UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2025 Radim Řehák

Univerzita Pardubice
Fakulta ekonomicko-správní

Analýza současné situace v oblasti phishingu

Bakalářská práce

2025 **Radim Řehák**

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Radim Řehák**
Osobní číslo:	**E22691**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Analýza současné situace v oblasti phishingu**
Zadávající katedra:	**Ústav matematiky a kvantitativních metod**

Zásady pro vypracování

Cílem práce je analyzovat současnou situaci v oblasti kyberbezpečnosti s důrazem na phishingové útoky. V rámci práce bude posouzena důležitost lidského faktoru pro úspěšnost phishingových útoků a důvody, proč jsou mají uživatelé sklony těmto útokům podléhat. Součástí práce bude rovněž ověření povědomí uživatelů o phishingu a zjištění jejich osobních zkušeností a bezpečnostních návyků. V závěru práce budou formulována doporučení, jak co nejlépe čelit phishingovým útokům.

Osnova:
- Historie phishingu.
- Typy phishingových útoků a důvody útoků.
- Následky phishingových útoků.
- Ověření povědomí uživatelů informačních technologií o phishingu.
- Doporučení, jak nejlépe čelit phishingovým útokům.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

CHAUDHARY, Sunil. Recognition of phishing attacks utilizing anomalies in phishing websites [online]. Tampere, 2012 [cit. 2021-7-20]. Dostupné z: https://trepo.tuni.fi/bitstream/handle/10024/84169/gradu06373.pdf. Diplomová práce. University of Tampere. Vedoucí práce Eleni Berki.
JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.
JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
KOLOUCH, Jan. CyberCrime. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168–15-7.
LANCE, James. Phishing bez záhad. 1. vyd. Přeložil Lubomír Moudrý. Praha: Grada, 2007. ISBN 978-80-247–1766-1.

Vedoucí bakalářské práce: **Mgr. Hana Boháčová, Ph.D.**
Ústav matematiky a kvantitativních metod

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

PROHLÁŠENÍ

Prohlašuji:
Práci s názvem **Analýza současné situace v oblasti phishingu,** jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2025 Radim Řehák v.r.

PODĚKOVÁNÍ:

Tímto bych moc rád poděkoval své vedoucí práce paní Mgr. Haně Boháčové, Ph.D. za její podporu, ochotu a konzultace, které mi pomohly při zpracování této bakalářské práce. Dále bych chtěl poděkovat především mé rodině a kamarádům, bez kterých by studium bylo mnohem náročnější.

ANOTACE

Bakalářská práce se zabývá problematikou phishingu jako jedné z nejrozšířenějších forem kybernetické kriminality. V teoretické části je představena základní terminologie související s kyberprostorem, kybernetickými hrozbami, bezpečností a kriminalitou. Dále se práce věnuje samotnému phishingu, jeho vývoji, průběhu útoku a způsobům, jakými může být proveden. Součástí textu je také rozbor možností trestněprávní odpovědnosti pachatelů. Praktická část je založena na dotazníkovém šetření, které zjišťovalo míru povědomí veřejnosti o phishingu, zkušenosti respondentů s tímto typem útoku a jejich bezpečnostní návyky. Výsledky výzkumu jsou dále analyzovány a interpretovány ve vztahu k teoretickým poznatkům. Práce si klade za cíl přispět k lepšímu porozumění problematice phishingu a zdůraznit význam prevence a informovanosti v oblasti kybernetické bezpečnosti.

KLÍČOVÁ SLOVA

Phishing, podvodné jednání, útok, kybernetická kriminalita, e-mail, internet

TITLE

Analysis of the current situation in the field of phishing

ANNOTATION

The bachelor's thesis focuses on the issue of phishing as one of the most widespread forms of cybercrime. The theoretical part introduces the basic terminology related to cyberspace, cyber threats, security, and criminal activity. Furthermore, the thesis examines phishing itself, its development, the course of an attack, and the methods by which it can be carried out. The text also includes an analysis of the possible forms of criminal liability of offenders. The practical part is based on a questionnaire survey that aimed to assess public awareness of phishing, respondents' experiences with this type of attack, and their security habits. The results of the research are further analyzed and interpreted in relation to the theoretical background. The main objective of the thesis is to contribute to a better understanding of phishing and to emphasize the importance of prevention and awareness in the field of cybersecurity.

KEYWORDS

Phishing, fraudulent behavior, attack, cybercrime, e-mail, internet.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM ZKRATEK

IoT	Internet of Things (Internet věcí)
IT	Informační technologie
NÚKIB	Národní úřad pro kybernetickou bezpečnost
DDoS	Distributed Denial of Service
SI	Systémové inženýrství
PIN	Osobní identifikační číslo
AOL	America Online
IC3	Internet Crime Complaint Center
FBI	Federální úřad pro vyšetřování
WHO	Světová zdravotnická organizace
ZIP	Souborový formát
SMS	Short Message Service
CEO	Generální ředitel společnosti
SPF	Sender Policy Framework
DKIM	DomainKeys Identified Mail
DMARC	Domain based Message Authentication, Reporting and Conformance
VOIP	Voice over Internet Protocol
CVC	Card Verification Code
CVV	Card Verification Value
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
QR	Quick Response
TZ	Trestní zákoník

ÚVOD

V době rostoucí digitalizace a závislosti na online prostředí se zvyšuje i riziko kybernetických hrozeb, z nichž jednou z nejčastějších a nejnebezpečnějších je phishing. Tato bakalářská práce se věnuje problematice phishingu jako formy kybernetické kriminality, která cílí na uživatele internetu s cílem vylákat citlivé údaje prostřednictvím podvodných praktik. V teoretické části jsou nejprve objasněny základní pojmy, jako je kyberprostor, kybernetický útok, hrozba, bezpečnost a kriminalita. Následně je podrobně analyzován samotný phishing, jeho historie, způsoby provedení útoku a manipulační techniky útočníků.

Zvláštní pozornost je věnována rozdělení phishingu na jednotlivé typy útoků, mezi které patří klasický phishing, spear phishing, whaling, CEO fraud, smishing, vishing, quishing a page hijacking. U každého typu je popsán jeho průběh, možné důsledky úspěšného útoku a doporučené způsoby ochrany. Součástí teoretické části je rovněž charakteristika vybraných forem trestněprávní odpovědnosti, které se mohou k phishingovým útokům vztahovat. Jedná se především o skutkové podstaty podvodu, neoprávněného přístupu k počítačovým systémům, opatření a přechovávání přístupových údajů nebo neoprávněné nakládání s platebními prostředky.

Praktická část práce je zaměřena na dotazníkové šetření mezi běžnými uživateli internetu. Cílem bylo zjistit jejich povědomí o phishingových útocích, osobní zkušenosti s tímto typem podvodného jednání a bezpečnostní návyky, které v digitálním prostředí uplatňují. Získaná data poskytují ucelený obraz o míře informovanosti veřejnosti a tvoří základ pro doporučení směřující k posílení prevence a zvyšování kybernetické bezpečnosti.

1. KYBERPROSTOR

Podle § 2 písm. a) se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací tvořené informačními systémy a službami a sítěmi elektronických komunikací. (Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.)

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky... Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v mysli, shluky a souhvězdí dat. Jako světla města.“ Tak popisuje kyberprostor William Gibson ve svém díle „Neuromancer“ – Kybernetická kriminalita. (Jirovský, 2007)

Tento prostor umožňuje vznik zcela nových forem interakce, komunikace a sdílení informací. S rozvojem internetu věcí (IoT), umělé inteligence a cloudových technologií se kyberprostor stává stále komplexnějším a jeho význam roste.

Zároveň je však kyberprostor vystaven rostoucím rizikům spojeným s kybernetickými hrozbami, jako jsou útoky na kritickou infrastrukturu, krádeže dat, šíření dezinformací nebo zneužívání osobních údajů. V reakci na tato rizika je kladen důraz na jeho zabezpečení a vytvoření pravidel pro jeho efektivní a bezpečné fungování, což odrážejí například národní i mezinárodní legislativy, strategie kybernetické bezpečnosti či standardy.

1.1 Kybernetický útok

Kybernetický útok, jehož cílem je poškození IT infrastruktury a získání citlivých nebo strategicky důležitých informací. Často se objevuje v souvislosti s politicky nebo vojensky motivovanými akcemi. (Jirásek, Novák, Požár, 2022)

1.2 Kybernetická hrozba

Kybernetická hrozba je potenciální příčina nežádoucího kybernetického bezpečnostního incidentu, který může způsobit škodu systémům, lidem, společnostem, organizacím nebo jiným subjektům v kyberprostoru. (Jirásek, Novák, Požár, 2022)

1.3 Kybernetická bezpečnost

Podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) je kybernetická bezpečnost definována jako „ochrana informačních systémů a jejich součástí před nelegitimními zásahy, poškozením, zneužitím nebo ztrátou, které mohou ohrozit jejich dostupnost, důvěrnost nebo integritu“. Tento pojem zahrnuje nejen technické aspekty, jako je zabezpečení sítí a systémů proti útokům, ale i procesy, právní rámce a vzdělávání, které se zaměřují na ochranu před kybernetickými hrozbami a zajištění kontinuity činností v organizacích. Kybernetická bezpečnost tedy zahrnuje prevenci, detekci, reagování na incidenty a obnovu po jejich výskytu. (NÚKIB)

Jirásek, Novák a Požár ve svém výkladovém slovníku kybernetické bezpečnosti vysvětlují kybernetickou bezpečnost jako *„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru.“*. (Jirásek, Novák, Požár, 2022)

1.4 Kybernetická kriminalita

Kybernetická kriminalita, označovaná v anglické literatuře mnohdy jako „IT crime“ nebo „cybercrime“ může velmi zjednodušeně řečeno, znamenat jakýkoliv trestný čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených. Oficiálních definicí počítačové kriminality existuje celá řada, avšak většina z nich vychází z podstaty uvedené výše. (Jirovský, 2007)

Tento fenomén je charakterizován svou komplexností, anonymitou pachatelů a globálním dosahem, což jej činí zvlášť náročným na prevenci, detekci a stíhání.

Kybernetická kriminalita má poměrně vysokou míru latence, což znamená, že oběti často ani netuší, že se staly obětí nějakého trestného činu. Často je to způsobeno tím, že se oběti bojí nebo se stydí o tom mluvit, zvlášť když jde o mravnostní delikty. To může vést k tomu, že tyto případy zůstávají neohlášeny. (Jelínek, 2021)

Pro lepší pochopení lze kybernetickou kriminalitu rozdělit do následujících třech kategorií.

1.4.1 Trestné činy zaměřené na technologie

Do této kategorie spadají činy, které přímo poškozují počítačové systémy, data nebo sítě. Příklady zahrnují hacking, šíření malwaru, útoky typu ransomware nebo DDoS (Distributed Denial of Service) útoky.

1.4.2 Trestné činy využívající technologie

Zde počítač či síť slouží jako prostředek k provedení tradičních trestných činů, například finančních podvodů jako je phishing, či krádeže identity nebo šíření nelegálního obsahu, jako jsou dezinformace či nelegální obchod.

1.4.3 Trestné činy spáchané v kyberprostoru

Tato kategorie zahrnuje trestné činy, kde je kyberprostor přímo místem jejich páchání. Typickými příklady jsou kyberšikana, online stalking, šíření extremistických materiálů nebo obchodování na darknetu.

1.5 Sociální inženýrství

Šulc uvádí, že SI je v jeho knize „Kybernetická bezpečnost“ definováno jako “technika tzv. ovlivňování, přesvědčování a manipulace s lidmi”. Osoba, která využívá tuto techniku se nazývá sociotechnik. *“Snahou sociotechnika je přesvědčit oběť, aby provedla to, co chce, nebo aby poskytla informace, které sociotechnik potřebuje, aniž by si uvědomila, že byla zneužita.”*. (Šulc, 2018)

Jirovský v knize Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koní bez tajemství zmiňuje, že „existuje mnoho definic sociálního inženýrství, které jsou si více či méně podobné. Je to umění, jak přimět ostatní lidi, aby splnili Vaše přání nebo psychologické triky hrané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému“. Na světě neexistuje žádný počítačový systém, který by nebyl závislý na lidském faktoru. To znamená, že tato bezpečnostní slabina je univerzální a nezávisí na konkrétní platformě, síti nebo typu zařízení. Každý, kdo má přístup k jakékoli části systému, ať už fyzicky nebo elektronicky, představuje potenciální bezpečnostní riziko. (Jirovský, 2007)

Národní úřad pro kybernetickou bezpečnost popisuje SI takto: „všechny techniky sociálního inženýrství jsou založeny na specifických způsobech lidského rozhodování známých jako kognitivní chyby úsudku. Tyto chyby úsudku, založené na nedokonalosti lidského mozku, jsou využívány mnoha způsoby. Jednoduše řečeno, hacker útočí na nejslabší článek

zabezpečení jakéhokoliv systému – na člověka. Proč je člověk tou největší slabinou? Protože není strojem, který lze bezpečně naprogramovat, ale živým jedincem, který jedná na základě svých zkušeností, znalostí a emocí. Útočník tak může pomocí specifické přípravy a psychologické manipulace ovlivnit některá rozhodnutí člověka tak, že provede určitou konkrétní činnost, které by se za jiných okolností nedopustil“. (NÚKIB, 2016)

Sociální inženýrství je technika manipulace, která se zaměřuje na klamání jednotlivců nebo skupin s cílem získat citlivé informace nebo je přimět k vykonání kroků, které ohrožují jejich bezpečnost. Tento pojem se často používá nejen ve spojení s hackery, ale také s různými podvodníky, kteří se snaží poškodit jednotlivce či organizace, obvykle za účelem vlastního obohacení. Definice sociálního inženýrství může být složitá, zejména při odlišení od běžných podvodů nebo při záměně s pojmem sociotechnika, který je s ním úzce spjat.

Útočníci často využívají taktiku, kdy se vydávají za důvěryhodné osoby nebo zdroje, aby získali důvěru oběti. Například se mohou představit jako zaměstnanci technické podpory a snažit se přesvědčit oběť k poskytnutí cenných informací, jako jsou hesla nebo přístupové údaje. Tyto útoky mohou mít různé formy a jsou zaměřeny na zneužívání lidských slabin k dosažení konkrétních cílů, jako je neoprávněný přístup k systémům nebo krádež dat.

Sociální inženýrství není žádnou novinkou; o tomto tématu byly napsány mnohé články a vědecké práce. Je to technika, která se opírá o znalosti psychologie a lidského chování, což ji činí velmi efektivní v kybernetickém prostoru. Hlavním principem je zmanipulovat jednotlivce tak, aby nevědomky poskytli citlivé informace nebo vykonali akce, které by normálně neudělali. Důležité je si uvědomit, že sociální inženýrství útočí na lidský faktor, který je často nejslabším článkem v bezpečnostním řetězci. Úspěšné útoky se zakládají na důvěře a emocionálních reakcích obětí, což činí tuto techniku jednou z nejzrádnějších hrozeb v oblasti kybernetické bezpečnosti.

Je nutné zmínit, že všechny tyto definice sociálního inženýrství nejsou novým jevem; techniky SI existovaly již dlouho před vznikem moderních technologií. V současném digitálním světě však nabývají na významu a sofistikovanosti, což z nich činí jednu z nejvýznamnějších hrozeb pro bezpečnost informací. Naopak, principy sociálního inženýrství se v podstatě nemění, protože jsou neoddělitelně spojeny s využíváním lidských vzorců chování. (Consilium.europa.eu)

2. PHISHING A JEHO HISTORIE

V současném digitálním světě se kybernetická kriminalita stává stále propracovanější a jednou z nejčastějších hrozeb je tzv. phishing. Tato praktika, založená na principech sociálního inženýrství, se rozšířila do takové míry, že může zasáhnout jak jednotlivce, tak velké organizace. Než se však ponoříme do konkrétních definic a charakteristik phishingu, je důležité pochopit jeho místo v širším kontextu kybernetické bezpečnosti i to, jak je spojen s manipulací lidské psychiky. V následující části se proto zaměříme na obecné vymezení pojmu phishing a jeho hlavní rysy, abychom následně mohli detailně zkoumat jeho různé formy a obranné strategie.

Dle Lance Jamese *„Prozatím si definujme primitivní metodu, jakožto způsob odeslání falšovaného e-mailu příjemci, který klamavým způsobem napodobuje legální instituci s úmyslem vyzvědět od příjemce důvěrné informace jako číslo platební karty nebo heslo k bankovnímu účtu.“* (Lance, 2007)

V knize Výkladový slovník kybernetické bezpečnosti od autorů Jirásek, Novák a Požár definují tito autoři phishing jako: *„Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN.“* (Jirásek, Novák, Požár, 2022)

Chaudhary popisuje phishing takto: *„Phishing je podvodná činnost prováděná pomocí elektronické komunikace s cílem k získání osobních údajů pro nekalé účely. Tyto informace mohou zahrnovat bankovní autentizační údaje finanční instituce, čísla sociálního pojištění, kreditní karty, údaje o bankovních účtech a údaje o účtu pro online nakupování, s jejichž pomocí phisherové obvykle podvádějí své oběti.“* (Chaudhary, 2012)

Jakobbson a Myers popisují ve své knize Phishing and Countermeasures phishing jako: *„Forma sociálního inženýrství, při níž se útočník, známý také jako phisher, pokouší podvodně získat důvěryhodné nebo citlivé přihlašovací údaje legitimních uživatelů tím, že napodobuje elektronickou komunikaci důvěryhodné nebo veřejné organizace automatizovaným způsobem.*

Taková komunikace se nejčastěji uskutečňuje prostřednictvím e-mailů, které uživatele přesměrují na podvodné webové stránky, jež následně shromažďují dotyčná pověření. Příklady pověření, o které se phisheři často zajímají, jsou hesla, čísla kreditních karet a národní identifikační čísla.“ (Jakobsson & Myers, 2006)

Phishing, jako specifická forma sociálního inženýrství zaměřená na získání citlivých informací (zejména přihlašovacích údajů, finančních dat a osobních identifikátorů), má své kořeny v raných fázích masového rozšíření internetu a e-mailové komunikace v 90. letech 20. století. Zatímco počáteční aktivity kyberzločinců byly spíše nesystematické a technicky méně náročné, nárůst počtu uživatelů online služeb a rozvoj elektronického bankovnictví vytvořily podmínky pro sofistikovanější a systematičtější útoky, které mají globální dosah. (Jakobsson & Myers, 2006)

První předchůdci phishingových technik se objevili již na konci 80. a začátku 90. let, konkrétně v roce 1995. Útoky byly prováděny zejména v uzavřených online službách, jako byla populární platforma America Online (AOL). Útočníci využívali důvěřivosti uživatelů a vydávali se za pracovníky zákaznické podpory s cílem získat jejich hesla nebo jiné přihlašovací údaje. Ačkoli tyto útoky nebyly tehdy označovány termínem „phishing“, jasně ukazovaly, že lidé jsou v online prostředí zranitelní nejen z technického, ale i psychologického hlediska.

Termín „phishing“ se začal v hackerské komunitě běžně používat na přelomu 90. let a 21. století. Symbolika tohoto pojmu vychází z analogie k rybaření („fishing“), kdy útočníci tzv. „nahazují návnadu“ v podobě věrohodně vypadající elektronické zprávy a čekají, až se „oběť chytí“ a prozradí citlivé údaje. (Ollmann, 2004)

V první polovině 21. století byl zaznamenán rapidní růst objemu phishingových útoků, začínali oponovat technickou i psychologickou propracovaností. Zatímco počáteční strategie byla rozeslání velkého množství vygenerovaných zpráv, útočníci se naučili uplatňovat konkrétnější taktiky jako je spear-phishing. Tyto útoky využívaly osobní údaje o jednotlivcích či organizacích a zprávy pak působily věrohodněji a důvěryhodněji, což zvyšovalo úspěšnost útoků.

Podle zpráv FBI’s Internet Crime Complaint Center (IC3) došlo v letech 2020–2021 k výraznému zvýšení počtu stížností na phishing, vishing (hlasový phishing) a podobné sociálně-inženýrské techniky. Mezinárodní studie navíc potvrzují, že kriminalita spojená s phishingovými e-maily, které parazitují na tématu pandemie, byla obzvláště vysoká v prvních měsících roku 2020, kdy se veřejnost potýkala s nedostatkem kvalitních informací (Europol, 2021).

