zdrojů nebyla nalezena žádná jednoznačná definice, která by se zabývala typickými charakteristikami pachatelů phishingu. Není tedy zcela jasné, zda se této trestné činnosti dopouštějí častěji muži nebo ženy, ani zda existuje určité věkové rozpětí, které by mezi pachateli převládalo. Co je však zřejmé, je skutečnost, že pachatelé phishingu musí mít alespoň základní až pokročilé znalosti práce s počítačem a internetem, zejména v oblasti digitální komunikace a manipulace s daty. Dále lze předpokládat, že hlavní motivací těchto pachatelů je finanční zisk, ať už prostřednictvím získání citlivých údajů, které následně zneužijí k přímým podvodům, nebo jejich prodejem na černém trhu.

[58] JELÍNEK, J a kolektiv. *Kriminologie*. Praha: Leges, 2021. s 485.
[59] JAMES, L. *Phishing bez záhad*. Praha: Grada, 2007. s 26.
[60] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s 19.

5.6 Oběť

Oběti trestných činů jsou předmětem zkoumání vědní disciplíny zvané viktimologie. Tato disciplína zkoumá osobnostní charakteristiky obětí, včetně jejich biologických, psychologických a sociálních rysů, analyzuje vztah mezi pachatelem a obětí, zkoumá roli oběti při vzniku, odhalování a vyšetřování trestného činu, a také se zabývá pomocí obětem, způsoby jejich odškodnění a rehabilitace.[61]

V rámci kybernetických hrozeb, kam phishing patří, se viktimologie zabývá zkoumáním, jakým způsobem se mohou lidé stát oběťmi těchto útoků. Phishing může ohrozit prakticky kohokoliv a obětí se může stát prakticky kdokoliv, od běžných uživatelů digitální technologii až po technicky zdatné jedince. Zranitelní jsou zejména lidé, kteří aktivně využívají online bankovnictví nebo často nakupují na internetu, jelikož pravidelně zadávají své citlivé osobní či platební údaje. Mezi zranitelné uživatele patří také senioři, tito často nemusí být dostatečně informováni o kybernetických rizicích a bezpečném chování na internetu. Další skupinou ohroženou phishingovými útoky jsou mladí lidé, u kterých hraje důležitou roli impulzivita nebo nižší úroveň obezřetnosti, což zvyšuje pravděpodobnost, že podlehnou manipulaci ze strany útočníků.

Úspěšnost phishingového útoku nespočívá pouze v technických znalostech oběti. Velmi důležitou roli hraje také psychický stav oběti v okamžiku útoku. Pokud je oběť pod tlakem, nebo ve stresu může snadněji podlehnout manipulaci útočníků. Právě tyto momenty snížené pozornosti útočníci cíleně vyhledávají a využívají.

V souvislosti s pojmem oběť je vhodné zmínit i pojem viktimizace – nebo-li poškozování či způsobení újmy někomu, kdo se stal obětí trestného činu. Tato viktimizace se dále dělí na primární, sekundární a terciární. Primární se děje napřímo proti směřované oběti útoku, pachatel jde napřímo proti jedné osobě/skupině/společnosti. Sekundární lze chápat jako proces, kdy pachatel poškodí někoho za účelem provést další trestný čin vůči někomu jinému. Například bude spáchán útok na banku, kdy útočník získá citlivé údaje jejich klientů a nadále s těmito údaji, bude konat útoky již na konkrétní osoby či skupiny. V poslední viktimizaci – terciární, lze chápat celkový dopad na jedince způsobený těmito útoky. Může se jednat o celkovou nedůvěru vůči elektronickým

[61] ZOUBKOVÁ, I. *Kriminologie*. Praha : Vysoká škola regionálního rozvoje Praha, 2015. s 13.

platbám, mobilům a jiným dnes již standartně používaným zařízením, které lze v této souvislosti jednoduše zneužít skrz například nedostatečné zabezpečení hesly.[62]

Jedním z nejčastějších dopadů phishingových útoku na oběť jsou ztráty v podobě finančních škod, kdy útočníci neoprávněně převedou peníze z účtu oběti, provedou nákupy bez jejího vědomí, nebo zneužijí platební kartu či přístup k bankovnímu účtu. Takové útoky mají rovněž výrazný dopad na psychiku člověka. Oběti často prožívají obavy a stres spojené s možností zneužití jejich citlivých údajů, například hesel, rodných čísel nebo jiných osobních informací. V důsledku toho se mohou cítit dlouhodobě nejisté a mohou dokonce ztratit důvěru v používání digitálních technologií nebo online služeb.

5.7 Prevence

V oblasti kyberkriminality je prevence klíčovým faktorem, neboť v mnoha případech lze útokům předejít již pouhým zvýšením informovanosti potenciálních obětí. Vzhledem k vysoké míře latentnosti kybernetické kriminality je informovanost často efektivnější než následné řešení škod způsobených útoky.[63]

Ochrana před phishingovými útoky zahrnuje kombinaci různých opatření, včetně zvyšování povědomí uživatelů a zavedení bezpečnostních opatření. Informovanost, opatrnost, pravidelné vzdělávání a správná bezpečnostní opatření mohou výrazně snížit riziko úspěšného

Jak uvádí GoodAccess ve svém článku *Phishing – co to je a jak se bránit,* jedním z nejdůležitějších kroků je pravidelné vzdělávání a informování uživatelů, aby dokázali rozpoznat podezřelé e-maily a zprávy a nestali se obětí kybernetických podvodníků. Dalším důležitým bezpečnostním prvkem je zavedení multifaktorové autentizace (MFA), která kromě hesla vyžaduje další ověření identity, což výrazně snižuje riziko neoprávněného přístupu.

