

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 18: Informatika

**Kybernetická bezpečnost – techniky sociálního
inženýrství**

Cybersecurity – techniques of social engineering

Autoři: Vlastimil Pálfi

Škola: Střední průmyslová škola strojní a elektrotechnická a Vyšší
odborná škola, Liberec 1, Masarykova 3, příspěvková organizace;
Masarykova 3, 460 01 Liberec 1

Kraj: Liberecký kraj

Konzultant: Ing. Marek Pospíchal

Liberec 2022

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval/a samostatně a použil/a jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné.

Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Liberci dne 15. 3. 2022
Vlastimil Pálfi

Anotace

Práce se zabývá různými technikami sociálního inženýrství využívaných v oblasti kybernetické bezpečnosti. Bude obsahovat historii, metody, trendy sociálního inženýrství, a ochranou a prevencí před takovými útoky. Jedná se o praktický poklad pro školení zaměstnanců, ale i veřejnosti.

Klíčová slova

Kybernetická bezpečnost;

Sociální inženýrství;

Manipulace;

Annotation

This work deals with many different techniques of social engineering used in the field of cybersecurity. It's intended to familiarise employees, but also public to not only the history, methods and trends of social engineering, but also to protection and prevention against these attacks.

Keywords

Cybersecurity;

Social engineering;

Manipulation;

Obsah

Úvod.....	1
Sociální inženýrství.....	2
1 Historie.....	4
1.1 Trojská válka.....	4
1.2 Sociální inženýrství ze strany společenských věd.....	4
1.3 Popularizace sociálního inženýrství.....	5
1.3.1 Získání zdrojového kódu od firmy Motorola	5
2 Metodiky sociálního inženýrství	6
2.1 Phishing	6
2.1.1 Spear Phishing.....	6
2.1.2 Vishing (Voice Phishing)	7
2.1.3 Smishing (SMS Phishing)	8
2.2 Baiting.....	9
2.3 Pretexting.....	10
2.4 Tailgating.....	10
2.4.1 Piggybacking.....	11
2.5 Quid Pro Quo.....	12
2.6 Scareware.....	13
3 Trendy v dnešní době.....	15
3.1 Consent Phishing.....	15
3.2 SIM Swapping	16
3.3 BEC (Business Email Compromise)	18
3.4 Deepfake	19
3.5 Trh Phishing-as-a-Service.....	20
3.6 Útoky podporované státem.....	21
4 Nové komunikační platformy	23
4.1 Phishing na sociálních sítích	23

4.1.1	Clickbait Phishing.....	23
4.1.2	Podvodné Inzeráty na sociálních sítích	24
4.1.3	Ukradení identity	25
4.2	Láska na internetu aneb Catfishing.....	27
4.3	Kvízy.....	28
5	Stanovení organizačních pravidel pro školení zaměstnanců.....	30
5.1	GDPR	30
5.2	PDCA.....	30
6	Ochrana před kybernetickými útoky.....	32
6.1	Doporučené postupy ochrany před sociálním inženýrstvím	32
6.2	Příklady nesrovnalostí útoků	33
6.3	Dokážete rozpoznat phishingový útok od normální zprávy?	36
	Závěr.....	37
	Seznam zkratk a odborných výrazů.....	38
	Seznam obrázků.....	39
	Použité zdroje	41
A.	Seznam příložených souborů	I

Úvod

Při výběru zadání jsem přemýšlel nad vytvořením hry v Unity, jenže jsem neměl žádný konkrétní plán, co bych vytvářel a jestli bych to stihnul včas.

Tak jsem se rozhodl, že si vezmu zadání, které bylo nabízené našim učitelem, což bylo sociální inženýrství ze strany kybernetické bezpečnosti.

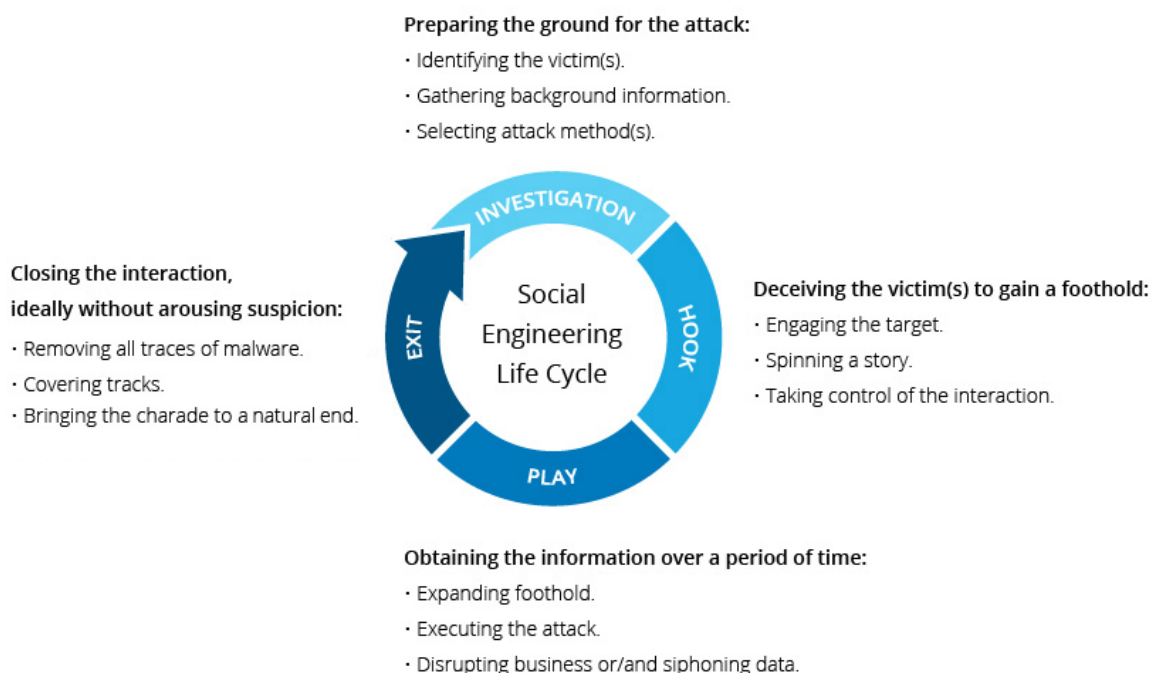
Vybral jsem si tuto práci, protože v dnešní době vzrůstá počet případů útoků, jejímž cílem (sociálních inženýrů) je napadnout hlavně jednotlivce firmy, společnosti, za účelem získat důležité informace, peníze, a/nebo způsobit spoušť. Nejenom, že lidé, hlavně postarší, ale i zaměstnanci nějaké firmy, nejsou zcela obeznámeni nebezpečím internetu, ale také vzrůstá přesvědčivost a technologie těchto útoků, které dokáží zmást i osobu se zkušenostmi identifikovat takové tzv. scamy.