Podvodníci rozesílali například falešné e maily vydávající se za Světovou zdravotnickou organizaci (WHO) či vládní úřady, ve kterých nabízeli údajným „pacientům“ nebo „občanům“ klamné aktuality a infekční mapy s cílem zcizit citlivé údaje (např. přístupová hesla či platební informace).

2.1 Proces phishingu

Phishing představuje složitý a systematický mechanismus, který se obvykle skládá z několika fází. Každý krok je navržen tak, aby podvedl oběť a získal její citlivé informace. Proces phishingu lze rozdělit do několika klíčových fází.

1) Plánování phishingového útoku

Během této fáze útočník určuje, na koho útok zaměří a jakou konkrétní techniku k tomu využije. Zkoumá přitom úroveň zabezpečení budoucí oběti a vyhodnocuje možná rizika, včetně pravděpodobnosti odhalení vlastní identity.

2) Vytvoření podmínek pro phishingový útok

V této části se útočník zaměřuje na konkrétní provedení útoku. Shromažďuje si seznamy e mailových adres určených k oslovení, zakládá úložiště pro přijímání získaných informací a vytváří důvěryhodně vypadající sdělení. Toto falešné sdělení pak rozesílá vybraným uživatelům s cílem získat jejich citlivá data.

3) Vlastní phishingový útok

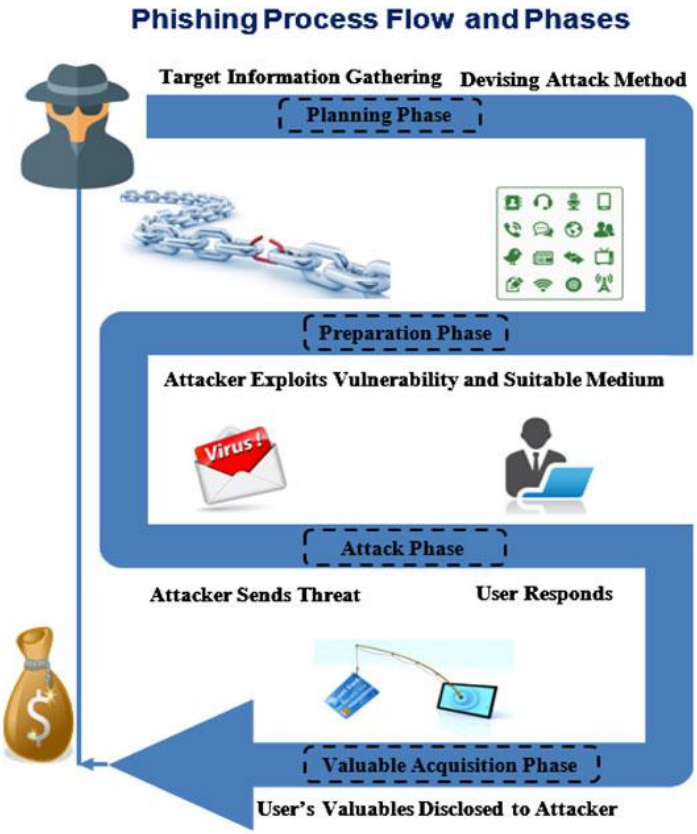
V této fázi je phishingový e-mail doručen vybraným uživatelům. Na základě jeho propracovanosti a dalších faktorů – například úrovně uživatelových zkušeností, jeho povědomí o phishingu nebo použití speciálního antiphishingového softwaru – mohou citlivé údaje skončit v útočníkově datovém úložišti. Teprve nyní se uživatel s podvodnou zprávou setkává poprvé.

4) Sběr dat

Nyní v této fázi útočník získává data, která byla zadaná do webové stránky jednotlivými uživateli.

5) Odčerpání peněžních prostředků či jiný profit z phishingového útoku.

Útočník používá dříve získané přihlašovací údaje k přístupu k reálným bankovním účtům obětí a odtud odčerpává finanční prostředky. Následně peníze převádí na další, často zahraniční, účty a rozděluje je nebo využívá jiné postupy, které způsobí, že ukradené finance jsou téměř nedohledatelné. (Kolouch, 2016)



Obrázek 1 Proces phishingu

Zdroj:https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full?ref=based.inc

2.2 Typy phishingových útoků

Jednotlivé typy útoků představují různé přístupy, které útočníci využívají k podvodu a získání citlivých informací od obětí. Každý typ útoku je navržen tak, aby co nejlépe odpovídal konkrétním situacím nebo technologickým prostředím, ve kterých se oběti nacházejí. Phishing není pouze jeden druh útoku, ale spíše široké spektrum metod, které se mohou lišit v použité technice, kanálech komunikace nebo cílové skupině. V této kapitole se podíváme na různé typy phishingových útoků a jejich charakteristiky, abychom lépe porozuměli, jakým způsobem útočníci získávají přístup k citlivým informacím.

2.2.2 Klasický phishing

V tomto případě útočník spoléhá především na masovou rozesílku podvodných e-mailů (či jiných zpráv), které napodobují důvěryhodné organizace – například banky, poskytovatele internetových služeb nebo sociální sítě.

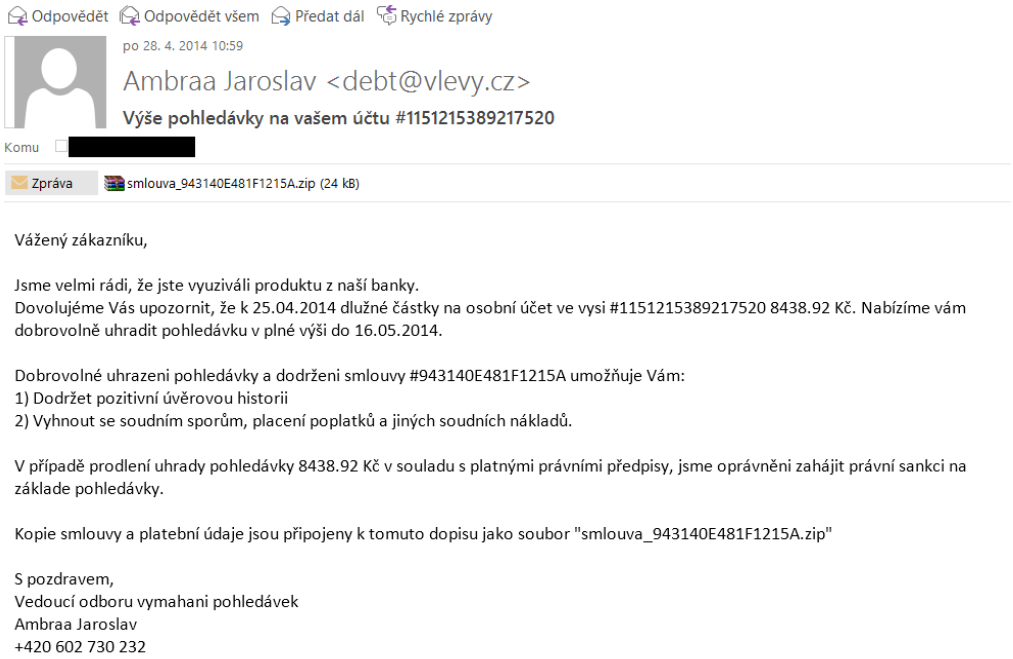
K útoku dochází ve chvíli, kdy uživatel obdrží e mail s výzvou k „ověření účtu“, „bezpečnostní kontrole“ nebo jiné naléhavé akci. Namísto skutečných stránek organizace však odkaz v e mailu směřuje na falešný web, který vzhledově a strukturou velice věrně kopíruje originál, a tím vzbuzuje důvěru uživatele. Jakmile uživatel na těchto falešných stránkách zadá své přihlašovací údaje, útočník je okamžitě získává a může je zneužít k přístupu k osobním nebo finančním účtům. Výhodou této metody pro útočníka je její masový charakter: i kdyby se na podvod chytil jen zlomek oslovených, úspěšnost je díky obrovskému objemu rozeslaných zpráv nadprůměrná. Klasický phishing proto i v současnosti zůstává jednou z nejúčinnějších a nejběžnějších technik kybernetických útoků. (Jakobsson & Myers, 2006)

Jak poznat klasický phishing

Klasický phishing se zavirovanou přílohou

Tento e-mail (Obrázek č.2) se opět vyznačuje několika typickými rysy podvodné korespondence. Odesílatel používá doménu „vlevy.cz“, která nevzbuzuje dojem oficiálního bankovního úřadu, a v textu e-mailu se vyskytují všeobecná tvrzení o údajném dluhu, aniž by bylo jasně identifikováno, o jakou banku se jedná. K doplňujícím varovným signálům patří přiložený soubor ve formátu ZIP („smlouva_943140E48F1F1215A.zip“), který je pro podobné situace atypický a často slouží k šíření malwaru. Text zároveň využívá manipulativního tónu a hrozí právními následky, čímž se snaží uživatele donutit k rychlému jednání. V souhrnu tyto

indicie nasvědčují, že zpráva nepochází od legitimní instituce, ale spadá do kategorie phishingových nebo jinak podvodných e-mailů.


Odpovědět Odpovědět všem Předat dál Rychlé zprávy

po 28. 4. 2014 10:59

Ambraa Jaroslav <debt@vlevy.cz>

Výše pohledávky na vašem účtu #1151215389217520

Komu [redacted]

Zpráva smlouva_943140E481F1215A.zip (24 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste vyuziváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1151215389217520 8438.92 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 16.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #943140E481F1215A umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 8438.92 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_943140E481F1215A.zip"

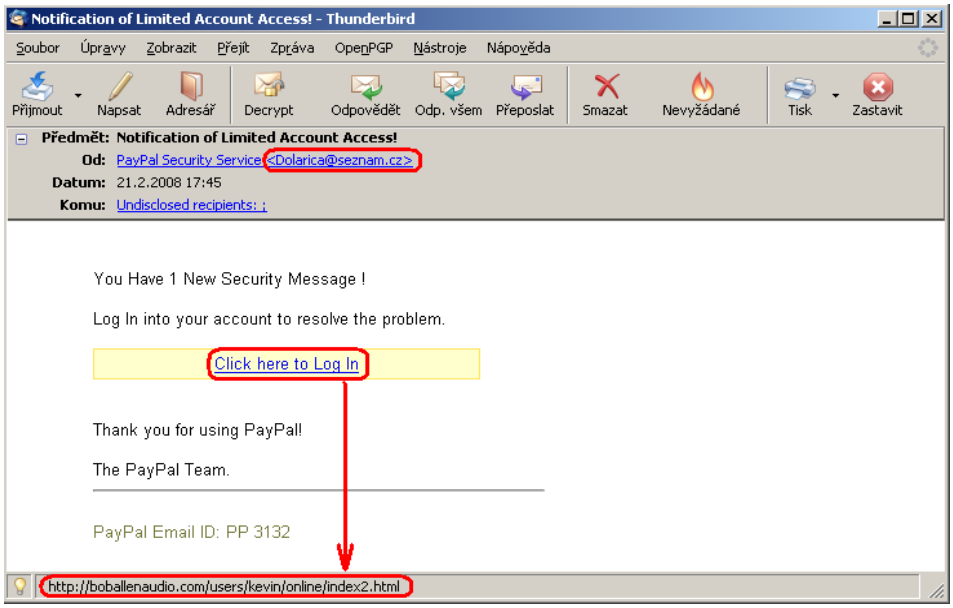
S pozdravem,
Vedoucí odboru vymahani pohledávek
Ambraa Jaroslav
+420 602 730 232

Obrázek 2 Příklad klasického phishingu se zavirovanou přílohou

Zdroj:https://helpdesk.zcu.cz/wiki/Phishing_-_p%C5%99%C3%ADklady

Příklad klasického phishingu s URL odkazem

Z dané ukázky (Obrázek č.3) je zřejmé, že se jedná o podvodnou zprávu vydávající se za oficiální komunikaci od společnosti PayPal. Hned několik prvků tuto domněnku podporuje: adresa odesílatele (např. „Dolarlica@seznam.cz“) naprosto neodpovídá oficiální firemní doméně; text zprávy vyvolává naléhavý dojem nutnosti „zabezpečení účtu“, čímž se snaží přimět uživatele ke kliknutí na odkaz; a samotný hypertextový odkaz vede na doménu, která se společností PayPal nemá nic společného („bboallenaudio.com/users/...“ namísto očekávané „paypal.com“). Tyto charakteristiky jsou typickými varovnými signály phishingu a upozorňují na nelegitimní pokus získat citlivé údaje, například přihlašovací jméno a heslo k účtu PayPal.



Obrázek 3 Příklad klasického phishingu s URL odkazem

Zdroj:https://helpdesk.zcu.cz/wiki/Phishing

Důsledek útoku

Pokud by adresát v reakci na takto formulovaný e mail otevřel přiložený soubor a nainstaloval si případný škodlivý kód nebo poskytl citlivé informace uvedené v údajné „smlouvě“, mohl by čelit závažným důsledkům. Primárním rizikem je finanční ztráta, neboť útočník získá přístup k bankovním či osobním údajům a může uskutečnit neautorizované transakce. Dalším možným dopadem je krádež identity, jelikož zcizené údaje mohou být zneužity k dalšímu úvěrovému podvodu či k přístupu k jiným online účtům oběti (např. sociálním sítím). V neposlední řadě ohrožuje příjemce i potenciální infikování systému malwarem, který může odcizit další data nebo umožnit útočníkovi vzdálený přístup k zařízení. Tato kombinace rizik ukazuje, jak zásadní je pečlivá kontrola příchozích e mailů a důsledná obezřetnost při zacházení s přílohami, zejména v neznámých formátech, jako je ZIP.

Jak se chránit proti útoku

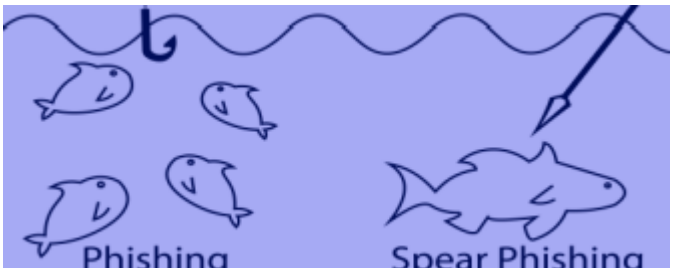
Základem obrany proti phishingovým útokům je zdravý rozum. Uživatel by si měl vždy položit jednoduchou otázku: „Opravdu by mi banka (nebo jiná podobná instituce) posílala nešifrovaný e-mail a žádala o takové důvěrné informace?“ Většinou na tuto otázku odpovíte záporně. Žádná instituce, zejména bankovní, vás nikdy nebude žádat o přihlašovací údaje prostřednictvím e-mailu; tyto záležitosti řeší oficiálními kanály, nikoli e-mailem. Je také důležité si uvědomit, že phishing se netýká pouze elektronického bankovnictví, ale může

zahrnovat i pokusy o získání hesel k e-mailovým účtům nebo jiným službám, které by mohly vést k odhalení vašich citlivých údajů. (NÚKIB, 2015)

2.2.3 Spear phishing

Spear phishing představuje cílenou a sofistikovanou formu podvodu, při které je oběť sledována po určité období s cílem shromáždit co nejvíce osobních informací. Tyto informace mohou pocházet z různých veřejně dostupných zdrojů, jako jsou osobní webové stránky, profily na sociálních sítích, diskusní fóra nebo účast na specifických akcích, například konferencích. Na základě těchto dat je následně vytvořen personalizovaný obsah e-mailu nebo SMS zprávy, který je přizpůsoben konkrétní oběti, což zvyšuje pravděpodobnost, že se stane cílem útoku. (NÚKIB,2015)

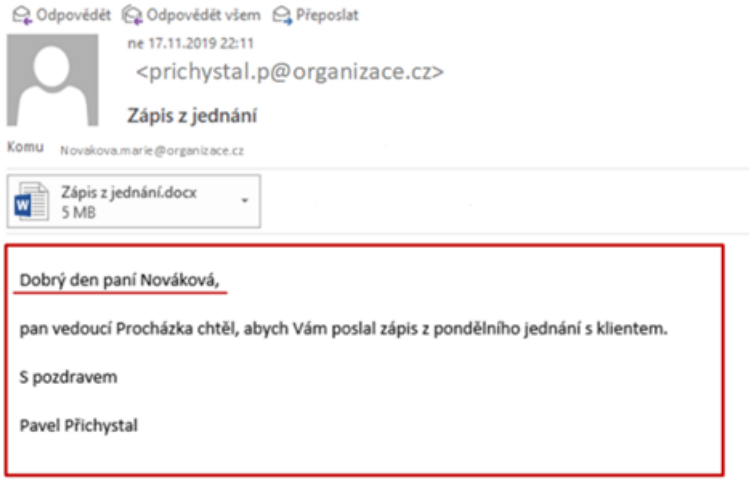
Zároveň je také nutné si říct rozdíl mezi phishingem a spear phishingem, při phishingu není cílová skupina vymezena, při spear phishingu je cílem konkrétní jednotlivec nebo specifická skupina (např. zaměstnanci firmy XY). (NÚKIB,2015). Rozdíl mezi klasickým phishingem a spear phishingem je schematicky znázorněn na obrázku 4.



Obrázek 4 Rozdíl mezi phishingem a spear phishingem

Zdroj: crossrealms.com

Na tomto příkladu (Obrázek č.5) jde o spear phishing, tedy cílený podvodný e-mail, který využívá personalizované informace o adresátovi i jeho pracovním prostředí. Útočník zřejmě ví, že oslovená osoba (paní Nováková) pracuje s určitým vedoucím (Procházkou) a posílá jí zprávu tak, aby působila důvěryhodně. Zmínka o „pondělním jednání s klientem“ a použití reálného jména vedoucího nebo spolupracovníka zvýší šanci, že oběť dokument (přílohu) otevře. Nejčastějším cílem takového útoku bývá získání přístupu do interních systémů či instalace škodlivého kódu skrytého v příloze. Útočník pak může zcizit citlivá data, získat přístup k dalším firemním účtům nebo v případě makro virů infikovat celý systém. Zásadními varovnými signály jsou právě velmi konkrétní obsah a překvapivá příloha, která odkazuje na údajných 5 MB „Zápisu z jednání“. Vždy je vhodné podobné nečekané požadavky ověřit u odesílatele (telefonicky či osobně), než soubor otevřete.



Obrázek 5 Příklad spear phishingu

Zdroj:https://nukib.gov.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/

Důsledek útoku

Pokud by uživatel dokument (přílohu) otevřel a povolil v něm například makra či jiné spustitelné prvky, existuje vysoké riziko, že se v pozadí nainstaluje škodlivý kód, který by mohl zaznamenávat přihlašovací údaje (keylogger), rozšířit se dále po síti a získat přístup k dalším systémům, případně zašifrovat data (ransomware) či vytvořit tzv. „backdoor“ pro dlouhodobé monitorování interní komunikace. Tím by došlo k závažné kompromitaci bezpečnosti organizace, potenciálnímu úniku citlivých informací a k finančním i reputačním škodám.

Jak se chránit proti útoku

V kontextu běžného uživatele je klíčové zachovávat obezřetnost vůči nevyžádaným nebo neobvyklým zprávám, pečlivě kontrolovat adresu odesílatele, odkazy i případné přílohy a v případě pochybností se dotázat kolegů či nadřízených. Uživatel by měl využívat více faktorovou autentizaci, silná hesla a pravidelně je měnit. Správce sítě by měl kromě standardních bezpečnostních opatření (firewall, antivirový software) zavádět i pokročilé detekční systémy, které dokážou rozpoznat a blokovat podezřelé e maily ještě předtím, než se dostanou k uživatelům. (NÚKIB, 2020)

2.2.4 Whaling

Whaling je specifický typ spear phishingu, který je obtížnější odhalit, protože je pečlivě přizpůsoben konkrétní firmě. Tento útok se zaměřuje na vysoké manažery a vedoucí pracovníky, přičemž útočníci se vydávají za důvěryhodné subjekty a snaží se oběti přimět k odhalení citlivých informací nebo k provedení bankovního převodu na podvodný účet.