Jak dále GoodAccess doporučuje, ochranu lze posílit také nasazením e-mailových filtrů, které automaticky blokují škodlivé zprávy ještě předtím, než dorazí k uživateli. Neméně důležité je rovněž DNS filtrování, které zamezuje přístupu na známé

[62] MARAS, M. *Cybercriminology.* New York: Oxford University Press, 2017. s. 3-5.
[63] JELÍNEK, J a kolektiv. *Kriminologie*. Praha: Leges, 2021. s 501.

phishingové stránky a tím minimalizuje riziko podvodu. Kombinace těchto opatření výrazně přispívá k prevenci phishingových útoků a ochraně citlivých informací.[64]

V oblasti kybernetické bezpečnosti může uživatel či organizace navštívit webovou stránku www.kybertest.cz. Tato platforma je určena k ověření znalostí a dovedností v kyberprostoru a byla vyvinuta pod záštitou NÚKIBU. Po vstupu na webové stránky si lze vybrat z několika tematických sekcí zabývajících se nejčastějšími kybernetickými riziky, například phishing, ransomware či sociální inženýrství. Každý test je doprovázen modelovými situacemi, na nichž si uživatel může vyzkoušet, zda rozpozná pokus o podvod či škodlivé chování. Po dokončení testu nástroj okamžitě poskytne zpětnou vazbu a praktická doporučení, jak identifikované nedostatky vylepšit. Díky tomu mohou uživatelé získat jasný přehled o úrovni svých znalostí a zjistit, jak mohou posílit svoji kybernetickou bezpečnost. Kybertest je zcela zdarma a je vhodný pro širokou veřejnost, kteří chtějí jednoduše a rychle vyhodnotit úroveň svých znalostí a následně zlepšit bezpečnostní návyky v online prostředí.

[64] GoodAccess. Blog. *Goodaccess.com*. [online]. [cit. 2025-03-01]. Dostupné z WWW: <https://www.goodaccess.com/cs-blog/phishing-co-to-je-obrana >.

6 Metodika prověřování policejního orgánu a zajišťování důkazních prostředků

Počítačová kriminalita je charakteristická značnou variabilitou, přičemž pachatelé po sobě obvykle nezanechávají žádné fyzické stopy, což ztěžuje jejich odhalení a identifikaci.[65]

Na rozdíl od běžné kriminality, kde lze při vyšetřování využít hmotné důkazy, jako jsou otisky prstů či DNA, v počítačové kriminalitě jsou vyšetřovatelé odkázáni především na digitální stopy, které často představují jedinou stopu vedoucí k odhalení pachatele. V těchto případech tak digitální stopy slouží jako klíčový důkazní materiál.

Digitální stopa představuje jakoukoli informaci zanechanou při používání elektronických zařízení, jako jsou soubory na disku, data v paměti počítače nebo odeslané zprávy. Tyto informace mohou být uchovány dlouhodobě na pevném disku, USB či CD, nebo pouze dočasně v operační paměti počítače, která se po vypnutí automaticky smaže.[66]

Mezi zdroje digitálních stop patří například poskytovatelé internetového připojení, mobilní operátoři, administrátoři webových stránek, finanční instituce nebo online inzertní portály. Tyto subjekty uchovávají různé informace o aktivitách uživatelů, jako jsou údaje o připojeních, provedených platbách nebo přihlášeních do účtů. Mezi tyto informace mohou spadat například IP adresy, záznamy o časech přihlášení, úpravy nastavení, pokusy o přístup k různým službám nebo proces tokenizace platební karty při jejím přidání do jiného zařízení.

Vzhledem k výše uvedeným skutečnostem postup policejního orgánů při vyšetřování phishingových útoků vyžaduje úzkou spolupráci s odborníky na informační a komunikační technologie, finančními institucemi, poskytovateli telekomunikačních a internetových služeb a také mezinárodní spolupráci. Mezinárodní spolupráce je klíčová zejména proto, že pachatelé často převádějí podvodně získané finanční prostředky na zahraniční bankovní účty nebo je směrují na kryptoměnové burzy, čímž se snaží ztížit jejich dohledání a zpětné získání.

[65] GŘIVNA, T. ; POLČÁK, R. et. al. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. s 87.
[66] SMEJKAL, V. *Kybernetická kriminalita*. 3. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s 834.

Postup policejního orgánu při prověřování a shromažďování důkazních materiálů je upraven trestním řádem, který stanovuje pravidla pro celý proces trestního řízení.

Prvním krokem při prověřování je získání vysvětlení od osob, zejména od poškozených, v souladu s § 158 odst. 6 trestního řádu. Poškozený by měl nejprve samostatně popsat okolnosti skutku a následně odpovídat na otázky vyslýchajícího policisty. V případě phishingového útoku je klíčové, aby měl vyslýchající policista odborné znalosti, které mu umožní efektivně vyhodnotit získané informace a zaměřit se na možné digitální stopy.

Dalším zásadním krokem je zajištění komunikace s pachatelem, včetně zařízení, ze kterého poškozený s pachatelem komunikoval, a to v případě, že se v zařízení mohou nacházet soubory uložené v mezipaměti aplikací. V případě, že osoba disponuje věcí, která by mohla sloužit jako důkaz, policejní orgán má podle § 78 trestního řádu právo ji vyzvat k dobrovolnému vydání této věci.

Pachatel při phishingovém útoku komunikuje s obětí prostřednictvím veřejných sítí nebo veřejně dostupných služeb elektronické komunikace, které mohou být provozovány fyzickými i právnickými osobami. Tyto služby zahrnují například mobilní operátory. V takových případech je možné od poskytovatelů těchto služeb vyžadovat provozní a lokalizační údaje. Vyžádání těchto údajů je upraveno v § 88a trestního řádu a může být realizováno pouze se souhlasem uživatele. Pokud je souhlas poskytnut, policejní orgány mohou získané informace využít k dalšímu vyšetřování a provázání s jinými důkazními materiály. Provozní a lokalizační údaje jsou pro potřeby trestního řízení uchovávány po dobu šesti měsíců.

Klíčovým zdrojem důkazů jsou také bankovní informace, protože obsahují digitální stopy související s průběhem trestné činnosti. Umožňují sledovat pohyb peněžních prostředků a způsoby jejich odčerpání. U phishingových útoků dochází ve většině případů k okamžitému odčerpání podvodně získaných finančních prostředků z bankovních účtů, což ztěžuje jejich zpětné dohledání. K urychlenému odhalení toku těchto prostředků slouží centrální evidence účtů, která umožňuje získat přehled o existenci bankovních účtů pachatelů a jejich transakcích. Návrh na vyžádání údajů z této evidence podává policejní orgán státnímu zástupci, který je následně oprávněn požadovat veškeré evidované údaje v souladu s § 6 odst. 1 písm. a) zákona č. 300/2016 Sb., o centrální evidenci účtů.