Práce se tedy bude zabývat tím, jak se těmto podvodům vyhnout a bránit se jim, jaké metody a typy metod útočníci používají, ale také jaká je historie těchto útoků a zároveň jaké trendy útoků používají v dnešní době. Bude se jednat o praktický podklad pro školení zaměstnanců, ale i veřejnosti, kteří se pořádně s pojmem „sociální inženýrství“ ještě nesetkali.

Sociální inženýrství

Jedná se o manipulaci lidí k tomu, aby vykonali nějakou akci nebo prozradili určité tajné informace útočníkovi, které může poté použít k dostání se do vnitřku firmy, společnosti (např. přes přihlašovací údaje) pro získání peněz a/nebo více citlivých informací, vytvoření chaosu (např. v podobě malwaru), nebo pouze prodání těchto informací za nějakou peněžní částku.

Existuje zde mnoho útočníků, kteří chtějí oklamat svoji oběť, ale nesmíte se nechat zmást, sociální inženýři (někdy se jim říká „Bad Actors“) jdou po větších rybách, než jsou peníze jedné osoby nebo rozesílání špatně zkonstruovaných emailů, plánování jejich útoků míří většinou k velkým firmám. Jsou velice dobrými manipulátory, jež mají systematicky naplánováno, jak se daná osoba zachová. Využívají lidské psychologie a sociálních technik a metod, aby se dostali ke svému cíli.



Obrázek 1: Průběh sociálního inženýrství (1)

Člověk nemusí ihned poznat, že se jedná o sociální inženýrství, to je ta pointa, osoba je rovnou v momentu dění. Motiv útočníka nemusí být přímo jasný, protože často jde po více než jedné věci.

Někteří sociální inženýři se precizně připravují týdny, dokonce měsíce, než se jejich útok uskuteční. Jejich plán spočívá ve vybrání osoby, nebo několika osob, které pracují v dané firmě. Zjistí si o nich různé cenné informace (dají se dohledat na internetu, nejčastěji na sociálních sítích => dávat si pozor, co na nich zveřejňovat), které dovolí útočnickovi vymyslet falešný příběh, nebo vytvořit uvěřitelnou situaci, jenž mu může dovolit získání potřebných informací k napadnutí firmy.

1 Historie

Dnes už známe, co je sociální inženýrství, ale dříve to tak přesně definované nebylo. Během historie lidstva ještě před vzestupem počítačů se objevilo mnoho příkladů sociálního inženýrství, ale samotný pojem dnešní definice byl poprvé použit až ke konci 2. pol. 20. stol.

Nejdříve bych chtěl krátce představit aspoň jeden příklad z historie pro lepší porozumění tematiky.

1.1 Trojská válka

Z Homérových eposů Ilias a Odysseia, přesněji z díla Ilias, se dozvídáme o desetileté válce mezi městem Trójou a Řeky. Pro nás je důležitý trojský kůň, jenž byl předán městu Trója jako forma vzdání se a dar, ale ve své podstatě se jednalo o past, protože se v něm skrývali Řekové, kteří v noci z koně vyšli a tajně vybili Tróju zevnitř.

Kůň představuje sociálního inženýra, jenž se ze zevnějšku tváří nevinně, ale jeho vnitřním cílem je získat něco, co ta druhá skupina střeží (důležité informace, peníze atd).

Tohle je jeden z příkladů sociálního inženýrství ještě před našim letopočtem, ale kdy se tedy poprvé použil jeho pojem?

1.2 Sociální inženýrství ze strany společenských věd

V roce 1894 byl pojem použit J. C. Van Markenem v jeho eseji, kde vyjadřuje, že moderní zaměstnavatelé potřebují pomoc specialistů při řešení jak lidských problémů, tak i problémů technických (materiály, stroje, procesy).

Tento pojem se dostal i do Ameriky pod stejným významem v roce 1899. V tom samém roce se objevil časopis s názvem „Sociální inženýrství“ a v roce 1909 to byl také název knihy bývalého redaktora časopisu Williama H. Tolmana. Tady se jedná o konec významu, který vytvořil sám Van Marken. Nový význam slova nastolil Edwin L. Earp ve své knize „The Social Engineer“, která byla vydána v roce 1911 v USA za doby „výkonového šílenství“, jenž známe dodnes.

1.3 Popularizace sociálního inženýrství

I když tento nápad a jeho techniky byly s námi už od počátku lidstva, jeho popularizace nastala až při vzestupu počítačů, přesněji řečeno v 90. letech 20. století hackerem (dnes bezpečnostním konzultantem, autorem odborných knih) Kevinem Mitnickem.

Během této doby byl mezi nejhledanějšími kyberzločinci v zemi. Mezi jeho nejsilnější stránky nebyly přímo znalosti o IT, ale spíše manipulace lidí, aby mu dali citlivé informace např. z firmy => sociální inženýrství. Mezi jeho zločiny patřila nabourání se do systémů firem Motorola, Nokia, Sun Microsystems, Fujitsu Siemens, dále společností jako je Apple, organizace FBI atd.

Mohli bychom si jeden ze příkladů detailněji uvést.

1.3.1 Získání zdrojového kódu od firmy Motorola

V roce 1992 si dal za cíl, že zavolá a zmanipuluje firmu Motorola, aby mu dala zdrojový kód ke v té době revolučnímu telefonu MicroTAC Ultra Lite. S tímto kódem by telefon dokázal modifikovat tak, že by zůstal v anonymitě před úřady.