(Eset.com). Vztah mezi klasickým phishingem, spear phishingem a whalingem je znázorněn na obrázku 6.

Obrázek 6 Rozdíl mezi spear phishingem a whalingem

Zdroj: https://www.techtarget.com/searchsecurity/definition/whaling

Důsledek útoku

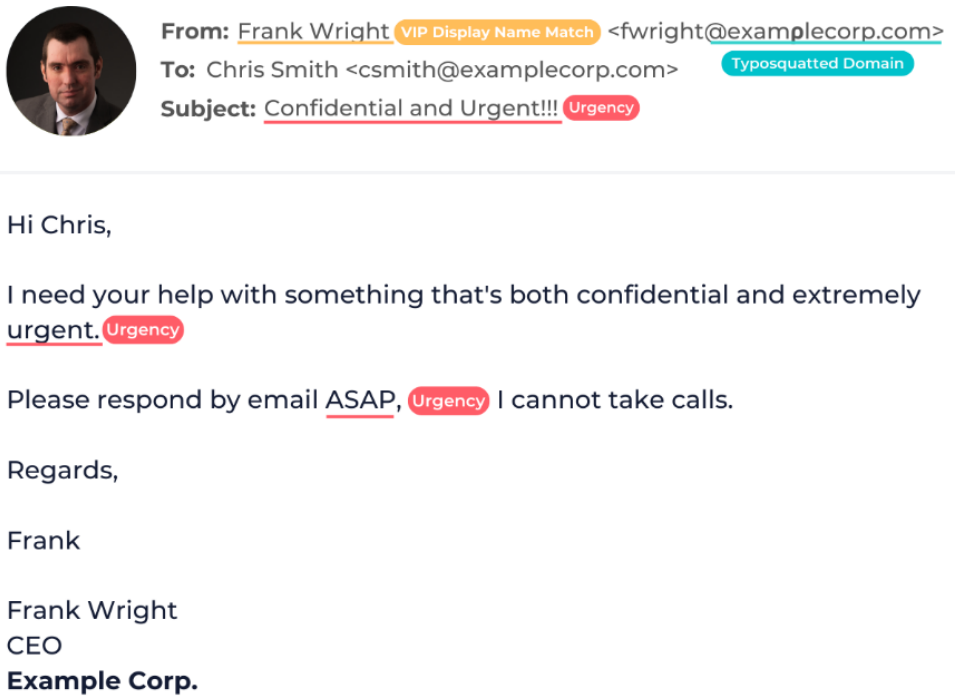
Důsledky útoků mohou být pro organizaci velmi závažné. Útočníci, kteří se zaměřují na vysoce postavené manažery či vedoucí pracovníky, totiž získávají přístup k interním strategickým informacím, finančním prostředkům či datům důležitým pro chod firmy. Úspěšný whalingový útok tak může vést k finančním ztrátám, reputačnímu poškození, úniku citlivých obchodních tajemství a v krajním případě i k paralýze provozu, pokud se například útočníkům podaří ochromit klíčové systémy.

Jak se chránit proti útoku

Z perspektivy běžného uživatele je klíčové nikdy slepě nevyhovět výzvám k naléhavým finančním převodům či poskytnutí citlivých údajů, a to ani v případě, kdy se pisatel vydává za vysoce postavenou osobu ve firmě. Uživatel by měl ověřovat podobné požadavky nezávislým kanálem (např. telefonem), kontrolovat zasílatelskou adresu a její shodu s oficiální doménou i případné gramatické nesrovnalosti.

2.2.5 CEO Fraud

CEO Fraud je opak whalingu. Tato podvodná praktika, při níž se útočník vydává za generálního ředitele (CEO) nebo jinou vysoce postavenou osobu ve vedení společnosti. Metoda je dokladem, že lidský faktor zůstává nejslabším článkem. Ukázka CEO fraud útoku je na obrázku 7.



Obrázek 7 Příklad CEO fraud

Zdroj:https://www.meshsecurity.io/ceo-fraud

Důsledek útoku

V tomto příkladě si útočník legálně zaregistroval doménu s malou změnou oproti originální doméně. Pokud se podíváte na první „p“ v „examplecorp.com“, ve skutečnosti je nahrazeno řeckým písmenem „Rho“ (ρ). Cyrilické znaky se často používají k vytváření podvodných domén, které je pro zaměstnance těžké odhalit, protože rozdíly jsou minimální. Tato podvodná doména pravděpodobně projde bezpečnostními kontrolami jako SPF, DKIM a DMARC. Absence odkazů nebo příloh znamená, že antivirové programy a bezpečnostní sandboxy nemají co analyzovat, což je činí neúčinnými. Pro příjemce tak může tento e-mail vypadat naprosto legitimně. Dále je důležité zmínit, že útočník se vydává za generálního ředitele a používá jazyk, který vyvolává pocit naléhavosti a vyvíjí tlak na příjemce, aby co nejrychleji odpověděl a splnil požadavek.

V případě úspěšného zcizení značného finančního obnosu dochází nejen k okamžitému ekonomickému poškození, ale také k narušení důvěry akcionářů, zákazníků či obchodních partnerů. Únik informací či narušení vnitřních procesů může rovněž ohrozit strategické projekty a oslabit konkurenceschopnost firmy. Reputace společnosti bývá narušena zveřejněním incidentu v médiích, což může v extrémních případech vést k dalším právním sporům nebo k nutnosti kompenzovat ztráty postižených subjektů.

Jak se chránit proti útoku

Základem ochrany proti útokům typu CEO fraud je propojení jasně stanovených vnitropodnikových postupů s pravidelnou bezpečnostní osvětou zaměstnanců. V rámci procesních opatření se doporučuje zřídit víceúrovňové schvalování peněžních převodů a důsledné prověřování všech požadavků, především těch spojených s vysokými finančními částkami nebo naléhavými požadavky. Z hlediska správce sítě je důležité nasazení bezpečnostních protokolů a antispamových filtrů, které většinu těchto podivných či podvodných emailů zablokují ještě dříve, než se dostanou k adresátovi.

2.2.6 Vishing

Vishing je druh telefonického phishingu, který využívá metody sociálního inženýrství k získávání důvěrných informací, jako jsou čísla účtů, přihlašovací jména či hesla a údaje o platebních kartách. V rámci tohoto podvodu útočník úmyslně předstírá falešnou identitu, nejčastěji se vydává za zástupce banky nebo jiné důvěryhodné instituce, aby u oslovených osob vyvolal dojem bezpečí. Tato forma útoku se realizuje v prostředí VoIP (Voice over Internet Protocol), které útočníkům usnadňuje napodobení pravé telefonní linky. (Kolouch, 2016)

Důsledek útoku

Vishingové útoky mohou mít pro oběti i organizace významné dopady. Finanční ztráty patří mezi nejčastější, kdy útočník získá přístup k bankovním účtům či platebním kartám a provádí neoprávněné transakce. Velkým rizikem je také krádež identity, jestliže útočníci shromáždí dostatek osobních údajů k otevírání falešných účtů nebo zneužití rodného čísla. Reputace firem a institucí může utrpět, pokud dojde k veřejnému odhalení podvodu spojeného s jejich jménem. Vishing navíc často zvyšuje pravděpodobnost následných útoků, získané informace mohou být použity k dalším útokům, například cílenému spear phishingu nebo sociálnímu inženýrství.

Jak se chránit proti útoku

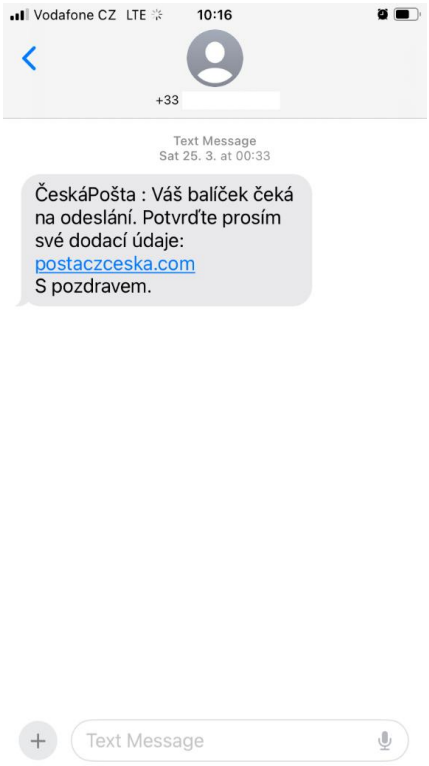
Pro ochranu před vishingem je klíčové zachovávat obezřetnost vůči nevyžádaným telefonním hovorům a důsledně ověřovat identitu volajícího, zejména pokud se představuje jako zástupce banky či jiné instituce. Zaměřte se na reálnost časového kontextu hovoru, formu komunikace a ochotu volajícího poskytnout dodatečné informace (např. číslo smlouvy či jinou interní informaci, jíž by správně disponoval pouze legitimní pracovník). Pokud je hovor nátlakový nebo se volající chová neadekvátně, ukončete jej a okamžitě kontaktujte příslušnou organizaci prostřednictvím veřejně dohledatelného telefonního čísla. Neposkytujte citlivé údaje, jako je přístup do internetového bankovnictví, PIN či CVC/CVV kódy, a v žádném případě nepřevádějte peníze na cizí účet na žádost neověřené osoby. Každý podezřelý případ oznamte oficiální infolince dané instituce a v případě potřeby i Policii ČR. (Eset.com)

2.2.7 Smishing

Smishing pracuje na obdobném principu jako vishing nebo phishing, avšak využívá SMS zprávy k šíření podvodného obsahu. Útočník se snaží uživatele přimět k zaplacení určité částky (například zavoláním na placenou linku či odesláním dárcovské SMS) nebo k otevření podezřelého odkazu. Ten následně vede na stránku, jež zneužívá bezpečnostních slabin systému nebo vyzývá uživatele k instalaci škodlivého softwaru či k poskytnutí citlivých údajů. (Kolouch, 2016). Obrázky 8 a 9 ukazují příklady smishingových útoků.

Obrázek 8 Příklad smishingu

Zdroj:Vlastní



Obrázek 9 Příklad smishingu

Zdroj:https://osveta.nukib.gov.cz/course/view.php?id=221

Důsledek útoku

Hlavním důsledkem smishingu je ztráta citlivých osobních či finančních údajů, které útočníci následně zneužívají k podvodným transakcím, krádeži identity nebo k dalším formám podvodů. Oběti často reagují na výzvy k zaplacení poplatku, vyplnění falešného formuláře či zavolání na placenou linku. Důsledkem bývají finanční ztráty, problémy s bankovními účty nebo blokace karet, a v některých případech také kompromitace soukromí, neboť získané informace lze použít k sestavení komplexního profilu oběti pro další útoky. Navíc podvodníci mohou pomocí textových zpráv (SMS) šířit odkazy na podvržené webové stránky, které dokážou zneužít bezpečnostní slabiny zařízení, nainstalovat malware či dalším způsobem poškodit uživatele.

Jak se chránit proti útoku

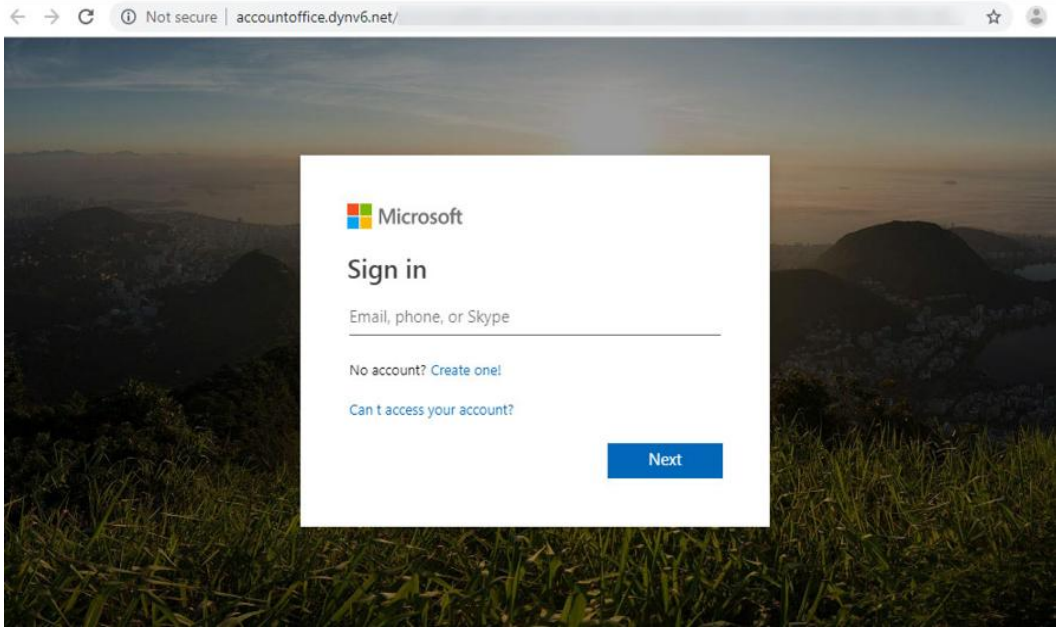
Proti smishingu se osvědčuje zejména obezřetnost a ověřování podezřelých zpráv. Za klíčové ochranné kroky lze považovat ignorování nevyžádaných SMS a nepodléhání naléhavým výzvám, které často vyžadují okamžité poskytnutí citlivých údajů. V případě upozornění na údajné problémy s účty je vhodné ověřit si věrohodnost zprávy přes oficiální web či telefonní číslo banky, nikoli reagovat přímo na SMS. Při kliknutí na odkaz je nezbytné kontrolovat, zda URL skutečně odpovídá oficiální doméně. Stejně tak je dobré být na pozoru před zdánlivě výhodnými nebo dokonce „výjimečnými“ nabídkami, které mohou mít za cíl vylákat další citlivá data. V případě podezřelého kontaktu nebo zjištěného podvodu je vhodné informovat příslušné instituce a policii, aby mohly varovat ostatní potenciální oběti.

2.2.8 Page hijacking

Tento typ phishingu spočívá v tom, že uživatelé jsou neúmyslně přesměrováni na falešnou webovou stránku. Útočníci vytvoří kopii existujícího webu a pomocí internetových vyhledávačů způsobí, že tento podvodný web je zobrazován jako první místo původního legitimního webu. Alternativně mohou útočníci kompromitovat skutečné stránky a přesměrovat návštěvníky na škodlivé verze. (Eset.com)

Podobně jako u page hijackingu, i pharming využívá techniky manipulace s internetovým připojením, ale místo kopírování webových stránek se zaměřuje na přesměrování uživatelů na falešné stránky na úrovni DNS nebo zařízení, což činí tento útok mnohem těžší k rozpoznání.

Ačkoli oba útoky mají podobný cíl, kterým je přesměrovat uživatele na podvodnou stránku, která vypadá legitimně, page hijacking se zaměřuje na konkrétní webové stránky a zasahuje přímo do jejich obsahu, zatímco pharming manipuluje s DNS („Domain Name System“) a směrováním uživatelova připojení na úrovni počítače nebo sítě, což je pro běžného uživatele těžké rozpoznat. (Kaspersky.com). Obrázek 10 znázorňuje



Obrázek 10: Příklad page hijackingu

Zdroj:https://nukib.gov.cz/download/publikace/analyzy/Spear-phishing_a_jak_se_pred_nim_chranit.pdf

Důsledek útoku

Důsledky page hijackingu jsou v podstatě podobné jako u ostatních typů phishingu, protože i zde mohou útočníci získat citlivé osobní údaje, jako jsou přihlašovací údaje, čísla platebních karet nebo jiné osobní informace. Tyto údaje mohou být následně zneužity k finančním podvodům, krádeži identity nebo jiným formám zneužití. Avšak vzhledem k tomu, že v tomto případě útočníci mohou kompromitovat legitimní webové stránky nebo vytvořit jejich podvodné kopie, mohou být právní důsledky výrazně závažnější. Organizace, jejichž weby jsou cílem tohoto útoku, mohou čelit reputačním škodám i právním problémům, pokud dojde k úniku dat nebo podvodu s jejich jménem.

Jak se chránit proti útoku

Ochrana proti page hijacking vyžaduje komplexní přístup, který zahrnuje několik klíčových strategií. Prvním krokem je implementace HTTPS na webových stránkách, což zajistí šifrování dat a ochranu proti neoprávněným přesměrováním. Další zásadní prevencí, co se týče firem a správců sítí je pravidelné provádění bezpečnostních auditů, které pomohou identifikovat

a opravit zranitelnosti, jež by mohly být zneužity pro hijacking. Je také důležité sledovat hodnocení ve vyhledávačích, abyste včas zachytili náhlé poklesy nebo duplikovaný obsah, které mohou naznačovat, že došlo k hijackingu. Použití nástrojů proti malwaru je další nezbytnou ochranou, protože detekují a zabraňují škodlivým aktivitám na webových stránkách. Konečně, vzdělávání týmu o nejnovějších kyber bezpečnostních postupech je klíčové pro zajištění, že všichni členové organizace budou schopni rozpoznat potenciální hrozby a vědí, jak jim předcházet. (twingate.com)

2.2.9 Quishing

Quishing je zcela nový a sofistikovanější typ phishingu, kde útočníci vytváří QR kód k podvodu. Tento kód vypadá ovšem neškodně do doby, než ho uživatel naskenuje, poté je přesměrován na falešnou webovou stránku, kde může být požádán o osobní údaje, jako jsou přihlašovací údaje do internetového bankovnictví, platební karty nebo další citlivé informace, které dotyčný rozhodně nechce ztratit.

Důsledek útoku

Tento typ phishingu je hodně nebezpečný, protože QR kódy jsou v dnešní době považovány za bezpečné a jsou používány čím dál víc, pro urychlení procesů v kyberprostoru. Útočníci je mohou umístit kamkoliv např. (na plakátnici, v emailech, webové stránky nebo taky sociální sítě) a jakkoliv s nimi manipulovat, aby vypadaly jako důvěryhodné odkazy, které mohou vést k poskytovatelům služeb, bank či jiné platformy. Po technické stránce pokud by se stalo, že dotyčný QR kód otevřel, může být stažen škodlivý software a nainstalován bez jakéhokoliv vědomí uživatele. Po finanční stránce útočník může získat přístup k internetovému bankovnictví a způsobit tak významné ztráty a škody.

Jak se chránit proti útoku

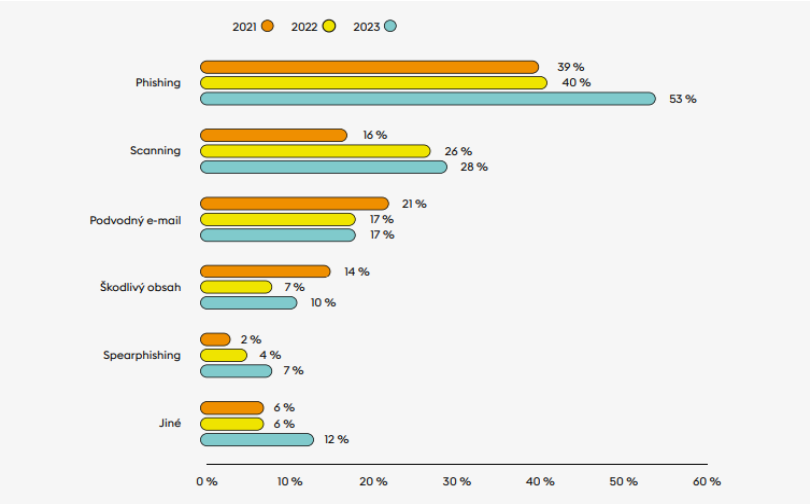
Při práci s QR kódy je důležité je skenovat pouze z důvěryhodných a ověřených zdrojů. Používání aplikací na skenování QR kódů může pomoci identifikovat a varovat před potenciálně nebezpečnými kódy. Kromě toho je nezbytné pravidelně aktualizovat software, včetně operačního systému a antivirového programu, aby bylo zajištěno, že vaše zařízení je chráněno před nejnovějšími hrozbami. Dále byste měli být opatrní a nikdy neposílat citlivé údaje prostřednictvím kódů, které pocházejí z neznámých nebo podezřelých zdrojů. (ebezpeci.com). Ukázka quishingu je na obrázku 11.