Bankovní informace jsou však chráněny bankovním tajemstvím, a proto jejich získání podléhá přísným pravidlům. K jejich vyžádání slouží § 8 odst. 2 trestního řádu, podle kterého policejní orgán podává státnímu zástupci návrh na získání informací podléhajících bankovnímu tajemství. Tento návrh musí být řádně odůvodněn a omezen pouze na nezbytný rozsah. Státní zástupce může rozsah žádosti upravit, buď jej zúžit, rozšířit, nebo žádosti nevyhovět. Bankovní informace mohou obsahovat klíčové informace o přístupu k bankovnímu účtu, jako je časový průběh podvodného jednání, IP adresy či použitá zařízení, což může výrazně přispět k odhalení pachatele.

V rámci získávání informací, na které se nevztahuje ochrana bankovního či telekomunikačního tajemství, může policejní orgán na základě § 8 odst. 1 trestního řádu vyžadovat údaje od fyzických i právnických osob. To se týká například informací webových stránkách, e-mailových schránkách, registračních údajích z herních účtů nebo z inzertních portálů. Subjekty, kterým je tato povinnost uložena, jsou povinny požadované informace poskytnout bezplatně.

Klíčový nástroj mezinárodní spolupráce při vyšetřování phishingových útoků v rámci Evropské unie je Evropský vyšetřovací příkaz, neboli zkráceně EVP. Pachatelé často převádění podvodně získané finanční prostředky na zahraniční bankovní účty nebo na kryptoměnové burzy, kdy prostřednictvím EVP je možné požádat jiný členský stát EU o provedení konkrétního vyšetřovacího úkonu, například o získání digitálních důkazů, výslech svědků, sledování finančních toků či dohledání provozních a lokalizačních údajů. EVP tak výrazně usnadňuje spolupráci mezi orgány činnými v trestním řízení a zrychluje proces získávání důkazů napříč členskými státy EU.

Vyšetřování phishingových útoků je složitý a časově náročný proces, především kvůli anonymizačním technikám, které pachatelé využívají k zakrytí své identity a pohybu podvodně získaných finančních prostředků ve prospěch zahraničních bankovních účtů, směnáren a kryptoměnových burz, což výrazně komplikuje jejich dohledání. Navzdory úzké spolupráci mezi orgány činnými v trestním řízení, finančními institucemi a dalšími subjekty zůstává odhalování pachatelů obtížné, jelikož pachatelé využívají stále sofistikovanější metody k maskování své činnosti. Tento fakt dále podtrhuje složitost celého procesu vyšetřování a ukazuje na nezbytnost mezinárodní spolupráce, právních nástrojů, jako je například Evropský vyšetřovací příkaz a neustálého rozvoje metod zaměřených na analýzu digitálních stop.

7 Praktická část

Praktická část této bakalářské práce se zaměřuje na analýzu konkrétních phishingových útoků, přičemž je zpracována formou kazuistiky. Cílem této části je detailně popsat průběh útoku, metody použité pachatelem, reakci oběti a následné kroky policie ČR v trestním řízení. Kazuistika byla zvolena jako vhodná metoda, neboť umožňuje podrobně analyzovat konkrétní případ, což poskytuje lepší pochopení mechanismu útoku a jeho širších dopadů. Na základě tohoto přístupu lze identifikovat klíčové faktory, které vedly k úspěšnému provedení phishingového útoku.

S ohledem na ochranu osobních údajů (GDPR) jsou jména a některé doplňující údaje v této práci pozměněny nebo anonymizovány, nicméně popis událostí vychází z reálných případů z praxe. Konkrétní případy byly vybrány s ohledem na jejich aktuálnost a zároveň reflektují charakteristické znaky phishingových útoků, které se v současnosti vyskytují v kybernetickém prostoru. Zpracování vybraných případů poskytne komplexní pohled na problematiku a umožní detailně rozebrat jednotlivé fáze útoku – od prvotního kontaktu s obětí až po finální dopady. Analýza konkrétních situací tak přispěje k lepšímu porozumění jejich společným znakům a umožní doporučit vhodná preventivní opatřen

7.1 Případ číslo 1

Tento případ slouží jako typická ukázka phishingového útoku, který je v současnosti jedním z nejčastějších způsobů internetového podvodu.

V tomto konkrétním případě pachatel uskutečnil útok prostřednictvím známého inzertního portálu Bazoš, kde si cíleně vytipoval běžného uživatele nabízejícího své zboží k prodeji. Obětí se stal uživatel, Tomáš Dvořák ročník 1980, který ze svého bydliště nacházejícího se na adrese 1. Máje 325 v Karviné, prostřednictvím tohoto portálu nabízel k prodeji rybářský naviják menší finanční hodnoty. Útočník, který se vydával za seriózního zájemce o zboží, vystupoval pod falešnou identitou a předstíral nemožnost osobního převzetí z důvodu geografické vzdálenosti. Navrhl proto využití údajné kurýrní služby, přičemž záměrně odkázal oběť na falešné internetové stránky, které svým vzhledem dokonale imitovaly skutečný portál služby Balíkovna.

V důsledku této manipulace oběť bez podezření vyplnila své citlivé osobní údaje, včetně čísla platební karty a přístupových údajů ke svému internetovému bankovnictví.

Pachatel tak získal kompletní kontrolu nad bankovním účtem oběti a následně zneužil získané informace k provedení neoprávněného finančního převodu, čímž způsobil oběti finanční škodu.

7.1.1 Popis průběhu útoku

Dne 15. listopadu 2024 v 12:00 hodin umístil poškozený Tomáš Dvořák ročník 1980, ze svého bydliště nacházejícího se na adrese 1. Máje 325 v Karviné, na inzertní portál Bazoš, nabídku k prodeji použitého rybářského navijáku značky Yomoshi SA 7000 za částku 350 Kč. Poškozený byl na této platformě již delší dobu registrován a využíval uživatelský účet vedený pod svým vlastním jménem. Svou nabídku zveřejnil standardním způsobem prostřednictvím přehledného formuláře, do kterého uvedl základní informace o prodávaném předmětu, včetně fotografie, krátkého popisu technického stavu navijáku a stanovené prodejní ceny.

Krátce poté, téhož dne kolem 14:00 hodin, tedy přibližně dvě hodiny po zveřejnění inzerátu, byl Tomáš Dvořák kontaktován zájemcem, který se představil pod jménem Jan Novák. Tento zájemce použil k navázání komunikace interní komunikační systém portálu Bazoš.cz a uvedl přitom emailovou adresu novakjanbazos155@gmail.com. Ve své zprávě projevil jednoznačný zájem o zakoupení navijáku, zároveň však uvedl, že osobní převzetí předmětu není možné, protože se aktuálně nachází v jiném kraji.