Kevina Mitnicka si při volání lidé z firmy několikrát přehazovali, během té doby zjistil jednu kritickou informaci, že Motorola má výzkumné centrum v Arlington Heights. Takže v dalším volání se představil jako zaměstnanec tohoto centra (tzv. pretexting => vydává se za někoho s autoritou, aby se mohl dostat blíže ke svému cíli) a znova si vyžádal mluvit s projektovým manažerem. Dostal „rozšíření“ k projektové manažerce jménem Pam, jen aby zjistil, že je na dovolené. Zanechal na hlasové poště kontakt, koho jiného má zavolat, pokud je pryč. Kevin zavolal na kontakt, Aleeshu, a zeptal se, jestli je Pam pořád na dovolené, aby jeho příběh zněl více uvěřitelně. Potom Aleeshe řekl, že Pam mu slíbila, že mu pošle ten zdrojový kód, ale pokud by to nějak nestihla, má to poslat ona. Aleesha tomu uvěřila a Kevin s menšími komplikacemi ten kód získal.

I když s tím nic dále neudělal, mohl klidně firmu s kódem vydírat, nebo ho prodat za velkou částku peněz.

2 Metodiky sociálního inženýrství

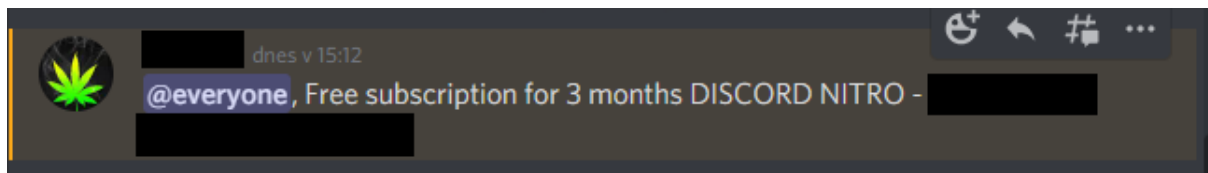
Jednou už bylo zmíněno, že útočník během provádění svých útoků (ale i v jejich plánování) použije různé metody, které mu pomůžou k dosažení jeho cíle.

Existují už více sofistikované metody, než byl ze začátku nigerijský princ (metoda, kdy ti „princ“ chce poslat své bohatství, ale potřebuje vaše osobní informace pro poslání), který dnes už je ohraný.

Metod sociálního inženýrství existuje mnoho, některé zahrnují malware, nebo se mohou dokonce lišit v mnoha variacích a kombinacích, ale je důležité, abychom si nějaké uvedli společně s příklady z reálného světa pro lepší pochopení tématu.

2.1 Phishing

Jedna z nejpobulárnější metod, kde útočník posílá emaily nebo textové zprávy, jenž mají za úkol vyvolat naléhavost, zvědavost, nebo strach u nic netušících lidí. Pobízí je to k otevření buď nějakého odkazu k důvěryhodně vypadající stránce, kde zadají své citlivé informace, nebo otevření přílohy s virem (malwarem).



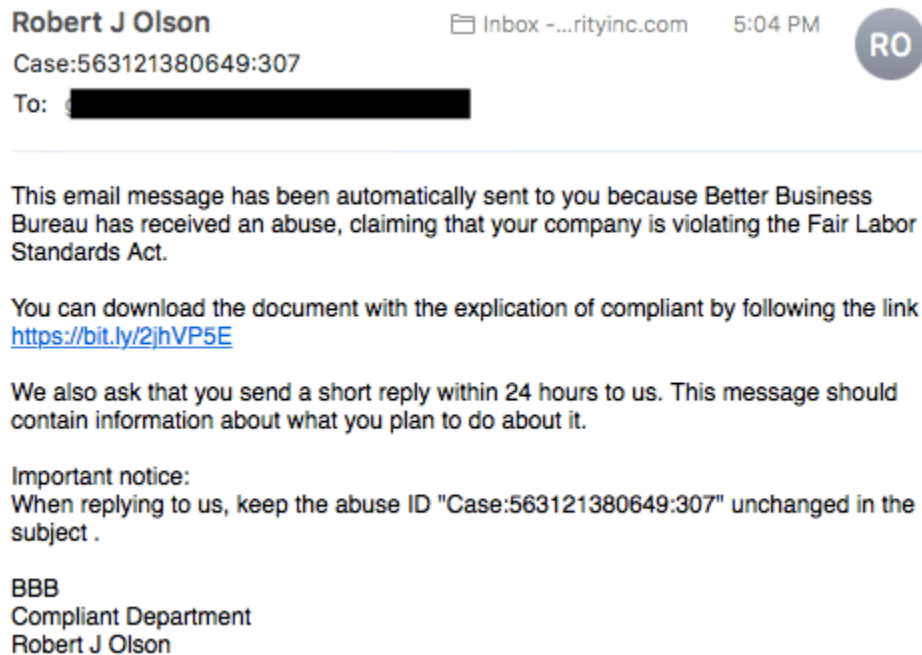
Obrázek 2: Speciální příklad amatérského phishingu (přesněji řečeno smishingu), který se nedávno udal na platformě Discord. Někdo ukradnul účet uživatele na serveru, účet poté použil jako „robota“, který všude automaticky přeposílal podvod na Discord Nitro (předplatné pro tuhle platformu s výhodami)

Tento typ phishingu se většinou dá dost dobře poznat, jsou (téměř) identické a posílají se ve většinou mnoha uživatelům. Jsou až generické, takže ne každý člověk se nachytá. Jedná se vlastně o amatérský kousek, kdy ne moc zkušený sociální inženýr se snaží ulovit spoustu malých rybek bez možné cesty k velkým rybám, proto se to nazývá phishing => fishing (rybaření).

2.1.1 Spear Phishing

Mnohem profesionálnější a více cílený typ phishingu. Sociální inženýr si vše plánuje, vyhledává informace a připravuje si příběh pro individuální osobu či vybranou skupinu uživatelů z nějakého velkého podniku, aby se dokázal plně přizpůsobit jejich chování a

udělal správné kroky pro získání přístupu k podniku, a zároveň aby to vypadalo co nejnenápadněji => chycení co největší ryby (pomocí kopí) => proto spear phishing.



Obrázek 3: Příklad Spear Phishingu (2)

Tento typ útoku vyžaduje více práce, příprava může trvat i několik týdnů až měsíců, než samotný plán začne. Jsou mnohem těžší k detekci a mají mnohem větší šanci na úspěch, pokud jsou správně provedeny.

