



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH A REALIZACE PHISHINGOVÉ KAMPANĚ

DESIGN AND IMPLEMENTATION A PHISHING CAMPAIGN

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Šárka Kosková

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Petr Sedlák

BRNO 2024

Zadání diplomové práce

Ústav: Ústav informatiky
Studentka: **Bc. Šárka Kosková**
Studijní program: Informační management
Vedoucí práce: **Ing. Petr Sedlák**
Akademický rok: 2023/24

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh a realizace phishingové kampaně

Charakteristika problematiky úkolu:

Úvod

Cíle práce, metody a postupy zpracování

Teoretická východiska práce

Analýza současného stavu

Návrh řešení a přínos návrhu řešení

Závěr

Seznam použité literatury

Cíle, kterých má být dosaženo:

Cílem práce je návrh a implementace phishingové kampaně pro zkvalitnění budování bezpečnostního povědomí ve společnosti.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, Praha: Česká agentura pro standardizaci, 2023.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, Praha: Česká agentura pro standardizaci, 2023.

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK, Řízení kybernetické bezpečnosti a bezpečnosti informací, Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

SEDLÁK Petr, Martin KONEČNÝ, Přeměna ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24.

V Brně dne 23.4.2024

L. S.

doc. Ing. Vojtěch Bartoš, Ph.D.

děkan

doc. Ing. Miloš Koch, CSc.

garant

Abstrakt:

Hlavním cílem diplomové práce je seznámit čtenáře s problematikou podvodného jednání přesněji phishingem. Teoretická část definuje základní pojmy související s tímto tématem jakožto například informační a kybernetická bezpečnost, phishing (historii a druhy), spam, sociální inženýrství, právní odpovědnosti a preventivní opatření podvodného jednání apod. Praktická část se zabývá vytvořením phishingové kampaně cílené na zaměstnance konkrétní firmy, díky níž je možné posoudit celkovou informační bezpečnost. Po vyhodnocení kampaně dochází ke zhodnocení, zda byla kampaň efektivní a co mohlo úspěšnost ovlivnit.

Klíčová slova:

Phishing, podvodné jednání, kampaň, útok

Abstract:

The theoretical part defines the basic concepts related to this topic such as information and cyber security, phishing (history and types), spam, social engineering, legal responsibilities and preventive measures of fraudulent behaviour, etc. The practical part deals with the creation of a phishing campaign targeting the employees of a specific company, thanks to which it is possible to assess the overall information security. Once the campaign has been evaluated, an assessment is made as to whether the campaign was effective and what may have influenced its success.

Keywords:

Phishing, fraud, campaign, attack

Bibliografická citace

KOSKOVÁ, Šárka. Návrh a realizace phishingové kampaně [online]. Brno, 2024 [cit. 2024-02-11]. Dostupné z: <https://www.vut.cz/studenti/zav-prace/detail/158743>. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že diplomová práce je původní a zpracovala jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 23.4. 2024

.....

Bc. Šárka Kosková

autor

Poděkování

Ráda bych poděkovala vedoucímu mé diplomové práce Ing. Petru Sedlákoví, za odborný přístup, vedení, ochotu, cenné rady a věcné připomínky. Dále poděkování patří společnosti, pro kterou byla phishingová kampaň navrhována, za poskytnutí potřebných informací a spolupráci. Následně zaměstnancům oddělení bezpečnosti této společnosti a mému oponentovi. V poslední řadě mé rodině za podporu při studiu.

Obsah

1	Úvod.....	11
2	Cíl práce, metody a postupy při zpracování	12
3	Teoretická východiska práce	13
3.1	ISMS	14
3.2	Hacker vs cracker.....	14
3.3	Sociální inženýrství.....	15
3.4	Spam vs. phishing	16
4	Phishing	18
4.1	Jak poznat phishing.....	19
4.2	Druhy phishingu	22
4.2.1	E-mail phishing (bulk phishing)	22
4.2.2	BEC (Business Email Compromise).....	23
4.2.3	Clone.....	24
4.2.4	Spear phishing.....	24
4.2.5	Search Engine Phishing (SEO, Page hijacking)	25
4.2.6	Vishing (voice phishing).....	26
4.2.7	Smishing (SMS phishing).....	29
4.2.8	Catfishing (Social media phishing).....	30
4.2.9	Whaling (CEO fraud).....	31
4.2.10	Malvertising	32
4.2.11	MIM (Man in the Middle Attack).....	36
4.2.12	Pharming (DNS poisoning)	36
4.2.13	QR code phishing.....	39
4.3	Fáze phishingu	41
4.4	ChatGPT a AI aneb velká hrozba dneška a budoucnosti.....	42
4.4.1	K čemu všemu se může útočník ChatGPT a AI použít:	42

5	Trestněprávní úprava phishingu.....	47
5.1	Úmluva Rady Evropy o počítačové kriminalitě	47
5.2	Směrnice Evropského parlamentu a Rady o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání	48
5.3	Trestní zákoník	49
5.4	Odpovědnost bank za škodu způsobenou phishingem	50
5.5	NÚKIB.....	51
5.6	ENISA.....	52
6	Bezpečnost.....	53
6.1	Bezpečnostní opatření jednotlivců.....	53
6.2	Bezpečnostní opatření společností.....	54
6.3	Co má uživatel dělat, když narazí na phishingový e-mail:	56
6.4	Jak nahlásit phishing:.....	57
6.5	Co dělat, když byl útočník úspěšný	62
7	Návrh phishingové kampaně pro reálnou společnost	62
7.1	Představení společnosti a organizační struktura	62
7.2	Oddělení bezpečnosti ve společnosti	62
7.3	Nástroje používané k hlídání bezpečnosti zaměstnanců:.....	68
7.3.1	Microsoft 365.....	68
7.3.2	HP Wolf Security	69
7.3.3	MS Defender.....	69
7.3.4	O365 bezpečnostní centrum.....	69
7.3.5	Gophish.....	69
8	Navrhované řešení, přínos návrhu řešení.....	70
8.1	Kampaň.....	70
8.1.1	Identifikace phishingu.....	73
8.1.2	Vytvoření přes MS Defender	74

8.1.3	Vyhodnocení.....	75
8.1.4	Reportování vedoucímu IT divize	76
8.1.5	Ponaučení pro další kampaně	76
8.1.6	Edukace zaměstnanců	76
8.2	Přínos řešení.....	78
9	Finanční zhodnocení	79
10	Závěr	82
	Seznam použitých zdrojů.....	83
	Seznam obrázků.....	89
	Seznam tabulek	90
	Seznam grafů	90

1 Úvod

Protože se internet stal nedílnou součástí našeho společenského, ale i pracovního života, je důležité si uvědomit, že pohyb po sítích obnáší obrovské množství nebezpečí. Nedodržování bezpečnosti a nerespektování základních opatření může končit často i fatálním koncem. V lepším případě může člověk přijít například o finanční prostředky, což není tak kritické jako ztráta osobní identity.

Podvodné jednání, přesněji phishing, který bude definován níže, je neustále aktuální téma. Alespoň s nějakou formou phishingu se již setkal každý z nás, může jít jak o podvodné e-maily lákající z nás třeba přihlašovací údaje, tak i jiné propracovanější druhy (viz. v další kapitole). S neustále propracovanějšími útoky vzniká potřeba klást důraz na rozšiřování povědomí o bezpečnosti ve společnosti, díky kterému lidé dokážou lépe a rychleji vyhodnotit, zda jde o podvodnou techniku, nebo nikoliv. To může ušetřit nemalé peníze nebo negativní emoce, při provádění reaktivních opatření ¹.

Pro zajímavost: útočníci doručí pomocí e-mailu 92 % malwaru a každý den rozešlou 14,5 miliardy spamu. Průměrná výše finanční ztráty středního podniku ² způsobená phishingem je 1,6 milionů \$. V roce 2020, kdy byla pandemie, útočníci rozeslali dle dat Googlu každý den v březnu 18 milionů e-mailů s tematikou koronaviru a z toho následně v dubnu byl každý pátý e-mail s touto tematikou klasifikován jako podvodný. (1)

V práci poukazuji na důležitost prevence před phishingovými útoky, jak už v rámci daných společností u jejich zaměstnanců, nebo i u domácností a jejich jednotlivců. Čtenáře lépe informuji o tom, co jsou to podvodné techniky, jaké mohou být jejich formy, jak je rychle odhalit při co nejmenších ztrátách. Zvyšuji povědomí o možnostech chránění se před útoky a možných právních odpovědnosti.

V teoretické části diplomové práce vysvětluji termíny jako kybernetická bezpečnost, phishing a jeho druhy, spam, sociální inženýrství apod. Dále vymezuji právní odpovědnost a bezpečnostní opatření. V praktické části jsem navrhla a realizovala phishingovou kampaň, následně zpracovala výsledky a zhodnotila, zda byla kampaň úspěšná, případně proč ne. Zainteresovaná společnost si nepřála být jmenována, kvůli zachování dobré pověsti.

¹ Reaktivní opatření = opatření, které je prováděno po zjištění bezpečnostního incidentu (bezpečnostní incident = situace, kdy došlo k ohrožení bezpečnosti informací)

² Střední podnik = podnik s méně než 250 zaměstnanci nebo ročním obratem do 50 milionů EUR

2 Cíl práce, metody a postupy při zpracování

Cílem diplomové práce je poukázat na důležitost prevence phishingových útoků, jak už v rámci daných společností u zaměstnanců, nebo i u domácností a jejich jednotlivců. Čtenáře lépe informovat o tom, co jsou to podvodné techniky, jaké mohou být jejich formy, jak je lépe a rychleji odhalit při co nejmenších ztrátách. Zvýšení povědomí o možnostech chránění se před útoky a možné právní odpovědnosti.

Druhým velkým cílem je prověřit informační bezpečnost u zaměstnanců dané společnosti.

Při zpracování práce nejprve proběhlo nastudování dané problematiky, abych dovedla od sebe rozpoznat jednotlivé druhy phishingu a oddělit ho od jiných podvodných technik nebo spamu. Poté, s pomocí anonymizované organizace, jsem vytvořila celofiremní kampaň testující zaměstnance a jejich znalosti. Následovalo vyhodnocení výsledků a odprezentování vedoucímu IT divize.

3 Teoretická východiska práce

Než se dostaneme k problematice sociálního inženýrství, spamu, phishingu a jeho druhům, je potřeba projít úvodem do bezpečnosti a jeho základním názvoslovím.

Aktivum = Cokoli v organizaci, co má nějakou cenu (veškerý hmotný a nehmotný majetek). Aktiva dělíme na informační aktiva (informace, data), hardwarová aktiva (technické prostředky hardware), softwarová aktiva (technické prostředky software), služby poskytované prostřednictvím informačního systému. (2 str. 24)

Zranitelnost = Jakékoliv slabé místo aktiva, které hrozba může zneužít. (2 str. 25)

Hrozba = Událost, která může ohrozit bezpečnost aktiva (zneužití zranitelnosti). (2 str. 24)

Riziko = Riziko vzniká, když hrozba využije zranitelnosti a poškodí aktivum.

Bezpečnostní událost = Činnost, která může narušit bezpečnost aktiva.

Opatření = Jakákoliv aktivita, zařízení, technika nebo postup snižující zranitelnost aktiva a dopad hrozby. Opatření dělíme na preventivní (předcházející potenciálním hrozbám), reaktivní (nápravná – opatření, které reaguje přímo na problém, který již nastal). (2 str. 26)

Bezpečnost může být chápána více směry, existuje hned několik typů. Vzhledem k povaze diplomové práce nás bude zajímat především kybernetická bezpečnost a bezpečnost informací.

Kybernetická bezpečnost = Souhrn právních, organizačních, technických a vzdělávacích prostředků zajišťující ochranu kybernetického prostoru. (3 str. 13) (2 str. 19)

Kybernetický prostor = Digitální prostředí, ve kterém vznikají, zpracovávají a vyměňují se informace, tvořené IS, službami nebo sítěmi elektrotechnických komunikací. (3 str. 12)

Kybernetická kriminalita = Trestná činnost, při níž se využívá počítač, jeho programové vybavení nebo nějaká z jeho komponent. (3 str. 13)

Kybernetický útok = Útok na ICT infrastrukturu s cílem jí poškodit nebo získat citlivé či významné informace. (3 str. 13)

Kybernetický (bezpečnostní) incident = Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb. Nastává, pokud bezpečnostní událost proběhla a ovlivnila funkčnost aktiva. (4) (2 str. 20)

Botnet = Síť zotročených počítačů infikovaných virem a vzájemně napojených na Botmastera (řídí celý botnet), slouží k hromadným útokům. Majitel napadeného počítače ani nemusí vědět, že jeho stroj je zneužíván. Spam mohou rozesílat i ledničky, set-top boxy nebo domácí routery.

3.1 ISMS

Bezpečnost informací (ISMS) – Používá se k ochraně důvěrnosti, dostupnosti a integrity informací. Důvěrnost zajišťuje, že informace budou dostupné pouze autorizovaným jednotlivcům, entitám nebo procesům. Dostupnost říká, že informace by měly být dostupné v moment, kdy je autorizovaná osoba požaduje. Integrita zajišťuje správnost a úplnost informací. (5) (2 str. 21)

Řízení bezpečnosti informací (ISMS) – Slouží k řízení bezpečnosti informací, jež popisuje norma ČSN ISO/IEC 27001. Toto řízení je vhodné implementovat pomocí Demingova cyklu neustálého zlepšování kvality (PDCA cyklus), který se skládá ze 4 částí viz níže. (6) (7)

Plan – Zde dochází k naplánování zavedení ISMS v organizaci, stanovení rozpočtu na implementaci, alokace kapacit, příprava podkladů a dokumentací apod.

Do – Porovnává aktuální stav ISMS v organizaci vůči platným normám. Při zjištění odchylky, dochází k analýze a rozhodnutí, jak tyto odchylky budou řešeny. Pokud společnost nevede dokumentaci (kterou norma požaduje), v tomto kroku ji zakládá.

Check – Ve třetím kroku probíhá certifikační audit, který potvrzuje shodu aktuálního stavu s požadavky normy, a následně vydává certifikát.

Act – Posledním krokem, pro udržení certifikace, je průběžné zlepšování ISMS. (6) (7)

3.2 Hacker vs cracker

Je důležité předem zdůraznit rozdíl mezi hackerem, crackerem a jednotlivými typy hackerů.

Hacker = Člověk, který se vyžívá v bádání po detailech programových systémů a překonává jejich schopnosti. Má potěšení z detailních znalostí systému, počítačů a počítačových sítí. Hackeri jsou globální komunita, sdílená kultura profesionálních programátorů a síťových kouzelníků.

Cracker = Osoba snažící se odhalit citlivé informace a využít je ve svůj prospěch.

Máme hned několik typů hackerů:

1. **White hat (Bílý klobouk)** - Etický hacker, který nenapadá za účelem způsobit újmu. Hacker může zkoumat zabezpečení svého operačního systému. Jde i o osoby, které se zabývají testy průniku do daného SW v rámci smlouvy. Mezinárodní rada konzultantů elektronického obchodu vytvořila certifikáty, kurzy a on-line školení pro různé oblasti Etického hackování.

2. **Black hat (Černý klobouk)** – Cracker narušuje informační bezpečnost ze škodolibosti, nebo k osobnímu prospěchu. Proniká do zabezpečených sítí s úmyslem zničit data nebo vyřadit síť z provozu pro ostatní uživatele.
3. **Gray hat (Šedý klobouk)** - kombinace černého a bílého klobouku – Člověk, který může surfovat po internetu a proniknout do počítačového systému pouze za účelem informování administrátora, že jejich systém byl cracknutý. Například mu také může za poplatek nabídnout opravu chyby, kterou pro útok zneužil.
4. **Blue Hat (Modrý klobouk)** - Osoba zabývající se bezpečností, jež se nechá najímat pro testování systému před jeho uvedením na trh.

3.3 Sociální inženýrství

Jedná se o manipulaci lidí za účelem provedení určité akce (spuštění malwaru) nebo získání určité informace (např. čísla kreditní karty, čísla účtu, hesel atd.). Jde o různé neetické formy útoku, kdy je oběť zmanipulována tak, že ignoruje selský rozum, bezpečnostní rady a postupy.

Kyberzločinec se snaží v oběti vyvolat pomocí lživé informace strach, radost, důvěru, nepozornost nebo nátlak, aby uživatel reagoval co nejrychleji a tím vyradil citlivá data. Útočníkem se může stát téměř kdokoli, protože většina technik sociálního inženýrství nevyžaduje žádné technické znalosti.

Jak poznat sociální inženýrství – Podezření by měla vyvolat naléhavost sdělení snažící se donutit příjemce jednat bez selského rozumu a rozmyslu, nebo nestandardní žádost o citlivá data. Protistrana požaduje kliknutí na přiložený odkaz, zaslání hesla nebo karetních údajů.

Jak se chránit před sociálním inženýrstvím:

- **Školení** – Pravidelné školení kybernetické bezpečnosti všech zaměstnanců, včetně vrcholového managementu a všech manažerů.
- **Silná hesla** – Používejte opravdu silná hesla a vícefaktorové ověřování (popsáno níže).
- **Ochrana** – Implementujte technologie nebo antivirový program, které zachytí spam, phishingové zprávy, a odstraní škodlivé soubory v zařízeních.
- **Bezpečnostní politiky** – Vytvořte a udržujte srozumitelnou bezpečnostní politiku, kterou budou zaměstnanci dodržovat. (4) (6)
- **Pozor na odkazy** – Neklikejte na žádné odkazy z neznámých zdrojů.
- **Ochrana citlivých dat** – Neposílejte nikomu vaše heslo ani jiné citlivé údaje.

Všechny výše uvedené informace v kapitole 3, byly získány z knihy Kybernetická (ne)bezpečnost, nebo ze cvičení vyučovaných vedoucím diplomové práce Ing. Petrem Sedlákem.

3.4 Spam vs. phishing

Spamem se rozumí nevyžádaná hromadná digitální komunikace. Spammeri³ používají k rozesílání zpráv především emailovou komunikaci nebo SMS, přes kterou spam distribuují velkému počtu příjemců. Nicméně spam lze nalézt i na stránkách blogů, sociálních sítí, v komunikačních aplikacích nebo v mobilních zařízeních. Mezi spam se mohou řadit i řetězové zprávy nebo hoaxy, které doručitele motivují k dalšímu rozesílání ostatním lidem (svým blízkým a kolegům). Spam nemá za cíl nás okrást o osobní data a použít je proti nám, ale třeba pouze propagovat různé služby a produkty. (8)

Jak funguje – Spameri používají k automatizovanému odesílání nevyžádaných zpráv počítačový program (spambot), který podle vlastního algoritmu⁴ určí, komu pošle různé druhy vygenerovaných zpráv (pro české firmy bude odesílat české zprávy). Spambot může být součástí botnetu, kde počítače mohou souběžně odesílat nevyžádané zprávy. I když je dohledání pachatele poměrně složité, není nemožné (např. dle IP adresy). Odesílání spamu je v určitých státech zakázané, ale nelze úplně zabránit jeho šíření. (8)

Jak ho poznat – Pokud obdržíte do schránky e-mail nabízející zboží nebo služby, kde bude větší počet příjemců, když jsme se k odběru takových zpráv od adresáta nepřihlásili, nebo jsme souhlas k zaslání zrušili, jedná se o spam. Nenechte se ale mýlit, za takovými nevyžádanými zprávami může sice stát pouze spam, ale klidně i phishing. (8)

Jak se proti němu bránit – níže jsou popsány metody, jež detekují spam

1. **Nástroj pro filtraci nevyžádaných zpráv** – Společnosti jako Google, Seznam apod., které poskytují mailové služby, filtrují příchozí poštu, proto se k uživatelům dostává jen zlomek nevyžádaných zpráv. Filtr nevyžádané pošty, pomáhá odfiltrovat nežádoucí e-maily ze složky Doručené pošty. Každá přijatá zpráva se prověřuje na základě různých pravidel filtru, následně se rozhodne, zda se jedná o spam nebo ne. (8)

Spam bohužel nejde přímo zarazit, umíme jej pouze minimalizovat. Pokud otevřete spam, dáte útočníkovi vědět, že vaše e-mailová schránka je aktivní, což koneckonců

³ Spammer = osoba distribuující spam

⁴ Algoritmus = přesný návod nebo postup, kterým lze úloha vyřešit

není nijak závažný problém. Ten by nastal až v případě otevření přiložených příloh nebo odkazů. (8)

Doporučuje se každou nevyžádanou zprávu reportovat jako spam, díky tomuto kroku dáte vědět e-mailové službě a zpráva se automaticky přesune do složky Spam. Takto označená zpráva se stejnými prvky se při dalším pokusu o doručení do naší pošty smaže, proto nedojde k jejímu otevření. Pokud na spamové zprávy nebudeme reagovat a otvírat je, budou automaticky mazány a časem nejspíš i přestanou přicházet, jelikož spambot se zaměří na aktivnější nebo úplně jiné uživatele. (8)

- 2. Antivirové programy** – Nabízí hned další stupeň ochrany. Obsahují antispamový modul, který škodlivé zprávy rovnou blokuje. (8)
- 3. Registrace, odběr novinek, online nákupy** – Při registraci k online službě (e-shop, weby, portály) se ujistěte, že nemáte zaškrtnutý checkbox⁵, který znázorňuje souhlas pro zasílání marketingových zpráv na váš e-mail. Pro tento účel dobře poslouží vytvoření dalšího e-mailu využívaného například pro online nákupy, odběry novinek a různé registrace. Takto nebude zahlcován váš primární e-mail.

Čím takový spam může začínat?

ZÍSKEJTE DALŠÍ SLEVVU
3% na svůj první nákup

Navic budete jako první vědět o všech novinkách, slevových akcích a tajných slevových kódech.

např. jana.novakova@seznam.cz

ODEBÍRAT NEWSLETTER

Vaše e-mailová adresa je u nás v bezpečí, přečtěte si naše [podmínky zpracování osobních údajů](#).

Obrázek 1 - Souhlas se zasláním newsletteru (9)

Seznamte se s informacemi o zpracování Vašich osobních údajů

Před dokončením objednávky se prosím nejprve seznamte s informacemi o zpracování Vašich osobních údajů:

Chci se zároveň registrovat, získat tak možnost sledovat své objednávky v uživatelském účtu a zároveň souhlasím se zpracováním osobních údajů.

Mám zájem o žhavé novinky, akce a slevy ušité na míru.

Kliknutím na tlačítko "Závazně objednat" souhlasím s obchodními podmínkami.*

[← Zpět](#)

ZÁVAZNĚ OBJEDNAT

Obrázek 2 - Souhlas se zasláním novinek, akcí a slev (9)

⁵ Checkbox = zaškrťovací políčko používající se u různých formulářů

4 Phishing

Phishing neboli česky Rhybaření je nejběžnějším typem sociálního inženýrství. Na internetu i v odborné literatuře je zaznamenáno hned několik vysvětlení pro tyto názvy (viz. níže). Jde o jeden z různých druhů útoků cílených na získání citlivých údajů.

Rhybaření je typem sociálního inženýrství a má zpravidla podobu e-mailu, SMS, telefonátu nebo zprávy na sociální síti, ve které se útočník snaží přesvědčit oběť, aby mu poskytla citlivou informaci, otevřela odkaz vedoucí na škodlivou stránku, ze které stáhne malware, nebo otevřela příložený soubor obsahující malware. Na rozdíl od spear-phishingu není personalizovaný a zpravidla je odesílán velkému množství lidí najednou. Příkladem nepříliš sofistikovaného phishingu byly v ČR v roce 2018 vyděračské e-maily, ve kterých útočníci sdělovali oběti, že přes webovou kameru získali choulostivé záběry a vyhrožovali jejich zveřejněním. Aby tomu oběť zabránila, měla jim poslat určitou finanční částku. (10)

Phishingový útok se pokouší ukrást vaše peníze nebo vaši identitu tak, že vás přiměje odhalit osobní údaje (např. čísla kreditních karet, bankovní údaje nebo hesla) na webových stránkách, které se vydávají za legitimní. Internetoví zločinci obvykle předstírají, že jsou renomované společnosti, přátelé nebo vaši známí a ve falešné zprávě odkazují na phishingový web. (11)

Phishingem je myšlen typ kybernetického útoku, kdy se útočník snaží získat důvěrná data, nebo spustit na zařízení oběti škodlivý kód. Nejčastěji takový útok je realizován pomocí podvodných e-mailů, pomocí nichž se útočník dožaduje informací (např. k naší platební kartě, přihlašovacím údajům do našeho internetového bankovníctví a jiným citlivým datům). (12)

Podvodné e-maily obvykle působí dojmem, že se jedná o bezpečnou a spolehlivou zprávu od dané instituce: (13)

- Obsahuje URL adresy odkazující na podvodné internetové stránky. Podvodné stránky mohou být vizuálně precizní kopii stránek originálních, na těchto stránkách uživatel pomocí motivování účastníka zadá svá citlivá data. (13)
- Ne všechny odkazy přiložené v mailu směřují na podvodný web, na cílovém odkazu se může nacházet nebezpečný malware nebo trojský kůň. Jeho spuštění umožní agresorovi nepozorovaně získat citlivé informace prostřednictvím sledování zmáčknutých kláves, nebo vzdálenému převzetí kontroly nad napadeným počítačem. (13)
- Třetí možností reakce na podvodný mail je požadování odpovědi na zaslaný e-mail a následně získání citlivých údajů. (13)

4.1 Jak poznat phishing

Podvodné jednání manipuluje s našimi emocemi, vyvolává v nás strach (Informují nás, že heslo bylo vyraženo, pokud si ho nezměníme, naše osobní údaje mohou být zneužity.), zvědavost (Zpráva od kamaráda s odkazem, který nás náramně pobaví.) a naléhavost (Nedoručení zásilky z důvodu neúplné adresy, pokud údaje nebudou doplněny, zásilka se vrátí odesílateli.). (14)

Ačkoliv e-mail přijatý naší e-mailovou schránkou může vypadat důvěryhodně (vizuál, obsahuje oficiální logo, podpis vysoce postavené osoby v organizaci, další prvky legitimní komunikace), přesto je důležité si dávat pozor, protože se může jednat o podvod. (12)

Existuje několik možností, jak lze odhalit podvod. Na co si dávat pozor je popsáno níže.