Obrázek 11 Příklad quishingu

Zdroj: (Kolouch,2016)

2.2.10 Současná četnost phishingových útoků

Zatímco předchozí části (2.2.1 až 2.2.9) popisovaly různé formy phishingu z hlediska technik a zaměření, následující kapitola se zaměří na statistické údaje a aktuální trendy v oblasti phishingových útoků. Pro lepší představu o tom, jak často se jednotlivé typy phishingu v praxi vyskytují, je zde uveden graf, který ukazuje rostoucí četnost phishingu. Jak můžeme vidět graf se od let 2021 a 2022 výrazně stupňuje a poukazuje na to, že sofistikovanost phishingových útoků roste a dominuje mezi kybernetickými hrozbami a je označován jako nejčastější typ kybernetického útoků.



Obrázek 12 Graf četnosti phishingových útoku k roku 2023

Zdroj: (NÚKIB, Zpráva o stavu kybernetické bezpečnosti ČR za rok 2023)

3. TRESTNĚPRÁVNÍ ODPOVĚDNOST

Phishing představuje formu kybernetické kriminality, při níž dochází k podvodnému získávání citlivých údajů, jako jsou přihlašovací údaje, čísla platebních karet, osobní informace, obchodní tajemství a spoustu dalších informací, které by mohly běžné uživatele ohrozit, za účelem jejich zneužití. V českém právním řádu je toto jednání postihováno zejména prostřednictvím trestního zákoníku (zákon č. 40/2009 Sb.), a to v několika ustanoveních.

V České republice se "klasický phishing" trestá podle § 209 trestního zákoníku (Podvod), který vyžaduje, aby se pachatel obohatil. Vytvoření falešné webové stránky a získání uživatelských jmen a hesel by se mohlo považovat za přípravu nebo pokus o podvod. Samotné shromažďování přístupových údajů (včetně čísel účtů, platebních karet a PIN kódů) bez jejich následného zneužití ale trestné není. (Kolouch,2016)

Pokud phishingový útok zahrnuje i použití malwaru k napadení počítače, může být pachatel stíhán také podle § 230 trestního zákoníku (Neoprávněný přístup k počítačovému systému a nosiči informací). Pokud je cílem phishingu získat neoprávněný prospěch pro sebe nebo někoho jiného, lze uplatnit i ustanovení § 230 odst. 3 trestního zákoníku. V některých případech by se dalo použít i ustanovení § 234 trestního zákoníku (Neoprávněné opatření, padělání a pozměnění platebního prostředku). (Kolouch,2016)

Rozsah škody je pro účely trestního řízení definován v ustanovení § 138 zákona č. 40/2009 Sb., TZ. Toto ustanovení stanovuje hranice výše škody, prospěchu, nákladů k odstranění poškození životního prostředí a hodnoty věci následovně:

„Za škodu nikoli nepatrnou je považována částka od 10 000 Kč, škoda nikoli malá dosahuje nejméně 50 000 Kč, větší škoda začíná na částce 100 000 Kč, značná škoda na 1 000 000 Kč a škoda velkého rozsahu je definována jako škoda nejméně ve výši 10 000 000 Kč.“

3.1 Podvod

Podle § 209 odst. 1 TZ se podvodem rozumí *„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.“*

Pokud byl pachatel za obdobný čin již v posledních třech letech odsouzen, trest se zvyšuje na šest měsíců až tři léta. Přísnější tresty jsou ukládány v případech, kdy phishingový

útok způsobí větší škodu, kdy může být pachatel potrestán odnětím svobody na jeden rok až pět let nebo peněžitým trestem. V případě organizovaného páchání, zvláštní povinnosti chránit zájmy poškozeného či spáchání činu v krizové situaci (např. za živelní pohromy), může být pachatel potrestán odnětím svobody na dvě léta až osm let. Nejvyšší trestní sazba pět až deset let hrozí v případě, že pachatel způsobí škodu velkého rozsahu nebo jeho jednání souvisí s usnadněním teroristického činu. Příprava tohoto trestného činu je rovněž postihována trestním zákoníkem. I když se pachateli phishingu nepodaří dokončit finanční transakci, jeho čin je stále trestný, protože se jedná o pokus trestného činu. (zakonyprolidi.cz)

3.2 Neoprávněný přístup k počítačovému systému a nosiči informací

Z původního ustanovení § 257 trestného zákoníku se stala dvě ustanovení. Ustanovení § 230 postihující neoprávněný přístup k počítačovému systému a nosiči informací a § 231, který postihuje opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. (Smejkal,2015)

Podle § 230 odstavce 1 TZ. *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“*

Tento paragraf postihuje jednání, při němž pachatel neoprávněně užije, vymaže, poškodí, změní nebo jinak manipuluje s daty uloženými v počítačovém systému či na nosiči informací. Dále zahrnuje i padělání nebo pozměnění dat, jejich neoprávněné vložení do systému či zásah do jeho technického nebo programového vybavení. Za takové jednání může být pachatel potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci. Přísnější tresty se uplatňují v případě, že čin byl spáchán s úmyslem způsobit škodu či neoprávněně omezit funkčnost počítačového systému, kdy hrozí trest šest měsíců až čtyři léta odnětí svobody.

Nejvyšší trestní sazba, tedy tři léta až osm let, je vyhrazena pro případy, kdy pachatel způsobil škodu velkého rozsahu nebo získal prospěch velkého rozsahu. Tento trestný čin je v kontextu phishingu klíčový, protože se vztahuje na zneužití získaných přístupových údajů ke škodlivým zásahům do informačních systémů obětí, například prostřednictvím podvodného přístupu k bankovním účtům či firemním datům. (zakonyprolidi.cz)

3.3 Opatření a přechovávání přístupového zařízení a hesla počítačovému systému a jiných takových dat

Phishingové útoky často neslouží pouze k okamžitému získání citlivých informací, ale také k jejich dalšímu ukládání, přechovávání nebo šíření, což podléhá trestní odpovědnosti podle § 231 odstavce 1. TZ,*"Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b),c) nebo trestný čin neoprávněného přístupu počítačovému systému a nosiči informací podle § 230 odst. 1,2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává."*

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoliv jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na 1 rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

Pokud je čin spáchán s úmyslem způsobit škodu, neoprávněně omezit funkčnost systému nebo získat prospěch, hrozí trestní sazba šest měsíců až tři léta. V případech, kdy pachatel jednal jako člen organizované skupiny, způsobil značnou škodu nebo narušil systém důležitý pro bezpečnost státu či hospodářství, může být uložen trest odnětí svobody na jeden rok až pět let nebo peněžitý trest.

Nejvyšší trestní sazba tři léta až osm let se vztahuje na případy, kdy pachatel svým jednáním způsobí škodu velkého rozsahu nebo získá prospěch velkého rozsahu. Tento trestný čin je zásadní zejména ve spojitosti s phishingovými kampaněmi, které se zaměřují na hromadné získávání přihlašovacích údajů a jejich následný prodej nebo využití k dalším kybernetickým útokům, včetně vydírání a finančních podvodů. (zakonyprolidi.cz)

3.4 Neoprávněné opatření, padělání a pozměnění platebního prostředku

Phishingové útoky často směřují právě k získání údajů o platebních kartách, které následně pachatelé používají k neoprávněným transakcím, výběrům hotovosti nebo prodeji na černém trhu. Podle § 234 trestního zákoníku je jakékoli opatření, padělání či držení platební

karty nebo jejích údajů s úmyslem podvodného použití trestné. Phishing je tedy často prvním krokem v řetězci kybernetické kriminality vedoucí ke spáchání tohoto trestného činu.

Podle § 234 odstavce 1. TZ. *„Kdo sobě nebo jinému bez souhlasu oprávněného uživatele opatří, zpřístupní, přijme nebo přechovává platební prostředek, který umožňuje výběr hotovosti nebo převod peněžních prostředků anebo virtuálních aktiv používaných namísto peněžních prostředků (dále jen "platební prostředek") a který náleží jinému, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“* Podle odstavce 2. TZ. *„Kdo sobě nebo jinému opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek, bude potrestán odnětím svobody na jeden rok až pět let.“* Podle odstavce 3. TZ. *„Kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý nebo platný, nebo kdo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný, bude potrestán odnětím svobody na tři léta až osm let.“* Také je důležité zmínit, že samotná příprava činu je trestná.

4. DOTAZNÍKOVÝ VÝZKUM

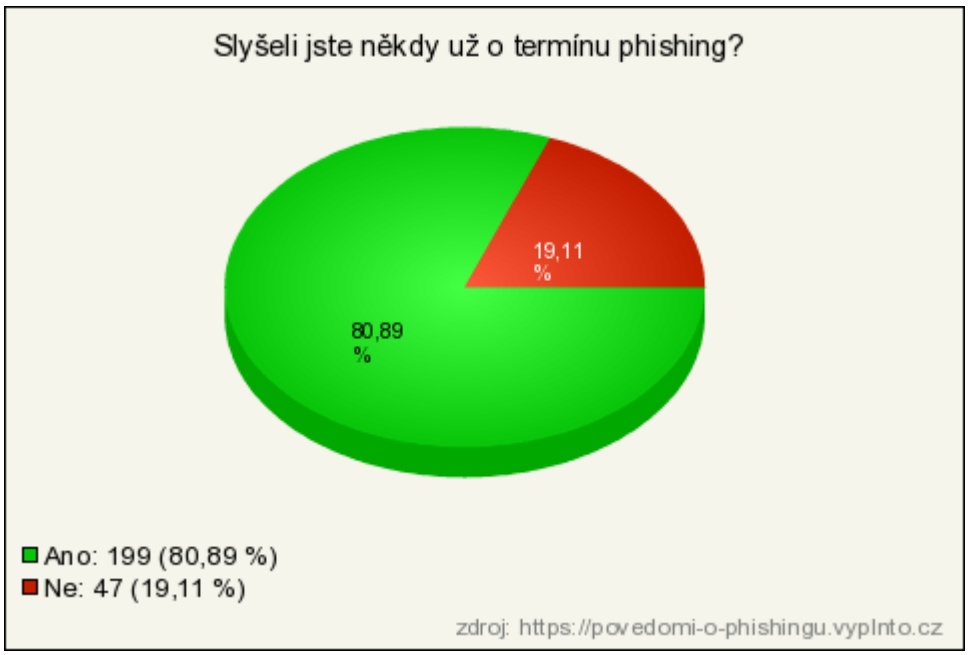
Tento výzkum měl za úkol získat empirická data týkající se povědomí veřejnosti o phishingových útocích a bezpečnostních návycích respondentů. Výzkum probíhal prostřednictvím anonymního elektronického dotazníku, který byl vytvořen na platformě Vyplnto.cz, specializující se na tvorbu dotazníků. Dotazník obsahoval celkem 19 otázek, z nichž 13 bylo uzavřených a 6 polouzavřených. Kompletní znění dotazníku je dostupné v Příloze A. Respondenti, kteří se zúčastnili šetření, představovali širokou veřejnost, přičemž šetření bylo zaměřeno na různé věkové skupiny a profesní oblasti. Dotazníkového výzkumu se zúčastnilo 246 lidí. Výzkum byl realizován v období od poloviny do konce března 2025.

4.1 Cíle výzkumu

Cílem tohoto výzkumu bylo zjistit a analyzovat současnou situaci v oblasti kyberbezpečnosti, se zaměřením na phishingové útoky. Hlavním zaměřením bylo ověření povědomí uživatelů o phishingu, zjištění jejich osobních zkušeností a identifikace bezpečnostních návyků, které mohou pomoci v prevenci těchto útoků. Výzkum se soustředil na několik klíčových oblastí: porovnání povědomí o phishingu mezi respondenty z odvětví IT a ostatními profesemi, rozdíly mezi uživateli, kteří pravidelně mění hesla, a těmi, kteří je mění zřídka či vůbec, a analýzu povědomí o phishingu v jednotlivých věkových skupinách. Dále se výzkum zaměřil na to, jak respondenti vnímají riziko phishingových útoků a jaká preventivní opatření považují za nejefektivnější v ochraně před těmito hrozbami:

4.2 Výsledky výzkumu

Graf: 1 Otázka č. 1: Slyšeli jste už někdy o termínu phishing?



Graf 1: Termín phishing

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

Podle výsledků první otázky 199 respondentů už někdy slyšelo o termínu phishing. Zatímco pouhých 47 respondentů o phishingu neslyšelo. Respondenti, kteří na první otázku odpověděli „Ne“, už na další otázky neodpovídali.

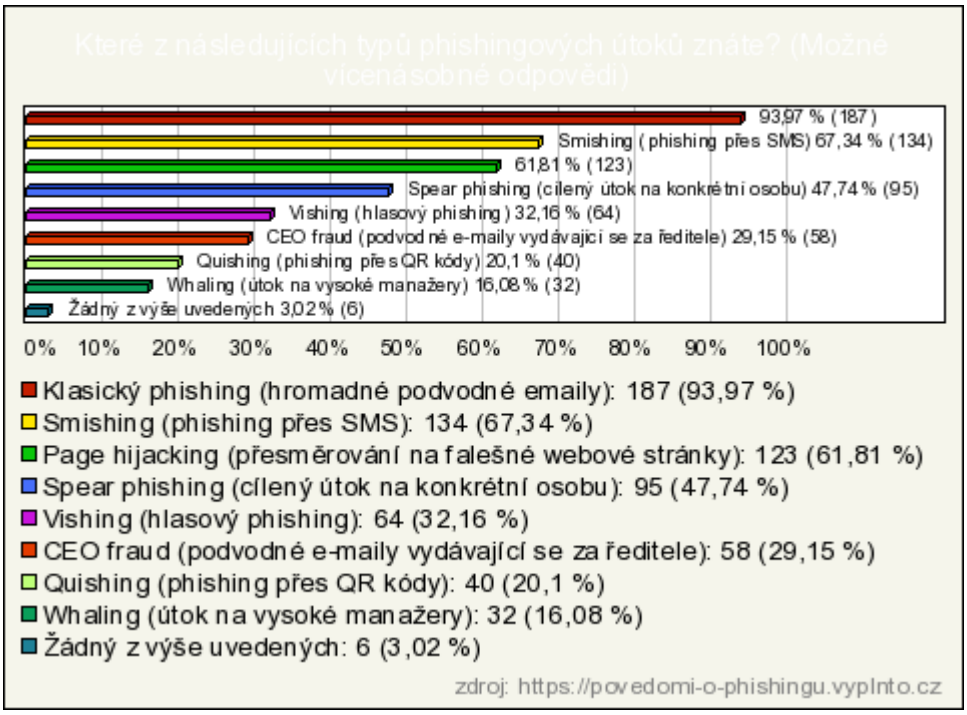
Graf 2: Otázka č.2 Jak byste definovali phishing?

Graf 2: Definice phishingu

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

Většina respondentů v otázce č. 2 byla schopna správně definovat pojem phishing. Z většiny odpovědí vyplývá, že respondenti rozumí phishingu jako podvodné technice, při níž útočník manipuluje oběť k odhalení citlivých údajů. Tento správný výklad byl zvolen většinou dotazovaných. Nicméně, někteří respondenti definovali phishing nesprávně. 2 respondenti označili phishing jako „způsob šifrování dat“, což je terminologicky nesprávné, protože šifrování dat je proces zabezpečení informací, zatímco phishing je technika podvodného získávání citlivých údajů. Další 2 respondenti se domnívali, že phishing je „počítačový virus, který infikuje zařízení“, což také není přesná definice. Tato definice by spíše odpovídala popisu malwaru, nikoli phishingu. Jeden respondent si nebyl jistý a zvolil odpověď „Nevím“, což ukazuje na malou nejistotu ohledně přesného vymezení phishingu.

Graf 3: Otázka č.3 Které z následujících typů phishingových útoků znáte (Možné vícenásobné odpovědi)

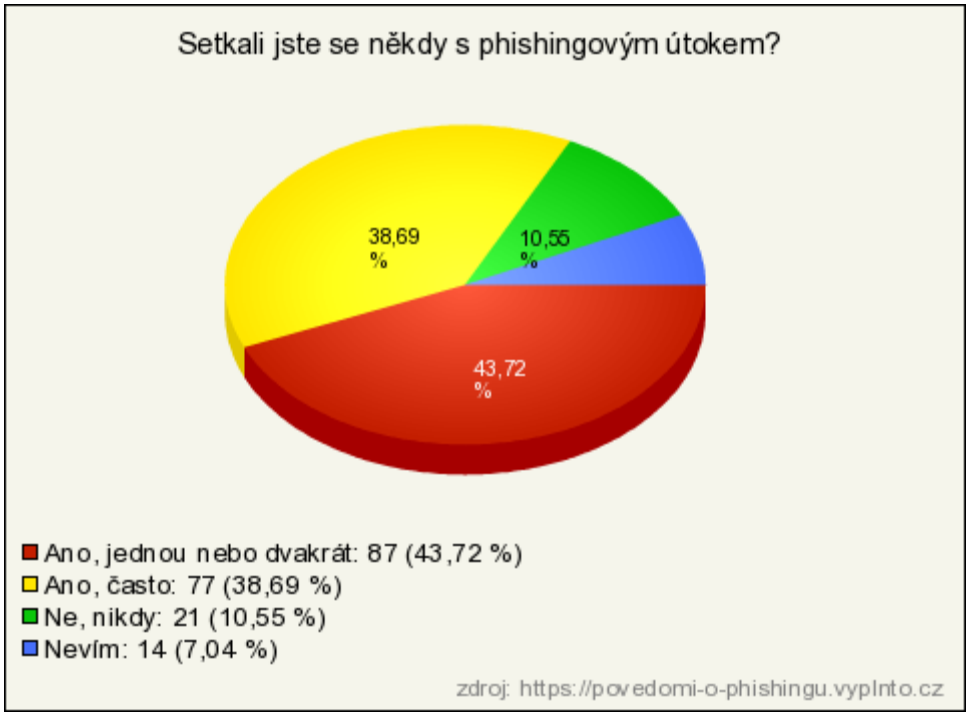


Graf 3: Povědomí o typech phishingových útoků

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V rámci otázky č. 3, která se zaměřovala na povědomí o různých typech phishingových útoků, většina respondentů uvedla, že je známý klasický phishing (93,97 %), což potvrzuje, že tento typ je nejčastěji rozpoznáván. Dále bylo zaznamenáno poměrně vysoké povědomí o smishingu (67,34 %) a page hijacking (61,81 %), což ukazuje na určitou znalost specifických metod phishingu. Ostatní typy phishingu, jako spear phishing (47,74 %), vishing (32,16 %) a CEO fraud (29,15 %), byly méně rozpoznávány, přičemž u méně běžných typů, jako je quishing (20,1 %) a whaling (16,08 %), byla povědomost ještě nižší. Pouze 6 respondentů označilo, že se s žádným z těchto typů phishingu nesetkali. Tento výsledek naznačuje, že i když většina respondentů rozpozná běžné formy phishingu, pokročilejší a cílené útoky jsou méně známé.

Graf 4: Otázka č. 4 Setkali jste se někdy s phishingovým útokem?