2.1.2 Vishing (Voice Phishing)

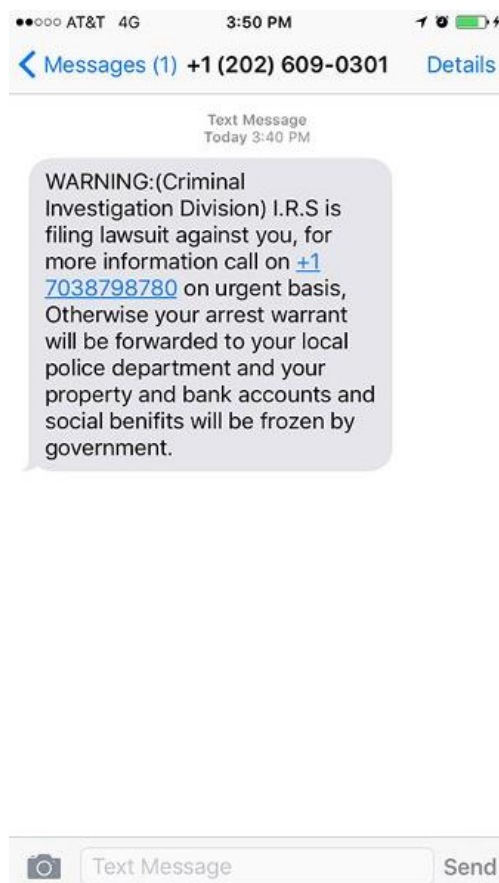
Další typ phishingu, který se odehrává přes telefon. Může to být samotný útočník, který volá pod nějakou identitou a používá přátelský hlas, nebo použije tzv. interaktivní hlasový odpovědní systém (IVR) pro reakci volaného (například banky a další instituce s IVR systémem), anebo jednoduše zanechá v hlasové schránce vzkaz s požadavkem na zpětné zavolání. Tím zvýší potřebu volaného zavolat zpět.



Obrázek 4: Příklad Vishingu, útočník se může vydávat za banku a vyžadovat peníze (3)

2.1.3 Smishing (SMS Phishing)

Je to jakýkoliv phishing zahrnující textové zprávy (SMS). Je větší šance, že uživatel bude věřit manipulativní textové zprávě přes mobilní telefon než přes email. Účelem těchto zpráv je získat soukromé osobní a firemní informace od lidí. Může to být zpráva o zaplacení něčeho, co uživatel nezaplatil, s připojeným falešným odkazem. Chtějí, aby se uživatel zapojil do konverzace.



Obrázek 5: Příklad Smishingu, v téhle zprávě jsou velmi agresivní a pospíchají na uživatele, aby provedl akci (4)

2.2 Baiting

Už z významu slova Baiting (neboli vnaďení/lákání) je zřejmé, že účelem této metody je nalákat uživatele do pasti ve formě „falešného slibu“. Buď virtuálně, jako např. příloha z emailu s lákavým názvem, obrázkem inzerátu, nebo fyzicky, že někde leží nějaké CD/DVD nebo USB infikovaný malwarem na místě, kde ho člověk s velkou pravděpodobností najde.

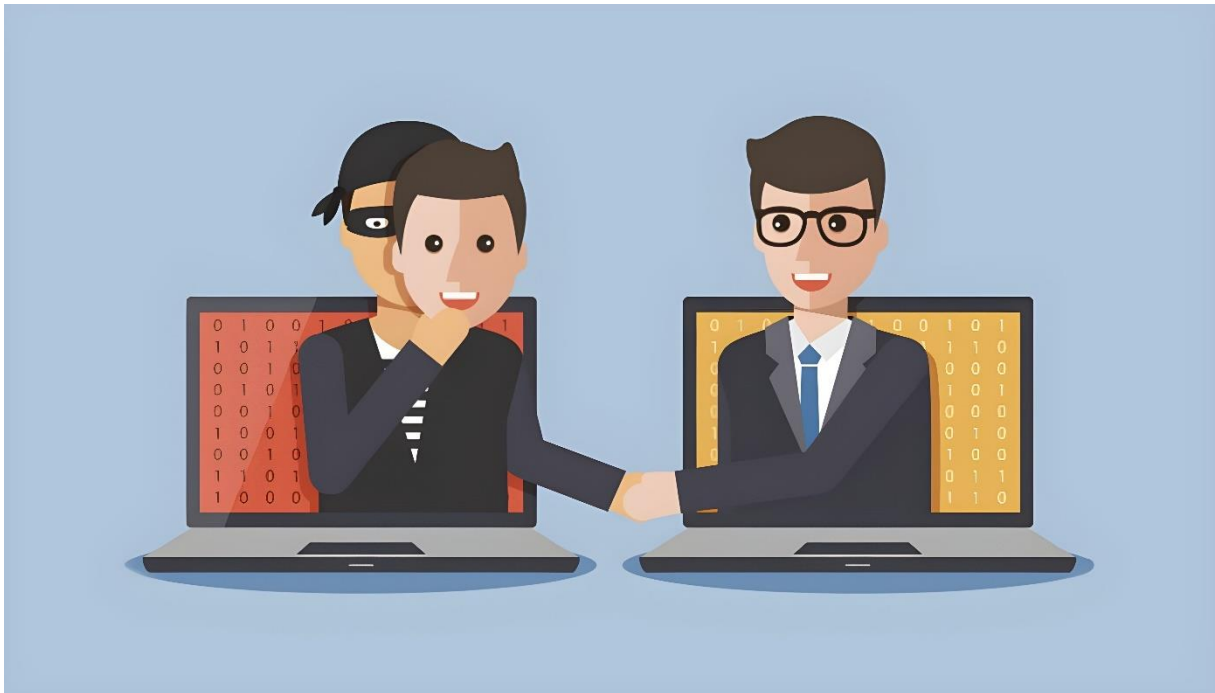


Obrázek 6: Příklad Baitingu (5)

Nechá se na uživateli, jestli sám ze zvědavosti na to neklikne či nepřipojí paměť ke svému nebo pracovnímu počítači.