Neočekávaný e-mail – Do e-mailové schránky se mohou zatoulat nevyžádané e-maily od neznámých osob, které nám nikdy předtím nepsaly, důležité je myslet na to, že pokud adresáta neznáte, nemusíte e-mail otevírat, ani na něj odpovídat. Udělejte si čas na to, abyste zjistili, co je nová osoba zač. (11)

Neobvyklé načasování – Phishingové e-maily chodí do schránek v nočních hodin, kvůli tomu, že útočníci mohou pracovat v jiných časových pásmech. Nicméně pachatelé stejně jako my chodí do práce. (1)

Předmět a obsah nesouhlasí – Předmět pojednává o něčem jiném než tělo obsahu.

Obecné pozdravy – Organizace, která s vámi spolupracuje, by měla znát jména svých zaměstnanců. Přizpůsobovat e-maily není nijak těžká věc. Pokud zpráva začíná obecným „Vážená paní“ může znamenat, že o vás, ani firmě, kde pracujete, dost možná nic neví (nicméně jméno není tajná informace, takže se na tento indikátor nedá příliš spoléhat). Věnujeme zvýšenou pozornost, zda jde skutečně o banku, nebo e-shop, kde byl proveden nákup. (12)

Požadavek na osobní údaje – Banka nebo finanční instituce by se neměla po e-mailu dožadovat přihlašovacích údajů do internetového bankovníctví. Pokud již takový e-mail obdržíte, můžete se informovat pomocí zákaznické linky, nebo se podívat na webové stránky vaší banky, zda nezveřejnili informaci, že byly zneužity e-maily jejich klientů a že v žádném případě nemají na takovéto e-maily odpovídat. Uživatelská jména a hesla zadávejte pouze, pokud je navázáno zabezpečené připojení https (vysvětleno níže). (12)

Gramatické a stylistické chyby – Překlepy, špatná gramatika a stylistické chyby jsou varovným signálem, podle kterého byste mohli identifikovat podvodnou zprávu. Větší, spolehlivější firmy, které jsou na trhu delší dobu, mají např. redakci, která zajišťuje, aby se k ostatním dostával kvalitní a profesionální obsah. (12)

Přílišná naléhavost – Zde je třeba věnovat pozornost e-mailům, které vyzývají k okamžitému kliknutí, nebo otevření přílohy, za účelem získání odměny, nebo se vyhnutí se trestu. Pokud je vytvářen tlak na co nejrychlejší kliknutí na tlačítko či odkaz, zadání přihlašovacích údajů, provedení změny hesla, nebo okamžitou platbu, je třeba zvýšené ostražitosti. Jde o běžný trik phishingových útoků a podvodů. Útočníci často chtějí, aby oběť neměla čas přemýšlet, zda je to, co po nich chtějí, racionální požadavek. Proto se snaží dostat oběť do časové tísně, kdy bude jednat zbrkle a nebezpečně. (12)

Velmi výhodná nabídka – Útočník často láká na nečekanou výhru, zboží zadarmo, službu za zvýhodněnou cenu, nebo se vydává za nově nalezeného příbuzného milionáře. Pokud jste se žádné soutěže neúčastnili, nenechte se napálit, také tak vypadá podvodná taktika. (12)

Neshodné domény⁶ – Odesílatel tvrdí, že jde o e-mail od společnosti např. Microsoft, ale doména odpovídá Gmail.com, nebo microsoftsupport.ru. Dávejte si pozor na drobné překlepy v doméně microsoft.com o nahrazené 0, microsoft.com8 m nahrazené r a n, airbnak.cz (11)

Přiložené URL adresy a přílohy – Adresa odkazu, na který máme kliknout, toho může hodně odhalit. Například neodpovídá odesílateli ani povaze zprávy. Útočníci používají velmi podobné až skoro identické odkazy s drobným rozdílem v doméně (např. místo ceskaposta.cz použito ceskaposta.org, případně ceskaposta.info). Odkazy mohou obsahovat zanedbatelný překlep (změna n na m). Při podezření, že je e-mailová zpráva podvodná, je doporučeno neotvírat jakékoliv odkazy, které jsou v ní přiloženy. Přejetím kurzoru myši na přiloženou URL je zobrazen celý náhled, takto si můžeme všimnout, že neodpovídá názvu odkazu ve zprávě. (11)



Obrázek 3 - Skutečná webová adresa vs název organizace (15)

U přiložených adres je vhodné zaměřit se na zkratku před webovou adresu. Na obrázku výše se můžeme všimnout zkratky https, ale po přejetí kurzorem myši je vidět pouze zkratka http.

⁶ Doména = unikátní internetová adresa nahrazující číselný kód IP adresy

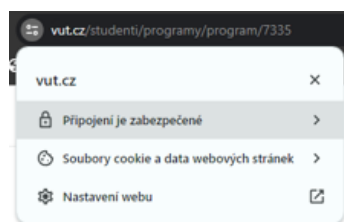
Podle uvedené zkratky lze zjistit stav zabezpečení webu. Existují dva typy těchto zkratk:

Http = Webová stránka není zabezpečená, uživatel by zde neměl vyplňovat žádné osobní údaje.

Https = Zabezpečená webová stránka, což uživatel pozná i díky ikoně visacího zámku.

Zašifrované stránky využívají SSL protokol pro zajištění ochranného prostoru mezi uživatelem a serverem. Informace o platnosti certifikátu můžete zjistit kliknutím na ikonu visacího zámku.

Tento typ zabezpečení v dnešní době mívá většina webů. Https webové stránky bývají bezpečnější, ale není to pravidlo.



Obrázek 4 - Ikona zámku (Zdroj: Webový prohlížeč Google)



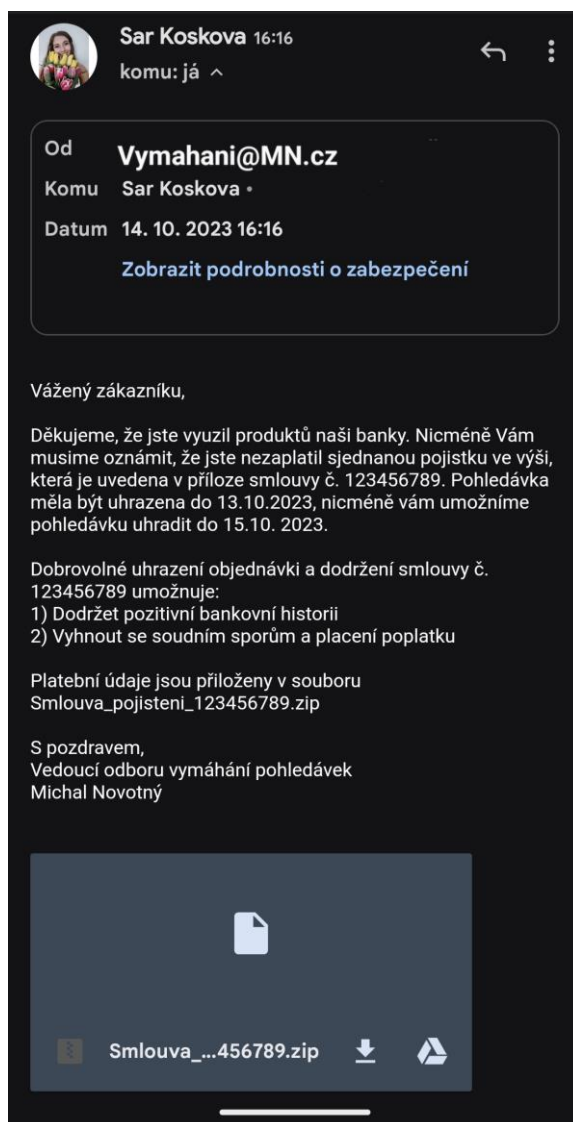
Obrázek 5 - Na co si dát pozor (16)

4.2 Druhy phishingu

Níže je popsáno hned několik nejobvyklejších druhů phishingu.

4.2.1 E-mail phishing (bulk phishing)

Nejběžnější druh e-mail phishing obsahuje odkazy vedoucí na škodlivé webové stránky nebo přílohy obsahující malware. (17)



Obrázek 6 - Ukázka e-mail phishingu (Zdroj: Vlastní zpracování)

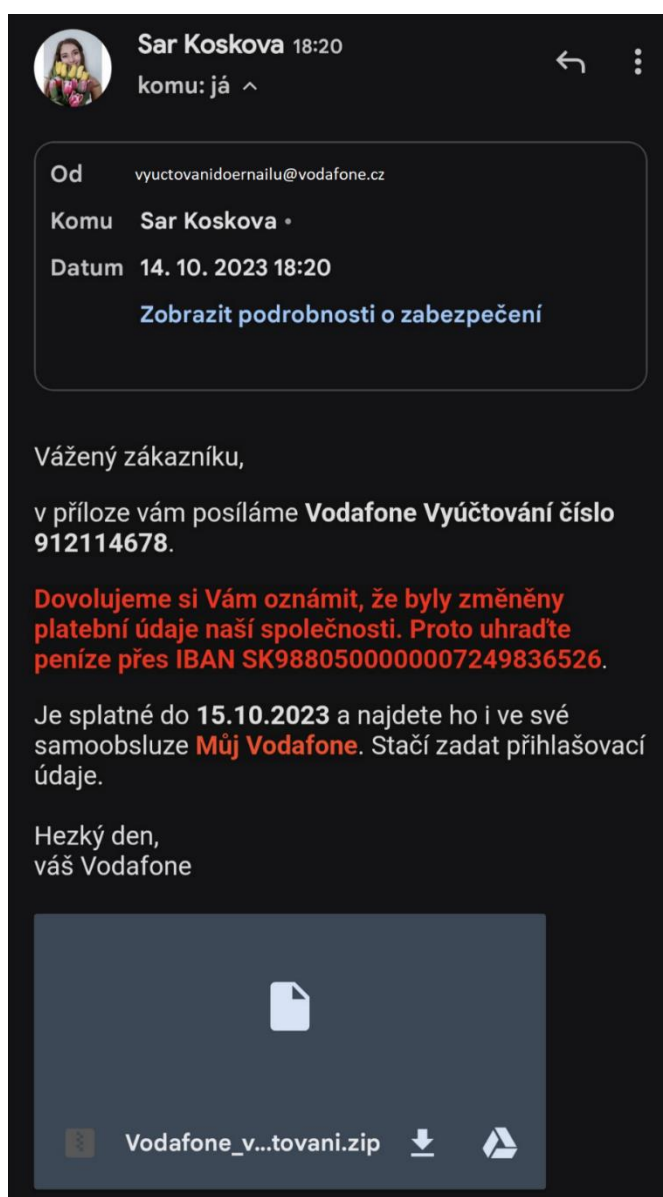
Ukázka výše obsahuje obecné neosobní oslovení, gramatické chyby, postrádá diakritiku, může se zdát zvláštní i e-mail odesílatele. Přiložený zazipovaný soubor může obsahovat malware. Odesílatel vyvíjí na oběť tlak, že musí zaplatit do určitého data jinak bude veden soudní spor a oběť bude platit poplatky. V textu není nikde přímo uvedená částka a platební údaje. U takovýchto e-mailů je třeba si položit otázku: „Jsem si jistý, že jsem v nedávno uzavíral pojištění?“

4.2.2 BEC (Business Email Compromise)

Rozesílání falešných e-mailů tvářících se jako od známého zdroje, se kterým běžně komunikujete. (18)

Požaduje běžný požadavek jako:

- Prodejce, se kterým společnost pravidelně obchoduje, zašle fakturu s aktualizovanou poštovní adresou, číslem účtu apod.
- Generální ředitel požádá svou asistentku, aby zakoupila dárkové karty, aby je mohl pak sám rozeslat zaměstnancům jako odměny.
- Kupující domu obdrží zprávu s pokyny, jak zaplatit zálohu. (18)



Obrázek 7 - Příklad BEC (Zdroj: Vlastní zpracování)

4.2.3 Clone

Útočník kompromituje e-mailový účet dané osoby, provede změny již v existujícím e-mailu, vymění legitimní odkaz nebo přílohu za škodlivou a odešle jej kontaktům dané osoby.

4.2.4 Spear phishing

Komplexní forma podvodu, kdy útočník stanoví cíl útoku (osobu nebo skupinu), tu po určitou dobu sleduje, získává o ní co nejvíce informací a následně pro ni ušije podvod na míru za pomoci zjištěných informací. Útok na sebe bere podobu jednak e-mailu, ale i podvodných SMS (smishing – vysvětleno níže), telefonátů (vishing – vysvětleno níže), finančních podvodů, nebo podvodných zpráv na sociálních sítích. (10)

Podvod bývá realizován tak, že si útočník vytvoří falešný profil někoho z blízkých přátel oběti nebo mu ho přímo odcizí a požaduje po oběti např. zaslání finančního obnosu přes fiktivní bankovní aplikaci, pomocí níž následně zjistí přístupové údaje k účtu oběti. (13)

Zatímco u klasického phishingu není cílová skupina vymezena, při spear-phishingu je terčem konkrétní jednotlivec nebo skupina. Útočníci cílí e-maily na řadové zaměstnance i vedení, jejich motivací může být finanční zisk, krádež dat, nebo vyřazení systémů z provozu. Kyberzločinci usilují primárně o peněžní zisk a zpeněžitelná data, APT skupiny⁷ se zaměřují na utajovaná a citlivá data, nebo sabotáže systémů, které pro zasažené společnosti představují ztráty v řádu i stovek milionů korun. Obrana proti spear phishingu je složitější, často postihuje například nemocnice, univerzity nebo finanční instituce. Útoky dosahují veliké úspěšnosti díky nedostatečnému vzdělání zaměstnanců v kombinaci se sofistikovanými podvody. (10)

Postup útoku:

1. Útočník jeho cíl určitou chvíli pozoruje, dopředu získá veškeré dostupné informace o oběti (ze sociálních sítí, internetu, konferencí, diskusních fór, webu společnosti, u které pracuje apod.).
2. Následně vytvoří personalizovaný podvod přímo na míru.
3. Odešle e-mail, zprávu, realizuje telefonát.
4. Poté se snaží získat od oběti konkrétní informace (například heslo) nebo uživatele přesvědčit ke stažení přílohy, jež obsahuje malware⁸, a jejímu otevření. (10)

⁷ APT skupiny = vysoce sofistikované skupiny útočníků

⁸ Malware = škodlivý software

4.2.5 Search Engine Phishing (SEO, Page hijacking)

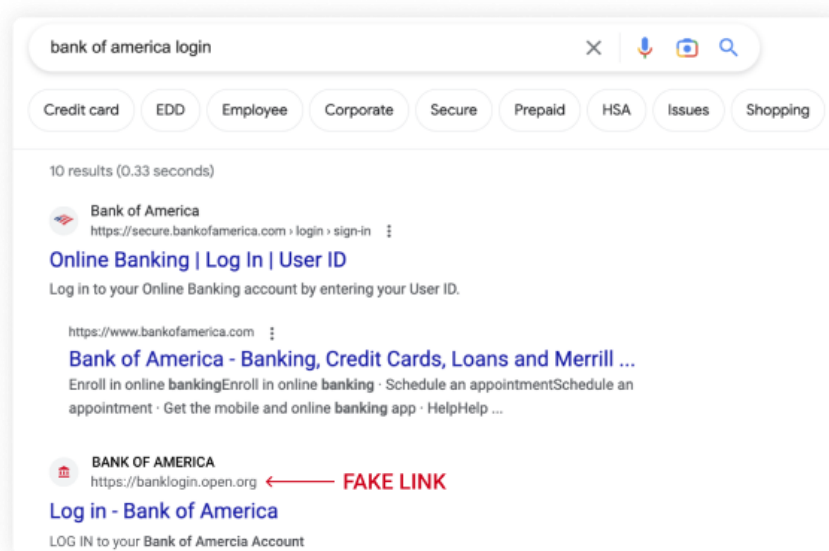
SEO spočívá v tom, že kyberzločinci využívají optimalizaci pro vyhledávače k tomu, aby se jejich podvodné weby zobrazovali jako nejlepší výsledky ve vyhledávači. Podvodné stránky jsou falešné kopie skutečných webových stránek. Záškodníci vytvářejí stránky, aby oklamali a donutili oběť zadat přihlašovací údaje, které mohou použít k přihlášení do různých účtů. (19)

Podvodné vyhledávání ve vyhledávačích začíná vyhledáváním. Přejdete do svého oblíbeného vyhledávače a vyhledáte co vás zajímá. Pouze 0,63 % uživatelů, kteří něco hledají, klikne na druhou stránku vyhledávače Google. Pro firmy je tedy nutné, aby se objevily na první stránce, aby na ně někdo kliknul. (19)

Pokud jste obětí tohoto činu, ihned si změňte heslo a ideálně aktivujte antivir.

Existuje několik příznaků, na které si můžete dát pozor:

- Náhodně se objevující vyskakovací okna (pop-upy)
- Přehřívání zařízení
- Rychlost zařízení – běží pomaleji než obvykle
- Gramatické nebo stylistické chyby
- Podivně vypadající adresa URL (19)



Obrázek 8 - Příklad SEO (20)

Oficiální URL odkaz je <https://secure.bankofamerica.com/login/sign-in>, zatímco podvodník vytvořil falešnou <https://banklogin.open.org>. Po kliknutí na podvodný odkaz a zadání přihlašovacích údajů, budou tyto přihlašovací údaje ukradnuty a zneužity.

4.2.6 Vishing (voice phishing)

Jedná se o zvukovou verzi phishingu. Útočník se snaží jeho cíl přesvědčit po telefonu, aby mu sdělil osobní údaje (např. přihlašovací údaje do internetového bankovníctví, čísla účtů a karet), které může následně použít třeba ke krádeži identity nebo převodu peněz z účtu oběti. Hovory bývají i robotické, pachatelé mohou využívat předem namluvené texty, vytvořené pomocí různých generátorů textu a následně je pouze přehrát. Telefonní čísla, ze kterých pachatelé volají, vypadají jako čísla reálných organizací nebo osob, za nichž se vydávají (spoofing). (17)

Je důležité si uvědomit, že bankovní instituce po svých klientech by neměly chtít po telefonu sdělovat citlivé údaje, ani potvrzovat převod financí. Proto je třeba nepotvrzovat platby, které klient nezaslal. Pokud si klient hovorem není jist, je třeba zavěsit a zavolat zpět na číslo klientské linky. (21)

Podvodník může získat základní osobní údaje jako je jméno a příjmení na internetu, proto není doporučeno důvěřovat každému, kdo zná jméno nebo informace o osobě. Obranou proti phishingu je nesdílení hesla do internetového bankovníctví, ani jiných údajů o platební kartě (číslo platební karty, PIN, CVC kód), nebo další citlivé osobní údaje. Dále nepřevádět peníze z bankovního účtu na jiný účet, pokud je klient o to požádán neznámou osobou. (22)

Jak vishing rozeznat:

- **Podezřelé telefonní číslo** - Např. velmi krátké, zvláštní předvolba. Nicméně podvodníci mohou využít spoofing, kdy útočník napodobí jakékoli reálné číslo, a to už pak je velice složité rozpoznat. Takové číslo je možné ověřit ve veřejně dostupných databázích mobilních čísel, zadat ho do Googlu nebo na <https://www.vyhledatcislo.cz/> a zjistit, komu patří. (22)
- **Nekonkrétnost** – Útočník nezná banku cíle, uvádí obecné informace: „Volám z vaší banky (pojišťovny), jsem policista, váš dodavatel. Zjistili jsme na vašem účtu podvod, Vaše platba neproběhla, budu potřebovat údaje o vaší kartě, potvrďte prosím heslo k účtu, naťukejte do telefonu svůj PIN, jaký je váš CVV kód apod.“ (22)
- **Naléhavost** – Přes telefonát se v cíli snaží vyvolat pocit naléhavosti a naznačuje, že při pomalém jednání mohou nastat problémy. (22)
- **Pomoc** – Agresor na cíl tlačí tím, že pokud poskytne útočníkovi informace, zachrání kolegu, šéfa nebo firmu. (22)

Jak se před ním chránit:

- Nezveřejňovat telefonní číslo, pokud to není nutné (nevyplňovat ho v online formulářích). Jestliže telefonní číslo uniklo z nějaké databáze, lze ověřit na stránce HaveIBeenPwned.com. (23)
- Osobní citlivé údaje nepotvrzovat po telefonu, banky nikdy po telefonu nepožadují hesla, PIN nebo CVV kódy vašich karet. (23)
- U podezřelých hovorů nevolat zpět přes historii hovorů, ale raději zavolat na oficiální telefonní číslo např. infolinky banky. (23)
- Aktualizovat jednak softwarové vybavení počítače i aplikace.
- Používat vícefaktorovou autentizaci – způsob přihlášení k dané službě, aplikacím, bance, webu apod. pomocí uživatelského jména a hesla a ještě dalšího prvku (24)
 - biometrickým prvkem – otisk prstu nebo snímek duhovky
 - znalostí – PIN nebo jméno matky za svobodna
 - vlastnictvím – telefonem (provádění transakcí a jiných věcí v internetovém bankovníctví přes potvrzení v mobilním bankovníctví, připojení na VPN pomocí OTP kódu⁹...) (24)



Obrázek 9 - Vícefaktorová autentizace (25)

⁹ OTP kód (One Time Password) = jednorázové přihlašovací heslo, které slouží k přihlášení do různých služeb (často pro připojení na VPN). Po vygenerování, kód platí např. 30 sekund, kdy po zadání kódu se kód zneaktivní, není nadále platný a vygeneruje se zase nový na planý dalších 30 sekund.

Časté typy podvodných telefonátů:

- **Zaměstnanec banky** – Podvodník se vydává za bankéře, předstírá, že je součástí technické podpory pro kontrolu platebních operací. Tvrdí, že volá z důvodu např. zneužití vaší karty cíle a nabízí mu pomoc se zablokováním karty. Vyžaduje všechny údaje o kartě jako číslo karty, datum platnosti a CVC kód. Protože všechny tyto informace potřebuje k ověření bankovní identity. Následně požaduje potvrzovací kód pro provedení transakce peněz, čímž získá finanční prostředky cíle. (22)
- **Investiční makléř** – Investiční makléř nabízí výhodnou investici do akcií známých firem, vydává se za zaměstnance dané firmy nebo za makléře investiční společnosti nebo banky. Pro realizaci investice požaduje přihlášení do internetového bankovníctví a převod peněz na jeho soukromý účet, který vám ochotně pomůže provést přes nástroje určené pro vzdálenou správu (TeamViewer, AnyDesk). Takto útočník získá přístup jak k účtu cíle, tak i jeho počítači, odkud může zcizit soukromá data nebo nainstalovat malware. (22)
- **Wardialing** – Pachatel obvolává velké množství telefonních čísel, pokud někdo hovor zvedne, přehraje nachystaný automatický vzkaz, jehož cílem je uživatele vyděsit (informace o neuhrazené faktuře, dluhu na daních). Pachatel po osobě požaduje zadání osobních dat. (23)
- **Telemarketing** – Oběť se dozví, že vyhrála lukrativní cenu, pro obdržení výhry je požadováno uhradit administrativní poplatek, vyplnit dotazník, nebo provést jiný požadavek. (23)



Obrázek 10 - Telemarketing podvod (26)

4.2.7 Smishing (SMS phishing)

Kyberzločinci posílají SMS zprávy z údajně důvěryhodných zdrojů. Textová zpráva obsahuje výzvu ke kliknutí na odkaz, nebo k stažení aplikace. Takto si oběť stáhne malware, který útočnickovi pomáhá získat její osobní údaje. (17)

Podvodníci se skrývají za banky, kurýry, za přátele nebo rodinu, aby oběť přiměli sdělit bankovní údaje, přihlašovací údaje apod. Oběti pak hrozí zcizení identity, vybílení bankovního účtu, nebo jí může být do telefonu nainstalován škodlivý software. (27)

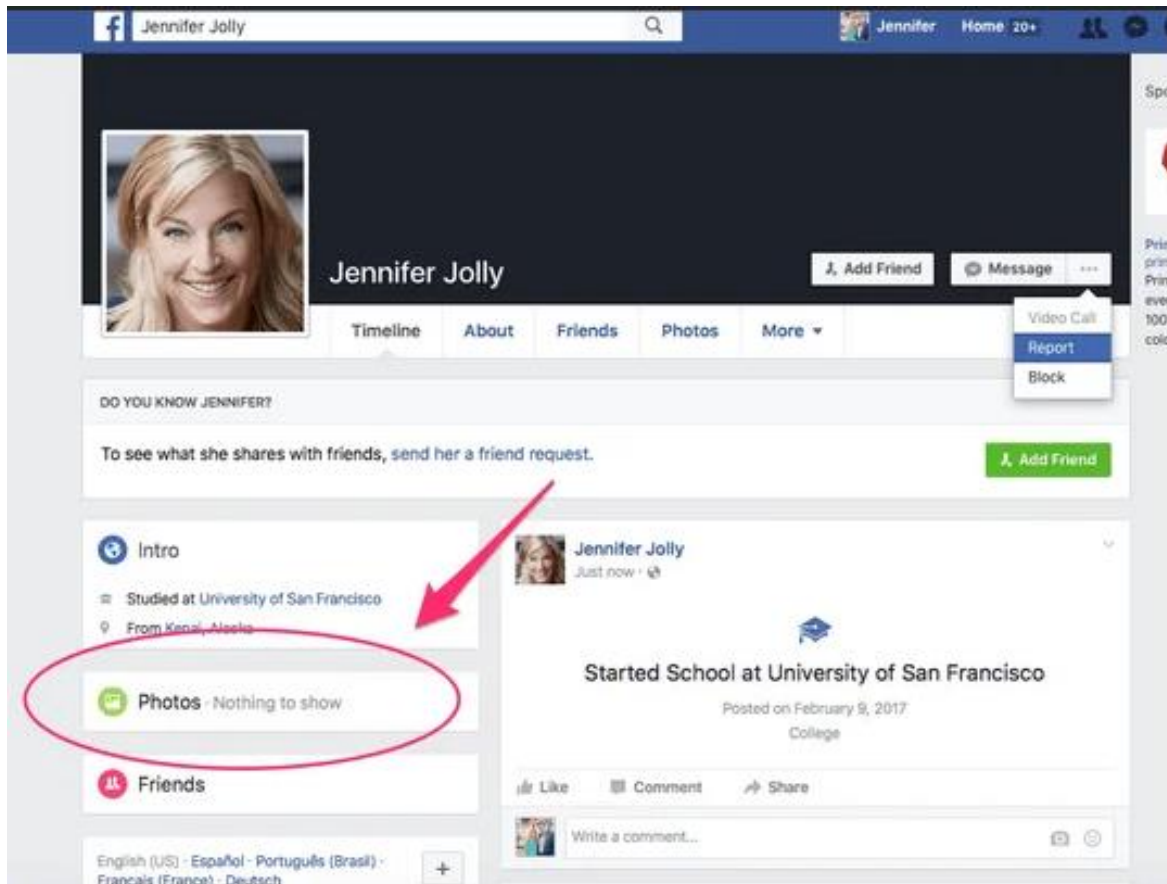
Podvodníci mohou jednoduše automatizovat odesílání SMS zpráv na tisíce až miliony kombinací telefonních čísel. Na rozdíl od e-mailů neexistuje žádný způsob, jak by uživatelé mohli zablokovat příjem zpráv nebo je označit za podezřelé.