Jako alternativní řešení navrhl, že si zboží vyzvedne kurýrní služba a úhrada za zboží proběhne přímo převodem na bankovní účet prodávajícího prostřednictvím služby Balíkovna. Z tohoto důvodu požadoval od Tomáše Dvořáka zaslání osobních údajů, konkrétně telefonního čísla, adresy bydliště a čísla bankovního účtu. Poškozený tyto informace důvěřivě poskytl.

Následně byla poškozenému zaslána další zpráva obsahující aktivní odkaz, který vedl na internetovou stránku https://balikovna.slimrhow.com/receive/1289725558389. Tato stránka, která svým vzhledem věrohodně napodobovala skutečný web služby Balíkovna, vyzvala poškozeného k vyplnění dalších citlivých údajů – konkrétně čísla bankovního účtu, údajů z platební karty a dalších osobních informací. Tomáš Dvořák v domnění, že se jedná o oficiální platební formulář služby Balíkovna, své citlivé údaje na webu vyplnil. Bezprostředně poté byl automaticky přesměrován na falešnou přihlašovací stránku internetového bankovnictví, kde zadal také své přihlašovací údaje (uživatelské ID a heslo).

Po vyplnění a odeslání těchto údajů došlo okamžitě k automatickému odhlášení z falešné stránky. Poškozený Tomáš Dvořák se poté opakovaně, několikrát neúspěšně, zkoušel znovu se přihlásit do svého skutečného internetového bankovnictví. Po několika pokusech se mu přihlášení nakonec podařilo, přičemž zjistil, že z jeho bankovního účtu byla neoprávněně odeslána částka ve výši 35 500 Kč. Transakce byla provedena na bankovní účet s označením CT TNHH TT KB 0949942222 VN, což nasvědčovalo tomu, že finanční prostředky byly okamžitě převedeny do zahraničí a oběť se stala obětí cíleného phishingového útoku.

7.1.2 Postup pachatele a zneužité phishingové techniky

V uvedeném případě pachatel nejprve cíleně vyhledal osobu, která prostřednictvím inzertního portálu Bazoš.cz nabízela k prodeji zboží menší hodnoty. Následně vytvořil falešnou identitu vystupující pod běžným jménem „Jan Novák“ a použil e-mailovou adresu, která působila důvěryhodným dojmem. Cílem této strategie bylo vyvolat pocit bezpečí u oběti a eliminovat možné podezření.

K navázání kontaktu pachatel využil interní komunikační systém samotného inzertního portálu, čímž se snažil dále zvýšit věrohodnost své komunikace a snížit opatrnost oběti. Pro větší psychologický nátlak uvedl, že si nemůže zboží převzít osobně z důvodu vzdálenosti svého bydliště, čímž vytvořil situaci, ve které oběť měla pocit, že je nutné jednat rychle, aniž by si pečlivě ověřila důvěryhodnost jeho požadavků.

Jako řešení pachatel nabídl využití známé a běžně užívané služby Balíkovna, která mezi uživateli internetu působí velmi důvěryhodně. Tímto krokem opět snížil možná podezření oběti, která předpokládala, že transakce proběhne bezpečně a bez rizika. Pachatel však následně odeslal oběti odkaz na podvodnou webovou stránku, která věrně napodobovala oficiální web Balíkovny. Oběť v domnění, že jde o skutečnou službu, vyplnila na této stránce citlivé údaje včetně informací z platební karty a bankovního účtu.

Ihned poté byla oběť automaticky přesměrována na další falešnou stránku, tentokrát napodobující přihlašovací rozhraní jejího internetového bankovnictví. Zde pak zadala své přístupové údaje, čímž pachatel získal kompletní kontrolu nad jejím bankovním účtem. Díky tomu mohl následně provést neoprávněné finanční transakce a převést peníze oběti na vlastní účet.

Tyto techniky dohromady tvoří typický scénář phishingového útoku, který kombinuje sociální inženýrství s technickými metodami pro získání citlivých údajů obětí.

7.1.3 Postupu policejního orgánu při vyšetřování

Jedním z prvních kroků policejního vyšetřování bylo získání bankovního výpisu poškozeného, aby bylo možné přesně určit, kam byla neoprávněná platba odeslána. Po doručení a analýze výpisu bylo zjištěno, že transakce směřovala na účet vietnamské společnost Thanh Truc Kinh Bac Ltd. podnikající pod značkou DownMega. Šetřením bylo zjištěno, že tato společnost poskytuje on-line elektronický obsah. V tomto případě byl za výnos z trestné činnosti nejspíše zakoupen digitální klíč poskytnutý prostřednictvím internetu. Majitel bankovního účtu tak není pachatelem, ale obchodníkem, u něhož bylo za výnos z trestné činnosti zakoupeno zboží.

Dalším klíčovým krokem vyšetřování bylo ověření přihlášení do internetového bankovnictví poškozeného. Policie identifikovala IP adresy, ze kterých došlo k přístupu na účet, a následně provedla jejich analýzu.

Zjištění ukázala, že pachatel využíval VPN (virtuální privátní síť), což mu umožnilo skrýt svou skutečnou identitu a geografickou polohu. VPN je běžný nástroj používaný pachateli phishingových útoku k anonymizaci jejich aktivit na internetu, čímž se výrazně ztěžuje jejich vystopování.

Policejní orgán následně oslovil provozovatele platformy Bazoš.cz se žádostí o poskytnutí dostupných údajů o uživateli, který reagoval na inzerát poškozeného pod e-mailovou adresou novakjanbazos155@gmail.com

Prověřování ukázalo, že pachatel využil spoofing IP adresy, tedy techniku, která mu umožnila maskovat skutečnou identitu a geografickou polohu při připojení k serverům Bazoš.cz. Tímto způsobem mohl pachatel působit dojmem, že se připojuje z jiného místa, než kde se skutečně nacházel.

Dále bylo zjištěno, že při registraci uživatelského účtu pachatel uvedl telefonní číslo předplacené SIM karty operátora T-Mobile, což mu umožnilo zůstat v anonymitě, protože tyto SIM karty lze zakoupit a aktivovat bez nutnosti poskytnutí osobních údajů.