2.3 Pretexting

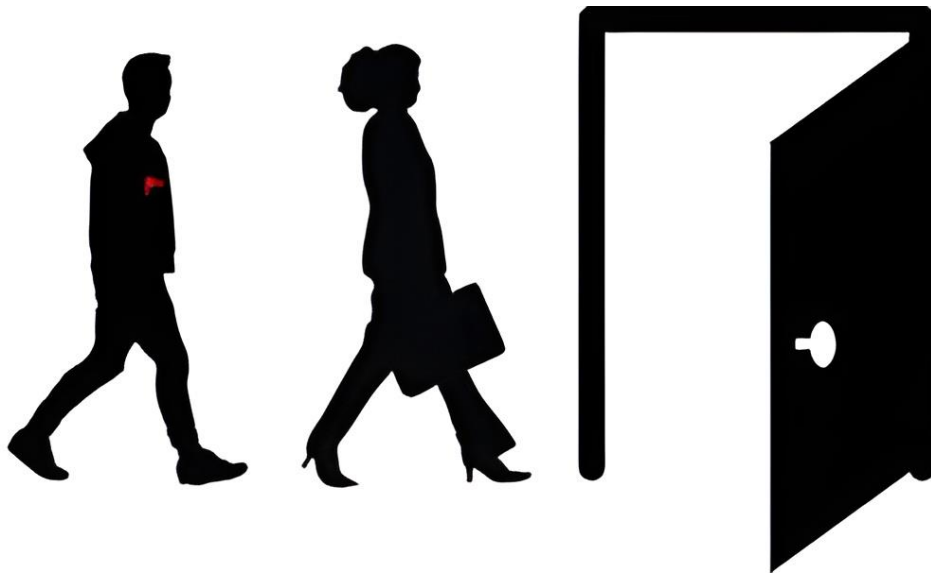
Každý útok má svůj tzv. pretext => vytvoření si nějakého příběhu, vydávání se za někoho s autoritou v průběhu útoku. Příběh je vymyšlený na základě útočnickových výzkumů o osobě nebo firmě, aby je dokázal přesvědčit o své důvěryhodnosti.



Obrázek 7: Příklad Pretextu (6)

2.4 Tailgating

Jedná se o metodu, kdy se útočník snaží o fyzický přístup do zabezpečeného prostoru v nějakém pretextu (jako zaměstnanec firmy, dodavatel), jenž těsně následuje autorizované zaměstnance firmy.



Obrázek 8: Příklad Tailgatingu (7)

Příkladem může být následováním zaměstnance do zabezpečeného prostoru a projití otevřenými dveřmi (bez jejich souhlasu/nevěděli o něm).

2.4.1 Piggybacking

Skoro to samé jako tailgating, ale autorizovaný zaměstnanec si je vědom a dovolí útočnickovi (buď přesvědčen útočníkem, projevuje laskavost, nebo vědomě napomáhá) se dostat do míst, kam má bad actor namířeno. Může si například myslet, že se jedná o zaměstnance, který si zapomněl svoji např. identifikační kartu pro vstup do zabezpečeného prostoru.

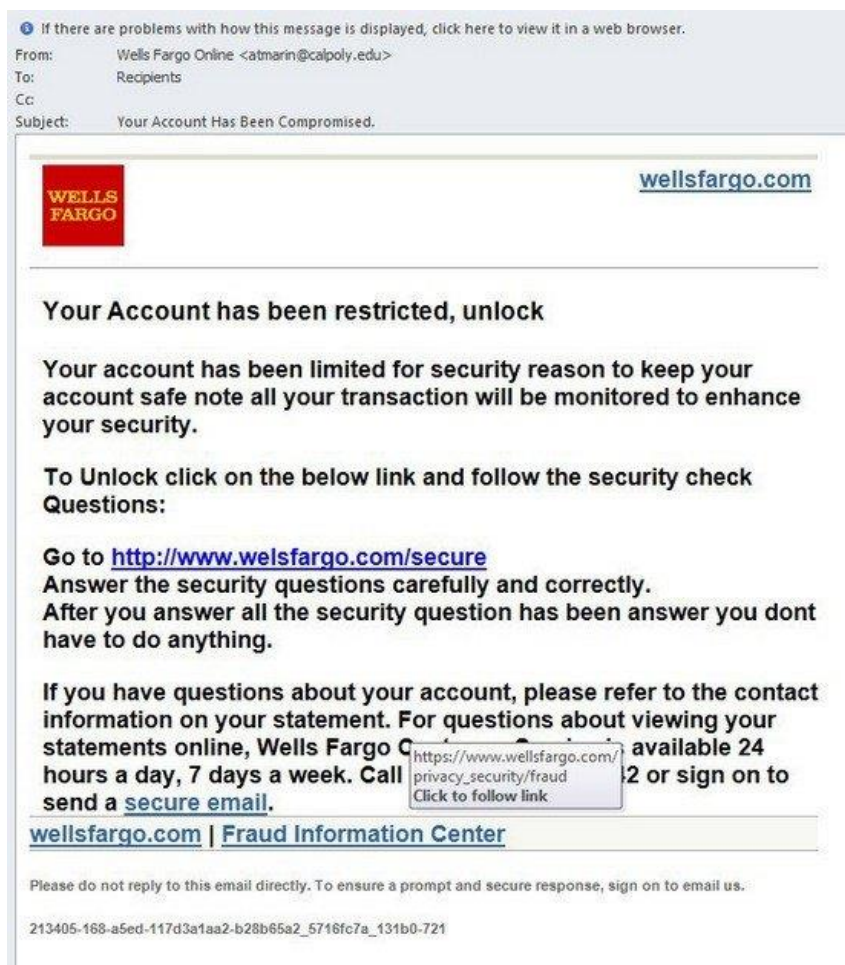


Obrázek 9: Příklad Piggybackingu (8)

Dalším klasickým příkladem bývá dodavatel s plnými rukami (např. nese krabice) za účelem, aby zaměstnanec projevil laskavost a podržel dveře útočníkovi.

2.5 Quid Pro Quo

Z latiny „Něco za něco“ je taktika sociálního inženýra požadující výměnu citlivých údajů za službu. Jeden z příkladů může být pretext inženýra z IT servisu, kde přesvědčí uživatele, že jim vyřeší problém za použití jejich přihlašovacích údajů.



Obrázek 10: Příklad metody Quid Pro Quo (5)

2.6 Scareware

Forma malwaru, jenž má vystrašit lidi (například, že jejich počítač byl infikovaný virem) a přimět je k navštívení infikovaných stránek, zavolání na mobilní číslo, nebo stáhnutí nástroje pro opravu „problému“ => falešný antivirus. Bývá ve formě klamné pop-up reklamy na webových stránkách, která vyskočí na uživatele PC.



Obrázek 11: Příklad scarewaru (9)

Většinou se jedná pouze o vystrašení, tedy vir sám o sobě je fiktivní, dokud neprovedeme akci, kterou od nás očekávají.