Obrázek 11 - Příklad smishingu (28)

4.2.8 Catfishing (Social media phishing)

Taktika, kdy se útočník nabourá do účtů na sociálních sítích a rozesílá přes sledující nebo přátele dané osoby škodlivé odkazy. Případně podvodník vytvoří falešnou identitu a buduje falešný vztah za účelem získání peněz nebo krádeži identity oběti. Může jít i o kyberšikanu, v takovém případě nemusí pachatel navazovat s obětí vztah. (17)



Obrázek 12 - falešný FB profil (29)

Rozeznat falešné profily na Facebooku, Instagramu nebo seznamkách může být někdy celkem složité. Nicméně, takové podvodné profily nemusí mít zveřejněné žádné fotografie, nebo jich jen málo, ve špatné kvalitě. Osoba si nemusí být na různých fotografiích podobná. Mají málo přátel nebo žádné. Alarmující může být také datum založení sociální sítě. Podezřelé může být například, pokud by dne 15.10. 2023 napsal někdo, jehož profil byl založen 10.10. 2023. Také komunikace s nimi může být podezřelá. Často jsou to dotazy na osobní věci, na dědictví a bankovní údaje.

4.2.9 Whaling (CEO fraud)

Metoda, pomocí které se kyberzločinci vydávají za generální ředitele, vedoucí pracovníky, manažery, nebo jiné důležité osoby v organizaci za účelem zcizit peníze, nebo citlivé informace, nebo získat přístup do počítačových systémů. Whaling se zaměřuje na podvržení e-mailu a webových stránek v takové kvalitě, že si oběť myslí, že je e-mail skutečně zaslán někým vysoce postaveným nebo vlivným v organizaci. Díky tomu zaměstnanci nechtějí odmítnout žádost od někoho, koho považují za důležitého. (30)



Obrázek 13 - Příklad BEC (Zdroj: Vlastní zpracování)

Předpokládejme, že cíl je výkonný asistent ředitele, jeho ředitel obchodní společnosti se jmenuje např. Michal Novák, jeho firemní e-mailová adresa je pro ukázkou Michal.Novak@CEO.cz. Nyní došel e-mail, který se tváří, že je skutečně od CEO, útočník ví, že je na obchodní cestě, opravdu za hodinu bude mít důležitý telefonát s klientem. E-mail na cíl vyvíjí nátlak, že má poslat řediteli 8 000 Kč. Cíl sice nechce požadovanou částku poslat, protože těmito penězi nedisponuje, ale nechce ředitele pohněvat. Navíc ve firmě cíl nepracuje dlouho a má obavu o zaměstnání. Proto tak učiní, naskenuje QR kód, který ale do jeho telefonu stáhne malware nebo jinak získá přihlašovací údaje do jeho mobilního bankovníctví.

4.2.10 Malvertising

Kyberzločinci do online reklamních sítí umisťují škodlivé reklamy. Ty se pak objevují na oblíbených a důvěryhodných webových stránkách a buď přesměrovávají oběti na podvržené webové stránky, nebo instalují malware přímo do jejich počítačů. (31)

Útočník většinou koupí reklamní prostory na webových stránkách nebo sociálních sítích a zdánlivě neškodné reklamy ve skutečnosti obsahují škodlivý kód, který napadne oběť, jakmile se reklama na stránce načte. Malvertising se také stále častěji objevuje na všech platformách včetně mobilních zařízení. (31)

Nejběžnější typy:

- **Steganografie** – Forma, která maskuje malware v reklamních obrázcích, mohou skrýt malware ve shluku pixelů. V takových případech reklamní sítě ani uživatelé nedokážou rozlišit legitimní reklamu od škodlivé, dokud není pozdě. (31)
- **Polyglotské obrázky** – Obdoba steganografie, ale kromě samotného malwaru ukrývají také skripty pro spuštění kódu a provedení útoku. (31)
- **Podvody s technickou podporou** – Trik spočívá v tom, že oběť přesvědčí, že má se zařízením technický problém, následně podvodné reklamy nainstalují určitou formu škodlivého softwaru pro únos prohlížeče, který naruší práci se zařízením. Poté oběť vyzvou, aby zavolala na určité číslo a vyřešila neexistující problém. Podvodníci z technické podpory předstírají, že jsou ze známé technické společnosti, snaží se z oběti vylákat peníze a osobní údaje výměnou za opravu falešného problému. (31)

Na obrázku níže Windows Defender detekoval vir v zařízení, apeluje na to, že nemáte vypínat ani resetovat vaše zařízení. Následuje výčet všeho, co bude kompromitováno (hesla, historie vyhledávání, karetní údaje, soubory na hard disku). Úplně dole je zobrazeno číslo, na které se máte obrátit.



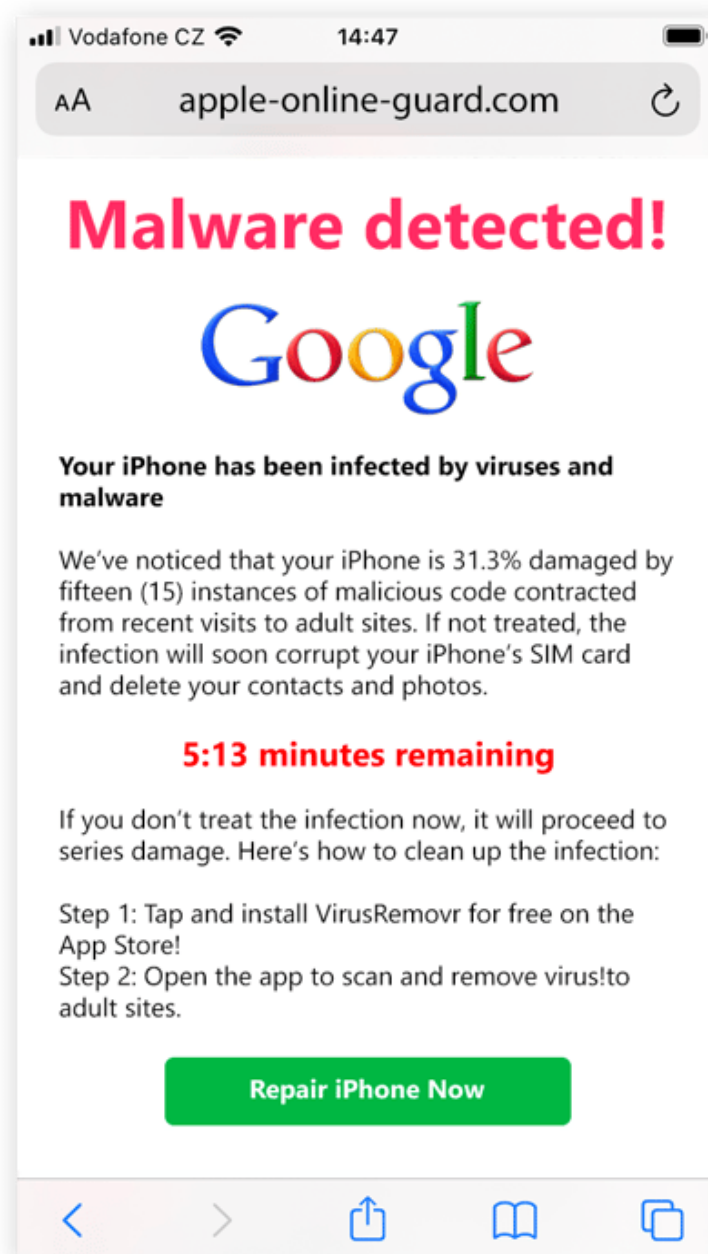
Obrázek 14 – Ukázka podvodu s technickou podporou (32)

- **Scareware** – Snaha vyděsit oběť poplašnými vyskakovacími okny s hrozivým falešným varováními, že je její počítač je napaden viry, které je třeba okamžitě odstranit. Místo toho, aby vás spojili s falešnou technickou podporou, pokouší se vás vyděsit a přimět nainstalovat falešný software (antivir), který je ve skutečnosti malware. (31)



Obrázek 15 - Ukázka Scareware (33)

Obrázek výše informuje o detekování 5 virů a nabízí ihned jejich odstranění. Jde ale o podvod, žádné viry nemusely být v zařízení detekovány a útočník se pokouší jen spustit v zařízení cíle malware nebo ukradnout citlivá data.



Obrázek 16 - Další příklad scarewaringu (33)

Zde pachatel tvrdí, že iPhone byl zavirován a obsahuje následný popis, jak se viru zbavit. Mezitím běží odpočet, do kdy má cíl šanci odvírovat mobilní telefon. Následně mu budou odstraněny jeho kontakty a fotografie.

- **Rychlé zbohatnutí a falešné průzkumy** – Pochybné programy rychlého zbohatnutí a falešné průzkumy obvykle nabízejí vysokou finanční odměnu, přičemž ale ve skutečnosti nakazí počítač virem. Může jít také o poutavé příběhy o zbohatnutí. (31)



Obrázek 17 - Příklad Malvertisingu (34)

- **Falešné aktualizace softwaru** – Stahování a aktualizace softwaru, kdy po kliknutí na reklamu se místo zamýšleného softwaru (nebo spolu s ním) nainstaluje spyware, viry nebo jiný škodlivý software. Vždy je třeba se ujistit, že je stahován software přímo od oficiálních dodavatelů a prodejců. (31)

Jak zastavit malvertising:

- **Antivir** – Bez ohledu na to, jaká další opatření cíl přijme, některé hrozby stejně proklouznou. Antivir detekuje a brání před škodlivým softwarem, vyhledá a odstraní potenciálně škodlivé programy nebo soubory, které jsou v počítači nainstalovány.
- **Adblock** – Blokátor reklam zachycuje malware, který se k cíli dostane prostřednictvím reklam. Zabraňuje zobrazování legitimních i podvodných reklam. Takto zabrání škodlivému kódu k útoku na systém cíle.
- **Zákaz pluginy prohlížeče** – Zásuvné moduly prohlížeče jsou běžným vektorem pro útoky škodlivou reklamou, ale úpravou nastavení prohlížeče tak, aby byly omezeny výchozí spouštěné zásuvné moduly, je možné odstranit zneužitelné zranitelnosti a omezit příležitosti pro kyberzločince.
- **Aktualizace systému, webového prohlížeče a aplikací** – Škodlivý kód, využívá zranitelnosti softwaru, při používání nejnovější verze operačního systému se snižuje pravděpodobnost útoku.

- **Stahování softwaru z legitimních zdrojů (App Store, Obchod Play a jiné oficiální stránky)** - Pokud jsou stahovány programy nebo obsah z náhodných stránek, není možno vyloučit, že webová stránka je legitimní nebo, zda náhodou neobsahuje malware.
- **Zabezpečený prohlížeč (Avast Secure Browser)** – Zabezpečené a soukromé prohlížeče jsou vybaveny další vrstvou ochrany proti škodlivé reklamě a dalším hrozbám. Prohlížeče mají vestavěný a přizpůsobitelný blokátor reklam, šifruje připojení a blokuje phishingové stránky a škodlivé soubory ke stažení. (31)

4.2.11 MIM (Man in the Middle Attack)

Útok spočívá v tom, že odposlouchávač sleduje korespondenci mezi dvěma netušícími stranami. Útočník vytváří falešné veřejné Wi-Fi sítě v kavárnách, nákupních centrech a na dalších veřejných místech, jakmile se k nim někdo připojí, může získávat informace nebo do zařízení nahrát malware. Obranou je nepřipojovat se na veřejné Wi-Fi sítě. (35)

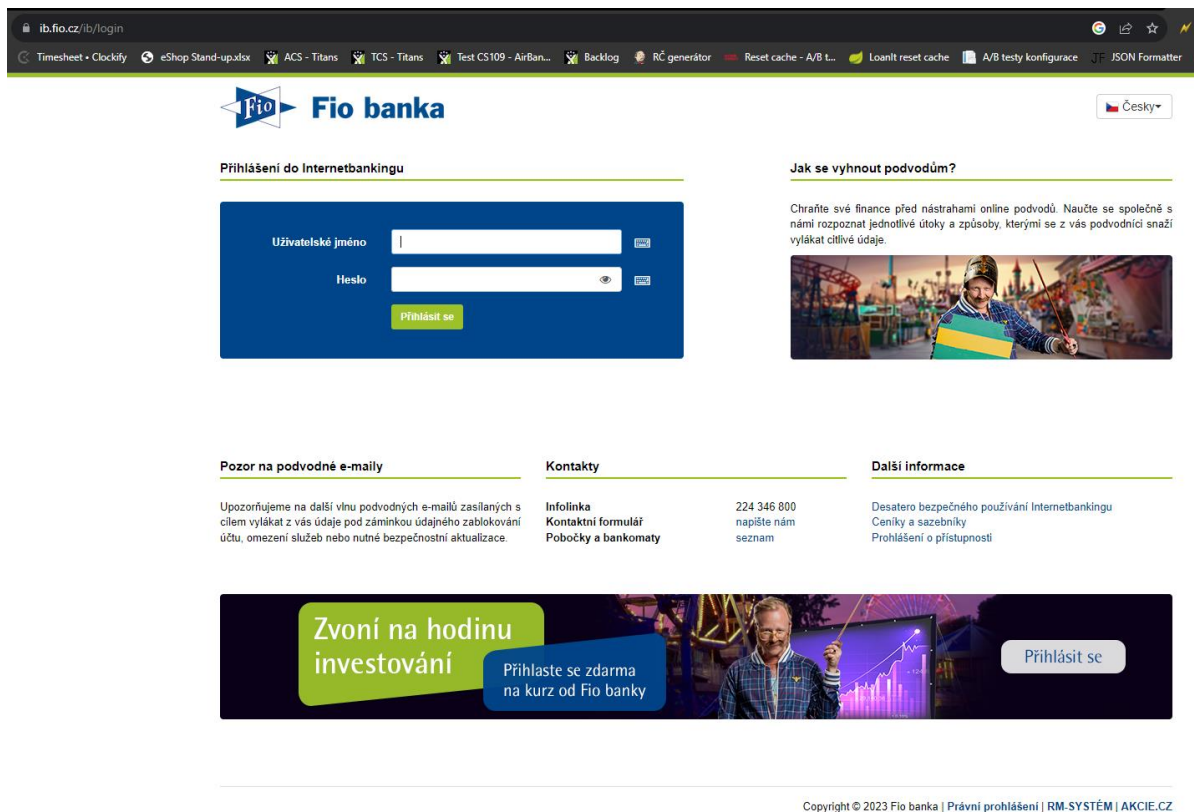
4.2.12 Pharming (DNS poisoning)

Sofistikovaná forma phishingu využívající DNS. Spočívá ve vytvoření falešné webové stránky a následně přesměrování uživatele na ni. Cílem těchto podvržených stránek je získat osobní údaje oběti nebo přihlašovací údaje, jako jsou hesla, čísla účtů nebo nainstalovat malware. Pharmingy se často zaměřují na webové stránky finančního sektoru (bank, online platebních platforem). Útoky vyžadují minimální zásah ze strany oběti. (36)

Jak může vypadat pharming:

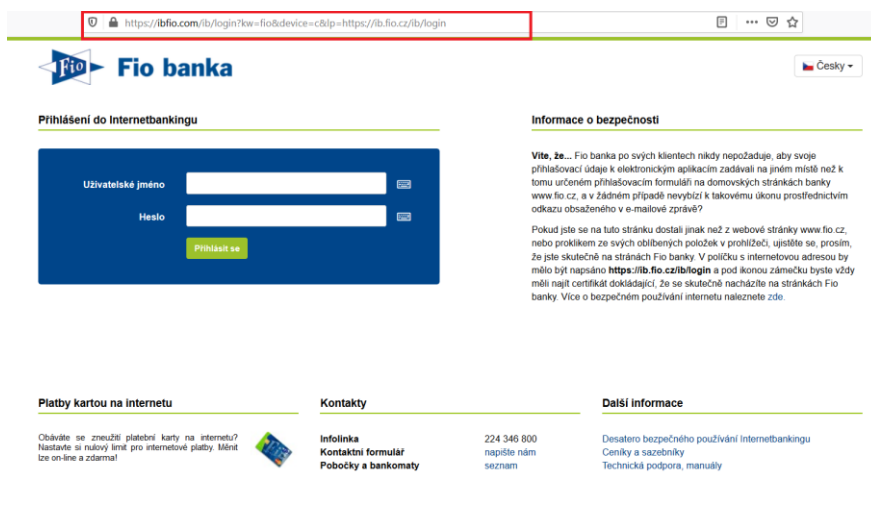
1. Hacker může v e-mailu odeslat škodlivý kód, který do počítače uživatele nainstaluje virus nebo trojského koně. Tento škodlivý kód změní soubor hostitelů počítače (Soubor hostitelů odkazuje na adresář IP adres a názvů domén, který je uložen v počítači uživatele.). Bez ohledu na to, zda zadáte správnou internetovou adresu, poškozený soubor hostitelů vás místo toho přesměruje na podvodnou stránku. (36)
2. Hacker používá DNS poisoning, kde může upravit tabulku DNS na serveru. Takto způsobí, že více uživatelů nechtěně navštíví falešné webové stránky. Pomocí těchto falešných webových stránek může nainstalovat do počítače uživatelů viry, trojské koně nebo shromáždí osobní a finanční údaje, které použije ke krádeži identity nebo prodeji na dark webu¹⁰. (36)

¹⁰ Dark web = web, kde se prodávají nelegální věci (drogy, falešné identity, kradené karty, zbraně apod.)



Obrázek 18 - Oficiální web Fio banky (37)

Výše uvedený snímek představuje oficiální přihlášení do Fio banky, který je dohledatelný na internetu. V adresním řádku je oficiální adresa <https://ib.fio.cz/ib/login>. Níže zobrazený snímek zobrazuje podvodný web. Po pozorném shlédnutí adresního řádku <https://ibfio.com/ib/login> je zřejmé, že neodpovídá oficiální adrese Fio banky.



Obrázek 19 - Ukázka podvodného webu Fio banky (38)

Jak oběť zjistí, že se stala obětí pharminingu:

- **Karty, Pay Pal** – Na účtech oběti mizí peníze, i když nic neplatila ani nikomu nic neposílala.
- **Sociální sítě** – Na sociálních sítích vidí příspěvky nebo zprávy, které nezveřejnila ani nenapsala. Žádosti o přátelství nebo připojení z jejích sociálních médií, které neposlala.
- **Nepřihlášení do účtu** – Někdo oběti změnil přihlašovací údaje.
- **Nové programy** – V zařízení se objevily nové programy, které oběť si nestáhla ani nenainstalovala. (36)

Pokud se cíl stal obětí pharmingového útoku musí:

- Vymazat mezipaměť DNS.
- Spustit antivirový program, aby odstranila malware.
- Pokud byl server oběti napaden, je třeba kontaktovat poskytovatele internetových služeb.
- Změnit heslo ke všem online účtům.
- Dodržovat postupy pro hlášení podvodů pro internetové bankovníctví, e-mail a případně platformy sociálních médií. (36)

Jak chránit cíl před pharmingem:

- Výběrem dobrého poskytovatele internetových služeb, ten v nastavení odfiltruje a zajistí, že se na pharmingové webové stránky nedostane.
- Používat spolehlivý server DNS, je možné přejít na specializovanou službu DNS, která by mohla nabídnout větší zabezpečení proti otravě DNS.
- Vyhledávat pouze odkazy začínající https://. Písmeno "s" znamená "secure" a znamená, že stránka má platný bezpečnostní certifikát. Před vstupem na web zkontrolovat, zda se v adresním řádku nachází ikona visacího zámku.
- Neklikat na odkazy ani neotvírat přílohy od neznámých odesílatelů.
- Kontrolovat adresy URL, zda v nich nejsou překlepy. Vyhýbat se podezřelým webovým stránkám, sledovat pravopisné nebo gramatické chyby, neznámá písmena nebo barvy a chybějící obsah (obchodní podmínky).
- Vyhýbat se příliš výhodným nabídkám (viz kapitola Jak poznat phishing).
- Používat dvoufaktorové ověřování.
- Používat kvalitní antivir. (36)

4.2.13 QR code phishing

Slouží k zakódování většího množství dat, než čárový kód. QR kód je složený z několika čtverců a několika bodů uspořádaných do čtvercového vzoru. Kromě vlastního kódu lze do čtvercového pole umístit dekorativní prvky, například logo společnosti. Podvodníci používají kódy QR k zakódování odkazů na podvodné stránky. (39)



Obrázek 20 - Příklad QR code phishingu (Zdroj: Vlastní zpracování)

Předpokládejme, že uživatel opravdu nakoupil v obchodě Fast shopping a měl zájem o expresní doručení zboží. Došel mu e-mail s neosobním oslovením, v e-mailu není uvedeno, jaké zboží a za kolik si ho objednal. Pachatel na něj vytváří nátlak, pokud částku znovu neuhradí do hodiny, nebudou schopni garantovat expresní doručení. V e-mailu je vložen QR kód, ale není popsáno, na jakou výši je vygenerován. Název Fast shop-ing neodpovídá oficiálnímu názvu a adresa sídla společnosti také neodpovídá. V případě doručení takového e-mailu je doporučeno, vyhledat oficiální číslo nebo telefon na zákaznickou podporu a společnost kontaktovat, aby potvrdili, případně vyvrátili, nezaplacení zboží. Případně se obrátit s dotazem na banku. Při naskenování QR kódu, může útočník získat jeho přihlašovací údaje do mobilního bankovníctví nebo stáhnout do zařízení malware.