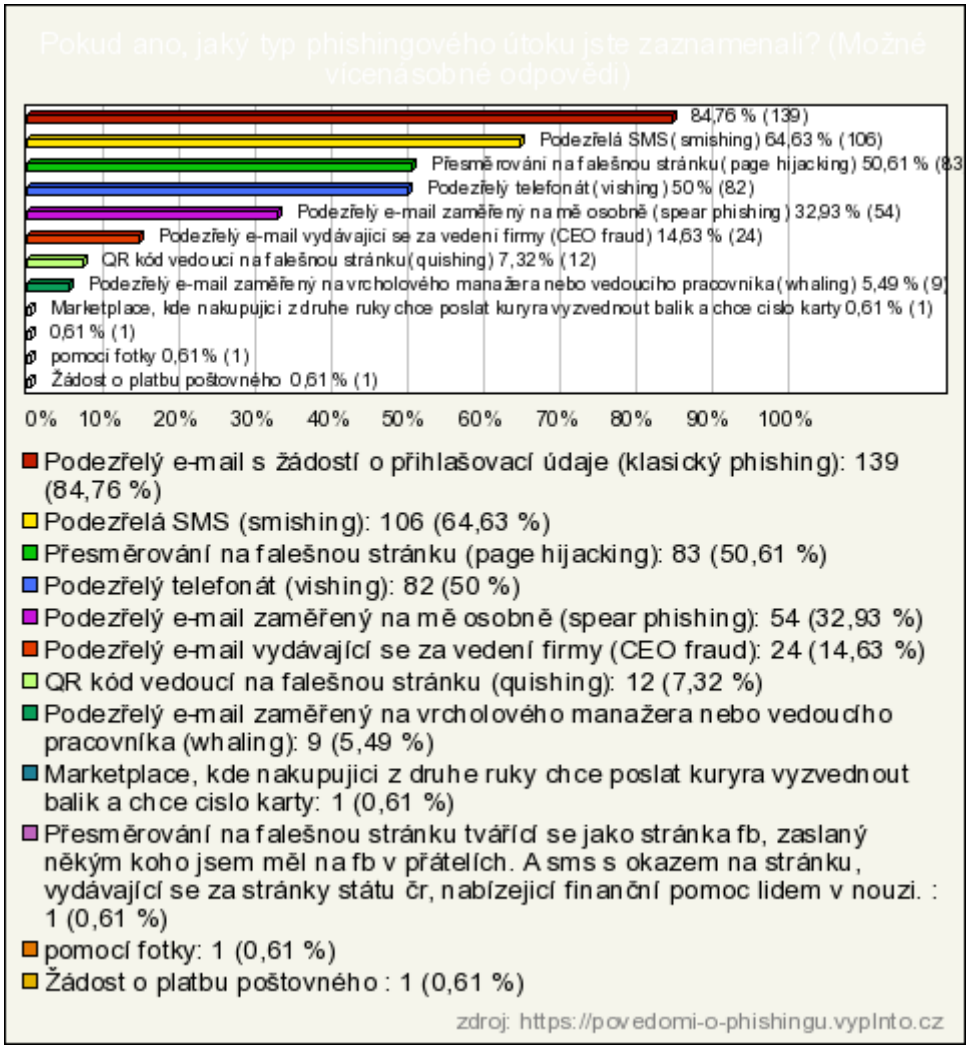


Graf 4: Zkušenost s phishingem

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 4, která se zaměřovala na to, zda se respondenti někdy setkali s phishingovým útokem, většina respondentů uvedla, že se s phishingem setkali alespoň jednou nebo dvakrát (43,72 %). Dalších 38,69 % respondentů uvedlo, že se s phishingem setkali častěji. Téměř 10,55 % respondentů přiznalo, že se s phishingem nikdy nesetkali. Pouze 7,04 % respondentů uvedlo, že si nejsou jisti, zda s phishingovým útokem někdy přišli do kontaktu. Tento výsledek ukazuje, že phishingové útoky jsou relativně běžným jevem, který většina respondentů alespoň jednou zažila, což zdůrazňuje důležitost prevence a osvěty v této oblasti. Pokud respondent odpověděl „Ne, nikdy“ nebo „Nevím“, byl přesunut na otázku č.7.

Graf 5: Otázka č.5 Pokud ano, jaký typ phishingového útoku jste zaznamenali (Možné vícenásobné odpovědi)



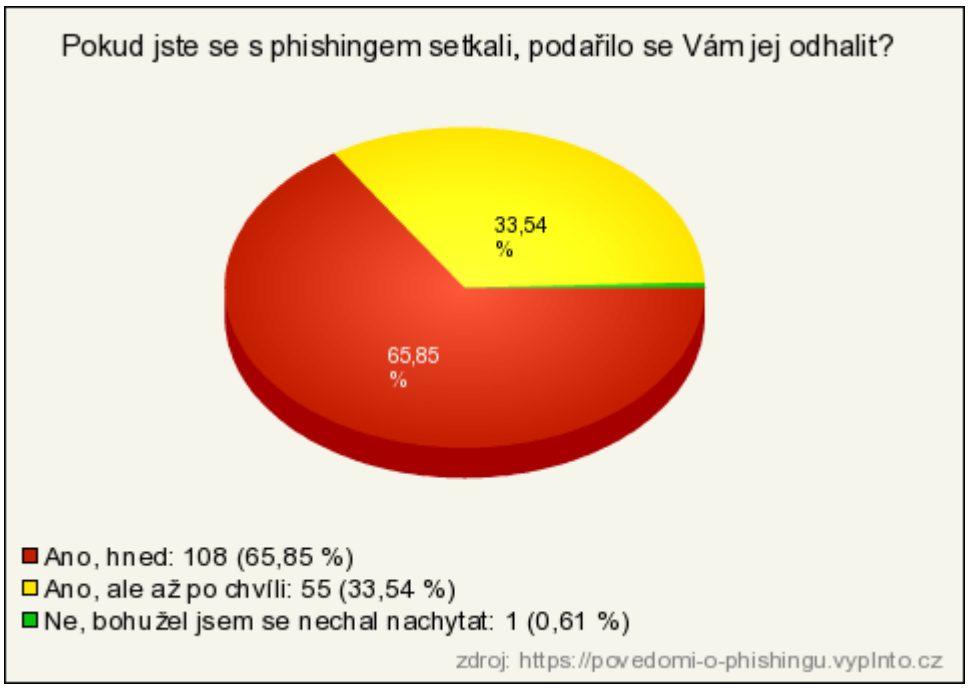
Graf 5: S jakým typem phishingu se respondenti setkali

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 5, která se zaměřovala na typy phishingových útoků, které respondenti zaznamenali, se ukázalo, že nejběžnější formou phishingu, kterou respondenti zažili, byl klasický phishing, tedy podezřelé e-maily s žádostí o přihlašovací údaje (84,76 %). Smishing, tedy phishing prostřednictvím SMS, byl zaznamenán u 64,63 % respondentů. Dále 50,61 % respondentů uvedlo, že se setkali s přesměrováním na falešnou webovou stránku (page hijacking), a 50 % s vishingem (hlasový phishing). Spear phishing, zaměřený na konkrétní osoby, uvedlo 32,93 % respondentů, a CEO fraud, podvodné e-maily vydávající se za vedení firmy, zaznamenalo 14,63 % dotazovaných. Další méně časté typy phishingu, jako quishing (QR kódy vedoucí na falešnou stránku), se vyskytly u 7,32 % respondentů. Ostatní specifické formy, jako whaling, marketplace podvody nebo požadavky na platbu poštovného, byly

zmíněny pouze u jednotlivých respondentů. Tento výsledek ukazuje, že phishingové útoky mají širokou škálu podob, přičemž některé, jako klasický phishing, jsou mnohem běžnější než jiné, více cílené metody.

Graf 6: Otázka č. 6 Pokud jste se s phishingem setkali, podařilo se Vám jej odhalit?

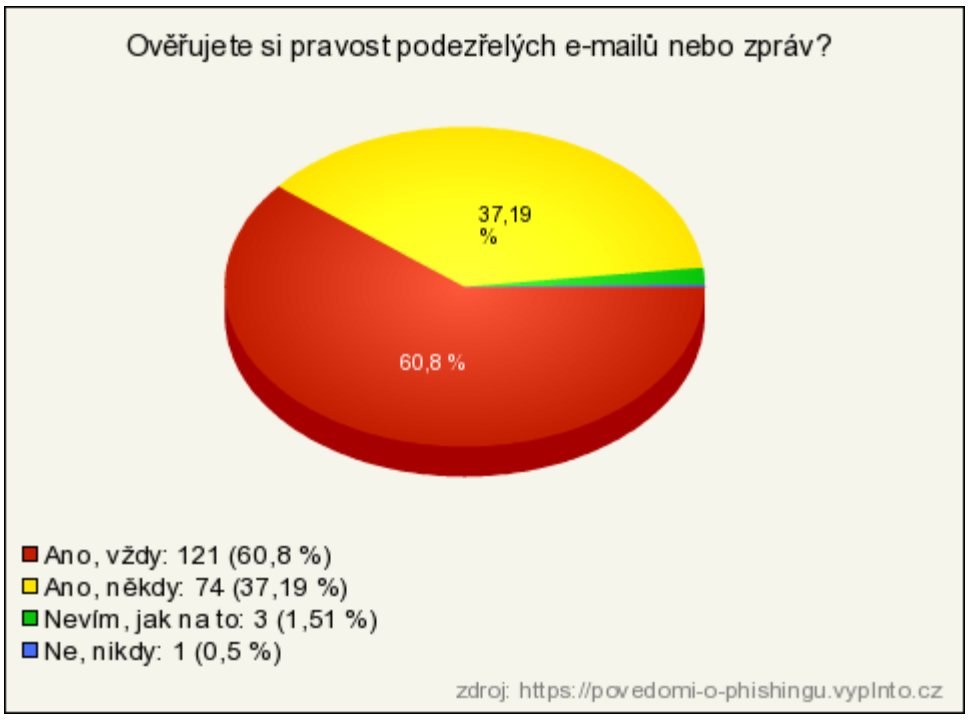


Graf 6: Odhalení phishingu

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 6, která se ptala, zda se respondentům podařilo phishing odhalit, pokud se s ním setkali, 65,85 % respondentů uvedlo, že phishing odhalili ihned. To naznačuje, že většina respondentů je schopná rozpoznat podvodné e-maily nebo zprávy ve chvíli, kdy je obdrží. 33,54 % respondentů přiznalo, že phishing odhalili až po nějaké chvíli, což ukazuje na určitou míru zranitelnosti, kdy podvodné zprávy působí přesvědčivě. Pouze 0,61 % respondentů uvedlo, že se nechali nachytat phishingovým útokem, což naznačuje, že většina účastníků výzkumu má dostatečné povědomí o této hrozbě. Tento výsledek naznačuje, že i když mnoho lidí phishing rozpozná, stále existuje prostor pro zlepšení rychlosti identifikace a prevence.

Graf 7: Otázka č.7 Ověřujete si pravost podezřelých e-mailů nebo zpráv?

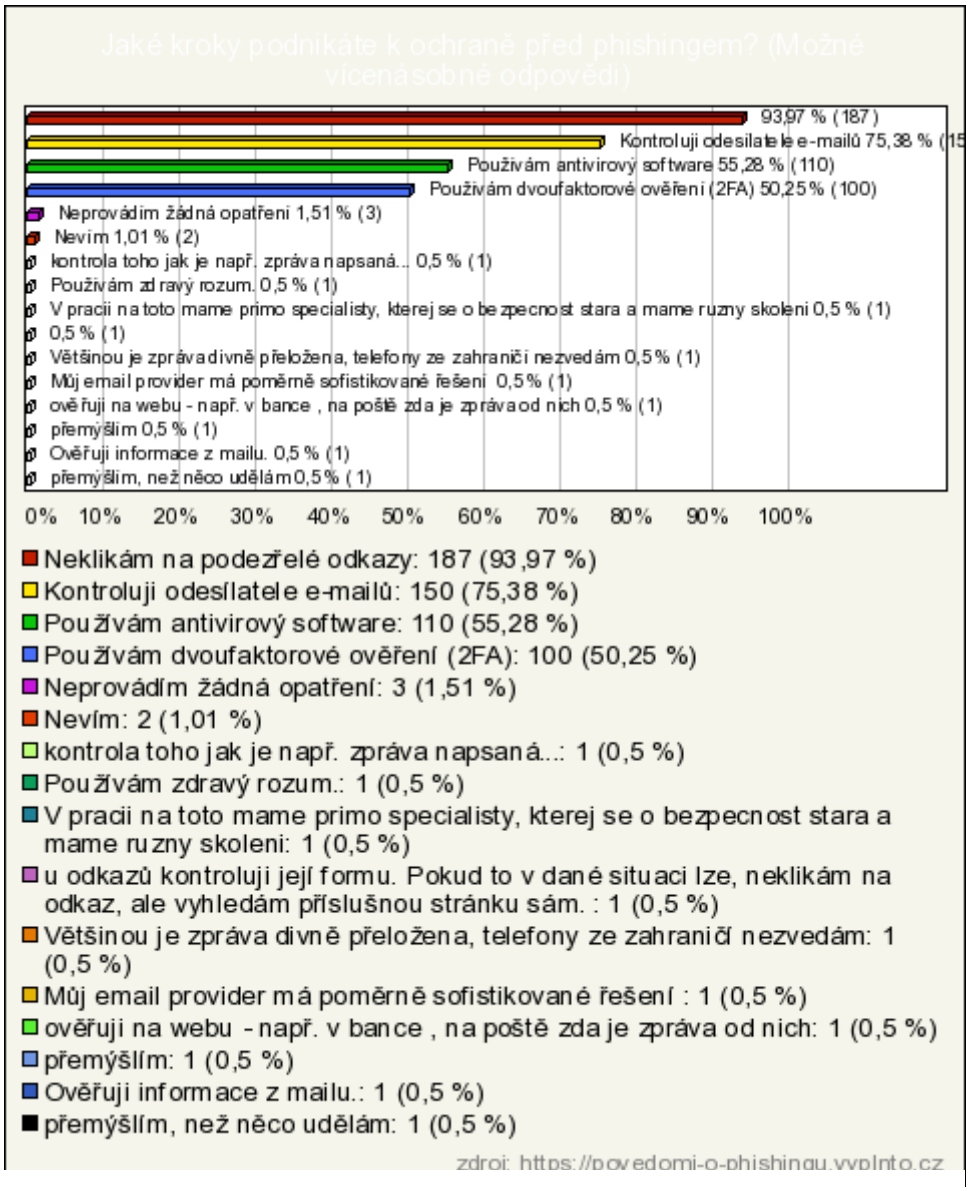


Graf 7: Ověření pravosti podezřelých e-mailů

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 7, která se týkala ověřování pravosti podezřelých e-mailů nebo zpráv, 60,8 % respondentů uvedlo, že vždy ověřují podezřelé zprávy, což naznačuje, že většina lidí má dobré bezpečnostní návyky a je obezřetná vůči phishingovým hrozbám. Dalších 37,19 % respondentů ověřuje pravost zpráv někdy, což znamená, že jsou si vědomi rizik, ale ověření neprovádějí vždy. Pouze 1,51 % respondentů si není jistých, jak správně ověřit pravost zpráv, a 0,5 % uvedlo, že nikdy podezřelé e-maily neověřují. Tento výsledek naznačuje, že většina respondentů věnuje pozornost bezpečnosti, ale stále existuje prostor pro zlepšení ve vzdělávání a prevenčních opatřeních v oblasti ověřování podezřelých e-mailů.

Graf 8: Otázka č.8 Jaké kroky podnikáte k ochraně před phishingem? (Možné vícenásobné odpovědi)



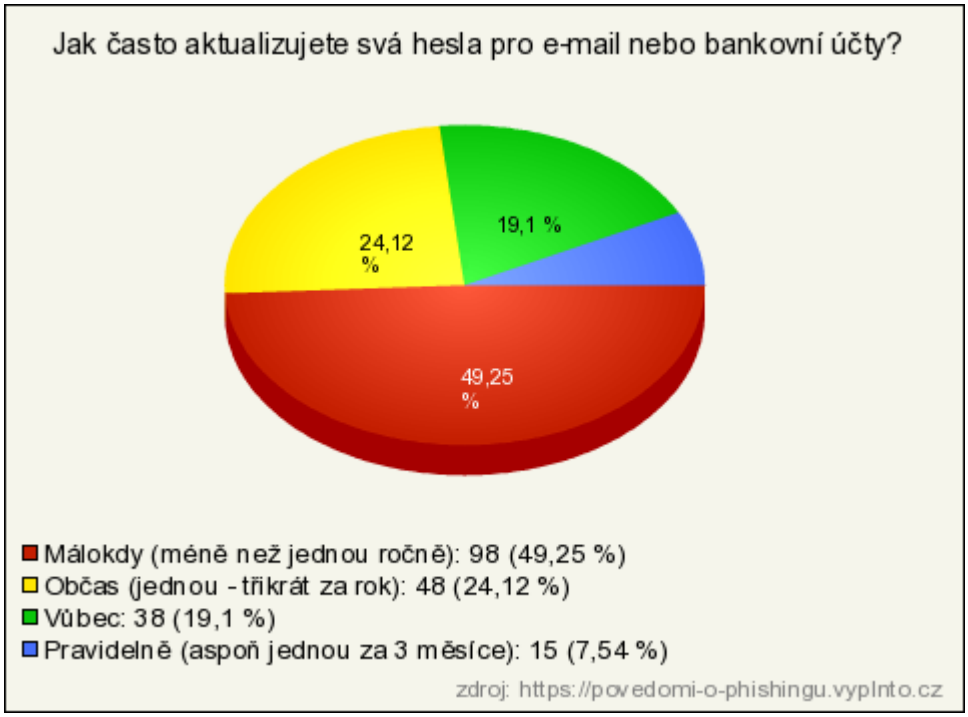
Graf 8: Ochrané kroky před phishingem

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 8, která se zaměřovala na konkrétní kroky, jež respondenti podnikají k ochraně před phishingem, 93,97 % respondentů uvedlo, že neklikají na podezřelé odkazy, což je nejčastěji zmiňované preventivní opatření. 75,38 % respondentů kontroluje odesílatele e-mailů, což svědčí o dobré obezřetnosti při práci s elektronickou poštou. Antivirový software používá 55,28 % dotazovaných a dvoufaktorové ověření (2FA) využívá 50,25 % respondentů. Naopak žádná opatření neprovádí 1,51 % a další 1,01 % si není jisto, jak se před phishingem chránit. Objevily se i zajímavé individuální odpovědi, například používání „zdravého rozumu“ nebo důvěra v zabezpečení firemního prostředí. Výsledky ukazují, že většina respondentů má

alespoň základní povědomí o preventivních opatřeních a aktivně je využívá, ačkoli stále existuje malá část, která ochranu podceňuje.

Graf 9: Otázka č.9 Jak často aktualizujete svá hesla pro e-mail nebo bankovní účty?



Graf 9: Jak často si respondenti mění heslo

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 9, která se týkala frekvence aktualizace hesel k e-mailovým nebo bankovním účtům, uvedla téměř polovina respondentů (49,25 %), že svá hesla mění méně než jednou ročně. Dalších 24,12 % hesla mění občas, tedy jednou až třikrát za rok, a 19,1 % respondentů přiznalo, že hesla nemění vůbec. Pouze 7,54 % dotazovaných uvedlo, že hesla aktualizují pravidelně, alespoň jednou za tři měsíce, což je z hlediska kybernetické bezpečnosti doporučovaný interval. Výsledky naznačují, že většina uživatelů nevěnuje dostatečnou pozornost pravidelné změně hesel, čímž zvyšuje riziko zneužití osobních údajů v případě úniku dat nebo phishingového útoku.