Cíl téhle metody se může lišit od prodávání nepotřebných služeb až po instalaci falešných nástrojů, které mohou být jenom malware odhalující citlivá data. Scareware je často spojován s pojmem Ransomware, což je typ malwaru, který zablokuje celý počítač a drží data uživatele jako rukojmí. Útočník pak vyžaduje peníze po uživateli (ne vždy však útočník data po zaplacení vrátí).

3 Trendy v dnešní době

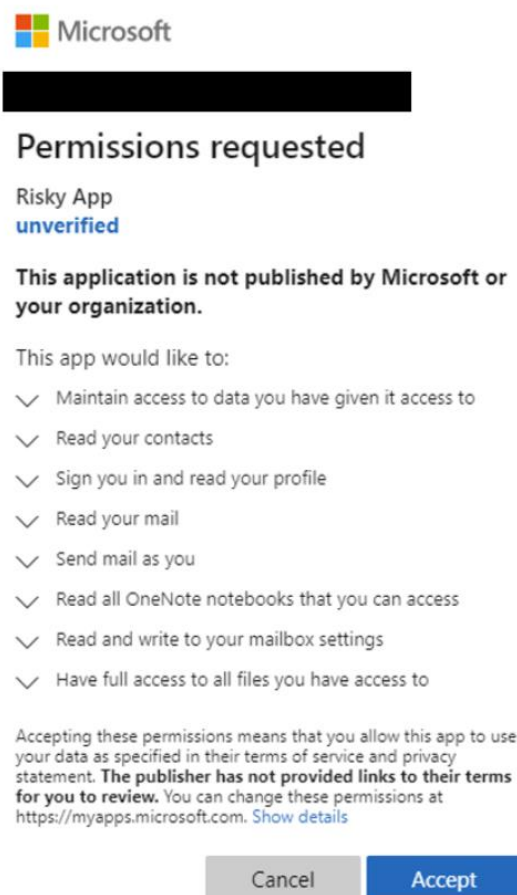
I přes seznámení se s dnešními metodami sociálního inženýrství nelze zaručit, že budou vylistovány všechny. Existuje jich spousta, existující se neustále vyvíjejí a nové přibývají každým dnem. Hlavně od března 2020 až na nový rok 2022 se potýkáme s pandemií Covid-19, kdy každý z nás zažil lockdown, popř. karanténu a homeoffice. Tohoto momentu využili sociální inženýři, kdy využívají stálé metody, které fungují na dálku (což je většina), nebo je dále vyvíjejí, popř. vymýšlejí kompletně nové techniky.

Během této doby vzrostla popularita sociálního inženýrství kvůli jeho závislosti na propojení s lidmi v online prostoru. Tím pádem vzniklo několik trendů, o kterých si teď popovídáme.

3.1 Consent Phishing

Mnoho businessmanů si uvědomilo dobrou možnost pracovat v domovském prostředí, tedy distančně. Firmy se proto přesouvají ke cloudovému úložišti, uložení práce na vzdálený server.

Bad Actors přicházejí s geniální nápadem, novou technikou nazývanou se Consent Phishing. Je to speciální typ phishingu, jenž zahrnuje aplikaci vytvořenou útočníkem, která požaduje souhlas od uživatele (místo toho, aby se ptali na heslo), aby aplikace měla přístup ke cloudovému úložišti. Bývají to nějaké addony či rozšíření pro legitimní aplikaci (např. Office 365).



Obrázek 12: Příklad Consent Phishingu (10)

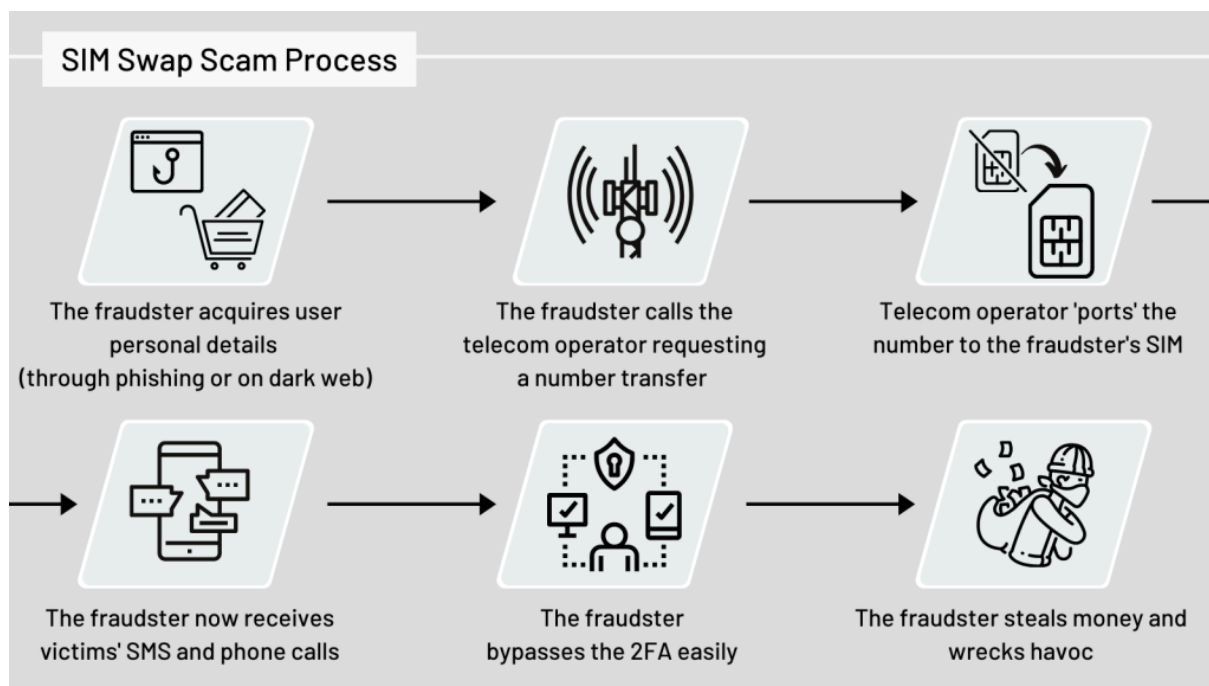
Tato technika také vznikla kvůli autorizační technologii OAuth 2.0 používaná mnoha obrovskými firmami, např. Google, Microsoft, Facebook atd. Kvůli této metodě nebezpečné aplikace dokážou spustit skript mimo uživatelský počítač, tímto způsobem obejdou další zabezpečení (koncových bodů).