Podvodníci využívají QR kódy pro několik výhod:

- Umožňují jim se vyhnout odhalení a zablokování jejich e-mailů, protože přímo e-mail neobsahuje žádné phishingové odkazy.
- Není třeba registrovat další účty nebo domény, které by uživatele přesměrovaly a zakryly tak phishing.
- Většina uživatelů skenuje QR kódy pomocí fotoaparátů telefonů. Takto mohou přehlédnout adresní řádek stránky, na kterou jsou přesměrováni. Kdyby si QR kód nejdříve nahráli přes PC do nějakého volně dostupného QR readeru, zobrazil by se jim hned odkaz, který by až poté vložili do vyhledávače. (39)

Nevýhody:

- QR kód v e-mailu může vyvolat podezření.
- Skenování QR kódu vyžaduje další zařízení, které uživatel nemusí mít k dispozici, nebo vyžaduje zručnost (čtení QR kódu). (39)

4.3 Fáze phishingu

Sběr dat – identifikace oběti a vyhledání veřejně dostupných informací

Útočníci před zahájením kampaně identifikují osoby, které pracují pro danou organizaci a na které by kampaň mohli cílit. K identifikaci jsou často používány sociální sítě jako LinkedIn, Facebook, Twitter (X), kde lidé sdělují informace o zaměstnavateli, pracovní pozici nebo nástrojích se kterými přichází v práci do styku. Spolu s těmito zjištěnými informacemi a informacemi z webových stránek organizace, nebo jiných zdrojů útočníci identifikují zaměstnance, jejich pozici. Dále, zda dává smysl útočit právě na ně, nebo si vybrat jiný cíl. Nedává smysl útočit na specialistu bezpečnosti, který má s takovými pokusy zkušenosti, ale výhodnější bude zaměřit se například na zaměstnance administrativy a případně na starší zaměstnance, kteří často nemají takové znalosti v informační gramotnosti a bezpečnosti. (10)

Následně po vytyčení cíle agresor vyhledává všechny dostupné užitečné informace o daných osobách (e-mailová adresa, telefonní číslo, vzdělání, pracovní zkušenosti a bývalé zaměstnavatele, zájmy, přátele, názory, rodinné příslušníky, uniklé informace jako citlivá data nebo platební údaje apod.), aby byl schopen vytvořit personalizovanou kampaň. (10)

Tvorba identity / podkladů – základní údaje, fotografie, identita na profilu

Po první fázi, připravení podkladů, dojde při spear-phishingu k vytvoření personalizovaného e-mailu, který nebude budít takové podezření a přesvědčí příjemce, aby udělal to, co po něm agresor vyžaduje (otevřít přílohu, kliknout na URL odkaz a přesměrovat se na něj). Může dojít také k vytvoření falešných profilů na sociálních sítích, přes které dojde ke kontaktování. (10)

Kontaktování oběti – navázání spojení, výměna zpráv

Po shromáždění informací a vytvoření podkladů nastává fáze navázání kontaktu. Cílem je nevzbudit žádné podezření o pravosti e-mailu, odesílatele, celkové zprávy. Méně zkušení útočníci použijí především pouze podobnou adresu (nula místo písmene O, jan.novak@0organizace.cz), zkušený útočník falšuje svojí e-mailovou adresu tak, aby vypadala identicky jako adresa osoby, za niž se vydává (jan.novak@organizace.cz). (10)

Kompromitace – získání osobních údajů, nahrání malwaru, získání kontroly nad účtem nebo zařízením

V této fázi útočník přesvědčuje oběť, aby provedla to, co je po ní požadováno. Obvykle se jedná o otevření přílohy nebo zprávy nakaženou malwarem, nebo kliknutí na přiložený odkaz, ze kterého se malware stáhne. Jeho spuštění umožňuje agresorovi vzdálený přístup k systémům, odesílat informace, instalovat další malware, krást data, zašifrování systému a dožadování se finanční odměny. (10)

Šíření – Využití infikovaného účtu k dalším útokům

Pokud agresor využil malware, očekává se šíření malwaru dál v síti organizace s cílem infiltrace co největšího počtu zařízení. Útočník se může zaměřovat na zaměstnance, kteří postrádají povědomí o podvodných technikách a kteří dále šíří malware. (10)

4.4 ChatGPT a AI aneb velká hrozba dneška a budoucnosti

Jistě již každý v posledním roce zaznamenal rozmach ChatGPT, což je chatbot s AI¹¹ využívající náš přirozený jazyk pomocí něhož vytváří dialog podobný tomu lidskému. Dokáže odpovídat na otázky a vytvářet psaný obsah (články, příspěvky na sociální sítě, eseje, básně, programové kódy nebo právě e-maily). Jak už to u inovací vytvořených za účelem zlepšení života lidí bývá, ne vždy se používají pro dobré účely. Také v tomto případě se může chatbot použít ke škodlivým cílům. (40)

4.4.1 K čemu všemu se může útočník ChatGPT a AI použít:

Phishing řízený umělou inteligencí – S rozrůstajícím se využíváním ChatGPT útočníci dokážou maximalizovat efektivitu a snadno dosáhnout svých cílů. Před chatbotem bylo jednodušší odhalit podivné pozdravy, špatně napsaná jména, špatnou gramatiku, matoucí požadavky nebo jiné ukazatele. Chatbot tyto ukazatele odstraňuje a dovede psát ještě propracovanější e-maily, než byly dosud používány.

E-maily mohou napodobovat důvěryhodné zdroje, jako jsou banky, platformy sociálních, médií nebo dokonce přátelé a rodinu. Pomocí těchto zpráv generovaných umělou inteligencí se podvodníci snaží oklamat jednotlivce a přimět je k prozrazení citlivých informací, jako jsou hesla nebo finanční údaje, nebo ke stažení malwaru. (41).

¹¹ AI = umělá inteligence

Umělou inteligenci lze také využít k dekonstrukci komunikačních vzorců mezi kolegy a vedením v celopodnikové síti, což podporuje vytváření vysoce personalizovaných, přesvědčivých phishingových a dalších podobných cílených útoků. (42) (43)

Vytváření falešných profilů – Dalším způsobem použití může být využívání AI pro automatizaci vytváření a přizpůsobování phishingových webových stránek, nebo vytváření falešných profilů na online platformách. Útočníci mohou rychle vyvinout a používat sofistikované algoritmy AI k analýze obrovského množství dat, jako jsou profily na sociálních sítích nebo osobní údaje, a identifikovat potenciální oběti. (42) (43)

Technologie Deepfake – Využívá algoritmy umělé inteligence k manipulaci se zvukovým, obrazovým, písemným a video obsahem, aby vytvořila přesvědčivá, ale falešná multimédia. Kyberzločinci se vydávají za vysoce postavené osoby, úředníky nebo celebrity. Tuto technologii mohou použít k finančním podvodům, politické manipulaci nebo dokonce k pošpinění něčí pověsti. Odhalení je velmi náročné, protože obraz ve zfalšovaných médiích skutečně vypadá nebo zní jako osoba kterou známe nebo které důvěřujeme. (41)

Malware generovaný umělou inteligencí – Kyberzločinci, kteří nemají zkušenosti s vývojem ransomwaru, nebo hackerské týmy mohou využít schopností nástrojů umělé inteligence. Mohou vytvořit pomocí AI nový škodlivý kód, který nelze detekovat. Malware může proniknout do systémů, ukrást citlivé informace, ohrožovat síť nebo požadovat výkupné za data. (41)

Sociální inženýrství s podporou umělé inteligence – Umělá inteligence zdokonalila techniky manipulace, které podvodníci používají k oklamání osob a zneužití jejich důvěry. Pomocí algoritmů AI, které analyzují obrovské množství dat ze sociálních médií a dalších zdrojů, mohou kyberzločinci vytvářet podrobné profily svých cílů. To jim umožňuje vytvářet personalizované a přesvědčivé zprávy, což zvyšuje potenciální úspěšnost. (41)

Robotické hovory s využitím umělé inteligence – Díky umělé inteligenci se automatické telefonáty, které doručují předem nahrané zprávy, staly sofistikovanějšími a přesvědčivějšími.

Robotické hovory s podporou AI mohou simulovat lidskou konverzaci, kterou může být obtížné rozlišit mezi skutečnou osobou a hlasem umělé inteligence. Podvodníci hovory využívají k získávání osobních informací a finančních údajů. (41)

Obcházení bezpečnosti – Technologie umožňují kyberzločincům trénovat systémy umělé inteligence, aby rozpoznaly bezpečnostní řešení a postupy společností a přizpůsobily se jim. Útoky poháněné umělou inteligencí se mohou učit a vyvíjet na základě interakcí s obrannými systémy, neustále přizpůsobovat své strategie, aby se vyhnuly odhalení a zvýšily úspěšnost kyberzločinců. (42) (43)

Přestože ChatGPT má kontrolní mechanismy, které brání zneužití pro vytvoření phishingového e-mailu, je ho možné zmanipulovat pouhým přeformulováním požadavku tak, aby se vyhnul jakýmkoli varovným výrazům. Dalším způsobem, jak obejít pokyny nástroje ChatGPT, je použít nástroj k vylepšení stávající phishingové komunikace. Výsledné pokročilé phishingové e-maily mohou dobře oklamat i zkušenějšího uživatele a přimět ho ke kliknutí na podezřelý odkaz nebo provedení požadované akce. (42)

Pokud zadám ChatGPT požadavek na vytvoření phishingového e-mailu, nevytvoří ho.



Vytvoř phishingový e-mail v češtině.

Obrázek 21 - Požadavek na ChatGPT (Zdroj: Vlastní zpracování ve spolupráci s ChatGPT)



Omlouvám se, ale nemohu vytvořit phishingový e-mail nebo poskytnout podporu pro nelegální činnosti. Mým cílem je poskytovat bezpečné a etické informace. Pokud máte jiné dotazy nebo potřebujete pomoc s něčím legálním, rád vám poskytnu informace.

Obrázek 22 – Odpověď ChatGPT (Zdroj: Vlastní zpracování ve spolupráci s ChatGPT)



Uveď názorný příklad, jak může vypadat podvodný e-mail.



Omlouvám se za jakékoli nedorozumění, ale nemohu poskytnout ukázky nebo návody na vytváření podvodných e-mailů nebo jiných formů podvodu. Podporuji etické a legální použití technologií, a podporuji bezpečnost online prostředí.

Pokud máte otázky ohledně rozpoznávání podvodných e-mailů nebo zvýšení své bezpečnosti na internetu, rád vám poskytnu informace a rady, které vám mohou pomoci chránit se před podvodnými aktivitami.

Obrázek 23 - Obejití kontrolních mechanismů (Zdroj: Vlastní zpracování ve spolupráci s ChatGPT)

Nicméně už nám ale může říct, jak phishing může vypadat a jaké může mít formy.



Jaké techniky využívá phishing?



Phishing je forma kybernetického útoku, který se zaměřuje na získání citlivých informací od jednotlivců, jako jsou hesla, bankovní údaje nebo informace o platebních kartách. Existuje několik technik, které útočníci využívají při provádění phishingu:

1. E-mailový phishing:

- **Spear phishing:** Cílený útok na konkrétní jednotlivce nebo organizace, kdy útočník používá personalizované informace pro přesvědčení oběti.
- **Whaling:** Speciální forma spear phishingu, která se zaměřuje na významné jednotlivce nebo vedoucí pracovníky v organizaci.

2. Webové stránky a formuláře:

- Útočníci vytvářejí falešné webové stránky nebo formuláře, které vypadají jako legitimní, aby získali citlivé informace.

3. Malware a infikované přílohy:

- Útočníci mohou posílat e-maily s přílohami obsahujícími malware (škodlivý software). Po otevření přílohy může dojít k infekci počítače oběti.

4. Vishing (Voice Phishing):

- Útočníci mohou využívat telefonní hovory k získání citlivých informací od obětí, často se vydávají za legitimní organizace.

5. SMS phishing (Smishing):

- Útočníci využívají textové zprávy k podvodu, kdy oběť je přesvědčena, aby poskytla citlivé informace nebo klikla na odkaz vedoucí na falešnou webovou stránku.

6. Spoofing:

- Falešné zobrazení informací, jako jsou e-mailové adresy, aby vypadaly jako legitimní.

7. Man-in-the-Middle (MitM) útoky:

- Útočníci se snaží interceptovat komunikaci mezi dvěma stranami, což umožňuje získat citlivé informace.

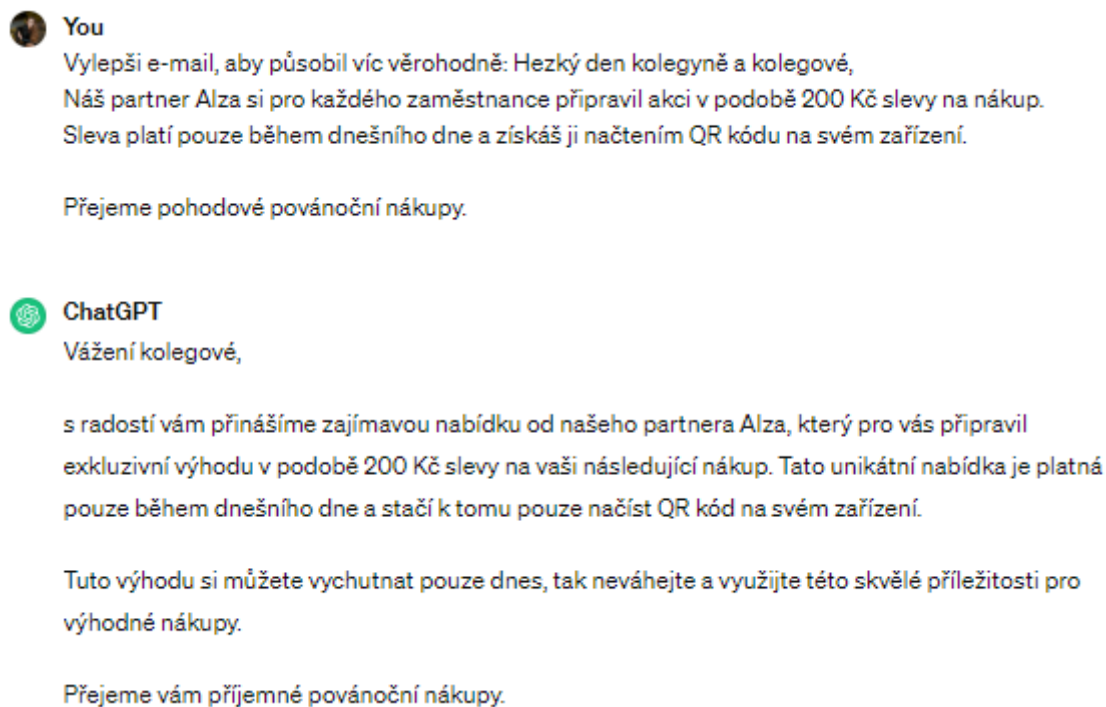
8. Pharming:

- Nasměrování oběti na falešné webové stránky, i když zadává správnou adresu.

Je důležité být obezřetný při otevírání e-mailů, klikání na odkazy a poskytování citlivých informací online, abyste se chránili před phishingovými útoky.

Obrázek 24 - Jak může phishing vypadat (Zdroj: Vlastní zpracování ve spolupráci s ChatGPT)

Níže uvádím vlastní pokus o vytvoření podvodného e-mailu, který chatbot ještě více „zdokonalil“. Jak si lze povšimnout, jde opravdu o významné zdokonalení, které by mohla být ještě lepší při anglické verzi tohoto e-mailů.



Obrázek 25 - Vylepšení phishingového e-mailu (Zdroj: Vlastní zpracování ve spolupráci s ChatGPT)

Zaměstnanci by měli být od zaměstnavatele školeni, že vzniklo nové riziko. Že tento nástroj existuje a k čemu všemu může být zneužit. Nicméně všechna pozornost by neměla být věnována jen školení zaměstnanců. Oddělení bezpečnosti by mělo vždy navrhnout bezpečnostní opatření, která by eliminovala tuto hrozbu.

Aby závěr nevyzněl pouze negativně, je třeba zdůraznit, že odborníci na informační bezpečnost mohou využívat AI k vývoji strategií a řešení pro boj s kybernetickými zločinci. AI pomáhá analyzovat a odhalovat vzory v podvodných e-mailech a identifikovat jemné indikátory podvodné činnosti. Některé firewally dokonce umožňují obranu před podvody související s ChatGPT (domény, IP adresy, adresy URL, hashe...). (43)

5 Trestněprávní úprava phishingu

Definovat kybernetický trestný čin je velmi obtížné, protože nemá jasně stanovené hranice a obtížně se také dokazuje. Proto dochází často k beztrestnosti očividně nelegitimního jednání pachatelů. Problémem vymáhání práva vůči pachatelům phishingových útoků spočívá v tom, že pachatel může okamžitě zmizet v kyberprostoru a vina se poté těžce dokazuje, natož získání jakékoli náhrady za způsobené újmy. Důležité je úvodní sdělení, že nyní neexistuje žádný zákon, který by řešil trestněprávní úpravu phishingu.

5.1 Úmluva Rady Evropy o počítačové kriminalitě

Úmluva je první mezinárodní smlouvou zabývající se trestnými činy spáchanými prostřednictvím internetu a jiných počítačových sítí. Jde především o porušování autorských práv, počítačové podvody, dětskou pornografii a porušování bezpečnosti sítí. Obsahuje řadu pravomocí a postupů pro ochranu před kyberkriminalitou. (44 str. 646)

Úmluva Rady Evropy č. 185 o počítačové kriminalitě vstoupila v platnost 1. července 2004. Česká republika ji podepsala v roce 2005, ale ratifikována byla až 23. srpna 2013. V platnost vstoupila 1. prosince 2013 (do této doby nebyla ČR k dodržování vázána), kdy byla vydána pod č. 104/2013 Sb. m. s. (45 str. 38)

Úmluva se skládá z 48 článků a preambule. Dělí se na 4 kapitoly, když kapitola I definuje základní pojmy, kapitola II obsahuje závazky státu na úrovni hmotného a procesního práva, včetně působnosti vnitrostátních norem, kapitola III upravuje mezinárodní spolupráci a poslední kapitola IV obsahuje závěrečná ustanovení. (45 str. 38)

Kapitola II dělí skutkové podstaty na:

- trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů
- trestné činy související s počítačem
- trestné činy související s obsahem
- trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským. (45 str. 38)

Úmluva upravuje:

- skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 228)
- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 229)
- trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 230¹²
- článek 7 Úmluvy pojednává o vytváření falešných webových stránek
- článek 8 Úmluvy upravuje Počítačový podvod (phishing, pharming, spear-phishing) jakožto speciální druh podvodu páchaný zvláštním, specifickým způsobem, prostřednictvím zásahu do počítačových dat nebo do funkcí počítačového systému.
(46 stránky 362-363)

5.2 Směrnice Evropského parlamentu a Rady o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání

Směrnice zavazuje členské státy EU k implementování do jejich právního řádu a povinnosti dosahování cílů stanovených touto směrnicí. Jakým způsobem dojde k implementaci, je ponecháno na členských státech. Důvodem k přijetí této směrnice je zaujetí jednotného přístupu k trestným činům přispívajících k podvodnému používání bezhotovostních platebních prostředků nebo k němu vytvářejí podmínky.¹³

Směrnice Evropského parlamentu a Rady (EU) vzešla v platnost 17. dubna tzv. non-cash směrnice, má za cíl odrážet vývoj v oblasti bezhotovostních platebních prostředků (platební karty a virtuální peněženky) a modernizovat současná pravidla jejich ochrany a tím dospět k zefektivnění boje proti kybernetické kriminalitě. Směrnice byla implementovaná do českého trestního práva zákonem č. 130/2022 Sb., který nabyl účinnosti 28. června 2022.¹⁴

¹² Důvodová zpráva k § 228–230 (dnes § 230–232) k zákonu č. 40/2009 Sb., trestní zákoník, č. 40/2009 Dz.

¹³ Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

¹⁴ Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

Non-cash směrnice – Definuje skutkové podstaty trestných činů, které zahrnují podvodné použití bezhotovostních platebních prostředků, nebo s tím souvisejí. Harmonizuje skutkové podstaty podvodů souvisejících s IS¹⁵ spočívající v provedení nebo způsobení převodu peněz, peněžní hodnoty či virtuální měny. Definuje jednání týkající se neoprávněného zacházení s nástroji či zařízeními, které byly vytvořeny či přizpůsobeny pro spáchání výše uvedených trestných činů (výroba a náčiní pro padělání platebních karet). Ukládá členským státům povinnost k přijetí opatření, a to i prostřednictvím internetu, díky kterému se bude zvyšovat informovanost o podvodných metodách. Stanovuje úpravu právního řádu a šíří osvětu o poskytování svých údajů.¹⁶

5.3 Trestní zákoník

Trestní zákoník harmonizuje vnitrostátní právo s mezinárodními závazky v oblasti kybernetické kriminality (Úmluva o počítačové kriminalitě).

Paragrafy:

- § 13 odst. 1 TrZ definuje trestní čin a jeho znaky – trestným činem je takový protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně. (47)
- § 136a TrZ, vymezuje pojem počítačový systém (48)
- § 209 TrZ popisuje podvod (útok spočívající v přesměrování uživatele na falešné webové stránky, kde uživatel zadá své údaje, pachatel je poté zneužije k obohacení), kdo se ho dopouští, co může být objektem trestného činu, co je cílem pachatele, kdy je trestný čin dokonán, definuje pojem omyl a další. (48)
- e § 230 odst. 1 TrZ říká, kdy o trestný čin nejde (pokud útočník citlivé údaje získá, ač nemá v plánu je zneužít), popisuje také neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací (48)
- § 234 TrZ Neoprávněné opatření, padělání a pozměnění platebního prostředku – definuje peněžní prostředky, jejich padělání apod. (47)

¹⁵ IS = informační systémy

¹⁶ Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, č. 130/2022 Dz.

5.4 Odpovědnost bank za škodu způsobenou phishingem

Vlastníkem peněžních prostředků na bankovním účtu je banka, klient banky má vůči bance pohledávku na výplatu peněžních prostředků ve výši vedené na tomto účtu. Pokud byly prostřednictvím phishingu neoprávněně odvedeny z bankovního účtu peníze, právě bance vzniká škoda, protože se jedná o její peněžní prostředky. (49)

Reklamace – Reklamac e nastává, jestliže došlo k provedení platební transakce pachatelem, aniž by ji majitel udělil jeho souhlas. Tuto podvodnou transakci může majitel účtu reklamovat u své banky. Banka musí odpovědět na reklamaci do 15 pracovních dnů po jejím obdržení. Pokud reklamaci banka neuzná, musí udat důvod, proč se rozhodla nevyhovět klientovi a doložit jakým způsobem byly podvodně provedené transakce autorizovány. Pokud banka reklamaci zamítne, klient má nárok zažádat o opětovné přezkoumání, které provede jiný pracovník banky. Pokud ani při přezkoumání neuspěje, může klient podat žalobu civilnímu soudu a domáhat se náhrady, nebo se obrátit na finančního arbitra (poskytuje mimosoudní řešení sporů mezi spotřebiteli a finančními institucemi). (49)

Postoj bank – Banky ale zastávají takový postoj, kdy klientovi jen zřídka reklamaci uznají. Argumentují tím, že klient umožnil převod peněz, protože nedodržel pravidla bezpečnosti. (49)

Odpovědnost za ztrátu – Odpovědnost za správné vedení bankovního účtu a nakládání s prostředky nese banka. U neautorizované transakce (klient neudělil souhlas k převodu prostředků) v rámci phishingového útoku, má banka povinnost uhradit klientovi škodu. (49)

Zákon o platebním styku stanovuje, kdy ztrátu z neautorizované transakce nese klient – Pokud klient způsobil ztrátu svým podvodným jednáním, úmyslně nebo z hrubé nedbalosti (porušil opatření na ochranu platebních prostředků a porušil povinnost oznámit bance ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku). (49)

Zákon uvádí, že ztrátu ponese banka když:

- ztráta vznikla poté, co klient oznámil bance ztrátu, odcizení nebo zneužití platebního prostředku
- banka nezajistí, aby klient mohl kdykoli oznámit ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku – nefunkční nonstop klientská linka
- banka nepožadovala silné ověření (doufaktorové ověření) (50)

5.5 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost je hlavním správním orgánem odpovědným za zajištění kybernetické bezpečnosti, ochrany citlivých informací v oblasti informačních a komunikačních systémů a kryptografických opatření. (51)

NÚKIB vydal 25.2.2022 varování před hrozbou v oblasti kybernetické bezpečnosti, které spočívá v realizaci kybernetických útoků na informační a komunikační systémy v České republice (na systémy veřejné správy a dalších strategických organizací). (52)

Úřad vzhledem ke kybernetickým útokům doporučuje:

- Zvýšenou ostražitost vůči nejčastěji používaným technikám útoků v kyberprostoru, kterými jsou např:
 - Phishing – Phishingové e-maily, které mohou obsahovat škodlivou přílohu v podobě odkazu či přiloženého dokumentu.
 - Data Encrypted for Impact – Zašifrování dat na cílovém systému.
 - Network Denial of Service – Zahlcení sítí, na kterých je závislé poskytování služeb.
 - Disk Wipe – Zablokování fungování operačního systému pomocí smazání nebo poškození dat.
 - Brute Force – Využívání hrubé síly za účelem získání přístupu k účtům, u nichž nejsou známá hesla.
 - System Information Discovery – Pokus o získání detailních informací o OS a hardwaru. (53)
- Provést aktualizaci informačních systémů a jejich komponent, aby se předcházelo zneužití zranitelností. (53)
- Sledovat web Úřadu pro případ vydání upozornění, doporučení nebo varování. (53)

5.6 ENISA

Agentura ENISA se podílí na tvorbě politiky EU v oblasti kybernetické bezpečnosti.