Vzhledem k tomu, že pachatel použil několik technik k zakrytí své identity, jako je VPN a spoofing IP adres, což mu umožnilo anonymizovat své připojení, dále využil anonymní SIM kartu a vytvořil falešné e-mailové adresy. V neposlední řadě převedl finanční prostředky na zahraniční účet, čímž zkomplikoval možnost zablokování transakce a dohledání skutečné identity se nepodařilo zjistit skutečnosti opravňující

zahájit trestní stíhání proti konkrétní osobě, a proto bylo nutné věc dle ustanovení § 159a odst. 5 trestního řádu odložit.

7.1.4 Případ číslo 2

Případ číslo 2 popisuje phishingový útok uskutečněný dne 30. září 2024 prostřednictvím sociální sítě Facebook. Pachatel vystupoval pod falešným profilem „Gilbert Naslund“ a zveřejnil na facebookové stránce univerzitního hokejového týmu BO Ostrava Vítkovice STEEL podvodný odkaz slibující živý online přenos zápasu mezi týmy Hradec Králové a Ostrava. Na tento odkaz klikl poškozený Petr Makovecký (ročník 1975) ze svého bydliště na adrese Dolní 233, Petrovice u Karviné.

Po kliknutí na odkaz byl přesměrován na falešnou stránku Hockey-Tv, kde pachatel požadoval uhrazení symbolického poplatku ve výši 1 EUR (cca 25 Kč) za přístup k vysílání. Makovecký důvěřivě zadal požadované platební údaje včetně čísla karty a CVV kódu. Pachatel následně tyto údaje zneužil a dne 3. října 2024 provedl neoprávněnou platbu ve výši 60 EUR (přibližně 1600 Kč) ve prospěch zahraničního obchodníka HPY*fitnessbill.com CAMBERLEY FR. Oběť nebyla o této transakci informována ani ji nemohla zastavit.

Celková škoda způsobená phishingovým útokem činila 1625 Kč. Tento případ názorně ukazuje, jak pachatelé využívají falešné profily, atraktivní události a manipulativní techniky k získání citlivých údajů a upozorňuje na nutnost větší obezřetnosti při online platbách a poskytování osobních informací.

7.1.5 Popis průběhu útoku

Dne 30. září 2024 kolem 19:00 hodin poškozený Petr Makovecký ze svého bydliště v obci Petrovice u Karvin, Dolní 233, prostřednictvím svého mobilního telefonu navštívil stránky „BO Ostrava Vítkovice STEEL – univerzitní hokejový tým“ na sociální síti Facebook za účelem sledování on-line přenosu hokejového utkání mezi týmy Hradec Králové a BO Ostrava. Při procházení této stránky si v komentářích všiml příspěvku zveřejněného uživatelem vystupujícím pod profilem „Gilbert Naslud“, který obsahoval odkaz slibující možnost sledování živého přenosu tohoto zápasu. Na tento odkaz poškozený bez jakýchkoliv podezření klikl.

Bezprostředně po kliknutí na uvedený odkaz byl automaticky přesměrován na neznámou internetovou stránku, na níž byl vyzván k vyplnění svých osobních údajů,

konkrétně své e-mailové adresy společně s heslem, za účelem údajné aktivace účtu, který měl umožnit přístup ke slíbenému online vysílání zápasu. Dále byla pro aktivaci vyžadována úhrada symbolického registračního poplatku ve výši 1 EUR. Poškozený Petr Makovecký, vedený snahou sledovat avizovaný přenos utkání, následně bez většího podezření vyplnil do připraveného formuláře všechny požadované údaje ze své platební karty, včetně čísla karty a CVV kódu. Ihned poté mu byla z jeho bankovního účtu skutečně odečtena částka ve výši 1 EUR. Ani přes uhrazení tohoto poplatku mu však sledování zápasu nebylo umožněno. Jelikož se jednalo pouze o zanedbatelnou částku, této situaci v danou chvíli nevěnoval další pozornost.

Teprve o několik dní později, dne 03. října 2024 přibližně ve 20:00 hodin, zjistil poškozený kontrolou svého bankovního účtu, že mu byla neoprávněně stržena další finanční částka ve výši 60 EUR (přibližně 1600 Kč). Tato platba směřovala na účet zahraničního obchodníka označeného jako HPY*fitnessbill.com CAMBERLEY FR. Poškozený ihned po tomto zjištění telefonicky kontaktoval infolinku své banky (ČSOB), kde mu bylo sděleno, že finanční prostředky již odešly na zahraniční bankovní účet. Na základě tohoto zjištění nechal poškozený okamžitě platební kartu zablokovat, aby zabránil dalším neoprávněným transakcím.

Tento útok je ukázkovým příkladem phishingového podvodu, kdy pachatel za pomoci falešných profilů na sociálních sítích, klamavých internetových odkazů a manipulativních technik sociálního inženýrství získal od poškozeného citlivé údaje, které následně využil ke krádeži finančních prostředků.

7.1.6 Postup pachatele a zneužité phishingové techniky

V tomto případě pachatel nejprve založil anonymní profil na sociální síti Facebook, díky kterému mohl bez rizika zveřejnit podvodný odkaz v komentářích na stránce univerzitního hokejového týmu BO Ostrava Vítkovice STEEL. K upoutání pozornosti fanoušků zneužil populární sportovní utkání mezi týmy Hradec Králové a Ostrava, čímž zvýšil pravděpodobnost, že uživatelé kliknou na jím připravený odkaz.

Kliknutím na odkaz byla oběť přesměrována na falešnou stránku, která vzhledově dokonale napodobovala legitimní platformu pro sledování živých sportovních přenosů. Zde byla oběť nejprve manipulativně vyzvána k zadání své e-mailové adresy a hesla, čímž pachatel mohl získat přístupové údaje oběti pro případné další zneužití.

Poté byla oběť požádána o uhrazení symbolického poplatku 1 EUR za zpřístupnění přenosu. Tato malá částka měla snížit její podezření vůči legitimnosti platby. Při platbě však oběť zadala kompletní údaje ke své platební kartě včetně čísla karty a CVV bezpečnostního kódu. Pachatel tím získal plnou kontrolu nad platebním nástrojem oběti a bez jejího vědomí následně provedl neoprávněnou transakci ve prospěch zahraničního obchodníka. Platba proběhla v režimu bez dodatečného ověření, a proto oběť neměla možnost tuto transakci včas odhalit ani zastavit.