Jedním příkladem by mohl být v celku nedávný útok na SANS Institute, kde jeden ze zaměstnanců si stáhl addon do Office 365. Jeho účet byl přeposlán útočníkovi, který se následně naboural do dalších 28000 záznamů.

3.2 SIM Swapping

Pojednáváme o další zpopularizované technice, kdy útočník převezme kontrolu nad mobilním číslem legitimního uživatele. Útočník si zjistí informace o uživateli a vytvoří si pretext pro zmanipulování telefonního poskytovatele, aby mu přehodil telefonní číslo na jinou SIM kartu v jeho rukou. Bad actor dostane kompletní přístup ke všem účtům,

kontaktům a zprávám, protože když někdo získá vlastnictví telefonního čísla, dovolí mu to kompletně přeskočit jakoukoliv SMS formu dvoufázové autentizace, jenž používá mnoho online služeb.



Obrázek 13: Vysvětlení, jak vlastně SIM Swapping funguje (11)

Jeden z příkladů, kdy se použil tento typ útoku, je na sociálních sítích, přesněji řečeno na Twitteru. Účet výkonného ředitele Twitteru Jacka Dorseyse byl napadnut touto metodou.

Dokonce Google donutil přes 150 miliónů uživatelů Googlovských služeb použít 2FA pro lepší zabezpečení účtu (pouze jen ty účty, které byly „nastaveny“ => mají přidružené telefonní číslo, druhou emailovou adresu, nebo mobilní telefon, aby dostávali push notifikace) => zvýšená šance použití této metody.

Dá se tomu napřímo bránit nastavením si na účet PIN, kdokoliv volá, musí vědět PIN pro provedení změn. Nedoporučuje se posílat SMS zprávy s kódem, kvůli vlastnostem tohoto útoku a phishingu jako takového, doporučují se proto push notifikace. Dále se doporučuje použití lepší 2FA, například Google Authenticator, který propojí autentizaci pomocí mobilního telefonu, nikoli pouze mobilního telefonního čísla => Bad Actor by se musel zmocnit telefonu fyzicky.

3.3 BEC (Business Email Compromise)

Technika, kdy se útočník vydává za důvěryhodný obchodní kontakt. Pod tímhle pretextem (např. někdo uvnitř organizace, prodejce hardwaru) se útočník snaží přesvědčit vybrané společnosti/firmy k zaplacení faktur, bankovnímu převodu peněz atd.

Průměrná cena tohoto útoku se odhaduje okolo 80 000 dolarů, toto číslo se nadále zvyšuje každým rokem a je čím dál tím dražší pro firmy. Jedná se pouze o jediný útok na jednu organizaci. Během roku 2022 bylo ukradeno organizacím přibližně 1,8 miliardy dolarů.

Například v roce 2019 litevský útočník, vydávající se za prodejce hardwaru, přesvědčil Google a Facebook, aby mu převedli 123 miliónů dolarů na jeho bankovní účty (měl firmu s podobným jménem Quanta, která s těmito firmami spolupracuje).

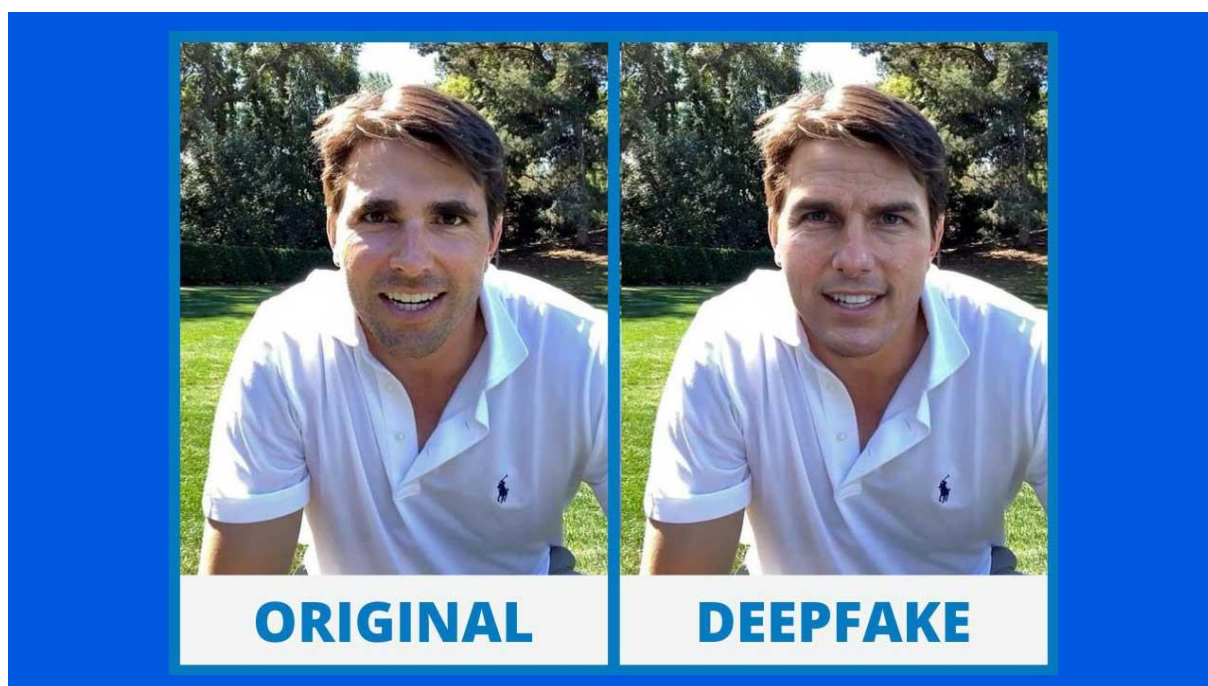
By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,866,642,107	Overpayment	\$51,039,922
Confidence Fraud/Romance	\$600,249,821	Ransomware	**\$29,157,405
Investment	\$336,469,000	Health Care Related	\$29,042,515
Non-Payment/Non-Delivery	\$265,011,249	Civil Matter	\$24,915,958
Identity Theft	\$219,484,699	Misrepresentation	\$19,707,242
Spoofing	\$216,513,728	Malware/Scareware/Virus	\$6,904,054
Real Estate/Rental	\$213,196,082	Harassment/Threats Violence	\$6,547,449
Personal Data Breach	\$194,473,055	IPR/Copyright/Counterfeit	\$5,910,617
Tech Support	\$146,477,709	Charity	\$4,428,766
Credit Card Fraud	\$129,820,792	Gambling	\$3,961,508
Corporate Data Breach	\$128,916,648	Re-shipping	\$3,095,265
Government Impersonation	\$109,938,030	Crimes Against Children	\$660,044
Other	\$101,523,082	Denial of Service/TDoS	\$512,127
Advanced Fee	\$83,215,405	Hactivist	\$50
Extortion	\$70,935,939	Terrorism	\$0
Employment	\$62,314,015		
Lottery/Sweepstakes/Inheritance	\$61,111,319		
Phishing/Vishing/Smishing/Pharming	\$54,241,075		

Obrázek 14: Přehled statistik ztrát z roku 2020 zveřejněno FBI, BEC představoval 37% všech ztrát (12)

FBI často připomíná firmám, jaká neuvěřitelná ztráta peněz BEC je. Označují tuto metodu jako jednu z nejškodlivějších online zločinů.