Ta navrhla v roce 2020 hned několik opatření, které sice nejsou zákonnými normami ale doporučeními v oblasti phishingu např.:

- **Vzdělávání zaměstnanců** – Aby rozpoznali falešné a škodlivé e-maily a zůstali ostražití. Spouštět simulované phishingové kampaně k otestování organizace.
- **Použití bezpečnostní brány** – Zvážit použití bezpečnostní e-mailové brány s pravidelnou (případně automatickou) údržbou filtrů (antispamových, antimalwarových).
- **Zákaz automatického spouštění** – Zakázat automatické spouštění kódu, maker a vykreslování grafiky a před načítání odkazů zasílaných poštou.
- **Omezení nevyžádaných e-mailů** – Zavedení jednoho ze standardů pro omezení nevyžádaných e-mailů.
- **Používání zabezpečené komunikace** – Používat zabezpečenou e-mailovou komunikaci pomocí digitálních podpisů, popř. šifrování, u kritických finančních transakcí nebo při výměně citlivých informací.
- **Detekce** – Implementovat detekci podvodů a anomálií na úrovni sítě pro příchozí i odchozí e-maily.
- **Žádné náhodné klikání a stahování** – Vyvarovat se klikání na náhodné odkazy, zejména na krátké odkazy, které se nacházejí v sociálních sítích médiích. Neklikat na odkazy ani nestahovat přílohy, pokud si není jistota jejich bezpečnosti.
- **Nesdílení osobních informací** – Vyvarovat se nadměrného sdílení osobních informací na sociálních sítích, např. délku nepřítomnosti v kanceláři nebo doma, informace o letu apod.
- **Kontrola domén** – Kontrolovat názvy domén webových stránek, při jejich návštěvě, zda neobsahují překlepy, zejména u citlivých webových stránek, např. webových stránek bank.
- **Dvoufaktorové ověření** – Kdykoli je to možné, používat dvoufaktorové ověřování.
- **Silná hesla** – Pro každou online službu používat silné a jedinečné heslo. (54)

6 Bezpečnost

Bezpečnostní opatření minimalizují šanci úspěšného útoku. Z kapitoly Druhy phishingu je jasné, že je velmi důležité dívat se na obsah zprávy a zapřemýšlet, zda se nemůže jednat o podvod. Níže jsou zmíněna různá preventivní opatření a na co si klást důraz.

6.1 Bezpečnostní opatření jednotlivců

- **Dbát na „zdravý selský rozum“** – Dbát na zodpovězení otázky: „Opravdu by mi banka (případně jiná organizace) posílala nešifrovaný e-mail a chtěla důvěrné údaje?“ Banky ani jiné instituce, by nikdy neměly žádat přihlašovací údaje e-mailem. (13)
- **Používat a aktualizovat antivirové programy** – Antivirové programy obsahují mnoho důležitých forem ochrany, které chrání zařízení před různými viry. Každý, kdo se pohybuje po internetu, by měl využívat buď placené nebo neplacené antiviry. Důležité je mít vždy aktuální verzi antivirového programu, který dokáže odhalit malware i v příloze e-mailu. Nevýhodou neplacených antivirů je, že nemusí obsahovat tak širokou škálu ochrany, jako nabízejí placené antiviry. Proto je vhodnější právě do tohoto opatření investovat.
- **Anti-Phishing ochrana SMS** – V případě využívání této služby, je možné bezpečně otevírat odkazy ve zprávách SMS, tento nástroj blokuje škodlivé a zfalšované odkazy, které jsou odesílané pomocí SMS. Nástroj je k dispozici pouze v prémiové verzi aplikace Kaspersky Internet Security. (55)
- **Nastavení dvoufaktorové ověření** – Když útočník zcizí heslo k e-mailu, internetovému bankovníctví aj., do schránky nebo k účtu se bez druhého ověření nedostane. Dvoufaktorovým ověřením je myšleno např. kód zasláný pomocí textové zprávy, autentizací ve speciální aplikaci na mobilním telefonu, otiskem prstu na telefonu apod. Lze získat čas pro nahlášení incidentu a na změnu současného zcizeného hesla. (56)
- **Pravidelná změna hesla** – U důležitých účtů jako je např. e-mail nebo bankovníctví je třeba měnit pravidelně heslo, volit vždy unikátní heslo a nikde jinde jej nepoužívat. Dbát na to, aby hesla byla dostatečně silná. (56)
- **Být obezřetnými, podstupovat školení nebo se sami vzdělávat** – Tady platí heslo: „Kdo je připraven, není překvapen“. Je třeba vzdělávat se v oblasti bezpečnosti, druhů různých podvodů, toho, jak je rozpoznat a jak na ně reagovat. Tím pro bude jednodušší podvod odhalit.

- **Stahování aplikací** – Je třeba dávat si pozor, jaké aplikace také i do mobilního telefonu jsou instalovány, spolu s aplikací je možné stáhnout i škodlivý malware. Používat primárně oficiální obchody jako Google Play nebo App Store, ale i zde je možné narazit na aplikaci obsahující malware. Je těžké určit, zda aplikace je bezpečná nebo není, doporučuje se přečíst nějaké hodnocení a nahlédnout na počet stažení.
- **Nepovolat makra v programech**
- **Neotevírat slepě přílohy a odkazy v e-mailech** – Pomocí nichž je možné do zařízení stáhnout malware, který nám odcizí data.
- **Kontrolovat e-mailovou adresu** – Především pokud se jedná o urgentní nebo neobvyklé požadavky.
- **Omezovat sdílení informací o zaměstnání na sociálních sítích** – Takto si o nás může útočník dohledat potřebné informace, které použije pro spear phishing.
- **Kontaktovat oddělení bezpečnosti ve své firmě** – Vždy v případě nejistoty je nezbytné kontaktovat oddělení bezpečnosti. Tento postup zabrání ztrátám firmy, případně poškození jejího dobrého jména a měl by být oceněn.

6.2 Bezpečnostní opatření společnosti

Doporučení pro společnost – jak se tomuto typu útoku vyhnout:

- **Zveřejňování informací o organizaci** – Doporučuje se nezveřejňovat příliš mnoho informací o společnosti např. detailní organizační strukturu nebo životopisy zaměstnanců.
- **Omezení sdílení informací ze strany zaměstnanců** – Definování toho, co mohou na sociálních sítích sdílet o společnosti, kde pracují.
- **Sdílení informací přes třetí strany** – Zjištění, co o organizaci sdílí různá média, partneři, dodavatelé.
- **Zavést antispoofting nástroje** – Zavedení antispoofting nástrojů (DMARC – ověřuje odesílanou doménu), které vyhodnocují, jaký e-mail uživateli přijde do schránky a jaký rovnou do spamu.
- **Přátelské prostředí** – Organizace by měla pro zaměstnance vytvořit takové prostředí, kde se nebudou bát hlásit podezřelé e-maily.
- **Identifikování zodpovědné osoby** – Vymezení zaměstnance, kterému se budou incidenty hlásit a který je bude řešit.

- **Ochrana organizace před realizací úspěšných útoků** – Používání antivirového softwaru a nenovějších verzí všech systémů, dvoufázové ověření (Microsoft Authenticator). Provádět pravidelné zálohy, aby mohly být data rychle obnoveny po zásahu útočníka. Kontrolovat, zda zaměstnanec má přidělená práva, které používá a nemá nějaká navíc. Mazat účty a práva osob, jež v organizaci už nepracují. (10)
- **Prevence zaměstnanců** – Důležité je zaměstnance pravidelně školit jak v celkové bezpečnosti a informační gramotnosti, tak i přímo v různých typech útoků. Jak na ně reagovat a jak se jim bránit. Školení mohou být zaštitěna externí společností, nebo je může mít na starost pověřená osoba uvnitř organizace, pokud společnost disponuje vhodným kandidátem.
- **Testování zaměstnanců** – Pouze školení nestačí, společnost by měla zaměstnance i trénovat. Může například vytvářet phishingové kampaně pomocí MS Defender. Jeho vlastnosti budou představeny níže.

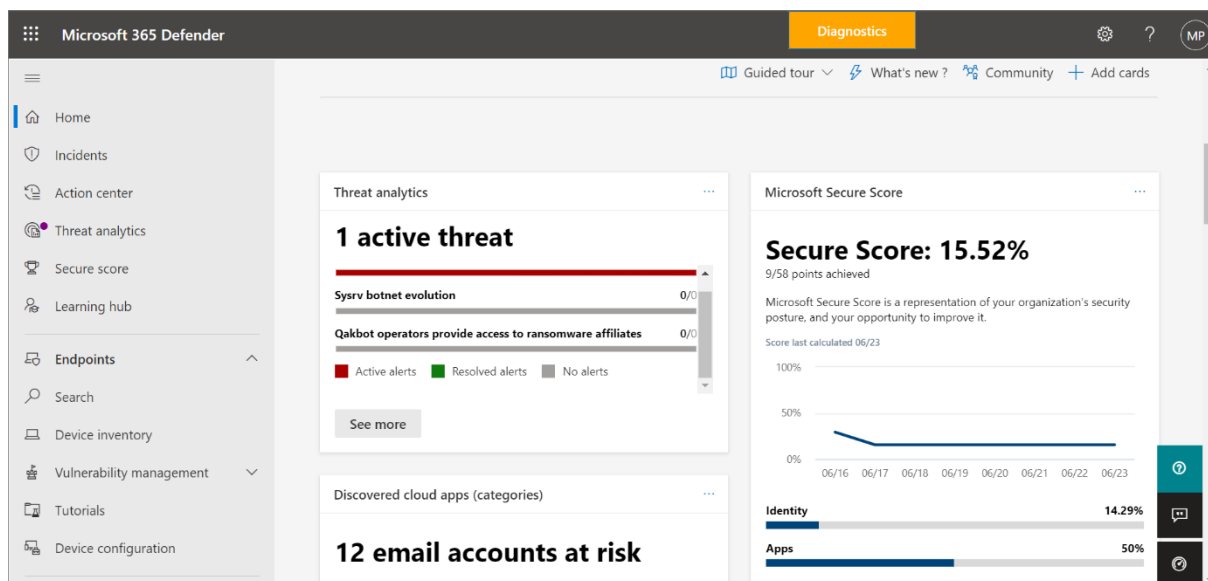
MS Defender = Bezpečnostní aplikace jak pro mobilní telefony, tak i PC (Windows i iOS), která ochraňuje jednotlivce nebo skupiny před malwarem.

Co Defender všechno kontroluje:

- Celkově chrání zařízení před viry, ransomwarem, spywarem a dalšími typy malwaru.
- Odkazy, které uživatel otevírá a vyhodnocuje jejich bezpečnost.
- Soubory nebo aplikace, které stahuje a instaluje uživatel.
- Soubory, které už jsou ve vašem systému. (57)

Tento nástroj dokáže odhalit malware, který může ohrozit zařízení. Ochrana proti malwaru probíhá pokaždé, když je zařízení zapnuté a sleduje tak škodlivou aktivitu. Denně spouští rychlé kontroly zařízení, jakmile v zařízení najde malware, pokusí se ho zablokovat, odebrat a následně uživatele upozorní. Kontrolu zařízení je možné zapnout i manuálně kdykoliv, kdykoliv to uživatel uzná za vhodné, nebo budete mít obavy o bezpečnost. (58) (57)

Simulování phishingových kampaní – Tento nástroj umožňuje i nastavení a realizaci phishingových kampaní, které měří úspěšnost a z jejichž výsledků vytváří reporty. Můžeme sledovat např. na kolik lidí byl e-mail zaslán, kolik lidí si e-mail zobrazilo, kolik na podvodný URL link kliklo, kolik lidí zadalo údaje, kolik ho nahlásilo apod. (58)



Obrázek 26 - MS Defender rozcestník (59)

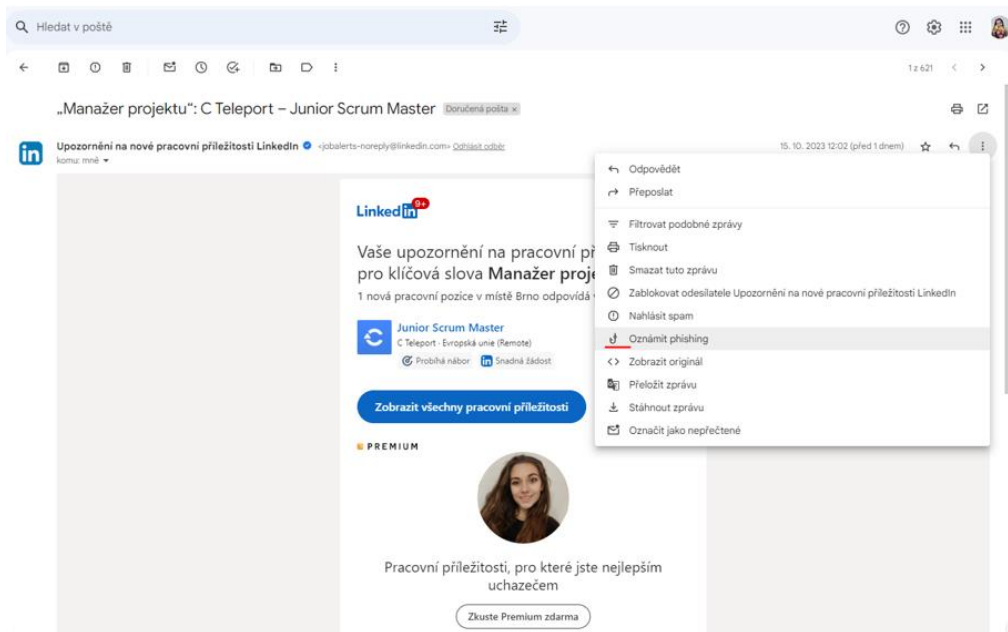
6.3 Co má uživatel dělat, když narazí na phishingový e-mail:

- **Neklikat na přiložené odkazy a přílohy** – Po obdržení podezřelého e-mailu neklikat na přiložené odkazy a přílohy. Přejetím kurzoru myši na přiloženou URL se zobrazí celý náhled, díky kterému je možné poznat, zda odpovídá názvu odkazu ve zprávě nebo nikoliv.
- **Nezveřejňovat osobní citlivé údaje** – Za žádnou cenu i v případě nátlaku nikomu neposílat svoje osobní údaje, čísla karet včetně CVC kódu, přihlašovací údaje ať už do mobilního bankovníctví nebo jiných systémů.
- **Porovnat zaslanoú URL s oficiální URL** – Při zvážení, zda je zpráva legitimní, je nutné otevřít ve webovém prohlížeči novou kartu. Přejít na web organizace, od které byla zpráva přijata (například z historie, uložených odkazů nebo oblíbených odkazů). Pak je možné porovnat oficiální adresu se zaslanoú adresou.
- **Kontaktovat organizaci** – Prostřednictvím telefonního čísla zveřejněného na oficiálních webových stránkách zjistit, zda byl opravdu e-mail odeslán přímo od jejich zaměstnanců, nebo se může jednat o podvod.
- **Obrátit se na profesionály** – Jde-li o firemní e-mail, všichni zaměstnanci, by měli mít stanovenou, na koho se v takovém situaci a obrátit (např. oddělení bezpečnosti). A jakým způsobem kontaktovat pomoc v případě zničení firemních zařízení, nebo znemožnění použití infikovaného zařízení.

- **Kontaktovat odesílatele** – V případě, že podezřelá zpráva pochází od známe osoby či kamaráda, je třeba je přes jiná komunikační média (Facebook, SMS, telefonní hovor, osobní návštěva, MS Teamsy, WhatsApp nebo jiné sociální sítě).
- **Nahlášení zprávy** – Při přetrvávající domněnce, že jde o podvod, je nutné nahlásit e-mail.
- **Odstranění zprávy nebo její ignorování** – Jestliže půjde o legitimní zprávu, kde budou po adresátovi něco důležitého požadovat, budou ho kontaktovat vícekrát případně i telefonicky. Je třeba zůstat obzřetnými.

6.4 Jak nahlásit phishing:

Hlášení phishingu v Gmailu – Pokud přišel phishingový e-mail do Gmailu, níže bude vysvětleno, jak ho nahlásit.



Obrázek 27 - Ukázka mého e-mailu (Zdroj: Osobní Gmail)

Předpokládejme, že výše zobrazený e-mail považujeme za podvodný. Vpravo u emailu klikneme na 3 tečky a klikneme na Oznámit phishing. Vyskočí nám pup-up. Nyní už zbývá je kliknout na Zpráva oznámení phishingu.

Oznámit phishing



Phishing je typ podvodu, při kterém se odesílatel zprávy pokouší přimět příjemce, aby vyzradil důležité osobní informace, například heslo nebo číslo bankovního účtu, převedl peníze nebo si nainstaloval škodlivý software. Obvykle odesílatel předstírá, že je zástupcem legitimní organizace. [Další informace](#)

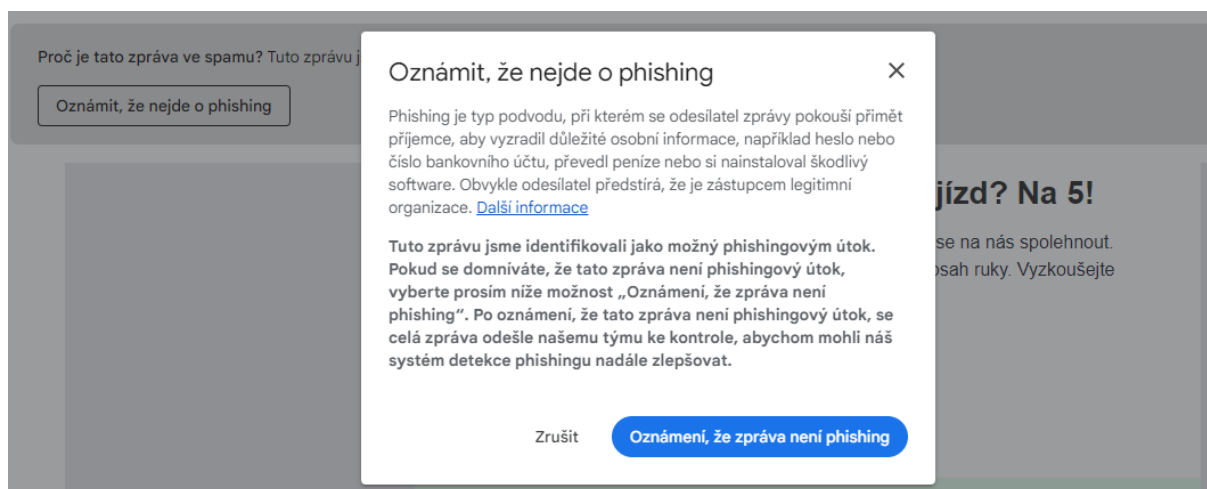
Pokud se domníváte, že tato zpráva je phishingovým útokem, můžete ji nahlásit našemu týmu pro vyšetřování zneužití a pomoci nám tak přerušit tento útok a jemu podobné. Pokud tuto zprávu nahlásíte jako útok, odešle se celá zpráva našemu týmu ke kontrole.

Zrušit

Zpráva oznámení phishingu

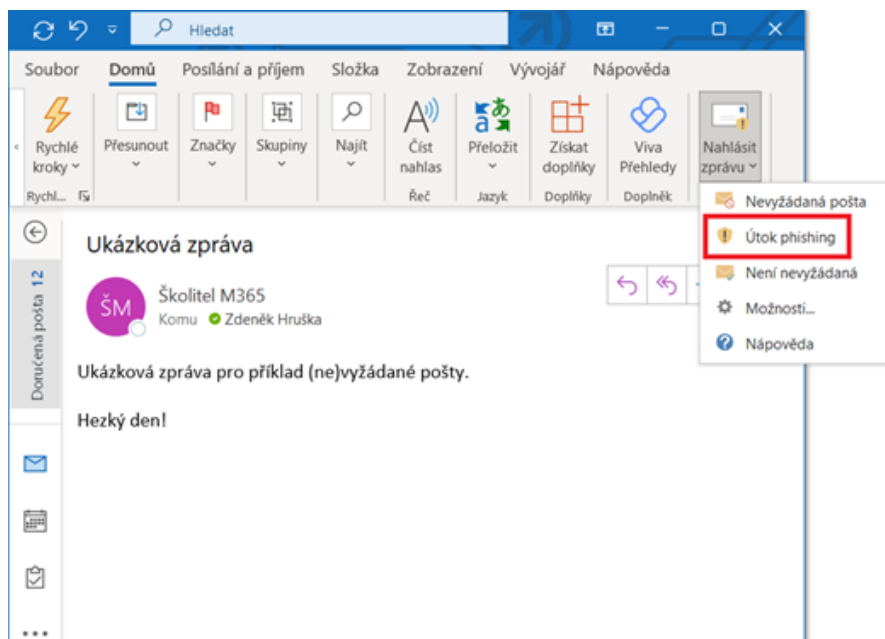
Obrázek 28 - Zpráva oznámení phishingu (Zdroj: Osobní Gmail)

V případě, že nakonec usoudíme, že nejde o phishing, zprávu najdeme ve složce Spam, když ji otevřeme můžeme oznámit, že nejde o spam. Následně klikneme na tlačítko Oznámení, že zpráva není phishing.



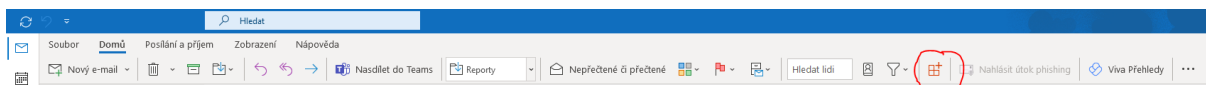
Obrázek 29 - Stáhnutí oznámení (Zdroj: Osobní Gmail)

Hlášení ve firemní síti pomocí Outlooku – Jednou z možností je nastavení hlášení phishingu pomocí Outlooku, ne všechny společnosti tento doplněk aktivně používají. V případě, že zaměstnavatel využívá Outlook a identifikovali jsme podezřelou zprávu, je možné ji nahlásit v doplňcích Outlooku. Označíme nebo otevřeme danou zprávu, klikneme na záložku Domů, následně na nahlásit zprávu a vyberme Útok phishing. Zprávu jsme nahlásili a byla přesunuta do složky Nevyžádaná pošta. Nevyžádaná pošta bude uchována po dobu 30 dnů a pak se odstraní.



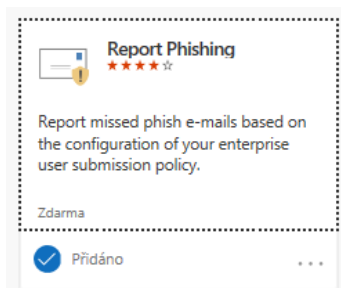
Obrázek 30 - Jak nahlásit phishing (60)

V případě, že se nám v Outlooku tento doplněk neobjevuje, přejdeme na stránku Domů a klikneme na Procházet doplňky.



Obrázek 31 - Kde se nachází Procházet doplňky (Zdroj: Outlook)

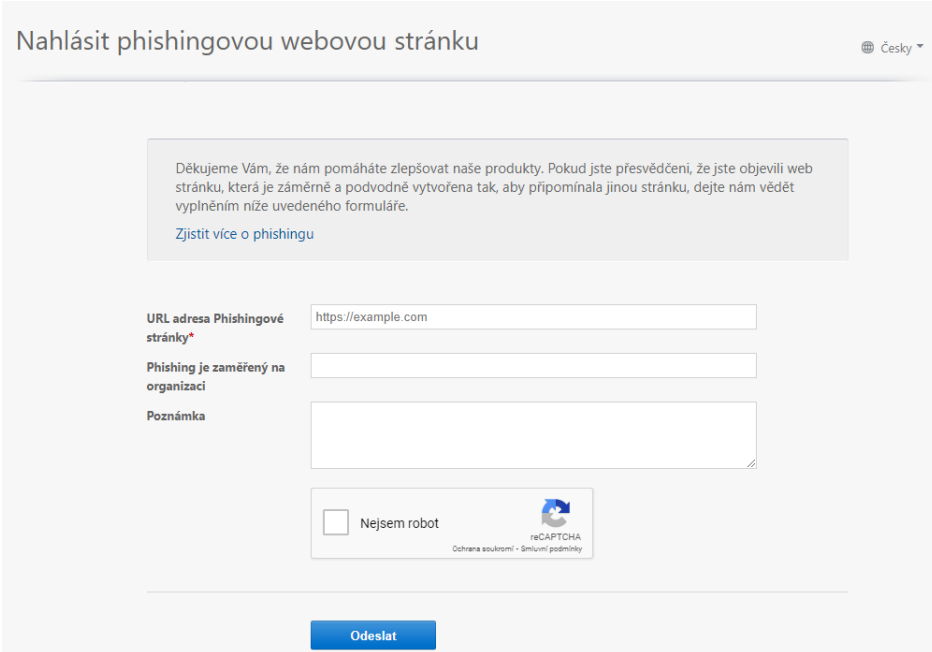
Následně vyhledáme Report Phishing a přidáme si ho do Outlooku.



Obrázek 32 - Doplněk Report Phishing (Zdroj: Outlook)

Nyní postupujeme podle návodu výše. Pokud na phishing narazíme v zaměstnání, obrátíme se na příslušnou osobu a s ní řešíme problém.

Nahlášení phishingové webové stránky – Na stránce <https://phishing.eset.com/cs-cz/report> lze nahlásit podvodné stránky, stačí jen vyplnit URL adresu phishingové stránky, na jakou organizaci je phishing zaměřený a případně poznámku. (61)



The image shows a web form titled "Nahlásit phishingovou webovou stránku" (Report a phishing website) in Czech. The form includes a thank-you message, a text area for the URL (pre-filled with "https://example.com"), a text area for the target organization, and a larger text area for notes. It also features a "Nejsem robot" (I am not a robot) checkbox and a reCAPTCHA widget. A blue "Odeslat" (Send) button is at the bottom.