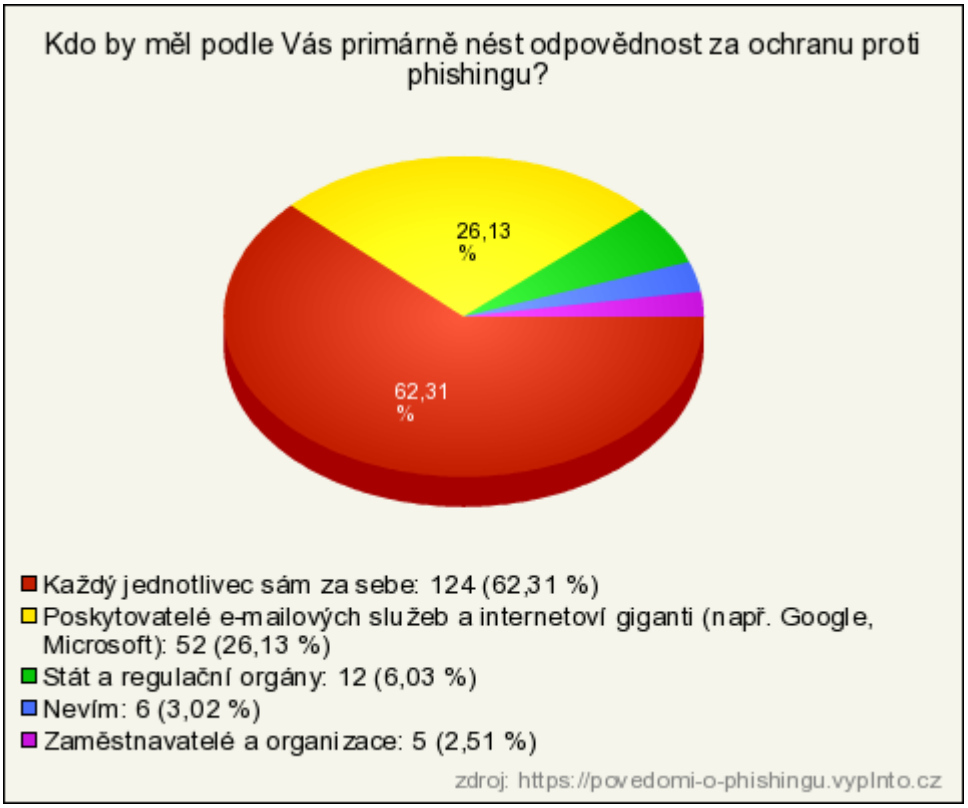
Graf 10: Otázka č.10 Jak závažnou hrozbu podle Vás phishing představuje?

Graf 10: Závažnost phishingu

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 10, která zjišťovala, jak závažnou hrozbu podle respondentů phishing představuje, označilo 46,23 % respondentů phishing za velmi závažnou hrozbu a dalších 44,72 % jej považuje za spíše závažný problém. To znamená, že téměř 91 % dotazovaných vnímá phishing jako riziko, kterému je třeba věnovat pozornost. Naopak pouze 5,53 % respondentů označilo phishing za spíše nezávažný a 1,01 % za zcela nezávažný. 2,51 % dotazovaných uvedlo, že nedokáže závažnost posoudit. Výsledky ukazují, že povědomí o rizicích spojených s phishingem je mezi veřejností vysoké, i když u malé části populace stále přetrvává nejistota nebo podcenění této hrozby.

Graf 11: Otázka č.11 Kdo by měl podle Vás primárně nést odpovědnost za ochranu proti phishingu?

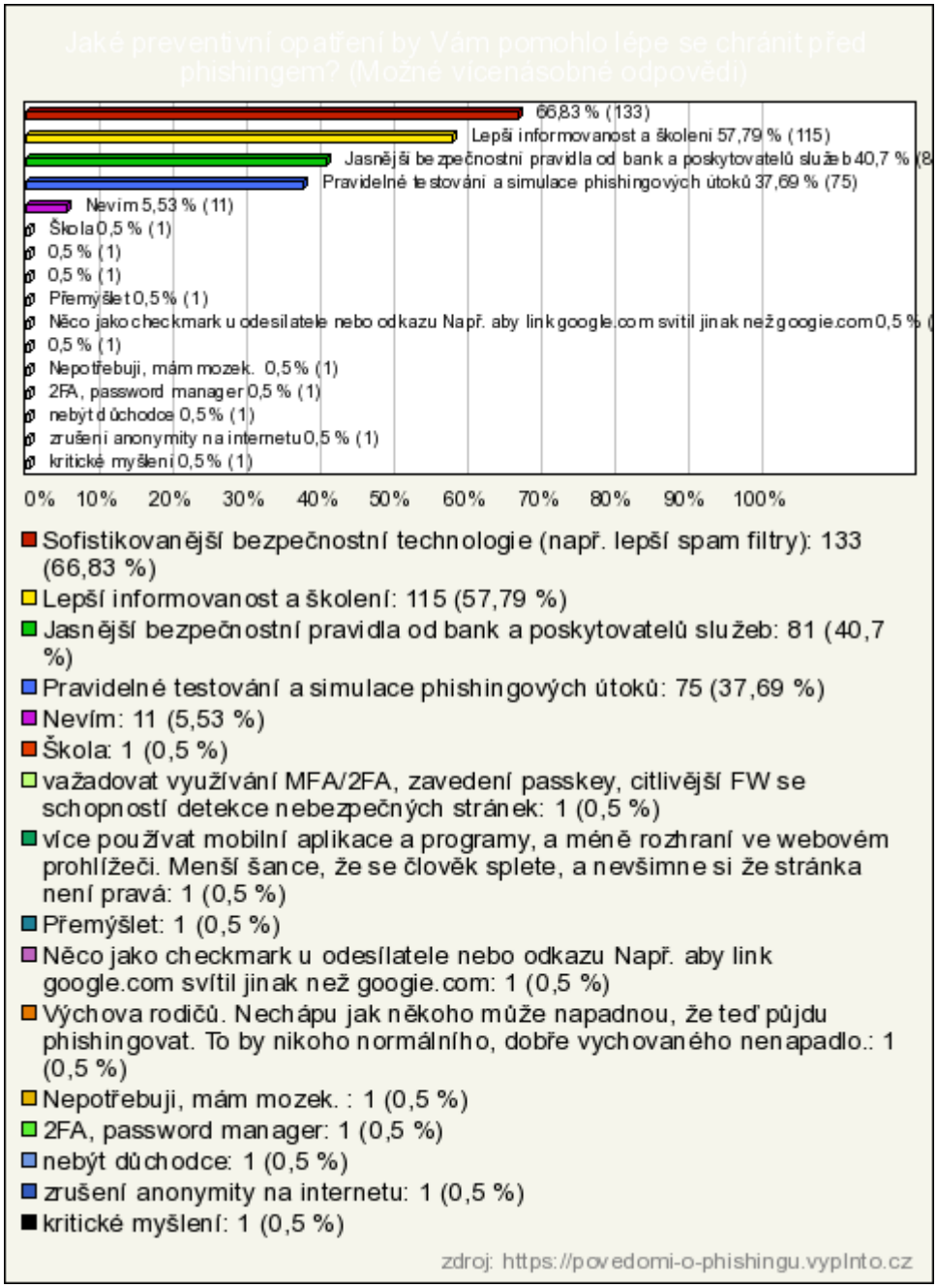


Graf 11: Odpovědnost za phishing

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 11, která se zaměřovala na to, kdo by měl podle respondentů nést primární odpovědnost za ochranu proti phishingu, uvedla většina respondentů (62,31 %), že odpovědnost by měl nést každý jednotlivec sám za sebe. Dalších 26,13 % respondentů přisuzuje tuto odpovědnost poskytovatelům e-mailových služeb a internetovým gigantům, jako jsou Google nebo Microsoft. 6,03 % se domnívá, že hlavní odpovědnost by měl mít stát a regulační orgány, zatímco pouze 2,51 % považuje za hlavní odpovědné zaměstnavatele a organizace. 3,02 % respondentů uvedlo, že neví, kdo by měl odpovědnost nést. Tyto výsledky ukazují, že veřejnost vnímá kybernetickou bezpečnost především jako osobní zodpovědnost, přestože technologické firmy a instituce hrají důležitou roli v ochraně uživatelů.

Graf 12: Otázka č.12 Jaké preventivní opatření by Vám pomohlo lépe se chránit před phishingem? (Možné vícenásobné odpovědi)



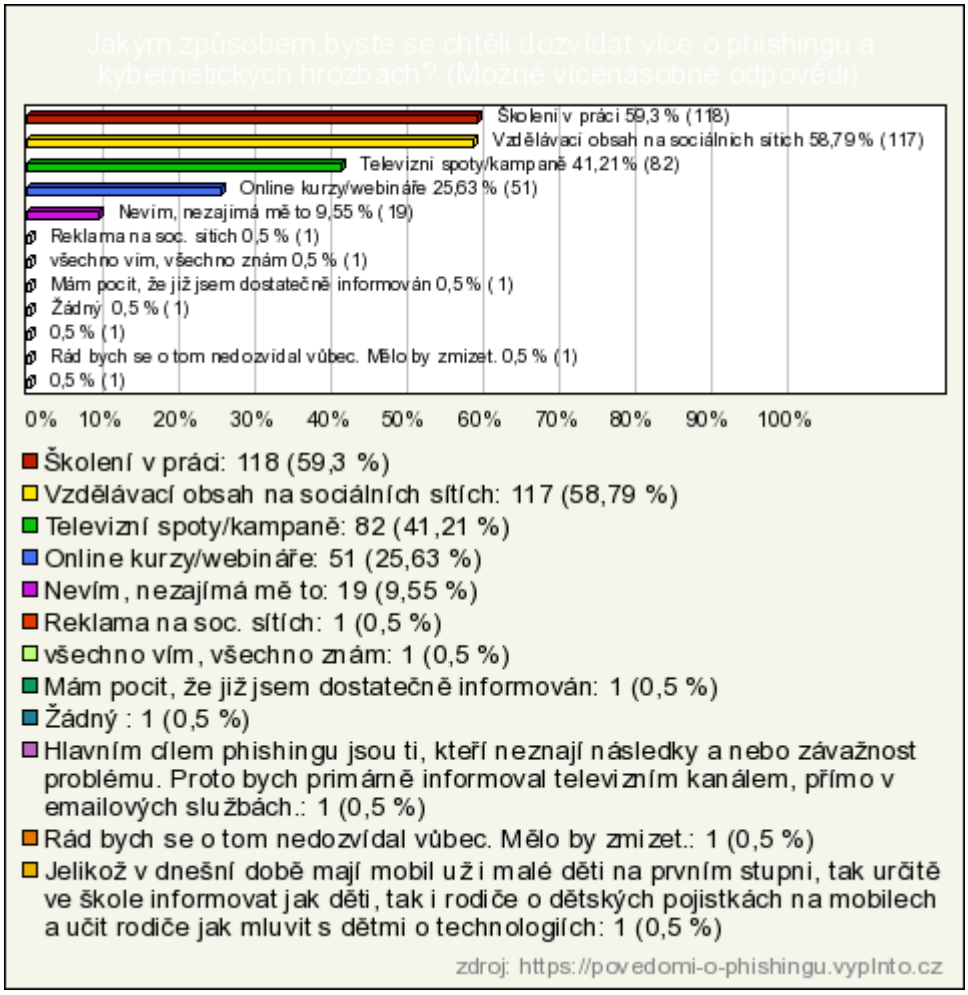
Graf 12: Opatření proti phishingu

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 12 respondenti vybírali, jaká preventivní opatření by jim nejvíce pomohla lépe se chránit před phishingem. Nejčastější odpovědí byla potřeba sofistikovanějších bezpečnostních technologií, například lepších spam filtrů, kterou zvolilo 66,83 % respondentů. Lepší informovanost a školení označilo jako užitečné 57,79 % dotazovaných, což ukazuje na vysokou poptávku po vzdělávání v oblasti kybernetické bezpečnosti. Jasnější bezpečnostní

pravidla od bank a poskytovatelů služeb by uvítalo 40,7 % respondentů a pravidelné testování a simulace phishingových útoků považuje za přínosné 37,69 % účastníků průzkumu. Menší podíl respondentů volil vlastní doplňující odpovědi, například důraz na kritické myšlení, anonymitu, školní výchovu nebo využívání dvoufaktorového ověření. Výsledky ukazují, že většina lidí by přivítala kombinaci technologických a vzdělávacích opatření, která by jim pomohla zvýšit svou bezpečnost v online prostředí.

Graf 13: Otázka č.13 Jakým způsobem byste se chtěli dozvídat více o phishingu a kybernetických hrozbách? (Možné vícenásobné odpovědi)



Graf 13: Způsob šíření povědomí o kyb. hrozbách

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 13 respondenti uváděli, jakou formou by se chtěli dozvídat více informací o phishingu a kybernetických hrozbách. Nejčastěji zmiňovanou formou bylo školení v práci, které by uvítalo 59,3 % dotazovaných. Těsně za tím následovala odpověď „vzdělávací obsah na sociálních sítích“ s 58,79 %, což ukazuje na rostoucí význam online platforem v oblasti osvěty. Televizní spoty a kampaně by preferovalo 41,21 % respondentů a online kurzy či webináře pak 25,63 %. Zároveň 9,55 % respondentů uvedlo, že je tato problematika nezajímá. Mezi doplňujícími odpověďmi se objevila například důvěra ve vlastní znalosti, návrhy na cílenou osvětu pro děti a rodiče, nebo i kritické postoje typu „rád bych se o tom nedozvídal vůbec“. Data ukazují, že většina veřejnosti má zájem o vzdělávání v oblasti phishingu, a to především v rámci zaměstnání nebo prostřednictvím běžně dostupných kanálů jako jsou sociální sítě a televize.

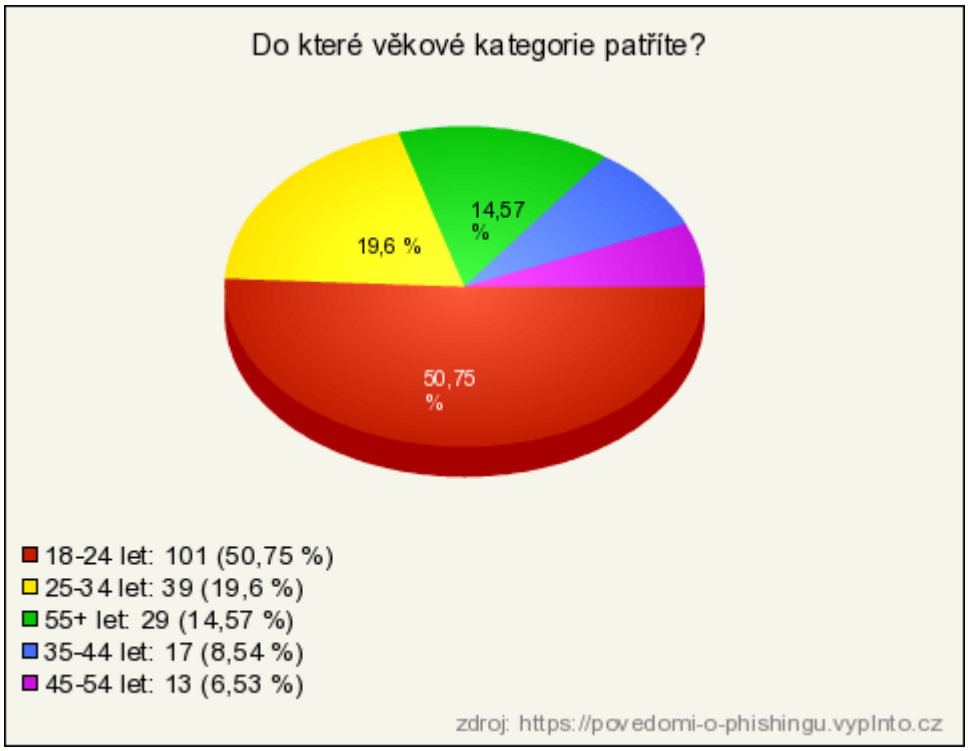
Graf 14: Otázka č.14 Jaké je Vaše pohlaví?

Graf 14: Pohlaví respondentů

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 14 respondenti uváděli své pohlaví. Největší podíl tvořili muži, kterých bylo 51,76 % (103 respondentů). Ženy představovaly 45,73 % (91 respondentek) a 2,51 % respondentů (5 osob) označilo jinou genderovou identitu nebo nechtělo na otázku odpovídat. Tyto výsledky ukazují, že se na dotazníkovém šetření podíleli respondenti poměrně rovnoměrně z obou hlavních genderových skupin, což napomáhá vyváženosti získaných dat a umožňuje případné srovnání v rámci analytické části výzkumu.

Graf 15: Otázka č.15 Do které věkové kategorie patříte?



Graf 15: Věkové skupiny respondentů

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 15 respondenti uváděli svou věkovou kategorii. Největší skupinu tvořili mladí lidé ve věku 18–24 let, kteří představovali 50,75 % všech dotázaných. Následovali respondenti ve věku 25–34 let s podílem 19,6 % a kategorie 55 a více let, kterou zastupovalo 14,57 % respondentů. Mezi věkovými skupinami 35–44 let a 45–54 let bylo zastoupení nižší, konkrétně 8,54 % a 6,53 %. Tyto výsledky ukazují, že se šetření zúčastnilo převážně mladší publikum, což může ovlivnit způsob vnímání kybernetických hrozeb i používané bezpečnostní návyky, zejména ve srovnání se staršími věkovými skupinami.

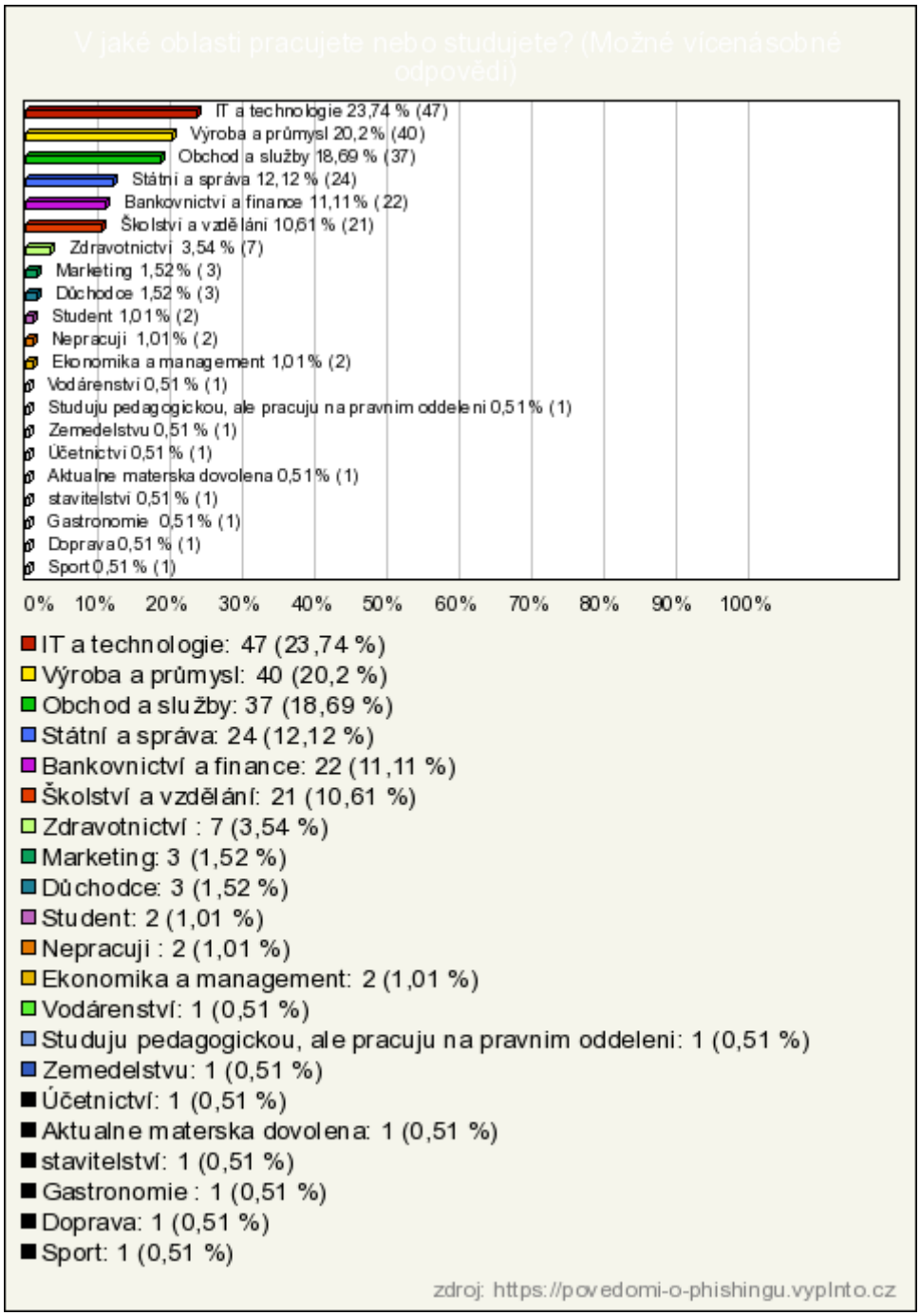
Graf 16: Otázka č.16 Jaké je Vaše nejvyšší dosažené vzdělání?