7.1.7 **Postupu policejního orgánu při vyšetřování**

Jedním z prvních kroků policejního orgánu v rámci vyšetřování tohoto případu bylo přijetí podání vysvětlení od poškozeného Petr Makoveckého, během kterého byly zajištěny důkazní materiály v podobě screenshotů z mobilního telefonu poškozeného, zachycující odchozí platby a podvodný odkaz na sociální síti Facebook. Poškozený rovněž poskytl souhlas s poskytnutím informací chráněných bankovním tajemstvím dle § 38 zákona č. 21/1992 Sb., o bankách.

Následně policie na základě tohoto souhlasu vyžádala od bankovní společnosti ČSOB podrobný výpis transakcí z účtu poškozeného, aby mohlo být jednoznačně určeno, kam odešly neoprávněně odčerpané finanční prostředky.

Po obdržení a analýze bankovního výpisu bylo zjištěno, že neoprávněná transakce odešla na zahraniční účet společnosti HPY*fitnessbill.com CAMBERLEY FR, která poskytuje předplatná různých online služeb.

V dalším kroku policejní orgán tuto společnost oslovil se žádostí o poskytnutí konkrétních údajů či elektronických identifikátorů, které by mohly vést k identifikaci osoby pachatele, případně místa jeho připojení. Prověřením však bylo zjištěno, že společnost nedisponuje žádnými použitelnými informacemi, neboť platba proběhla automaticky přes platební bránu a pachatel pravděpodobně použil falešné nebo odcizené údaje.

Současně s výše uvedeným postupem policejní orgán provedl technickou analýzu bankovních logů, díky které bylo ověřeno, že k bankovnímu účtu poškozeného nedošlo k aktivaci žádného dalšího mobilního zařízení, ani k tokenizaci platební karty. Přístup k účtu byl tedy realizován výhradně z mobilního telefonu poškozeného –Samsung A34 5G, a pachatel operoval pouze s údaji získanými přímo od poškozeného prostřednictvím podvodné stránky.

V návaznosti na to proběhlo prověřování a analýza elektronických stop, které realizovalo specializované oddělení analytiky a kybernetické kriminality. Ani zde však nebyly získány žádné relevantní informace, které by umožnily identifikovat pachatele.

V rámci dalšího postupu policie provedla lustraci a technickou analýzu atributů použitých pachatelem – domén a profilů jako HPY*fitnessbill.com CAMBERLEY FR, hockey-Tv a realsports.broadcasts4k.com. Tato analýza byla negativní, protože se nepodařilo zjistit žádnou shodu s jinými evidovanými případy kybernetických útoků.

Dalším krokem policisté analyzovali falešný facebookový profil, který pachatel vytvořil za účelem zveřejnění podvodného odkazu. Šetřením však bylo zjištěno, že tento profil byl vytvořen anonymně, neobsahoval žádné identifikační údaje ani fotografie a byl krátce po použití deaktivován, čímž se znemožnilo jeho další sledování.

Zároveň bylo prověřeno, že domény a webové stránky využité pachatelem byly registrovány prostřednictvím anonymních hostingových služeb, které nevyžadují ověření identity, což opět znemožnilo identifikaci pachatele.

V závěrečné fázi vyšetřování policie shrnula veškeré získané poznatky a vzhledem k tomu, že ani důkladné prověření všech dostupných elektronických stop nevedlo k identifikaci konkrétního pachatele, rozhodl policejní orgán podle ustanovení § 159a odst. 5 trestního řádu věc odložit.

7.2 Analýza jednotlivých kazuistik

7.2.1 Případ č. 1:

První případ představuje typický phishingový útok realizovaný prostřednictvím inzertního portálu Bazoš.cz. Pachatel využil falešné identity, komunikoval s obětí prostřednictvím důvěryhodného kanálu, čímž snížil její podezření. Následně vytvořil falešnou naléhavou situaci (údajná geografická vzdálenost) a navrhl využití falešné, avšak důvěryhodně působící služby Balíkovna. Oběť byla manipulací přesměrována na podvrženou webovou stránku, kde poskytla citlivé platební a přístupové údaje, které pachatel následně využil k neoprávněnému převodu finančních prostředků do zahraničí.

7.2.2 Případ č. 2:

Druhý případ rovněž popisuje phishingový útok, ovšem realizovaný prostřednictvím sociální sítě Facebook. Pachatel opět využil anonymní profil a aktuální

atraktivní událost (hokejový zápas), aby nalákal oběť na podvodný odkaz vedoucí na falešnou streamovací platformu. Oběť byla přiměna zadat své platební údaje, které útočník zneužil k neoprávněnému nákupu online služby. Také v tomto případě pachatel využil automatizovaných platebních bran, anonymních domén a neověřených profilů, čímž se efektivně vyhnul identifikaci.

7.3 Vymezení společných bodů

Oba uvedené případy vykazují následující společné rysy:

Oba útoky využívají phishingové stránky věrně imitující známé a důvěryhodné služby (Balíkovna, Hockey-Tv), což vede k vysoké míře důvěřivosti obětí.

Pachatelé manipulují oběti psychologickými technikami, jako je falešná naléhavost nebo nabídka atraktivního obsahu, aby snížili jejich ostražitost.

Útočníci v obou případech použili anonymní, falešné profily či e-mailové adresy bez reálných osobních údajů.

Pachatelé využili neopatrnost obětí, které zadaly své platební údaje na falešné webové stránky, a provedli neoprávněné platby.

Oba pachatelé efektivně anonymizovali své aktivity (využití VPN, anonymních hostingů a anonymních profilů), což znemožnilo jejich identifikaci i přes spolupráci s bankovními institucemi a odbornými policejními útvary.

V obou případech byly odcizené finanční prostředky převedeny na účty zahraničních obchodníků, což dále komplikuje možnost dohledání pachatelů a jejich identifikaci.

Kvůli nedostatku relevantních elektronických stop, použití anonymizačních technik a absenci upotřebitelných údajů od obchodníků byly oba případy odloženy dle ustanovení § 159a odst. 5 trestního řádu.

7.4 Preventivní opatření

Prevence phishingových útoků vyžaduje kombinaci individuální opatrnosti uživatelů a aktivního přístupu institucí k ochraně dat a informování veřejnosti. Spojením vzdělávacích aktivit, technických opatření a systematického varování před hrozbami lze

významně snížit riziko úspěšných phishingových podvodů a ochránit uživatele před ztrátou finančních prostředků či osobních údajů.