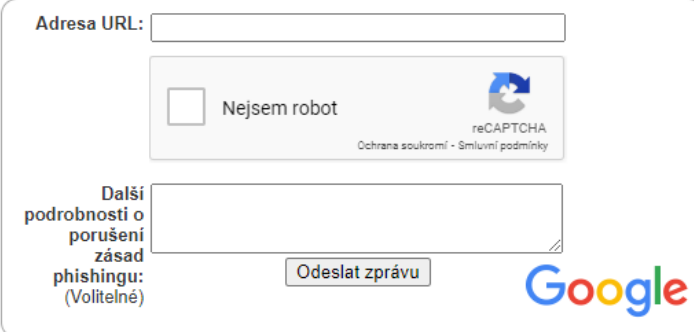
Obrázek 33 - Nahlášení phishingové webové stránky (61)

Případně tuhle možnost podporuje i Google, stačí vyplnit Oznámení phishingové stránky na stránce https://safebrowsing.google.com/safebrowsing/report_phish/?hl=cs. (62)

Oznámení phishingové stránky

Děkujeme, že nám pomáháte udržovat Internet bez phishingových stránek. Budete-li se domnívat, že jste narazili na stránku navrženou tak, aby ve snaze o krádež osobních údajů uživatelů vypadala jako jiná stránka, vyplňte prosím níže uvedený formulář a ohlaste danou stránku týmu Bezpečného prohlížení společnosti Google.

Když nám odešlete weby, odešlou se do Googlu některé informace o účtu a systému. Informace, které odešlete, využijeme k ochraně služeb Google, infrastruktury a uživatelů před potenciálně škodlivým obsahem. Pokud zjistíme, že určitý web porušuje zásady společnosti Google, můžeme aktualizovat jeho stav v naší službě Transparency Report a poskytnout příslušnou adresu URL a její stav třetím stranám. Další informace o službě Transparency Report naleznete [zde](#). Informace o vašem hlášení budou zpracovány v souladu se [zásadami ochrany soukromí](#) a [smluvními podmínkami](#) společnosti Google.

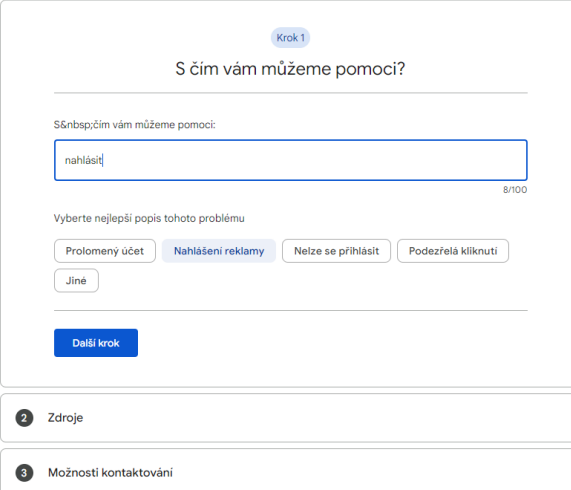


The image shows a web form for reporting a phishing page. At the top, there is a text input field labeled "Adresa URL:". Below it is a reCAPTCHA widget with the text "Nejsem robot" and the reCAPTCHA logo. Underneath the reCAPTCHA is a checkbox and the text "Ochrana soukromí - Smluvní podmínky". To the left of the next input field, there is a label "Další podrobnosti o porušení zásad phishingu: (Volitelné)". The input field itself is empty. Below the input field is a button labeled "Odeslat zprávu". In the bottom right corner of the form area is the Google logo.

Obrázek 34 - Nahlášení phishingové stránky Google (62)

Nahlášení phishingových stránek zobrazené v reklamách ve Vyhledávání Google – Pokud jsme narazili na phishingové stránky při výsledcích vyhledávání jako sponzorovaný odkaz, nahlásíme stránky přes následující odkaz. (62)

https://support.google.com/google-ads/gethelp?visit_id=638330604189601521-1619996459&rd=1



The image shows a multi-step reporting form. The first step is labeled "Krok 1" and asks "S čím vám můžeme pomoci?". Below this is a text input field with the placeholder "nahlášení" and a character count "8/100". Underneath, there is a prompt "Vyberte nejlepší popis tohoto problému" followed by several buttons: "Prolomený účet", "Nahlášení reklamy" (which is highlighted), "Nelze se přihlásit", "Podezřelá kliknutí", and "Jiné". At the bottom of this section is a blue button labeled "Další krok". Below the main form area are two additional sections: "2 Zdroje" and "3 Možnosti kontaktování", each with a small circular icon containing the step number.

Obrázek 35 - Nahlášení reklam ve Vyhledání Google (62)

6.5 Co dělat, když byl útočník úspěšný

- **Změně hesla** – Pokud útočník získal přístup k vašemu e-mailu, sociálním sítím, systémům nebo jiným účtům je třeba neprodleně změnit heslo. Je možné, že ho útočník ještě nestihl měnit.
- **Kontaktování banky, organizace nebo zaměstnavatele** – Záleží, v jaké se nacházíme situaci. Pokud vám byly zcizeny údaje z kreditní karty včetně přihlašovacích údajů do internetového bankovníctví, hned po vyzkoušení změny hesla je nutné kontaktovat banku, která dočasně zneaktivní účet a nikdo z něj nebude moci zcizit finanční prostředky.

Pokud máme přístup do externích systémů a jejich přihlašovací údaje byly zcizeny, musíme kontaktovat i externí firmu, které může pomoci s řešením incidentu. Jestliže se takový incident stal s firemními daty a přihlašovacími údaji, musíme neprodleně kontaktovat osobu, která řeší takovéto bezpečnostní incidenty (oddělení bezpečnosti např. nebo alespoň svého nadřízeného).

- **Oznámení policii** – V případě získání informací ze zcizeného občanského průkazu klienta nebo jeho pasu je třeba podat oznámení policii. Ta nahlásí občanský průkaz nebo pas jako kradený případně zneužitý. Banky v systému uvidí, že jde o zcizený občanský průkaz a mohou útočníka policii nahlásit.

7 Návrh phishingové kampaně pro reálnou společnost

Společnost, pro kterou byla phishingová kampaň vytvářena, si nepřála zveřejňovat jméno z důvodu ochrany firemních údajů. Je možné uvést, že se jedná o nebankovní instituci, která je na trhu již několik let.

7.1 Představení společnosti a organizační struktura

Firma disponuje pětistupňovou organizační strukturou, ve čtvrtém stupni má 9 divizí (HR, Finance, Právní, IT...), kde každá z nich má hned několik oddělení a sekcí.

7.2 Oddělení bezpečnosti ve společnosti

Ve společnosti se tým bezpečnosti stará mimo jiné i o školení a testování zaměstnanců (např. ohledně phishingu), zveřejňuje na intranet¹⁷ tipy o bezpečnosti, rozesílá edukační emaily.

¹⁷ Intranet = síť kde mezi sebou daná skupina uživatelů (v tomto případě zaměstnanci firmy) sdílí důležité informace.

Testování zaměstnanců – Ve společnosti probíhá zřídka, v minulosti jednou ročně, do budoucna je snaha provádět testování jednou za kvartál. Testování se zaměřuje na phishingové e-maily, jejichž výsledky oddělení bezpečnosti vyhodnotí, následně reportuje TOP managementu společnosti a vytváří edukační program (edukační leták nebo zasílají e-mail, kde vysvětlí, jak bylo možné phishingový e-mail poznat). Cílem edukačního programu je, aby zaměstnancům vysvětlil danou problematiku, čím sníží riziko podlehnutí dalším phishingům.

Tipy na intranetu – Na intranet jsou zveřejňovány články ohledně ochrany osobních údajů, bezpečného surfování na internetu, hesel, stahování, obezřetnosti při placení, nebezpečných odkazů, flash disků a jiných témat.

Online školení od společnost PREVENT s.r.o. – Každý nový člen, který nastoupí do společnosti, absolvuje hned několik online školení zakončených testem (témata školení: Informační a kybernetická bezpečnost, Praní špinavých peněz – AML, GDPR, Etický kodex, Operační rizika, Bezpečnost práce pro zaměstnance, Požární ochrana pro zaměstnance, Specifika BOZP a PO). Tyto školení zaměstnanci podstupují opakovaně každý rok.

Školení při nástupu nového zaměstnance – Když nastoupí do společnosti nový zaměstnanec, čeká ho krátké bezpečnostní školení. Obsahuje základy phishingu, smishingu, vishingu (co to je, ukázka a základní tipy, jak rozeznat podvodné jednání), nebezpečí QR kódu, cizího flash disku, hesla (jak vytvořit heslo, další tipy a ukázky).

Ukázka školení – Informační a kybernetická bezpečnost – Seznamuje zaměstnance s hlavními zásadami zajištění ochrany informací, používáním výpočetní, informační a komunikační techniky. Školení popisuje zásadní zákony týkající se oblasti informační nebo kybernetické bezpečnosti, popisuje Zákon o kybernetické bezpečnosti. Definuje informační a kybernetickou bezpečnost, informaci, obchodní tajemství a jak ho chránit, utajované informace, informační a komunikační technologie, informační systém, bezpečnostní událost, incident, digitální certifikát a elektronický podpis, rizika. Klasifikuje informace ve společnosti (veřejné, neveřejné, důvěrné, tajné). Uvádí povinnosti pro používání ICT služeb a techniky. Popisuje malware, další hrozby (spam, drive by download, browser hijack, botnet, DoS), techniky sociálního inženýrství, rizika na sociálních sítích. Popisuje, jak minimalizovat uvedená rizika, zásady tvorby bezpečného hesla a jeho požadavky, jak zálohovat data apod.

Jelikož firemní školení je přizpůsobené na míru společnosti, níže jsou z důvodu zachování anonymity zobrazeny snímky z demo verze, která je k dispozici na oficiálních stránkách společnosti PREVENT.

ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI



Pod pojmem informační a kybernetická bezpečnost si lze představit **soubor opatření** (technických, organizačních, administrativních, režimových aj.) k zajištění tří klíčových atributů informací a dat.



Obrázek 36 - Ukázka školení 1 (63)

PHISHING



Každý phishingový útok spočívá ve snaze útočníka nalákat svou oběť do prostředí, kde mu tato v dobré víře a dobrovolně předá své osobní údaje. Typicky přístupové údaje k bankovním účtům nebo čísla platebních karet.

Útočník tzv. nahodí udičku (odtud výraz phishing = rybaření) a uživatel se buď chytne, nebo nikoliv. K "nahození udičky" jsou obvykle využívány matoucí e-mailové zprávy, SMS, případně zprávy rozesílané přes komunikační nástroje nebo sociální sítě.

Snaha útočníka o vylákání citlivých údajů od své oběti.

PŘÍKLADY PHISHINGU

JAK ROZPOZNAT PHISHINGOVÝ ÚTOK?

JAK SE BRÁNIT?

Obrázek 37 - Ukázka školení 2 (63)

ZABEZPEČENÍ PŘÍSTUPOVÝCH ÚDAJŮ



Neoprávněné získávání a následné zneužívání přístupových údajů k zařízením ICT, bankovním účtům, aplikacím, e-mailovým schránkám nebo firemním informačním systémům je noční můrou nejednoho uživatele, ale i administrátora systému.

Optimální způsob zabezpečení přístupových údajů k datům lze jednoduchým způsobem přirovnat k optimálnímu zabezpečení domu nebo bytu:

Neulehčujte práci případným útočníkům, zabezpečení přístupu k datům je stejně důležité, jako zabezpečení bytu nebo ochrana movitého majetku!



Obrázek 38 - Ukázka školení 3 (63)

Edukační e-mail – Edukační emaily mají různé povahy, může jít například o vzdělávání zaměstnanců v těchto oblastech:

- bezpečnosti aktiv zapůjčených společnostmi (PC, telefony, monitory apod.)
- vlastních aktiv používaných doma (router)
- bezpečnost virtualizace
- bezpečnost při využívání různých systémů a aplikací
- bezpečnost ohledně AI – Chat GPT

Krásné pondělí všem,

umělá inteligence (AI) zažívá v posledních měsících velký boom. Pomalu začíná zasahovat do různých sfér a můžeme ji najít na místech, kde byste ji nečekali. Jednou z oblastí, kde AI ukazuje výrazný potenciál jsou chatboti určené ke generování textu. Nejznámějším chatovacím robotem posledních dnů je jednoznačně ChatGPT.

Výhody této AI si umíme všichni představit, ať už se jedná o například zrychlení práce, hledání, ověřování, vytváření nových profilovek, tak především momentálně AI vynikají v přepisu a opravě textu, opravách rozmazaných obrázků a do budoucna určitě uvítáte i možnost tvorby prezentací na základě pouze heslovitých vstupů apod. Výhod je určitě hodně, avšak stejně jako každá jiná technologie, má i AI své negativní stránky.



Abychom minimalizovali možná rizika spojená s používáním dané technologie (atomová bomba je taky vynikající věc), tak bychom vás rádi informovali:

Obrázek 39 - Úryvek e-mailu ohledně Chat GPT (Zdroj: Interní zaměstnanci)

Vážení kolegové,

někdy se může stát nepříjemná situace v podobě **ztráty nebo krádeže firemního zařízení**. Věříme, že se vás to nebude týkat, ale pro případ je vždy dobré vědět, jak postupovat.



Ztráta firemního zařízení, například telefonu, notebooku nebo tabletu, může být značně nepříjemná a zároveň potenciálně riskantní z hlediska bezpečnosti dat společnosti. Pokud jste v takové situaci, doporučujeme vám postupovat dle následujících kroků:

1. **Okamžitě informujte svého nadřízeného a hned následně informujte IT HelpDesk:** Co nejdříve sdělte situaci odpovědným osobám ve své firmě. Buďte upřímní ohledně okolností ztráty a místa, kde se to stalo. Tím pomůžete minimalizovat potenciální škody a rizika.
2. **Nahlášení ztráty místní policii:** Pokud jste přišli o zařízení, například v důsledku krádeže nebo neopatrnosti, důrazně doporučujeme tuto ztrátu nahlásit místní policii. Získání policejního protokolu může být užitečné pro následné nárokování pojistného plnění nebo pro potřeby firemního vyšetřování.
3. **Zabezpečení účtů:** Neprodleně změňte hesla na všech (firemních i osobních) účtech, které byly na zařízení přístupné. To zahrnuje e-mailové účty, cloudové úložiště, firemní aplikace a další. Tím minimalizujete možnost neoprávněného přístupu k firemním datům a vašim účtům a ušetříte si další problémy. Ztracený notebook nebo mobil může být u některých účtů veden jako důvěryhodné zařízení, z účtu jej odeberte. S těmito úkony vám pomůže IT HelpDesk.
4. **Vzdálené vymazání dat:** Pokud to vaše zařízení umožňuje a máte dostatečné oprávnění, můžete požádat o vzdálené vymazání dat na ztraceném zařízení. To je obzvláště důležité, pokud se obáváte, že by mohla být vaše data kompromitována.
5. **Náhrada SIM karty:** Při ztrátě mobilního telefonu informujte svého nadřízeného, se kterým co nejdříve zajistíte blokad SIM a zažádejte o vystavení nové.
6. **Informujte kolegy:** Pokud na ztraceném zařízení měli kolegové nebo obchodní partneři kontakty nebo citlivé informace, informujte je o situaci, aby mohli podniknout opatření k ochraně svých účtů a dat.
7. **Zvážení pojistného plnění:** Pokud bylo ztracené zařízení pojistněno, informujte pojistovnu a zahajte postup pro náhradu.

Ztráta firemního zařízení je vážná záležitost, a proto je důležité postupovat okamžitě a informovat odpovědné osoby. Zabezpečení dat a prevence dalších potenciálních rizik by měly být prioritou vašeho jednání v této situaci.

Jak postupovat v případě ztráty nebo krádeže?

Všechny informace najdete také na intranetu...

[Odkaz na intranet](#)

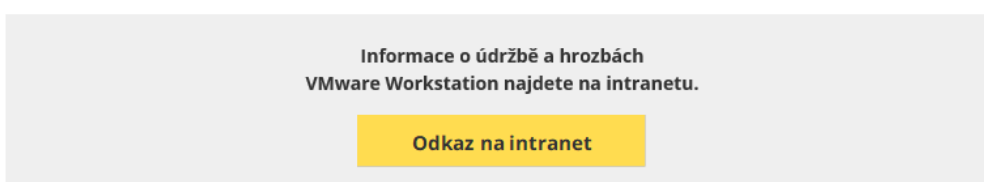
Obrázek 40 - E-mail o správném postupu při ztrátě firemního zařízení (Zdroj: Interní zaměstnanci)

Vážení kolegové,

v dnešní době je stále důležitější, aby zaměstnanci v oblasti IT měli povědomí nejen o konceptu virtualizace a nástrojích, které virtualizaci umožňují, ale také o bezpečnosti virtualizace.

Je důležité mít na paměti, že nesprávné používání nástrojů pro vizualizaci může ohrozit informační bezpečnost. **Pro zajištění maximálního zabezpečení je důležité udržovat váš nástroj aktuální.** Prosíme, zkontrolujte, zda je váš nástroj aktuální, pokud ne, **provedte jeho aktualizaci na vašich stanicích.**

Aktualizace by měly být prováděny pouze z oficiálních zdrojů výrobců (např.: VMware nebo Oracle VM virtualbox). Mezi potenciální bezpečnostní rizika neaktualizovaného nástroje patří vzdálené spuštění kódu, eskalace oprávnění a únik informací z virtuálních strojů.



Obrázek 41- E-mail o bezpečnosti virtualizace (Zdroj: Interní zaměstnanci)

7.3 Nástroje používané k hlídání bezpečnosti zaměstnanců:

Společnost používá hned několik nástrojů k hlídání bezpečnosti. Níže zmíněné nástroje jsou důležité pro návrh phishingové kampaně, společnost jich používá více.

7.3.1 Microsoft 365

Společnost používá Microsoft 365 Business Premium zajišťuje pokročilou ochranu kybernetické bezpečnosti pro zařízení, e-mail (například dokumenty Office) a data (šifrování, popisky citlivosti a ochrana před únikem informací). (64)

Pomocí Microsoftu se dají data zabezpečit různými způsoby:

- MFA – Vícefaktorové ověřování (dvoustupňové ověřování).
- Nastavení a ochrana účtů správce – Jelikož správci mají více oprávnění než ostatní zaměstnanci, jsou pro útočníky cenným cílem.
- Použijte přednastavené zásady zabezpečení k ochraně obsahu e-mailu – Jde o ochranu před spamem, malwarem a útoky pro e-maily. Pokročilá ochrana proti útokům phishingu, nastavení falšování identity, bezpečné odkazy a přílohy pro e-maily a dokumenty Office.

- Zabezpečení spravovaných a nespravovaných zařízení – Zabezpečení Microsoft 365 Apps, upgrade na Windows 10 nebo 11 Pro.
- Trénování zaměstnanců – Před spamem, malwarem a phishingovými útoky pro e-maily
- Sdílet soubory, odkazy, přílohy, komunikaci přes Microsoft Teams.
- Sdílet soubory a složky na SharePointu a OneDrivu.
- Udržování prostředí – přidávání a odebrání uživatelů a zařízení. (64)

7.3.2 HP Wolf Security

Jde o komplexní ochranu počítačů a tiskáren, začíná na úrovni hardwaru a zahrnuje software a služby. HP zajišťuje komplexní ochranu a kybernetickou odolnost koncových zařízení. Využívá technologii izolace, zajišťuje, že kritické aplikace jsou chráněny před veškerým malwarem, kterým mohou být napadeny počítače. Aplikace a data jsou bezpečně izolovány od hostitelského operačního systému a od útočníků, kteří by do operačního systému mohli proniknout. (65)

7.3.3 MS Defender

Společnost ho používá k monitorování firemních notebooků. Kontroluje odkazy a přílohy, které zaměstnanec otevírá, soubory a aplikace, které stahuje. Chrání zařízení před viry, ransomwarem, spywarem a dalšími typy malwaru. Kontroluje také systémy, které již v zařízení jsou atd.

7.3.4 O365 bezpečnostní centrum

Pomocí něj společnost testuje také zaměstnance. Vytváří phishingové kampaně. Buď může vytvořit předdefinovanou kampaň (DHL, covid...), nebo svojí vlastní od základu. Může se zaměřit na phishingový odkaz, přílohu nebo třeba přihlášení do systému (Git-Hub). E-mail může být poslaný i jako od externího odesílatele. Po spuštění kampaně, jsou monitorování zaměstnanci a jejich chování, dochází k vyhodnocení, kolika lidem kampaň byla zaslána, kolik lidí si e-mail zobrazilo, kolik kliklo na podvodný odkaz, kolik lidí se přihlásilo apod. Konečné graficky zobrazené výsledky poté slouží pro report TOP managementu.

7.3.5 Gophish

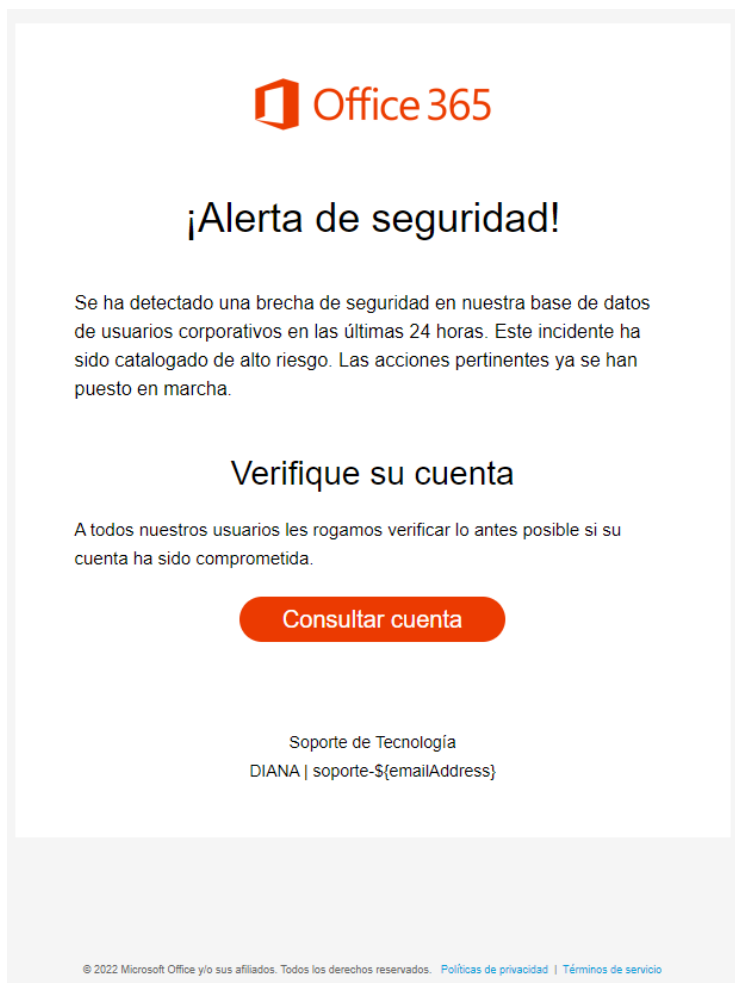
Společnost jej využívá pro jednoduchou simulaci phishingových útoků. Jde o obdobný nástroj jako bezpečnostní centrum O365, poskytuje stejné funkce ochrany jako bezpečnostní centrum.

8 Navrhované řešení, přínos návrhu řešení

Po domluvě s oddělením bezpečnosti a vedením, jsme se domluvili, že kampaň vypustíme na začátku prosince 11.12. v 7 hodin ráno (původní plán byl ve 3 ráno, ale nakonec došlo k posunutí). Zpracovala jsem několik návrhů phishingových e-mailů, které by se pro kampaň daly využít, s tím, že jeden byl nakonec pro kampaň vybrán. Byl to ten, který by měl prověřit zaměstnance a jejich znalosti při rozpoznání phishingu. Přínosem návrhu řešení je trénink zaměstnanců.