Graf 16: Vzdělání respondentů

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 16 respondenti uváděli své nejvyšší dosažené vzdělání. Největší podíl tvořili lidé se středoškolským vzděláním s maturitou, konkrétně 52,26 % respondentů. Vysokoškolské vzdělání magisterského nebo vyššího stupně uvedlo 18,09 % a bakalářský titul pak 15,58 % dotázaných. Středoškolské vzdělání bez maturity mělo 9,05 % respondentů a vyšší odborné vzdělání uvedlo 3,02 %. Základní vzdělání označilo 2,01 % účastníků šetření. Tyto výsledky ukazují, že se do výzkumu zapojila převážně vzdělanější část populace, což může ovlivňovat i jejich přístup k tématům kybernetické bezpečnosti a schopnost identifikovat phishingové hrozby.

Graf 17: Otázka č.17 V jaké oblasti pracujete nebo studujete? (Možné vícenásobné odpovědi)



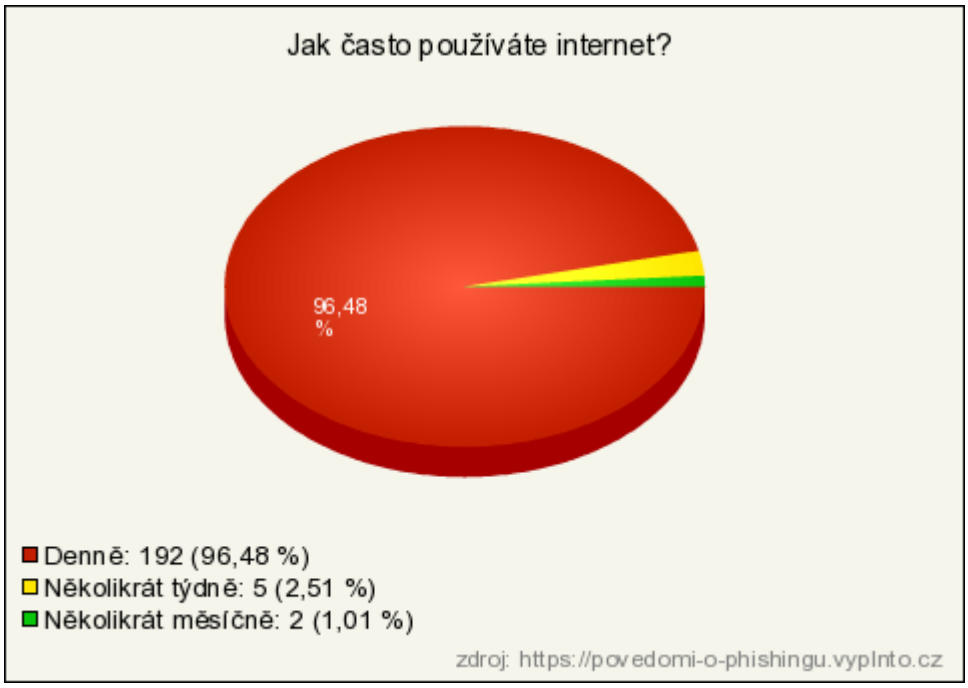
Graf 17: Oblast, v které respondenti pracují

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 17 respondenti uváděli oblast, ve které pracují nebo studují. Nejčastěji se v odpovědích objevovalo IT a technologie, které zastupovalo 23,74 % respondentů. Na druhém místě byla výroba a průmysl s 20,2 %, následovaná obchodem a službami (18,69 %) a státní správou (12,12 %). Poměrně rovnoměrně byli zastoupeni i respondenti z oblasti bankovnictví a financí (11,11 %) a školství a vzdělávání (10,61 %). Ostatní oblasti, jako je zdravotnictví,

marketing nebo účetnictví, byly zastoupeny méně. Mezi méně četnými odpověďmi se vyskytly i specifické poznámky jako „aktuálně na mateřské dovolené“ nebo „studuji pedagogickou, ale pracuji na právním oddělení“. Výsledky ukazují, že se dotazníkového šetření zúčastnili lidé z širokého spektra profesí, což přispívá k pestrosti pohledů na problematiku phishingu a kybernetické bezpečnosti.

Graf 18: Otázka č.18 Jak často používáte internet?

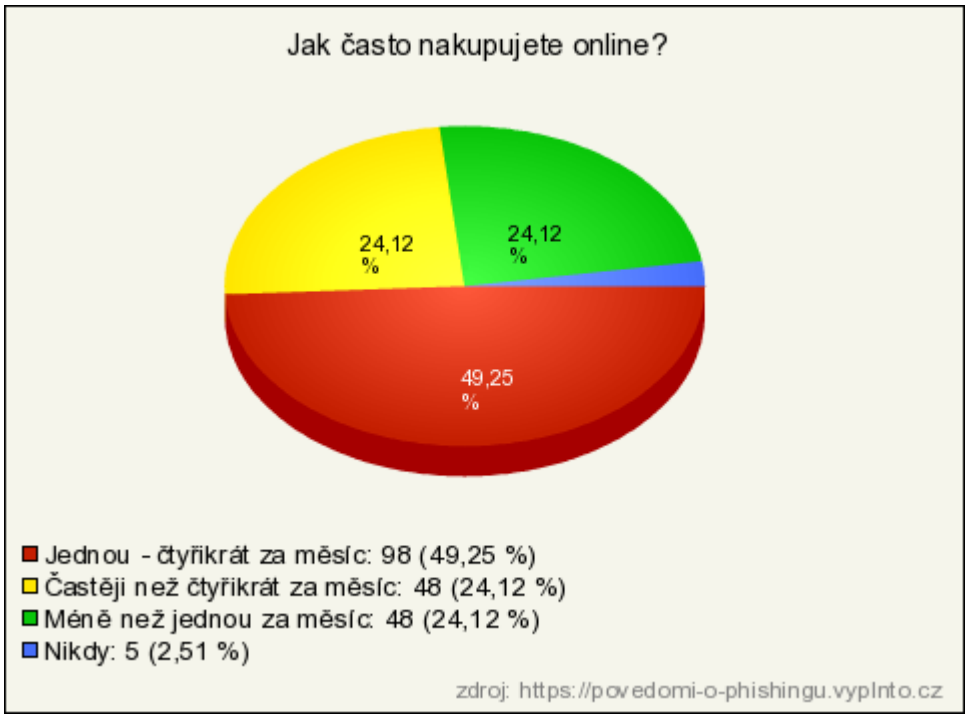


Graf 18: Jak často respondenti používají internet

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 18 respondenti odpovídali na frekvenci svého používání internetu. Drtivá většina dotazovaných (96,48 %) uvedla, že internet používá denně, což potvrzuje, že online prostředí je běžnou součástí každodenního života respondentů. Pouze 2,51 % respondentů používá internet několikrát týdně a 1,01 % uvedlo, že internet využívá jen několikrát měsíčně. Tyto výsledky ukazují, že většina účastníků průzkumu je pravidelně online, což je důležitý faktor při hodnocení jejich potenciální vystavenosti phishingovým útokům a dalších kybernetickým hrozbám.

Graf 19: Otázka č.19 Jak často nakupujete online? Rozdělení četností odpovědí.

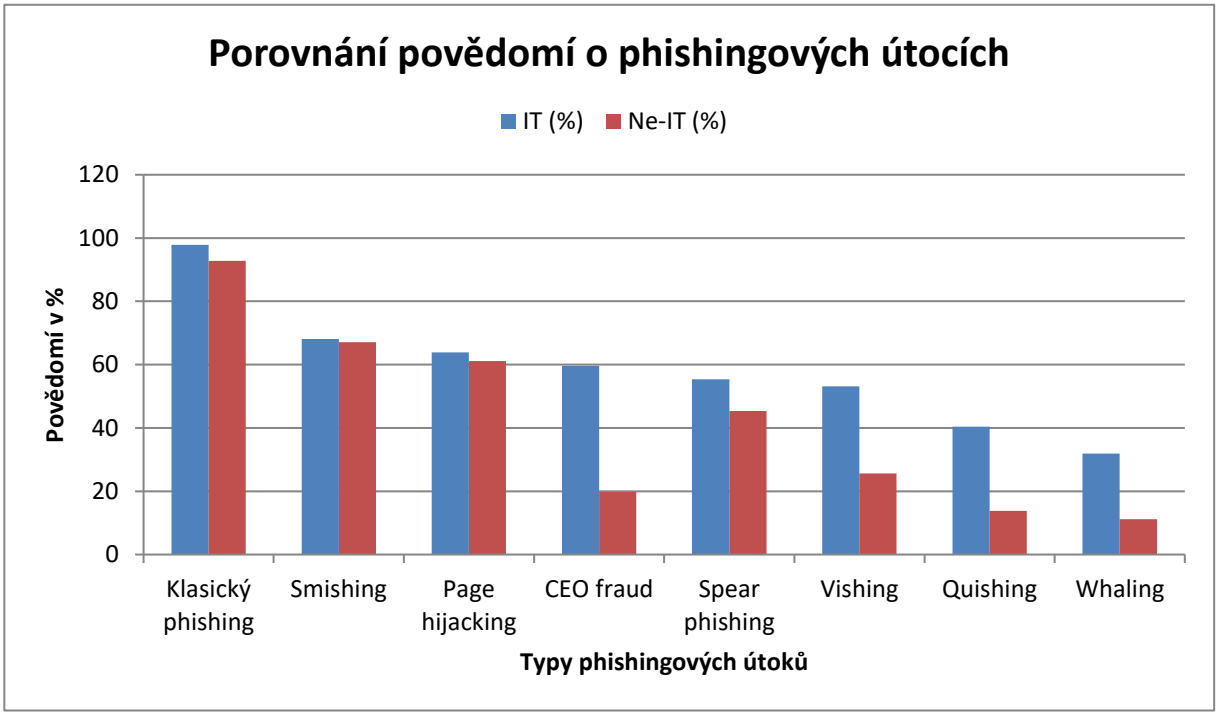


Graf 19: Nakupování online

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

V otázce č. 19 respondenti odpovídali, jak často nakupují online. Nejčastější odpovědí bylo, že nakupují jednou až čtyřikrát za měsíc, což uvedlo 49,25 % respondentů. Shodně po 24,12 % respondentů nakupuje buď častěji než čtyřikrát měsíčně, nebo naopak méně než jednou měsíčně. Pouze 2,51 % dotázaných odpovědělo, že online nenakupuje vůbec. Výsledky ukazují, že online nakupování je pro většinu respondentů běžnou součástí života, což je relevantní i z hlediska rizika phishingových útoků, které se často vážou právě k falešným e-shopům nebo podvodným e-mailům s informacemi o objednávkách.

V následující části se zaměřím na porovnání povědomí o phishingových útocích mezi respondenty z odvětví IT a těmi, kteří pocházejí z jiných profesních oblastí. Tento rozdíl je klíčový pro analýzu, zda má odvětví IT větší povědomí o phishingu díky své specializaci na technologické otázky. Je k tomu zde uveden graf, který vizuálně znázorní rozdíl v povědomí mezi těmito dvěma skupinami.

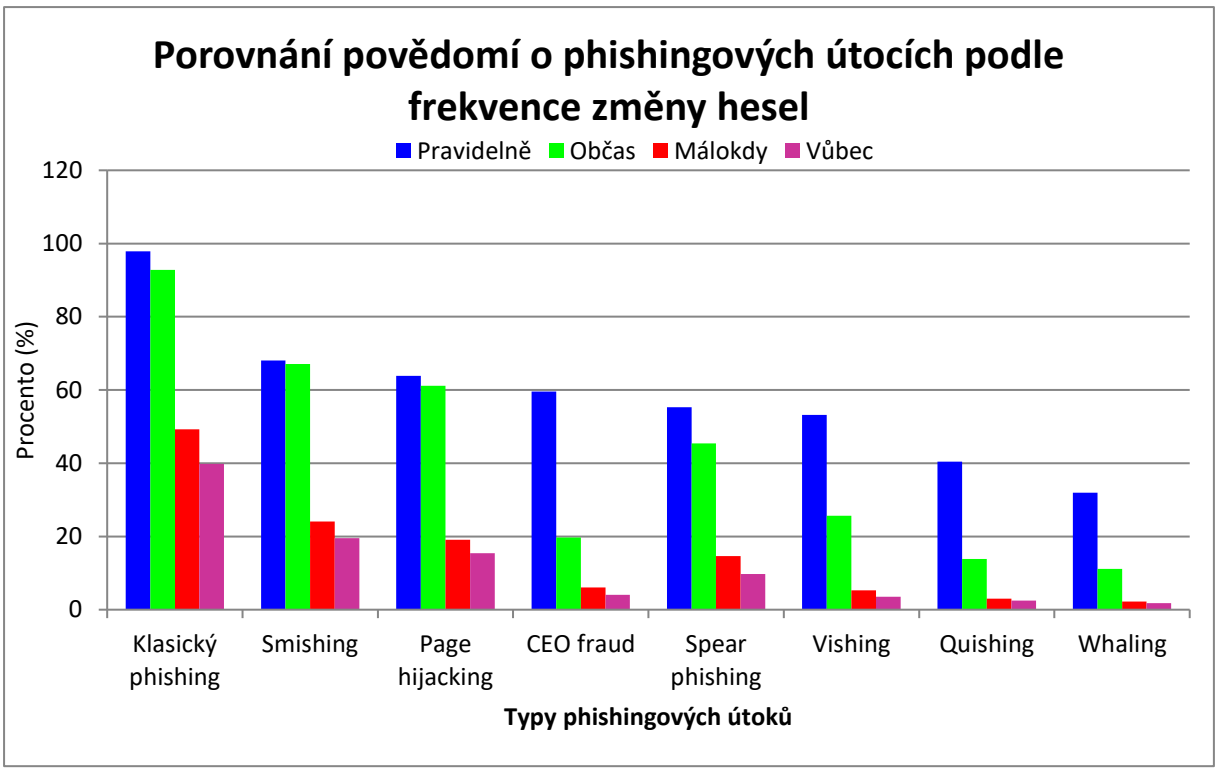


Graf 20: IT vs Ne-IT

Zdroj: vlastní zpracování

Na základě analýzy povědomí o phishingových útocích mezi respondenty z IT sektoru (47 respondentů) a ostatních profesních oblastí (152 respondentů) lze vyvodit, že odborníci z IT vykazují vyšší úroveň znalostí o phishingu, což naznačuje, že vzdělání, technologie a bezpečnostní školení v tomto sektoru přispívají k lepší schopnosti rozpoznat a reagovat na kyberhrozby. Naopak respondenti z jiných oblastí vykazují nižší povědomí, což zdůrazňuje potřebu širšího vzdělávání a osvěty o kybernetické bezpečnosti. Dále je patrné, že pravidelná změna hesel a další preventivní opatření vedou k lepší ochraně uživatelů. Tento výzkum tak podtrhuje nutnost investic do vzdělávání nejen pro IT odborníky, ale i pro veřejnost, aby byla celková kybernetická bezpečnost účinnější.

Následující část výzkumu je zaměřena na vztah mezi bezpečnostními návyky, konkrétně změnou hesel, a povědomím respondentů o phishingových útocích. Cílem bylo zjistit, zda respondenti, kteří si pravidelně mění hesla, vykazují vyšší úroveň informovanosti o phishingu než ti, kteří si hesla mění méně často nebo vůbec. Na základě výsledků tohoto výzkumu je zřejmé, že i když se pravidelná aktualizace hesel obecně považuje za důležitý krok k ochraně před kybernetickými hrozbami, toto chování není přímo propojeno s vyšší úrovní povědomí o phishingových útocích. Respondenti, kteří hesla nemění pravidelně, mohou mít stále dostatečné povědomí o těchto útocích, ale důvody pro jejich chování mohou být rozmanité. Tato zjištění ukazují, že samotná změna hesel není jediným indikátorem informovanosti o phishingu a že je třeba se zaměřit i na další aspekty kybernetické bezpečnosti.

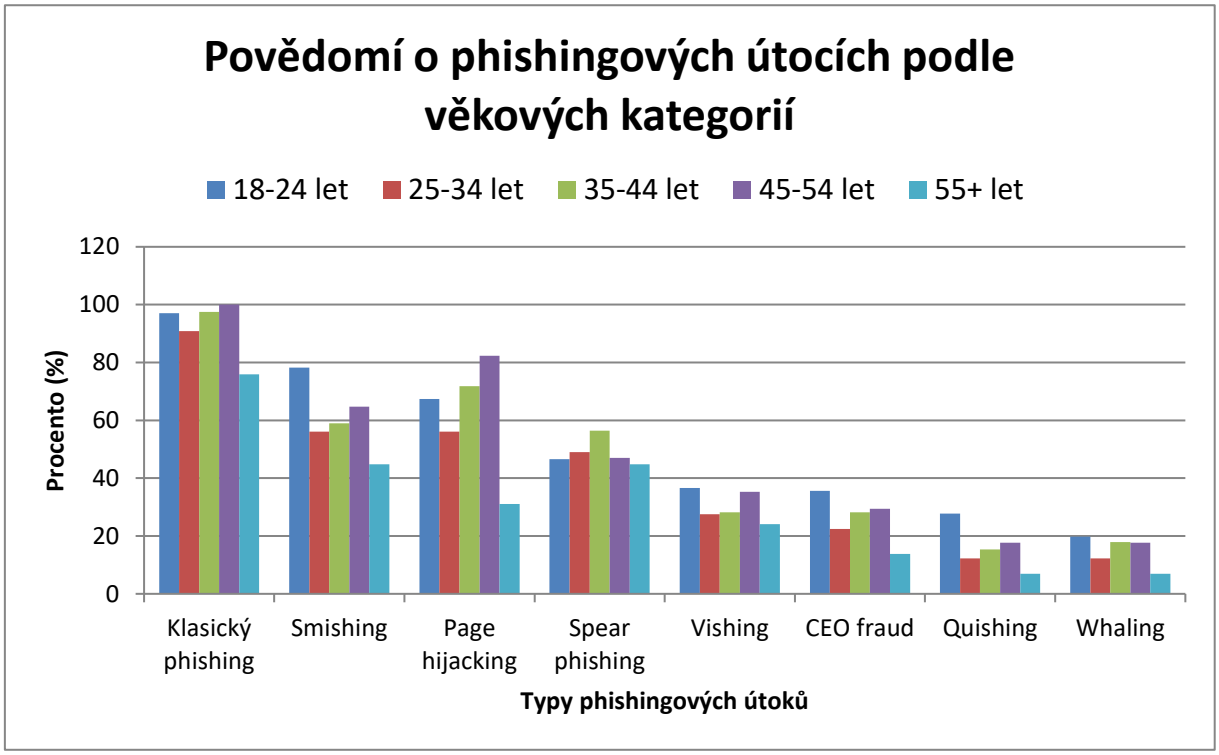


Graf 21: Vliv změny hesel na povědomí o phishingových útocích

Zdroj: vlastní zpracování

Na základě analýzy odpovědí není pravidelná změna hesel rozhodujícím faktorem pro vyšší informovanost o phishingu. I respondenti, kteří si hesla mění méně často, mohou mít dostatečné povědomí o phishingových útocích. Tento výsledek naznačuje, že povědomí o phishingu není automaticky spojeno s frekvencí změny hesel, a je potřeba se zaměřit na širší přístupy k zajištění kybernetické bezpečnosti.

Tato část výzkumu bude zaměřena na porovnání povědomí o phishingových útocích mezi jednotlivými věkovými skupinami. Cílem bylo zjistit, která věková kategorie vykazuje nejvyšší úroveň znalostí o různých typech phishingu a zda existují výrazné rozdíly mezi mladšími a staršími respondenty. V této souvislosti bude přiložen graf, který vizuálně ukáže, jak se povědomí o phishingových útocích liší mezi věkovými skupinami. Tento výzkum pomůže odhalit, zda mladší respondenti mají lepší přehled o phishingových hrozbách, nebo zda naopak starší generace vykazuje vyšší úroveň informovanosti, možná v důsledku jejich zkušeností s těmito hrozbami.