7.5 Opatření pro uživatele

7.5.1 Zvýšení povědomí bezpečného chování na internetu

Sami uživatelé by se měli vzdělávat v rozpoznávání podezřelých e-mailů, odkazů a podvodných webových stránek.

7.5.2 Technická opatření

Pro efektivní ochranu by měli uživatelé pravidelně aktualizovat antivirové programy, jako jsou ESET nebo Avast, které poskytují spolehlivou ochranu proti malwaru a online útokům.Dále je vhodné, aby využívali bezpečnostní nástroje s ochranou proti phishingu, například Windows Defender, který pomáhá blokovat škodlivé webové stránky a podezřelé odkazy. Pro vyšší úroveň zabezpečení si mohou do prohlížeče nainstalovat rozšíření varující před nebezpečnými weby, jako je Avast Online Security, které chrání před phishingovými útoky a škodlivým obsahem.

Přihlašování do internetového bankovnictví by měli zabezpečit dvoufaktorovou autentizací (2FA). Zároveň je vhodné aktivovat si notifikace od banky prostřednictvím SMS, e-mailu nebo mobilní aplikace, aby měli okamžitý přehled o pohybech na svém účtu a mohli včas reagovat na podezřelé transakce.

7.5.3 Obezřetnost při online komunikaci a transakcích

Na sociálních sítích a inzertních portálech by měli být obezřetní vůči falešným profilům, které lze často poznat podle absence historie nebo nedostatečných informací. Při prodeji či nákupu zboží by měli vždy upřednostnit osobní předání nebo přímou platbu na účet a vyhnout se transakcím přes neověřené odkazy.

Důležitá je také důsledná kontrola doménových jmen webových stránek, než na nich zadají jakékoli citlivé údaje. Například Balíkovna používá výhradně oficiální doménu balikovna.cz, přičemž jakákoli jiná varianta může být podvodná stránka určená k phishingovým útokům.

7.6 Opatření pro instituce

7.6.1 Informování uživatelů na sociálních sítí a inzertních portálech

Banky, provozovatelé inzertních portálů i sociální sítě by se měly aktivně zapojit do informování uživatelů o rizicích phishingu. Vhodným způsobem je poskytování krátkých vzdělávacích videí či upozornění, která by se zobrazovala například při přihlášení do internetového bankovnictví nebo při vkládání inzerátu na inzertních stránkách. Zároveň je nutné umisťovat výstrahy a bezpečnostní pokyny na populární platformy typu Bazoš.cz či Facebook, aby byla co nejširší skupina uživatelů varována a bylo tak sníženo riziko, že se nechají napálit podvodnými odkazy a nabídkami.

Dalším krokem je tvorba veřejně dostupných informačních materiálů a návodů pro bezpečné chování na internetu, například prostřednictvím jednoduchých infografik a krátkých videí. Tyto materiály by měly být snadno dostupné na webových stránkách bank, portálů a dalších frekventovaných online služeb.

7.6.2 Blokování podvodných stránek

Sociální sítě a inzertní portály by měly zavést systémy pro detekci a okamžité blokování falešných profilů, podezřelých e-mailových adres a odkazů vedoucích na podvodné weby.

Závěr

Tato bakalářská práce se zaměřila na problematiku phishingových útoků, které představují jednu z nejrozšířenějších forem internetové kriminality. V úvodu byly nejprve objasněny základní pojmy spojené s phishingem, včetně různých druhů a technik, které pachatelé využívají. Dále se práce věnovala právnímu rámci, v němž jsou tyto útoky postihovány, a vysvětlila, jaké konkrétní ustanovení trestního zákoníku mohou být aplikována při stíhání pachatelů. Analytická část byla navíc podložena statistickými daty a grafy, z nichž vyplývá neustálý nárůst počtu phishingových útoků, zatímco jejich objasněnost zůstává velmi nízká.

Z analýzy praktické části vyplývá, že pachatelem využívané techniky vycházejí z vhodně zvolené legendy a především z důvěřivosti, snahy o rychlé vyřešení situace a také z nízkého povědomí uživatelů o bezpečném chování v kyberprostoru.

K účinnému zamezení phishingových útoků je nezbytné, aby se na prevenci společně podíleli jak samotní uživatelé, tak instituce zajišťující internetové a platební služby, stejně jako provozovatelé inzertních portálů a sociálních sítí. Sami Uživatelé by si měli osvojit základní zásady bezpečného chování na internetu, dbát na pravidelné aktualizace antivirových programů, používat rozšíření pro ochranu před phishingem, ověřovat pravost odkazů a profilů či využívat dvoufaktorovou autentizaci.

Neméně podstatné je i to, aby banky a provozovatelé internetových služeb aktivně zvyšovali povědomí veřejnosti prostřednictvím vzdělávacích kampaní, varovných oznámení a praktických návodů pro bezpečné chování v kyberprostoru.

Zpracovaná kazuistika umožnila podrobně nahlédnout do mechanismu phishingových útoků a identifikovat nejčastější slabiny, které pachatelé využívají. Získané poznatky lze využít pro další výzkum a mohou posloužit k nastavení účinných preventivních opatření a k lepší informovanosti uživatelů.

Seznam použitých zdrojů

Literární zdroje

1. BURIAN, P. *Internet inteligentních aktivit*. Průvodce. Praha: Grada, 2014. 336 s. ISBN 978-80-247-5137-5.
2. GŘIVNA, T. ; POLČÁK, R. et. al. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
3. JAMES, L. *Phishing bez záhad*. Praha: Grada, 2007. 281 s. ISBN 978-80-247-1766-1.
4. JANSA, L.; OTEVŘEL, P.; ČERMÁK, J.; MALIŠ, P.; HOSTAŠ, P. et al. *Internetové právo*. Brno: Computer Press, 2016. 432 s. ISBN 978-80-251-4664-4.
5. JELÍNEK, J a kolektiv. *Kriminologie*. Praha: Leges, 2021. 592 s. ISBN 978-80-7502-499-2.
6. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
7. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. 524 s. ISBN 978-80-88168-15-7.
8. KOŽÍŠEK, M. ; PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online*. Grada, 2016. 176 s. ISBN 978-80-271-9074-4.
9. KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Průvodce. Praha: Grada Publishing, 2015. 184 s. ISBN 978-80-247-5453-6.
10. KRUPIČKA, J. Phishing a problémy s jeho trestněprávní kvalifikací v teorii a praxi. *AUC IURIDICA*. 2012, č. 58, ISSN 0323-0619.
11. MARAS, M. *Cybercriminology*. New York: Oxford University Press, 2017. 448 s. 5. ISBN 978-01-90278-44-1.
12. PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Tajemství. Liberec: Dialog, 2014. 243 s. ISBN 978-80-7424-066-9.
13. SEDLÁK, P.; KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. 440 s. ISBN 978-80-7623-068-2.
14. SMEJKAL, V. *Kybernetická kriminalita*. 3. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1 166 s. ISBN 978-80-7380-849-5.