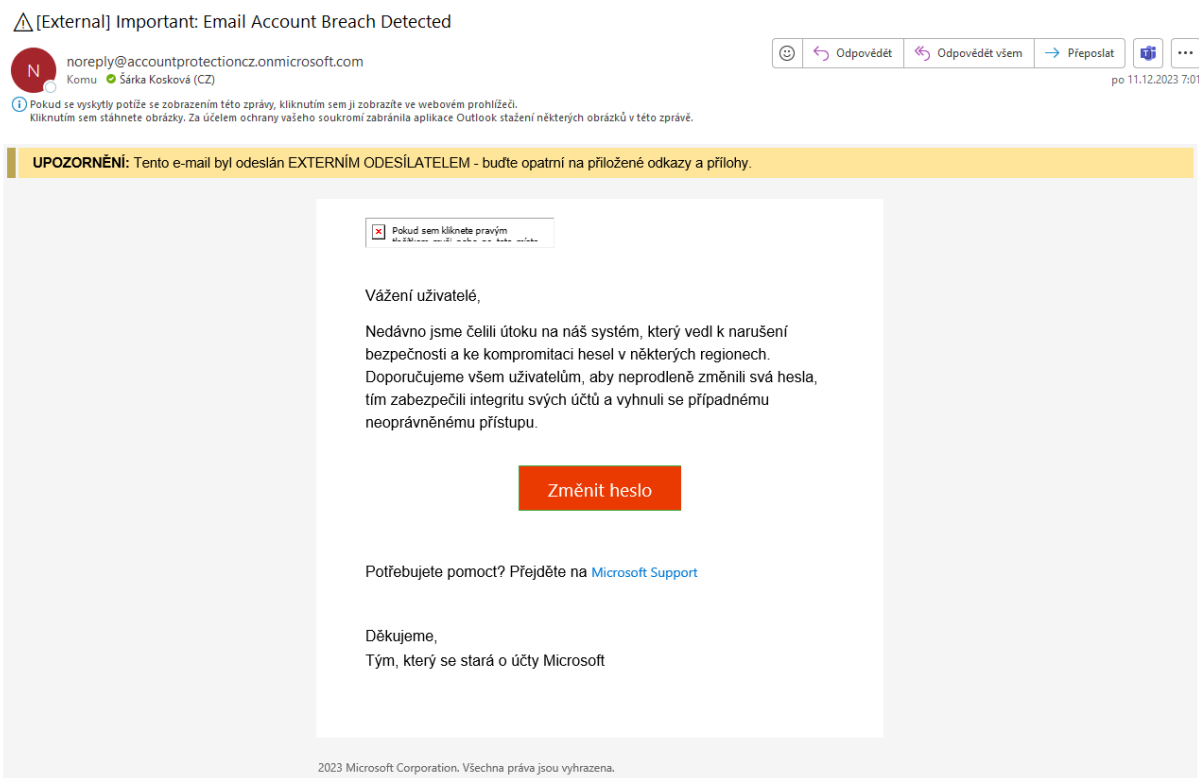
8.1 Kampaň

Zvolila jsem phishingový e-mail, který se tváří jako e-mail od společnosti Microsoft. S tím, že se v něm apeluje na změnu hesla přes přiložený URL link. Protože MS Defender nabízí různé šablony e-mailů, byla jedna z nich zvolena. Pak jsem upravila její HTML kód přes Visual Studio Code.

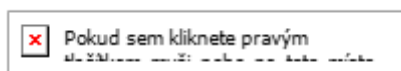


Obrázek 42 - Použitá neupravená šablona e-mailu (Zdroj: MS Defender)

Šablonu e-mailu, jsem upravila do konečné podoby viz níže. Původně jsme se domluvili na textaci e-mailu v anglickém jazyce, která by působila důvěryhodněji. Nicméně, nakonec byl vznesen požadavek na českou textaci, kvůli zaměstnancům, kteří cizí jazyk neovládají. Snažila jsem se napodobit vizuál interní komunikace, proto jsem přidala oranžový banner, který upozorňuje na to, že e-mail byl odeslán externím odesílatelem. Tlačítko „Změnit heslo“ má v html kódu kulaté okraje, nicméně Outlook si ho překresluje.



Obrázek 43 - Konečná phishingová kampaň (Zdroj: Vlastní zpracování)

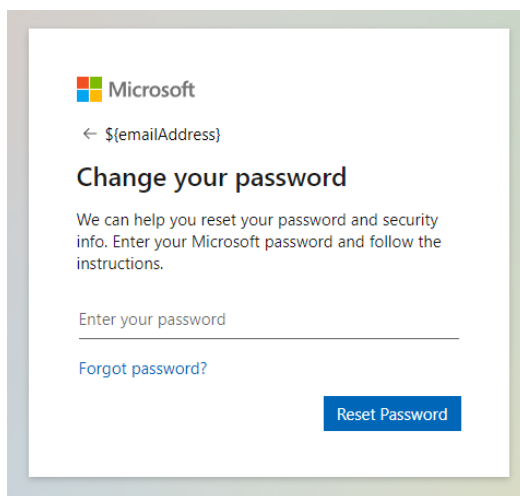


Obrázek 44 - Nezobrazené logo Microsoftu (Zdroj: Vlastní zpracování)

Sem jsem vložila obrázek Microsoftu, URL obrázku byla v HTML byl vložena pomocí base64¹⁸. Protože pokud bych vložila obrázek přímo, tak by se v e-mailu nezobrazil. Nicméně ani tak se nezobrazil, pouze po uložení e-mailu.

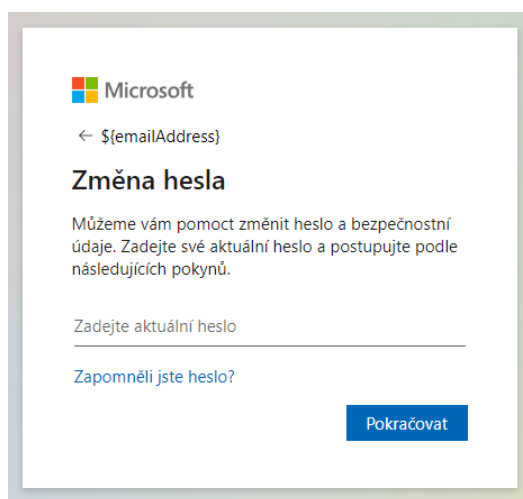
¹⁸ Base64 = kódování převádějící binární data na tisknutelné znaky

Po kliknutí na tlačítko „Změnit heslo“ byl uživatel přesměrován na stránku viz níže, kde si měl uživatel změnit heslo. Pro tuto stránku byla opět použita šablona z MS Defenderu, upravila jsem její html přes Visual Studio Code.

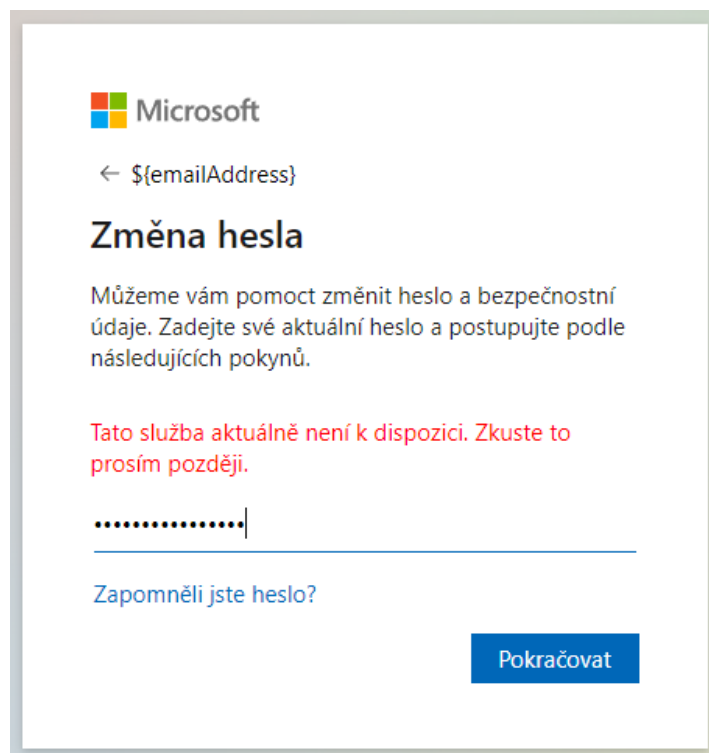


Obrázek 45 - Změna hesla šablona (Zdroj: Vlastní zpracování)

Níže je zobrazena konečná stránka, kde uživatelé mohli měnit svá hesla. Místo <code>\${emailAddress}</code> byl propsán e-mail uživatele, který na tlačítko Změnit heslo klikl. Původně jsem přidala input i pro napsání nového hesla a potvrzení nového hesla. Ale po dohodě s oddělením bezpečnosti jsme se ujednotili, že by mohlo dojít k problému, protože by si uživatelé mysleli, že si heslo změnili a při přihlašování v počítači by si zablokovali jejich účet. Tímto bychom přidělali práci zaměstnancům na oddělení podpory.



Obrázek 46 - Konečný návrh stránky pro změnu hesla (Zdroj: Vlastní zpracování)



Obrázek 47 - Co se stane po kliknutí na pokračovat (Zdroj: Vlastní zpracování)

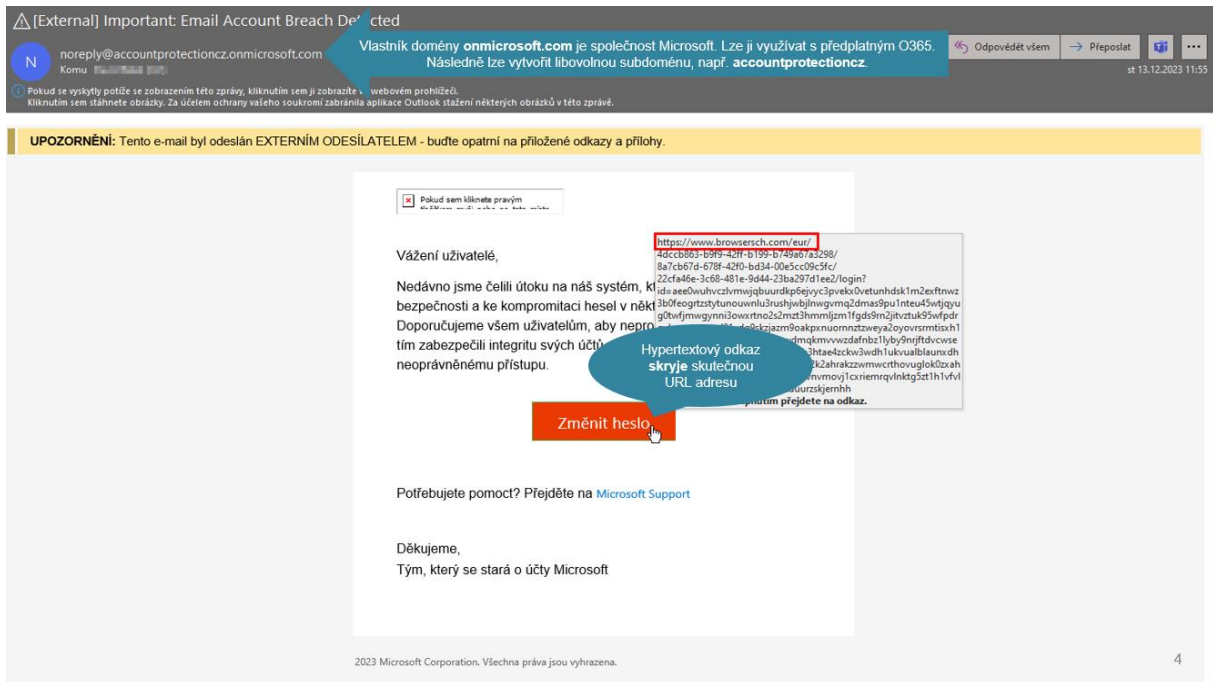
Po napsání aktuálního hesla a kliknutí na tlačítko „Pokračovat“, není uživatel nikam přesměrován, zůstává na stránce, pouze jsme ho upozornili pomocí červené textace „Tato služba aktuálně není k dispozici. Zkuste to prosím později.“.

8.1.1 Identifikace phishingu

Níže lze vidět dva prvky, podle kterých šlo identifikovat phishing.

Odesílatel – Vlastník domény onmicrosoft.com je opravdu Microsoft, lze ji využívat s předplatným Microsoft 365. Byla však vytvořena subdoména accountprotectioncz. Podle této subdomény, především „cz“ na konci, šlo identifikovat phishing. Subdoménu accountprotection je také používána společností Microsoft, ale používá ji ve formátu @accountprotection.microsoft.com. Microsoft používá doménu k odesílání e-mailových oznámení o dvoustupňovém ověření a změnách hesla. (66)

Hypertextový odkaz – V mém případě dobře posloužil ke skrytí podvodné URL adresy. Po najetí šipky na tlačítko „Změnit heslo“ se ale odkryje náhled skutečné URL adresy.

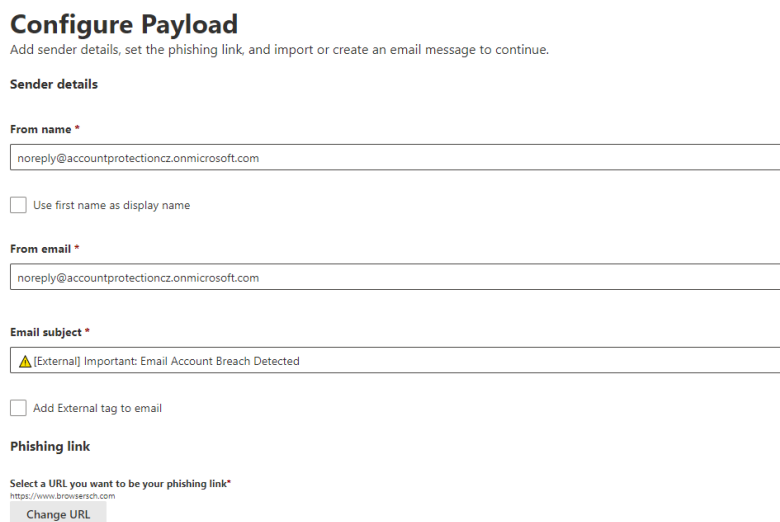


Obrázek 48 - Identifikace phishingu (Zdroj: Interní zaměstnanci)

8.1.2 Vytvoření přes MS Defender

Přes MS Defender byla nastavená kampaň, komu bude e-mail zaslán a na co všechno cílíme. V našem případě to bylo kliknutí na tlačítko „Změnit heslo“ a na stránce změnění hesla kliknutí na tlačítko „Pokračovat“.

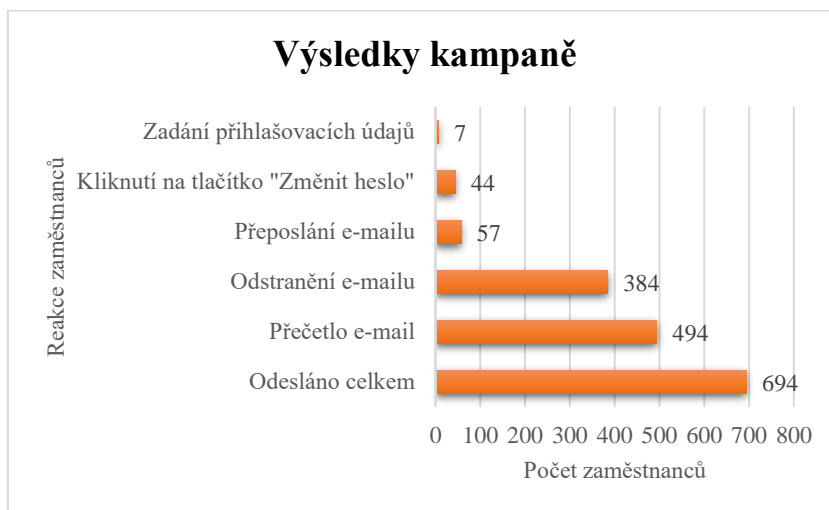
V nastavení kampaně se nastavil název kampaně, detaily odesílatele, předmět emailu, tělo podvodného e-mailu, URL phishingový email aj.



Obrázek 49 - Konfigurace MS Defender (Zdroj: MS Defender)

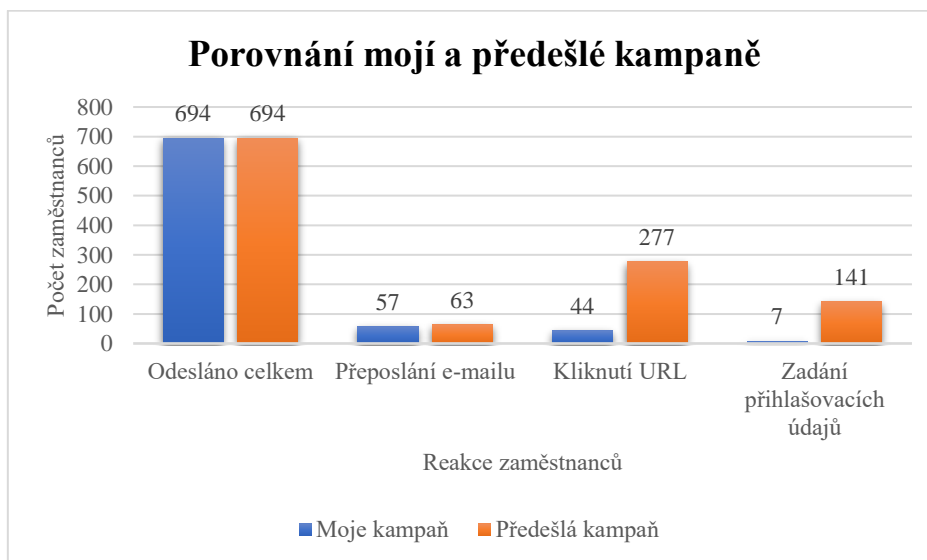
8.1.3 Vyhodnocení

Jak z níže uvedeného grafu vyplývá, byl e-mail zaslán téměř 700 zaměstnancům. E-mail si přečetlo 494 lidí, 384 lidí zprávu odstranilo, 44 lidí ji někomu přeposlalo. Sedm zaměstnanců kliklo na odkaz. Z těchto sedmi zaměstnanců pak 4 zaměstnanci zadali své přihlašovací údaje. Všichni tito zaměstnanci pracují na stejném oddělení (kde zaměstnanci neovládají tak dobře cizí jazyk a kvůli kterým byl phishing přeložen do češtiny). Nakonec 57 zaměstnanců poslalo e-mail na kontrolu zaměstnancům oddělení bezpečnosti.



Graf 1 - Výsledky kampaně (Zdroj: Vlastní zpracování)

Nízký počet obětí kampaně potvrzuje, že míra znalostí phishingu u zaměstnanců je vysoká.



Graf 2 - Porovnání kampaní (Zdroj: Vlastní zpracování)

Oproti předešlé kampani nejsou výsledky nyní nijak drastické, tomu pomohla i důkladná edukace po předešlé kampani.

8.1.4 Reportování vedoucímu IT divize

Výsledky kampaně byly zpracovány a prezentovány vedoucímu IT divize formou prezentace, kde byly zpracovány výsledky a porovnání s minulou kampaní.

8.1.5 Ponaučení pro další kampaně

Níže uvádím zjištění, která jsem si společně s oddělením bezpečnosti odnesla do další kampaně:

E-mail se ztratil v záplavě víkendových e-mailů – Po mém průzkumu jsem zjistila, že si několik zaměstnanců v záplavě e-mailů po víkendu nevšimlo phishingového e-mailu a jednoduše ho přešlo. E-mail byl zaslán v pondělí v 7,00 hod. Můžeme se jen domnívat, že pokud bychom ho odeslali třeba v půli dne nebo v pátek před koncem osmihodinové pracovní směny, byly by výsledky jiné. Ale je důležité si uvědomit, že i ignorování phishingu je bezpečný a pro bezpečnost chtěný výsledek.

Česká textace – Česká textace nepůsobí příliš věrohodně, e-maily obvykle společnost Microsoft zasílá v anglickém jazyce. Nicméně našla jsem i výjimky, kdy jsou odesílány česky, ale jde o opravdu staré e-maily.

Podpis e-mailu – Když jsem hledala české e-maily od Microsoftu, našla jsem, jak se společnost podepisuje. To opravdu odpovídá námi použitému „Tým, který se stará o účty Microsoft“. Z mého pohledu tento podpis evokuje podezření o jeho pravosti. Pokud bychom se nesnažili udělat kopii jedna ku jedné k reálným e-mailům, mohli bychom ho i změnit.

Nezadávání nového hesla – Na stránce, kde uživatelé zadávali aktuální heslo, by dle mého názoru přispělo k její věrohodnosti i pole pro napsání nového hesla a jeho potvrzení. Nicméně kvůli možnému přetížení helpdesku jsme od této možnosti opustili.

8.1.6 Edukace zaměstnanců

Kvůli dobrým výsledkům a podrobné edukaci na intranetu a v kancelářích z minulé kampaně se nyní edukace týkala pouze zaměstnanců, kteří pře poslali e-mail na oddělení bezpečnosti s obavou, že neví, zda se jedná o phishing, byla vysvětlena tato problematika formou e-mailu.

Nedávná kampaň a následná edukace zaměstnanců – Ve společnosti se obecně příliš phishingové kampaně zaměřené na zaměstnance nedělají, odhadem asi jedna každý půl rok. Koncem října byla spuštěna kampaň, která byla velmi propracovaná. E-mail se tvářil, jako by ho poslal CEO¹⁹, bylo v něm apelováno na vyzvednutí dokumentů z karantény.

¹⁹ CEO = výkonný ředitel společnosti

Do karantény padají e-maily, které jsou podezříváné z phishingových podvodů. Výsledky této kampaně byly alarmující. Z necelých 700 zaměstnanců kliklo na phishingový odkaz 277 zaměstnanců a 141 zaměstnanců zadalo své přihlašovací údaje. Pouze 63 zaměstnanců ji přeposlalo na oddělení bezpečnosti nebo oddělení podpory, které byly informovány, že byla spuštěna kampaň.

Kvůli těmto výsledkům následně došlo k edukování zaměstnanců pomocí intranetu, edukačních plakátů vyvěšených v kancelářích a také krátkého phishingového školení. Na intranetu byly popsány 4 kroky kontrol e-mailů, vysvětlen phishing, vishing a smishing i s názornými příklady a následně možnost zhlédnutí různých typů školení o phishingu apod.

Také proto lze vysvětlit nepoměrně lepší výsledky, mnou připravené kampaně, která následovala.

Víš, jaký je rozdíl mezi hackerem a rybářem?
Hacker svůj úlovek **nědy** navrácí.

Někdy neodívej svoje heslo
Aři kance nebo policii:
Heslo by mělo být unikátní a rozumně složitě.
Jak vytvořit kvalitní heslo?

Přihlášení do Microsoftu
Jediná platná adresa pro přihlášení do e-mailu nebo k dalším aplikacím Office 365 je:

- <https://login.microsoftonline.com/>
- <https://login.live.com/>

4 KONTROLY, které odhalí všechny typy podvodů

- 1. KONTROLA ODESÍLATELE (volajícího)**
Vždy zkontroluj e-mail nebo telefonní číslo, ze kterého ti přišla zpráva. Neznáš ho, nebo ti přijde podezřelý? Raději na něj nereaguj.
- 2. KONTROLA CHYB V TEXTU**
Obsahuje text chyby nebo nesmyslné věty? Raději takovou zprávu ignoruj...
- 3. KONTROLA ODKAZŮ A PŘÍLOH**
Po rjetí myšl na nad odkaz se rozbál nesmyslná změn písmen nebo stoměna neodpovídá odesílateli? Takovou zprávu raději smaž.
- 4. KONTROLA PAMĚTI**
Očekááš balíček, zprávu od kamaráda z Francie nebo telefonát z Amsterdamu? Ne! Tak proč na to vůbec reagovat?

- Kde Tě může útočník kontaktovat?
- Otevíraj své znalosti
- Školení od IT Bezpečnosti

Obrázek 50 - Edukace zaměstnanců 1 (Zdroj: Interní zaměstnanci)

PHISHING
VISHING
SMISHING

PHISHING
Nedůvěryhodný odesílatel. Podivná příloha. Znaky emočního nátlaku.

Může to být přešpionáž?
Ukázat řešení!

Česká pošta
Vážený zákazník,
váš balík je blokovany na Terminal 3!
Čeká na zpracování z důvodu nezaplacených nákladů na dopravu.
Ukudte nové náklady na dopravu (330 Kč) pomocí odkazu níže:
ODKAZ ZDE

Poznámka: Pokud nestápní, vaše objednávka bude vrácená dý 48 hodin.
2021 Česká pošta | Všechny práva vyhrazena

Může se jednat o PHISHING?
Důle mhnout na tento e-mail. Detektiv je proti, zkus si říct, co může být pravna nepravna, jestli a jak vlnit na tlačítko "Ukázat řešení".

Obrázek 51 - Edukace ukázka phishingu (Zdroj: Interní zaměstnanci)

8.2 Přínos řešení

Investice do vzdělávání zaměstnanců v oblasti bezpečnosti, prevence sociálního inženýrství a testování zaměstnanců zvyšuje povědomí a dovednosti zaměstnanců v dané problematice, což pozitivně ovlivňuje celkovou bezpečnost organizace, bezpečnosti informací a aktiv firmy.

Hlavní přínosy kampaně:

- **Snížení rizika úspěšného phishingu** – Kvalitní testování a edukace zaměstnance naučí lépe rozpoznávat podezřelé e-maily, webové stránky a jiné formy sociálního inženýrství, což snižuje riziko ztráty cenných informací a finanční ztrátu nebo ztrátu dobré pověsti a jména firmy.
- **Ochrana citlivých informací** – Pravidelné vzdělávání a testování zaměstnanců vede k lepšímu chránění citlivých informací organizace.
- **Prevence úniků dat** – Školení a testování zaměstnanců přispívá k prevenci úniků citlivých dat. Lépe informovaní zaměstnanci budou opatrnější při manipulaci s důvěrnými informacemi a minimalizují riziko náhodného nebo úmyslného úniku dat.
- **Zlepšení reputace firmy** – Díky vyšší úrovni bezpečnosti může firma zlepšit svou reputaci u zákazníků, partnerů a dalších zúčastněných stran. Tím pádem i navázat novou spolupráci s jinými organizacemi.
- **Efektivnější reakce na incidenty** – Proškolení a častěji trénovaní zaměstnanci rychleji a efektivněji reagují na bezpečnostní incidenty.

9 Finanční zhodnocení

Finanční zhodnocení bylo provedeno pomocí ukazatele ROSI (Return on Security Investment). Ukazatel poskytuje pohled na to, jak investice do bezpečnosti přispívají k ochraně organizace a předcházení potenciálním hrozbám a incidentům. Vyjadřuje se v procentech. (67)

$$ROSI = \frac{ALE * MR - \text{Náklady na řešení}}{\text{Náklady na řešení}}$$

Vzorec zobrazuje výpočet ROSI. Níže byly rozebrány jednotlivé položky obsažené ve vzorci.