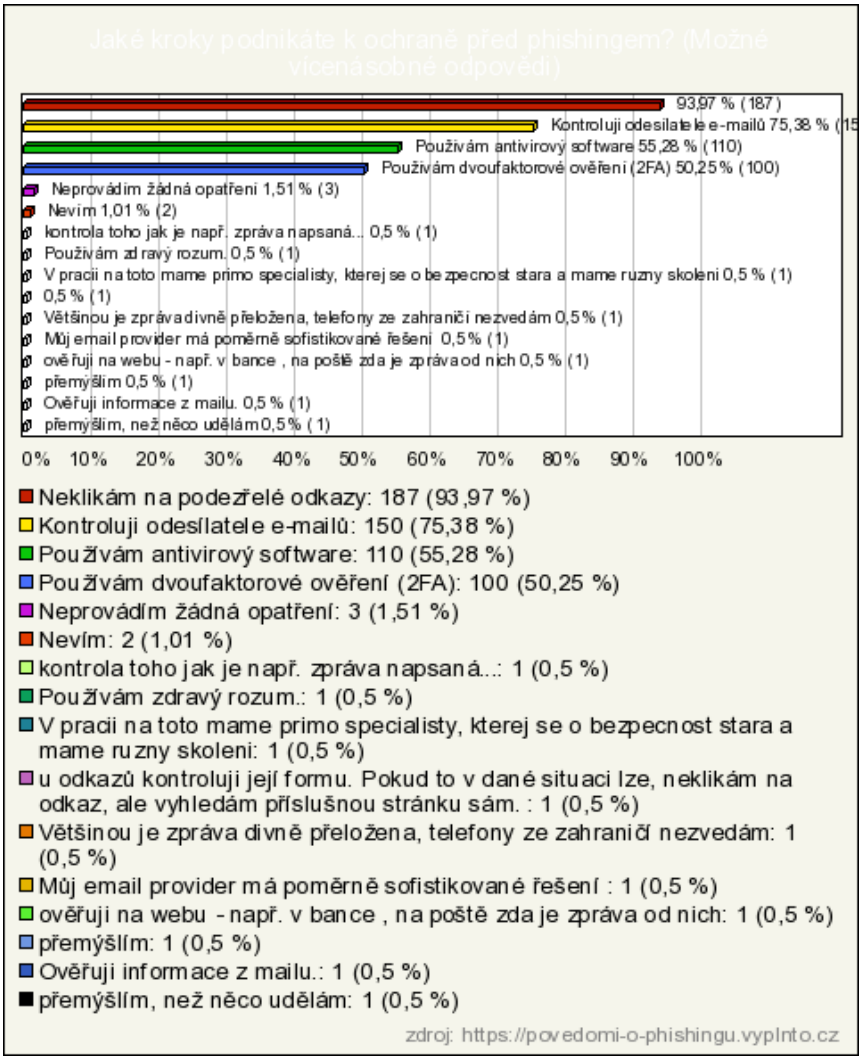


Graf 22: Povědomí o phishingových útocích podle věkových skupin

Zdroj: vlastní zpracování

Na základě analýzy dat z výzkumu můžeme konstatovat, že nejvíce informovaná je věková skupina 18-24 let, která měla nejen nejvyšší procento informovanosti o phishingu, ale také zahrnovala největší počet respondentů (101 z celkového vzorku). Tato skupina vykázala nejvyšší míru povědomí o phishingových útocích ve srovnání s ostatními věkovými kategoriemi, což může souviset s jejich častějšími online aktivitami a větší orientací na digitální technologie. Ostatní věkové skupiny vykazují nižší míru povědomí, což ukazuje na potřebu zacílit vzdělávací programy na starší věkové kategorie, které se často nacházejí mimo okruh digitálních technologií.

V rámci výzkumu o ochraně před phishingovými útoky se respondentům dostalo několika otázek týkajících se bezpečnostních opatření, která používají. Jedním z klíčových kroků, který byl často zmíněn, je neklikat na podezřelé odkazy, což je považováno za nejúčinnější ochranu proti phishingu. Tento krok zvolilo 93,97 % respondentů, což ukazuje, že je široce akceptován jako základní prevence. Tento výsledek podtrhuje i potřebu vyvinout sofistikovanější spam filtry a antivirový software, které by mohly zabránit doručení podezřelých e-mailů vůbec.



Graf 23: Kroky k ochraně

Zdroj: https://povedomi-o-phishingu.vyplnto.cz

Výsledky ukazují, že respondenti považují prevenci v podobě neklikání na podezřelé odkazy za nejdůležitější ochranný krok. Tento trend může být vnímán jako indikátor potřeby vývoje pokročilých nástrojů na ochranu proti phishingu, jako jsou efektivnější spam filtry a antivirové programy. Tyto nástroje by měly být navrženy tak, aby dokázaly včas a automaticky detekovat a blokovat podezřelé e-maily, než se dostanou k uživatelským schránkám.

ZÁVĚR

Hlavním cílem této bakalářské práce bylo komplexně představit problematiku podvodného jednání phishingu, zasadit jej do širšího rámce kybernetické kriminality a současně empiricky ověřit míru povědomí českých uživatelů internetu o této hrozbě.

Teoretická část nejprve objasnila základní pojmy, které tvoří východisko celé analýzy. Kyberprostor jako prostředí, v němž se odehrávají digitální interakce; kybernetický útok coby záměrná škodlivá aktivita v tomto prostoru; kybernetická hrozba jako potenciál způsobit škodu; kybernetická bezpečnost jako soubor opatření minimalizujících tato rizika; a konečně kybernetická kriminalita popsala vývoj phishingu, rozebrala jeho nejčastější podoby od klasického hromadného rozesílání podvodných e-mailů až po sofistikované techniky typu spear phishing, whaling, CEO fraud, page hijacking, smishing, vishing a quishing. U každého typu byly charakterizovány klíčové znaky, pravděpodobné následky pro oběť i doporučená preventivní opatření. Součástí práce bylo rovněž vymezení trestněprávních dopadů (např. § 209 Podvod, § 230 Neoprávněný přístup k počítačovému systému, § 231 Opatření a přechovávání přístupového zařízení či § 234 Padělání platebního prostředku) a hranice škody dle § 138 TZ, které určují závažnost skutku.

Praktická část se opírala o čtyři výzkumné otázky. Nejprve bylo zkoumáno, zda respondenti působící v IT oborech vykazují vyšší míru povědomí o phishingu než uživatelé z jiných profesních oblastí. Druhým sledovaným okruhem byla frekvence změny hesel: výzkum porovnával úroveň znalostí mezi těmi, kdo svá hesla pravidelně aktualizují (alespoň jednou za tři měsíce), a těmi, kteří je mění jen zřídka či vůbec. Třetí oblast se soustředila na vliv věku, konkrétně na to, zda skupina 18–24 let dosahuje nejvyšší informovanosti ve srovnání s ostatními věkovými kategoriemi. Poslední otázka mířila na preventivní praxi: zjišťovalo se, zda uživatelé vnímají jako nejúčinnější obranu „neklikat na podezřelé odkazy“ a nakolik toto zjištění podtrhuje potřebu vyvíjet pokročilejší spam-filtry a antivirové nástroje. Současně byly mapovány celkové postoje respondentů k riziku phishingu a jejich ochota přijímat další bezpečnostní opatření, jako jsou školení, dvoufaktorová autentizace či moderní technologie detekce hrozeb.

Na základě získaných výsledků lze doporučit několik kroků ke zlepšení povědomí a ochrany před phishingovými útoky. V první řadě by měly být školení zaměřena nejen na odborníky v IT, ale také na širší veřejnost, zejména starší generace, které mají nižší povědomí o moderních hrozbách. Je důležité se zaměřit na praktické ukázky, jak rozpoznat podvodné

e-maily nebo zprávy. Firmy by měly implementovat silnější bezpečnostní opatření, jako je dvoufaktorová autentizace a správci hesel, a ne spoléhat pouze na častou změnu hesel. Poskytovatelé e-mailových služeb by mohli zlepšit filtrování podezřelých zpráv, aby se k uživatelům vůbec nedostaly. Stát by mohl nabídnout snadno dostupné informace a nástroje pro nahlášení phishingových útoků, čímž by podpořil rychlou reakci a prevenci. V konečném důsledku je důležité, aby se bezpečnostní informace a strategie sdílely mezi jednotlivci, firmami a organizacemi, což pomůže lépe čelit novým hrozbám.

POUŽITÁ LITERATURA

ALKHALIL, Zainab, HEWAGE, Chaminda a NAWAF, Liqaa. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.* Frontiers in Computer Science [online]. 2021, vol. 3. Dostupné z: https://doi.org/10.3389/fcomp.2021.563060

CHAUDHARY, Sunil. *Recognition of phishing attacks utilizing anomalies in phishing websites.* Tampere: University of Tampere, 2012. Diplomová práce. Dostupné z: https://trepo.tuni.fi/handle/10024/84169

CROSSREALMS INTERNATIONAL. *CrossRealms International* [online]. Chicago: CrossRealms, [cit. 2025-04-13]. Dostupné z: https://crossrealms.com/

E-BEZPEČÍ. *Co je quishing* [online]. [n. d.] [cit. 2025-02-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/57-rizikove-jevy/4062-co-je-quishing

ESET, spol. s r.o. *ESET – Malware Protection & Internet Security* [online]. Bratislava: ESET, spol. s r.o., [cit. 2025-04-13]. Dostupné z: https://www.eset.com

EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2021* [online]. Haag: European Union Agency for Law Enforcement Cooperation, 2021 [cit. 2025-04-13]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

IC3 – Internet Crime Complaint Center. *HOLIDAY SHOPPING TIPS* [online]. 18. listopad 2010[cit. 2025-02-17]. Dostupné z: https://www.ic3.gov/PSA/2010/PSA101118.pdf

IC3 – Internet Crime Complaint Center. *PSA 170504* [online]. 4. květen 2017 [cit. 2025 02 17]. Dostupné z: https://www.ic3.gov/PSA/2017/PSA170504

JAKOBSSON, Markus a MYERS, Steven, eds. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* Hoboken: John Wiley & Sons, 2006. ISBN 978-0-471-99838-9.

JELÍNEK, Jiří. *Kriminologie.* Praha: Leges, 2021. Teoretik. ISBN 978-80-7502-499-2.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

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

KASPERSKY. *Phishing Prevention: 10 Tips to Stay Safe* [online]. [n. d.] [cit. 2025-02-17]. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

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

LANCE, James. *Phishing bez záhad.* 1. vyd. Přeložil Lubomír Moudrý. Praha: Grada, 2007. ISBN 978-80-247–1766-1.

MESH SECURITY LIMITED. *What is CEO Fraud and how do you protect against it?* [online]. Dublin: Mesh Security, [cit. 2025-04-13]. Dostupné z: https://www.meshsecurity.io/ceo-fraud

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Oficiální web NÚKIB* [online]. Brno: NÚKIB, [cit. 2025-04-13]. Dostupné z: https://www.nukib.gov.cz

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Phishing – stále aktuální hrozba* [online]. Brno: NÚKIB, 2015 [cit. 2025-04-13]. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Sociální inženýrství* [online]. Brno: NÚKIB, 2016 [cit. 2025-04-13]. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Spear phishing a jak se před ním chránit* [online]. Brno: NÚKIB, [cit. 2025-04-13]. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Spear phishing a jak se před ním chránit* [online]. Brno: NÚKIB, [cit. 2025-04-13]. Dostupné z: https://nukib.gov.cz/download/publikace/analyzy/Spear-phishing_a_jak_se_pred_nim_chranit.pdf

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Spear phishing a jak se před ním chránit* [online]. Brno: NÚKIB, 2020 [cit. 2025-04-13]. (Druhá verze téhož dokumentu)

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Základy kybernetické bezpečnosti 25* [online]. Brno: NÚKIB, [cit. 2025-04-13]. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=221

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023* [online]. Brno: NÚKIB, 2024 [cit. 2025-04-13]. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

OLLMANN, Gunter. *The Phishing Guide: Understanding & Preventing Phishing Attacks* [online]. Atlanta: IBM Internet Security Systems, 2004 [cit. 2025-04-13]. Dostupné z: https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems

RADA EVROPSKÉ UNIE. *Kybernetická bezpečnost: sociální inženýrství* [online]. Brusel: Consilium.europa.eu, [cit. 2025-04-13]. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity-social-engineering/

ŘEHÁK, R. *Povědomí o phishingu (výsledky průzkumu)* [online]. 2025 [cit. 2025-04-13]. Dostupné z: https://povedomi-o-phishingu.vyplnto.cz/

SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Pro praxi. ISBN 978-80-7380-501-2.

ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

TELECOM INFRASTRUCTURE CORP. *What is a whaling attack (whaling phishing)?* [online]. Needham: TechTarget, [cit. 2025-04-13]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/whaling

TWINGATE. *Page Hijacking Attack* [online]. [n. d.] [cit. 2025-02-17]. Dostupné z: https://www.twingate.com/blog/glossary/page-hijacking-attack

ZÁKON č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. *Praha: Sbírka*

zákonů, 2005. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127

ZÁPADOČESKÁ UNIVERZITA V PLZNI. *Phishing* [online]. Plzeň: HelpDesk ZČU, [cit. 2025-04-13]. Dostupné z: https://helpdesk.zcu.cz/wiki/Phishing

ZÁPADOČESKÁ UNIVERZITA V PLZNI. *Phishing – příklady* [online]. Plzeň: HelpDesk ZČU, [cit. 2025-04-13]. Dostupné z: https://helpdesk.zcu.cz/wiki/Phishing_-_p%C5%99%C3%ADklady

SEZNAM PŘÍLOH

PŘÍLOHA A

Dobrý den,

rád bych Vás poprosil o vyplnění dotazníku, který se týká phishingu (typ internetového podvodu). Cílem je zmapovat povědomí veřejnosti o různých typech phishingových útoků, jejich zkušenosti a také bezpečnostní návyky respondentů.

Dotazník je anonymní a Vaše odpovědi budou sloužit pouze pro lepší pochopení dané problematiky. Vyplnění dotazníku Vám zabere přibližně 5 minut.

Děkuji za Váš čas a upřímné odpovědi.

povinná otázka

1. Slyšeli jste někdy už o termínu phishing?

- ○ Ano
- ○ Ne

povinná otázka

2. Jak byste definovali phishing?

- ○ Podvodná technika, při níž útočník manipuluje oběť k odhalení citlivých údajů
- ○ Počítačový virus, který infikuje zařízení
- ○ Způsob šifrování dat
- ○ Nevím

povinná otázka

3. Které z následujících typů phishingových útoků znáte? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- ☐ Klasický phishing (hromadné podvodné emaily)
- ☐ Spear phishing (cílený útok na konkrétní osobu)
- ☐ Whaling (útok na vysoké manažery)
- ☐ CEO fraud (podvodné e-maily vydávající se za ředitele)
- ☐ Smishing (phishing přes SMS)
- ☐ Vishing (hlasový phishing)
- ☐ Quishing (phishing přes QR kódy)
- ☐ Page hijacking (přesměrování na falešné webové stránky)
- ☐ Žádný z výše uvedených

povinná otázka

4. Setkali jste se někdy s phishingovým útokem?

- ○ Ano, často
- ○ Ano, jednou nebo dvakrát
- ○ Ne, nikdy
- ○ Nevím

povinná otázka

5. Pokud ano, jaký typ phishingového útoku jste zaznamenali? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- ☐ Podezřelý e-mail s žádostí o přihlašovací údaje (klasický phishing)
- ☐ Podezřelý e-mail zaměřený na mě osobně (spear phishing)
- ☐ Podezřelý e-mail vydávající se za vedení firmy (CEO fraud)
- ☐ Podezřelý e-mail zaměřený na vrcholového manažera nebo vedoucího pracovníka (whaling)
- ☐ Podezřelá SMS (smishing)
- ☐ Podezřelý telefonát (vishing)
- ☐ QR kód vedoucí na falešnou stránku (quishing)
- ☐ Přesměrování na falešnou stránku (page hijacking)
- ☐ Jiný typ – prosím uveďte: _____

povinná otázka

6. Pokud jste se s phishingem setkali, podařilo se Vám jej odhalit?

- ○ Ano, hned
- ○ Ano, ale až po chvíli
- ○ Ne, bohužel jsem se nechal nachytat
- ○ Nevím

povinná otázka

7. Ověřujete si pravost podezřelých e-mailů nebo zpráv?

- ○ Ano, vždy
- ○ Ano, někdy
- ○ Ne, nikdy
- ○ Nevím, jak na to

povinná otázka

8. Jaké kroky podnikáte k ochraně před phishingem? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- ☐ Neklikám na podezřelé odkazy
- ☐ Kontroluji odesílatele e-mailů
- ☐ Používám dvoufaktorové ověření (2FA)
- ☐ Používám antivirový software
- ☐ Neprovádím žádná opatření
- ☐ Nevím
- ☐ Jiný typ – uveďte prosím jaký: _____

povinná otázka

9. Jak často aktualizujete svá hesla pro e-mail nebo bankovní účty?

- ○ Pravidelně (aspoň jednou za 3 měsíce)
- ○ Občas (jednou – třikrát za rok)
- ○ Málokdy (méně než jednou ročně)
- ○ Vůbec

povinná otázka

10. Jak závažnou hrozbu podle Vás phishing představuje?

- ○ Velmi závažnou
- ○ Spíše závažnou
- ○ Spíše nezávažnou
- ○ Nezávažnou

povinná otázka

11. Kdo by měl podle Vás primárně nést odpovědnost za ochranu proti phishingu?

- ○ Každý jednotlivec sám za sebe
- ○ Zaměstnavatelé a organizace
- ○ Poskytovatelé e-mailových služeb a internetoví giganti (např. Google, Microsoft)
- ○ Stát a regulační orgány
- ○ Nevím

povinná otázka

12. Jaké preventivní opatření by Vám pomohlo lépe se chránit před phishingem? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- [ ] Lepší informovanost a školení
- [ ] Jasnější bezpečnostní pravidla od bank a poskytovatelů služeb
- [ ] Sofistikovanější bezpečnostní technologie (např. lepší spam filtry)
- [ ] Pravidelné testování a simulace phishingových útoků
- [ ] Nevím
- [ ] Jiné – uveďte prosím jaké:

povinná otázka

13. Jakým způsobem byste se chtěli dozvídat více o phishingu a kybernetických hrozbách? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- [ ] Online kurzy/webináře
- [ ] Školení v práci
- [ ] Vzdělávací obsah na sociálních sítích
- [ ] Televizní spoty/kampaně
- [ ] Nevím, nezajímá mě to
- [ ] Jiný způsob – uveďte prosím jaký:

povinná otázka

14. Jaké je Vaše pohlaví?

- ○ Muž
- ○ Žena
- ○ Jiná identita / Nechci odpovídat

povinná otázka

15. Do které věkové kategorie patříte?

- ○ 18–24 let
- ○ 25–34 let
- ○ 35–44 let
- ○ 45–54 let
- ○ 55+ let

povinná otázka

16. Jaké je Vaše nejvyšší dosažené vzdělání?

- ○ Základní
- ○ Středoškolské bez maturity
- ○ Středoškolské s maturitou
- ○ Vyšší odborné vzdělání
- ○ Vysokoškolské (bakalářské)
- ○ Vysokoškolské (magisterské a vyšší)

povinná otázka

17. V jaké oblasti pracujete nebo studujete? (Možné vícenásobné odpovědi)

Zvolte alespoň jednu možnost.

- [ ] IT a technologie
- [ ] Bankovnictví a finance
- [ ] Státní a správa
- [ ] Školství a vzdělání
- [ ] Obchod a služby
- [ ] Výroba a průmysl
- [ ] Jiné – uveďte:

povinná otázka

18. Jak často používáte internet?

- ○ Denně
- ○ Několikrát týdně
- ○ Několikrát měsíčně
- ○ Zřídka

povinná otázka

19. Jak často nakupujete online?

- ○ Častěji než čtyřikrát za měsíc
- ○ Jednou – čtyřikrát za měsíc
- ○ Méně než jednou za měsíc
- ○ Nikdy