15. SMEJKAL, V.; SOKOL, T.; KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. 378 s. ISBN 978-80-7380-765-8.
16. ZAVRŠNIK, A. *Kyberkriminalita*. Právní monografie. Praha: Wolters Kluwer, 2017. 148 s. ISBN 978-80-7552-758-5.
17. ZOUBKOVÁ, I. *Kriminologie*. Praha : Vysoká škola regionálního rozvoje Praha, 2015. ISBN 978-80-87174-53-1.

Elektronické zdroje

1. Backlinko. Social Media Usage & Growth Statistics. *Backlinko.com*. [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: <https://backlinko.com/social-media-users?utm_source>.
2. CZ.NIC. Jak na Internet. *Nic.cz* [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: <https://www.jaknainternet.cz/page/1205/historie-internetu/>.
3. Eset. Slovník pojmů. *Eset.cz*. [online]. © 1992-2025 [cit. 2025-02-28]. Dostupné z WWW: <https://www.eset.com/cz/phishing/>.
4. GoodAccess. Blog. *Goodaccess.com*. [online]. [cit. 2025-03-01]. Dostupné z WWW: <https://www.goodaccess.com/cs-blog/phishing-co-to-je-obrana >.
5. Gov.cz. Český eGovernment. *Portal.gov.cz.* [online]. © 2025 [cit. 2025-02-26]. Dostupné z WWW: <https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky>.
6. Kurzy cz. Kyberkriminalita a bezpečnost. *Zprávy.kurzy.cz.* [online]. © 2000 - 2025 [cit. 2025-02-10]. *Dostupné z WWW:* <https://zpravy.kurzy.cz/797436-kyberkriminalita-statistika-kriminality-na-uzemi-ceske-republiky-s-priznakem-kyberneticke/>.
7. Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody>.
8. Kybertest. Typy podvodů. *Kybertest.cz*. [online]. © 2022 [cit. 2025-02-28]. Dostupné z WWW: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily>.
9. MORAVČÍK, O. *Vývoj registrované kriminality v roce 2021.* [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

10. MORAVČÍK, O. *Vývoj registrované kriminality v roce 2022.* [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx>.
11. MORAVČÍK, O., VINČÁLEK, J. *Vývoj registrované kriminality v roce 2023.* [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>.
12. MORAVČÍK, O., VINČÁLEK, J. *Vývoj registrované kriminality v roce 2024.* [online] Policie ČR. [cit. 2025-02-18] Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>.
13. Národní centrum průmyslu 4.0. Kybernetická válka. *Ncp40.cz* [online]. © 2025 [cit. 2025-02-20]. Dostupné z WWW: <https://www.ncp40.cz/aktuality/kyberneticka-valka>.
14. Národní úřad pro kybernetickou a informační bezpečnost. O NÚKIB. *Nukib.gov.cz* [online]. [cit. 2025-02-10]. Dostupné z WWW: < https://nukib.gov.cz/cs/o-nukib/>.
15. Phishing.org. History of Phishing. *Phishing.org.* [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.phishing.org/history-of-phishing>.
16. Policie České republiky. Prevence. *Policie.gov.cz.* [online]. © 2025 [cit. 2025-02-28]. Dostupné z WWW: <https://policie.gov.cz/clanek/vishing-a-spoofing.aspx>.
17. Policie ČR. Kyberkriminalita. *Policie.gov.cz* [online]. © 2025 [cit. 2025-02-10]. Dostupné z WWW: < https://policie.gov.cz/clanek/kyberkriminalita.aspx>.
18. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023*. [online] 17.07.2024 NUKIB [cit. 2025-02-20] Dostupné z WWW <https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf>.

Legislativní dokumenty

1. ČESKO. Zákon č. 181 ze dne 28. srpna 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In. *Sbírka zákonů Česká republiky*. 2014, částka 75, §2, odst. a). Dostupné také z WWW: < https://www.zakonyprolidi.cz/cs/2014-181>.

2. ČESKO. Zákon č. 40 ze dne 9. února 2009 o trestním zákoníku (trestní zákoník). In. *Sbírka zákonů Česká republiky*. 2009, částka 11. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2009-40/zneni-20250211>.
3. Rozsudek Nejvyššího soudu ze dne 16. května 2018, 4 Tdo 456/2018, nezveřejněný, ECLI:CZ:NS:2018. Dostupné také z WWW: <https://www.zakonyprolidi.cz/judikat/nscr/4-tdo-456-2018

Seznam zkratek

AOL – America On Line

ARPA - oblast pro parametry adresování a směrování

ARPANET - Advanced Research Projects Agency NETwork (počítačová síť)

CVV - Card Verification Value

ČSFD – Česko-slovenská filmová databáze

ČSOB – Československá obchodní banka

ČSSZ – Česká správa sociálních věcí

DNA – biologická makromolekula

ENISA - Evropská agentura pro informační a síťovou bezpečnost

ESSK – Evidenčně statistický systém kriminality

EU – Evropská Unie

EUR – oficiální měna Evropské Unie

EVP - Fenomén elektronického hlasu

GDPR - General data protection regulation (ochrana osobních údajů)

ID – Identifikační číslo

IP – Internetový protokol

MFA – vícefaktorové ověřování

MPSV – Ministerstvo práce a sociálních věcí

NATO – Severoatlantická aliance

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OSN – Organizace spojených národů

PIN - osobní identifikační číslo

SMS - Short Message Service (služba krátkých textových zpráv)

TSK – Takticko-statistická klasifikace

USB – Univerzální sériová sběrnice

VPN – Virtuální privátní síť

Seznam grafů

Seznam obrázků