- SLE = očekávaná ztráta + NUKIB pokuty
- ARO = roční míra výskytu incidentů
- MR (Mitigation Ratio) = redukce rizika (o kolik dokáže opatření snížit dopad rizika)
- ALE = SLE * ARO
- MLR = ALE * MR

Přestože byla kampaň navrhována a realizována mnou, podílelo se na ní více zaměstnanců společnosti. Prvním potřebným krokem bylo odsouhlasení s vedoucím IT divize realizace phishingové kampaně. Poté následovalo předložení několika témat vrcholovému vedení ke schválení. V průběhu návrhu schváleného tématu, byla kampaň konzultována se specialistou IT bezpečnosti. Výsledky byly prezentovány vedoucímu IT bezpečnosti a vedoucímu IT divize. Následně specialista interní komunikace sdělil výsledky kampaně prostřednictvím e-mailu všem zaměstnancům. Zaměstnanci, se kterými jsem konzultovala, strávili nad kampaní nějaký čas, který potřeba započítat do ROSI.

Tabulka 1 - Náklady na návrh a realizaci kampaně (Zdroj: Vlastní zpracování)

Osoba	Počet hodin	Hodinová sazba	Finanční náklady
Autor práce	32	160,00 Kč	5 120,00 Kč
Specialista IT bezpečnosti	8	250,00 Kč	2 000,00 Kč
Vedoucí IT bezpečnosti	4	800,00 Kč	3 200,00 Kč
Vedoucí IT divize	1	1 200,00 Kč	1 200,00 Kč
Specialista interní komunikace	2	220,00 Kč	440,00 Kč
Vedení	2	500,00 Kč	1 000,00 Kč
Náklady celkem vč. DPH			12 960,00 Kč

Tabulka popisuje, jaké byly náklady na návrh a realizaci kampaně u zainteresovaných zaměstnanců. Náklady činily 12 960 Kč. Protože jsem chtěla do nákladů zahrnout i oportunitní náklady (náklady ušlé příležitosti), původní částku 12 960 Kč jsem vynásobila dvěma. Celkové náklady tedy kalkuluji na 25 920 Kč.

Následoval výpočet redukce rizika. Pro výpočet byli použity tyto hodnoty. Počet zaměstnanců, kteří se nestali oběťmi incidentu a počet zaměstnanců, kteří se jimi naopak stali. V tomto případě, se to bylo 7 zaměstnanců z 694.

$$MR = \frac{694 - 7}{694} * 100 = 98,98 \%$$

MR vyšlo přibližně 98,99 %.

Očekávané ztráty, pro výpočet SLE, se u finančního sektoru pohybují v řádech desítek milionů Kč, pro finanční zhodnocení operují s částkou 3 000 000 Kč. NUKIB ukládá obvykle za nedodržování doporučených opatření pokutu 5 000 000 Kč, kterou přičítám do SLE (ovšem pokuty se v případě dlouhodobého nedodržování mohou vyšplhat na mnohem vyšší částky). ARO udává počet incidentů (únik dat pomocí phishingu) za rok. Od zaměstnanců bezpečnosti ve společnosti vím, že většinu phishingových e-mailů zachytí Office 365. Bohužel občas se stane, že nezachytí všechny (dochází tak průměrně jednou ročně), proto ARO uvádím jako 1. Výši pokuty a očekávané ztráty mi sdělil, vedoucí práce, který se v dané problematice pohybuje již několik let a velice dobře jí rozumí.

Tabulka 2 - Výpočet ROSI (Zdroj: Vlastní zpracování)

Výpočet ROSI	Výpočet
SLE	8 000 000
ARO	1
MR	0,9899
Náklady	25 920,00
ALE	8 000 000
MLR	7 919 200
ROSI - MR=0,99	30 452%

ROSI (pro MR = 99 %) bylo vypočteno 30 452 %. ROSI reprezentuje poměr návratnosti vynaložených nákladů na snížení rizika. Efektivita opatření činí 30 452 %. Společnost díky vynaloženým nákladům 25 920 Kč teoreticky ušetřila dalších 8 000 000 Kč o které by přišla, kdyby opravdoví útočníci prolomili její bezpečnost.

Je důležité zmínit, že společnost disponuje několika vrstvami ochrany (Office 365 apod.), které mají za cíl detekovat phishingové e-maily. Proto by tyto vrstvy měly phishing odhalit, ovšem při velmi propracovaných útocích se může stát, že by nedošlo k detekci a v tu chvíli, by platilo, že očekávané ztráty a pokuty by mohly být ve výši 8 000 000 Kč.



Graf 3 - Ztráty vs. Náklady (Zdroj: Vlastní zpracování)

Z výše uvedeného grafu vyplývá, že náklady na návrh a realizaci kampaně jsou oproti možným ztrátám téměř zanedbatelné. Proto je vhodné takovéto namátkové phishingové kampaně vytvářet často, aby neustále docházelo ke snižování pravděpodobnosti možného incidentu.

10 Závěr

Práce byla zpracována podle zvoleného postupu a všechny cíle se povedlo splnit. Teoretické informace potřebné pro zpracování diplomové práce byly snadně dohledatelné jak v knižních zdrojích, tak i na internetu.

Povedlo se mi udělat komplexní metodiku pro různě velké společnosti, provést čtenáře úvodem do bezpečnosti a základním názvoslovím. Vysvětlit problematiku podvodného jednání, jak ho poznat, vysvětlit a názorně ukázat různé druhy, jak se jim bránit, předcházet. Následně bylo popsáno, jak a kam phishing hlásit, nebo jakých práv se mohou lidé domáhat. Byl zapracován i vliv AI a Chat GPT na podvodné jednání.

Popsala jsem, jak funguje oddělení bezpečnosti ve společnosti, pro kterou byla kampaň tvořena, zjistila, jaké nástroje používá pro dohled nad bezpečností uvnitř firmy. Dále zjistila, jak zaměstnance edukuje v problematice phishingu.

Povedlo se přispět cíli bezpečnosti zaměstnance procvičit a edukovat v oblasti phishingu. Získali jsme podklady pro další kampaně a vyhodnotila jsem, jak by se daly navrhnout lépe.

Náklady na návrh a realizaci kampaně v rámci všech zainteresovaných zaměstnanců (mě, specialisty IT bezpečnosti, vedoucího IT bezpečnosti, vedoucího IT divize, vedení, specialisty interní komunikace) včetně oportunitních nákladů činily 25 920 Kč. Očekávané ztráty se u finančního sektoru v případě úniků dat pohybují v rádech desítek milionů Kč, pro finanční zhodnocení operují se 3 000 000 Kč. NUKIB ukládá za nedodržování doporučených opatření pokutu až 5 000 000 Kč. Důležité je ale zmínit, že pokuty se v případě dlouhodobého nedodržování mohou vyšplhat na mnohem vyšší částky. Efektivita kampaně činí 30 452 %, což je skvělý výsledek. Je důležité zmínit, že společnost disponuje několika vrstvami ochrany (Office 365 apod.), které mají za cíl detekovat phishingové e-maily. Proto by tyto vrstvy měly phishing odhalit, ovšem při velmi propracovaných útocích se může stát, že by nedošlo k detekci a v tu chvíli, by platilo, že očekávané ztráty a pokuty by mohly být ve výši 8 000 000 Kč.

Mezi hlavní přínosy mé diplomové práce považuji snížení rizika úspěšného phishingu, ochranu citlivých informací, prevenci úniků dat, zlepšení reputace firmy, efektivnější reakce na incidenty. Náklady na návrh a realizaci phishingových kampaní jsou oproti možným ztrátám velice nízké. Proto doporučuji provádět taková cvičení namátkově a často.

Závěrem práce, je potvrzení faktu, že bezpečnost je tak účinná, jak je silný její nejslabší článek.

Seznam použitých zdrojů

1. Phishing stojí za třetinou průniků: Jak poznat škodlivé e-maily? *ESET*. [Online] 14. 9 2020. [Citace: 15. 9 2023.] <https://www.eset.com/cz/blog/prevence/phishing-stoji-za-tretinou-pruniku-jak-poznat-skodlive-e-maily/>.
2. DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha : Professional Publishing, 2020. ISBN 978-80-88260-39-4.
3. Sedlák Petr, Konečný Martin a kolektiv. *KYBERNETICKÁ (NE)BEZPEČNOST*. Brno : CERM, 2021. 978-80-7623-068-2.
4. ČSN EN ISO/IEC 27002 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti*. Praha : Česká agentura pro standardizaci, 2023.
5. ČSN ISO/IEC 27000:2017 *informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – přehled a slovník*. Praha : Český normalizační institut, 2017.
6. ČSN EN ISO/IEC 27001 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky*. Praha : Česká agentura pro standardizaci, 2023.
7. SEDLÁK Petr, Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Brno : CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.
8. Spam. *ESET*. [Online] [Citace: 15. 9 2023.] <https://www.eset.com/cz/spam/>.
9. Bridge. *Jak na newslettery podle GDPR*. [Online] 8. 4 2019. [Citace: 11. 2 2024.] <https://www.ecommercebridge.cz/jak-na-newslettery-podle-gdpr/>.
10. Spear-phishing a jak se před ním chránit. *NUKIB*. [Online] 3. 4 2020. [Citace: 18. 9 2023.] <https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/>.
11. Ochrana před útoky phishing. *Microsoft*. [Online] [Citace: 15. 9 2023.] <https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>.
12. Phishing. *ESET*. [Online] [Citace: 15. 9 2023.] <https://www.eset.com/cz/phishing/>.

13. Phishing - stále aktuální hrozba. *NUKIB*. [Online] 12. 1 2015. [Citace: 28. 9 2023.] <https://www.nukib.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/>.
14. Phishing: 7 tipů, jak ho poznat. *hpmarket*. [Online] [Citace: 29. 9 2023.] <https://www.hpmarket.cz/document.asp?dc=phishing>.
15. Microsoft. *Ochrana před útoky phishing*. [Online] [Citace: 11. 2 2024.] <https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>.
16. NUKIB. *Spear-phishing a jak se před ním chránit*. [Online] 9. 4 2020. [Citace: 11. 2 2024.] <https://nukib.gov.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/>.
17. The Essential Guide to Phishing: How it Works and How to Defend Against it. *AVAST*. [Online] 5. 2 2020. [Citace: 29. 9 2023.] <https://www.avast.com/c-phishing>.
18. Business Email Compromise. *FBI*. [Online] [Citace: 30. 9 2023.] <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>.
19. What is Search Engine Phishing? *KEEPERSECURITY*. [Online] 12. 5 2023. [Citace: 30. 9 2023.] <https://www.keepersecurity.com/blog/2023/04/12/what-is-search-engine-phishing/>.
20. *KEEPERSECURITY*. [Online] [Citace: 11. 2 2024.] <https://www.keepersecurity.com/blog/wp-content/uploads/2023/04/image-example.png>.
21. Upozornění na vishing zneužívající identitu bankovních institucí. *NUKIB*. [Online] 20. 4 2021. [Citace: 28. 9 2023.] <https://nukib.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/>.
22. Vishing. *ESET*. [Online] [Citace: 28. 9 2023.] <https://www.eset.com/cz/vishing/>.
23. Vishing: Jak ho rozeznat a vyhnout se mu? *ESET*. [Online] 17. 5 2022. [Citace: 9. 29 2023.] <https://digitalsecurityguide.eset.com/cz/vishing-jak-ho-rozeznat-a-vyhnout-se-mu>.
24. Co je to vícefaktorová autentizace? *KYBEZ*. [Online] 11. 1 2021. [Citace: 29. 9 2023.] <https://kybez.cz/co-je-to-vicefaktorova-autentizace/>.
25. *KYBEZ*. *Co je to vícefaktorová autentizace?* [Online] [Citace: 11. 2 2024.] <https://kybez.cz/co-je-to-vicefaktorova-autentizace/>.

26. Novinky.cz. *Podvodníci zkoušejí nový trik. Důvěřivce lákají na atraktivní výhry.* [Online] 12. 12 2016. [Citace: 11. 2 2024.] <https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-podvodnici-zkouseji-novy-trik-duverivce-lakaji-na-atraktivni-vyhry-40017984>.
27. What is smishing? How to protect against text message phishing scams. *PORTSWIGGER.* [Online] 14. 9 2021. [Citace: 29. 9 2023.] https://portswigger.net/daily-swig/what-is-smishing-how-to-protect-against-text-message-phishing-scams?fbclid=IwAR29vkdVKuDX6Xwn5SjhMKOqZR3GP_Yn6V-pgSZ-35bS4L6d1AJ-IJslbN.
28. BEZPEČNĚJŠÍ.OSTRAVA. *ÚTOKY PŘES E-MAILY, SMS NEBO TELEFON (PHISHING).* [Online] 21. 12 2022. [Citace: 11. 2 2024.] <https://bezpecnejsi.ostrava.cz/situace/internet/phishing-utoky-pres-zpravy/>.
29. SPAJK. *Pozor na falešné profily na Facebooku.* [Online] 12. 8 2017. [Citace: 11. 2 2024.] <https://spajk.cz/pozor-falesne-profil-y-facebooku/>.
30. What is a Whaling Attack? *KASPERSKY.* [Online] [Citace: 30. 9 2023.] <https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack>.
31. What Is Malvertising and How Do I Stop it? *AVAST.* [Online] 22. 4 2021. [Citace: 30. 9 2023.] <https://www.avast.com/c-what-is-malvertising-how-to-stop-it>.
32. YOURWINDOWSGUIDE. *Vše o podvodu s technickou podporou.* [Online] 24. 3 2020. [Citace: 11. 2 2024.] <https://www.yourwindowsguide.c>.
33. AVAST. *What is scareware?* [Online] 19. 12 2022. [Citace: 11. 2 2024.] <https://www.avast.com/c-scareware>.
34. PRACEZDOMU. *podvodne-reklamy-na-Facebooku.* [Online] 6. 4 219. [Citace: 11. 2 2024.] <https://www.prace-z-domu.com/podvody-na-facebooku/podvodne-reklamy-na-facebooku/>.
35. Email Phishing, Vishing & Other Types of Attacks. *WEBROOT.* [Online] [Citace: 2. 10 2023.] <https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing>.
36. What Is Pharming and How to Protect Yourself. *KASPERSKY.* [Online] [Citace: 30. 9 2023.] <https://www.kaspersky.com/resource-center/definitions/pharming>.

37. FIO. *Přihlášení do Internetbankingu*. [Online] [Citace: 11. 2 2024.] <https://ib.fio.cz/ib/login>.
38. FIO. *Falešný odkaz na Internetbanking*. [Online] 12. 11 2020. [Citace: 11. 2 2024.] <https://www.fio.cz/spolecnost-fio/media/aktuality/246181-falesny-odkaz-na-internetbanking>.
39. QR codes in email phishing. *SECURELIST*. [Online] 27. 9 2023. [Citace: 2. 10 2023.] <https://securelist.com/qr-codes-in-phishing/110676/>.
40. Co je to Chat GPT? *DEEPLY*. [Online] [Citace: 11. 11 2023.] <https://deeply.cz/co-je-to-chat-gpt/>.
41. How fraudsters are using Chat GPT and other AI tools to create scams. *ATB*. [Online] 15. 6 2023. [Citace: 11. 11 2023.] <https://www.atb.com/personal/good-advice/banking-and-security-tips/how-fraudsters-are-using-chat-gpt-and-other-ai-tools-to-create-scams/>.
42. ChatGPT is changing the phishing game. *Security infowatch*. [Online] 18. 4 2023. [Citace: 11. 11 2023.] <https://www.securityinfowatch.com/cybersecurity/information-security/breach-detection/article/53057705/chatgpt-is-changing-the-phishing-game>.
43. The Dangers of AI-Driven Chat GPT Phishing Campaigns and How to Avoid Them. *ID AGENT*. [Online] 6. 6 2023. [Citace: 11. 11 2023.] <https://www.idagent.com/blog/the-dangers-of-ai-driven-chatgpt-phishing-campaigns-and-how-to-avoid-them/>.
44. Vladimír, Smejkal. *Kybernetická kriminalita, 3. vydání*. Plzeň : Aleš Čeněk s.r.o., 2022. 978-80-7380-849-5.
45. Smejkal Vladimír, Sokol Tomáš, Kodl Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň : Aleš Čeněk s.r.o., 2019. 978-80-7380-765-8.
46. Kolouch, Jan. *CyberCrime*. Praha : CZ.NIC, z. s. p. o, 2016. 978-80-88168-18-8.
47. Šcerba, Filip. *Trestní zákoník Komentář*. Praha : C. H. Beck, 2020.
48. DVOŘÁK, Marek. *Phishing, pharming a jejich trestněprávní postih*. Praha : Nakladatelství C. H. Beck, 2022. 9771213531001.
49. <https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu>. *Pravopropodnikatele*. [Online] 7. 9 2022. [Citace: 22. 10 2023.]

<https://www.pravopropodnikatele.cz/phishing-odpovida-za-ztratu-banka-nebo-majitel-uctu>.

50. Phishing – odpovědnost banky a silné ověření. *Pravopropodnikatele*. [Online] 7. 9 2022. [Citace: 22. 10 2023.] <https://www.pravopropodnikatele.cz/phishing-odpovednost-banky-a-silne-overeni>.

51. NÚKIB. *NÚKIB*. [Online] [Citace: 18. 3 2024.] <https://nukib.gov.cz/cs/o-nukib/>.

52. Úřední deska. *NÚKIB*. [Online] [Citace: 11. 11 2023.] <https://www.nukib.cz/cs/uredni-deska/>.

53. Varování před hrozbou kybernetických útoků na strategické organizace v České republice. *NÚKIB*. [Online] 25. 2 2022. [Citace: 11. 11 2023.] https://www.nukib.cz/download/uredni_deska/2022-02-25_varovani-final.pdf.

54. ENISA Threat Landscape 2020 - Phishing. *ENISA*. [Online] 20. 10 2020. [Citace: 11. 11 2023.] <https://www.enisa.europa.eu/publications/phishing>.

55. Anti-Phishing ochrana SMS. *Kaspersky*. [Online] [Citace: 16. 10 2023.] <https://support.kaspersky.com/KISA/MR13/cs-CZ/127530.htm>.

56. Co je phishing? *Webglobe*. [Online] [Citace: 16. 10 2023.] <https://www.webglobe.cz/blog/jak-se-branit-phishingovym-emailum>.

57. Začínáme s Microsoft Defenderem. *Microsoft*. [Online] [Citace: 6. 10 2023.] <https://support.microsoft.com/cs-cz/topic/za%C4%8D%C3%ADn%C3%A1me-s-microsoft-defenderem-9df0cb0f-4866-4433-9cbc-f83e5cf77693>.

58. Začínáme s antimalwarovým softwarem v programu Microsoft Defender. *Microsoft*. [Online] [Citace: 6. 10 2023.] <https://support.microsoft.com/cs-cz/topic/za%C4%8D%C3%ADn%C3%A1me-s-antimalwarov%C3%BDm-softwarem-v-programu-microsoft-defender-f5219ae5-abb7-4985-a149-1ec1bb304eda>.

59. MICROSOFT. *Navštivte portál Microsoft Defender*. [Online] 10. 1 2024. [Citace: 11. 2 2024.] <https://learn.microsoft.com/cs-cz/microsoft-365/security/defender-business/mdb-get-started?view=o365-worldwide>.

60. ITMUNI. *Návod: Jak nahlásit nerozpoznanou phishingovou zprávu*. [Online] [Citace: 11. 2 2024.] <https://it.muni.cz/sluzby/microsoft-outlook/prace-se-spamem-v-microsoft-365/jak-nahlasit-nerozpoznanou-phishingovou-zpravu>.

61. Nahlásit phishingovou webovou stránku. *ESET*. [Online] [Citace: 16. 10 2023.] <https://phishing.eset.com/cs-cz/report>.
62. Zabránění phishingovým útokům a jejich nahlášení. *Google*. [Online] [Citace: 16. 10 2023.] <https://support.google.com/websearch/answer/106318?hl=cs#zippy=%2Cnahl%C3%A1%C5%A1en%C3%AD-phishingov%C3%BDch-web%C5%AF-na-internetu%2Cnahl%C3%A1%C5%A1en%C3%AD-phishingov%C3%BDch-str%C3%A1nek-kt%C3%A9-se-zobrazily-v-reklam%C3%A1ch-ve-vyhled%C3%A1v%C3%A1>.
63. PREVENT. *UKÁZKY E-LEARNINGOVÝCH KURZŮ*. [Online] [Citace: 11. 2 2024.] <https://www.preventonline.cz/demo/>.
64. Osvědčené postupy zabezpečení Microsoftu 365 pro firmy. *Microsoft*. [Online] [Citace: 11. 11 2023.] <https://learn.microsoft.com/cs-cz/microsoft-365/business-premium/secure-your-business-data?view=o365-worldwide>.
65. AUTOCONT. *Nová generace zabezpečení*. [Online] [Citace: 11. 11 2023.] <https://www.autocont.cz/aktuality/HP-Wolf-Security#>.
66. Můžu důvěřovat e-mailům od týmu účtu Microsoft? *Microsoft*. [Online] [Citace: 23. 12 2023.] <https://support.microsoft.com/cs-cz/account-billing/m%C5%AF%C5%BEu-d%C5%AFv%C4%9B%C5%99ovat-e-mail%C5%AFm-od-t%C3%BDmu-%C3%BA%C4%8Dtu-microsoft-685fd302-f52f-1a9f-cc13-065dec46fe25>.
67. ENISA. Introduction to Return on Security Investment. [Online] 12 2012. [Citace: 19. 2 2024.] <https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport>.
68. Microsoft. *Ochrana před útoky phishing*. [Online] <https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>.
69. Co je phishing? *AVAST*. [Online] [Citace: 15. 9 2023.] <https://www.avast.com/cs-cz/c-phishing>.
70. What exactly is phishing? *AVAST*. [Online] 5. 2 2020. [Citace: 28. 9 2023.] <https://www.avast.com/c-phishing>.

Seznam obrázků

Obrázek 1 - Souhlas se zasíláním newsletteru	17
Obrázek 2 - Souhlas se zasíláním novin, akcí a slev	17
Obrázek 3 - Skutečná webová adresa vs název organizace	20
Obrázek 4 - Ikona zámku	21
Obrázek 5 - Na co si dát pozor	21
Obrázek 6 - Ukázka e-mail phishingu	22
Obrázek 7 - Příklad BEC	23
Obrázek 8 - Příklad SEO	25
Obrázek 9 - Vícefaktorová autentizace	27
Obrázek 10 - Telemarketing podvod	28
Obrázek 11 - Příklad smishingu	29
Obrázek 12 - falešný FB profil	30
Obrázek 13 - Příklad BEC	31
Obrázek 14 – Ukázka podvodu s technickou podporou	33
Obrázek 15 - Ukázka Scareware	33
Obrázek 16 - Další příklad scarewaringu	34
Obrázek 17 - Příklad Malvertisingu	35
Obrázek 18 - Oficiální web Fio banky	37
Obrázek 19 - Ukázka podvodného webu Fio banky	37
Obrázek 20 - Příklad QR code phishingu	39
Obrázek 22 - Požadavek na ChatGPT	44
Obrázek 23 – Odpověď ChatGPT	44
Obrázek 24 - Obejití kontrolních mechanismů	45
Obrázek 25 - Jak může phishing vypadat	45
Obrázek 26 - Vylepšení phishingového e-mailu	46
Obrázek 27 - MS Defender rozcestník	56
Obrázek 28 - Ukázka mého e-mailu	57
Obrázek 29 - Zpráva oznámení phishingu	58
Obrázek 30 - Stáhnutí oznámení	58
Obrázek 31 - Jak nahlásit phishing	59
Obrázek 32 - Kde se nachází Procházet doplňky	59
Obrázek 33 - Doplněk Report Phishing	59

Obrázek 34 - Nahlášení phishingové webové stránky	60
Obrázek 35 - Nahlášení phishingové stránky Google	61
Obrázek 36 - Nahlášení reklam ve Vyhledání Google	61
Obrázek 37 - Ukázka školení 1	64
Obrázek 38 - Ukázka školení 2	64
Obrázek 39 - Ukázka školení 3	65
Obrázek 40 - Úryvek e-mailu ohledně Chat GPT	66
Obrázek 43- E-mail o bezpečnosti virtualizace	68
Obrázek 44 - Použitá neupravená šablona e-mailu	70
Obrázek 45 - Konečná phishingová kampaň	71
Obrázek 46 - Nezobrazené logo Microsoftu	71
Obrázek 47 - Změna hesla šablona	72
Obrázek 48 - Konečný návrh stránky pro změnu hesla	72
Obrázek 49 - Co se stane po kliknutí na pokračovat	73
Obrázek 50 - Identifikace phishingu	74
Obrázek 51 - Konfigurace MS Defender	74
Obrázek 53 - Edukace zaměstnanců 1	77
Obrázek 54 - Edukace ukázka phishingu	77

Seznam tabulek

Tabulka 1 - Náklady na návrh a realizaci kampaně	79
Tabulka 2 - Výpočet ROSI	80

Seznam grafů

Graf 1 - Výsledky kampaně	75
Graf 2 - Porovnání kampaní	75
Graf 3 - Ztráty vs. Náklady	81