3.4 Deepfake

Deepfake je téměř nová a stále rozvíjející se technologie, syntetické médium, kdy osoba v existujícím obrázku nebo videu je nahrazena obličejem jiným, tedy vytvoření přesvědčivých obrázků, dokonce i audia za pomoci umělé inteligence. Laik si může myslet, že to půjde lehce poznat, upozorovat nedokonalosti obrázku/videa a zjistit, jestli to je „fake“ nebo pravé. Jenže technologie se posunula natolik, že to nelze ihned poznat, obličeje ve videích umějí téměř perfektně mimikovat pohyb rtů, obecně pohyb tváře atp.



Obrázek 15: Příklad použití technologie Deepfaku (13)



Tento typ technologie mohou sociální inženýři využít ke zničení důvěryhodnosti informací, vydávání se za důvěryhodné zdroje anebo manipulaci informací obecně. Mohou je vytvořit za účelem popuzení lidí mezi sebou, dokonce i států.

Sami sociální inženýři mohou využít tuto technologii ve svůj prospěch, pro např. vytváření falešných zpráv pro neexistující či podvodnickou firmu, vydávání se za celebrity/politika odkazujícího na stránku, která má za účel ukrást data/peníze atd.

Experti označili tuto technologii jako jedno z nejvíce znepokojujících použití umělé inteligence, která by mohla mít velký dopad na kyberkriminalitu a terorismus.

3.5 Trh Phishing-as-a-Service

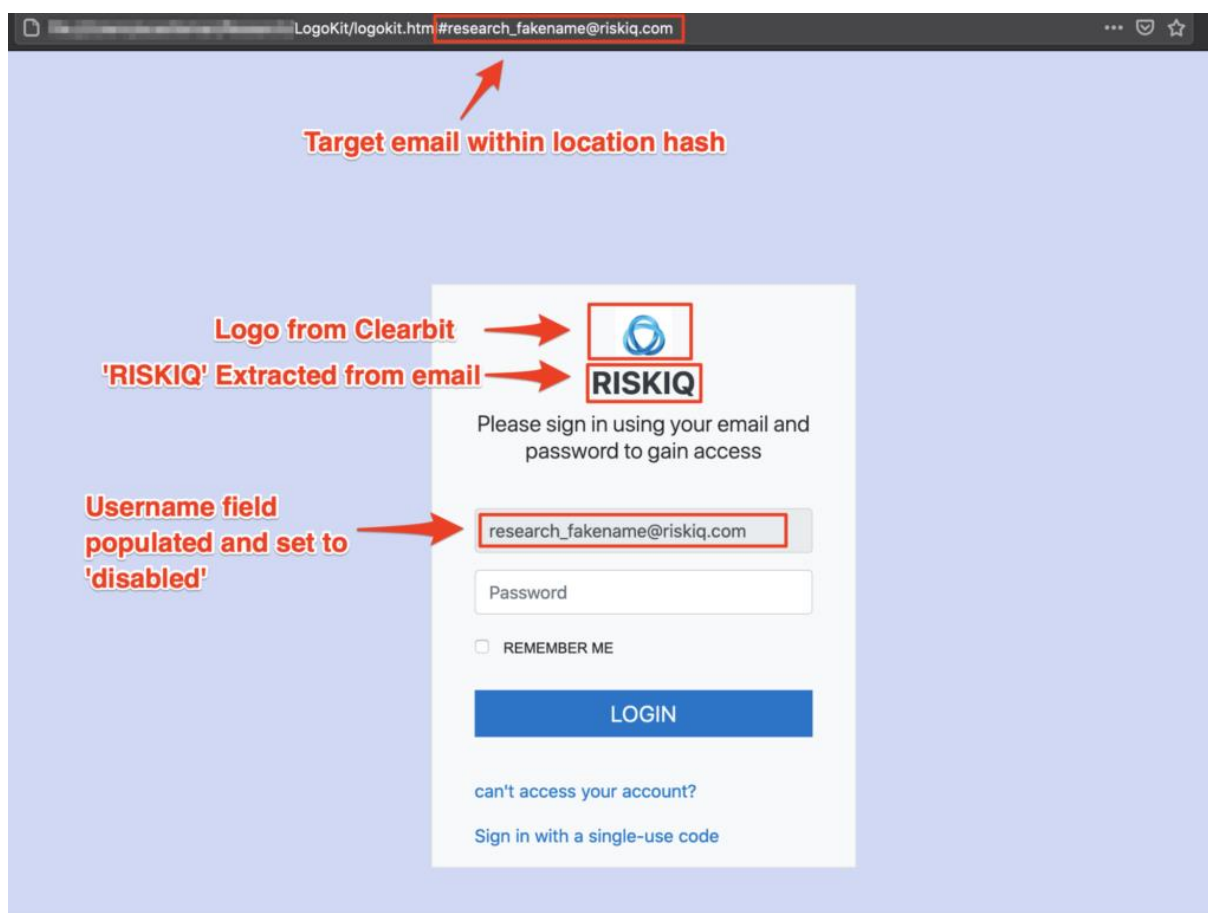
Jako Software-as-a-Service (SaaS), jedná se o model, kdy uživatelé dostanou přístup ke službě přes internet (v tomto případě k informacím související se softwarem) za měsíční či roční předplatné. Jenže na rozdíl od SaaS, Phishing-as-a-Service (PhaaS) dává přístup ke znalostem a nástrojům, jež jsou prodávány zkušenými kyberzločinci jako služba na černém trhu.

	 Phishing kits	 Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based <i>(Available weekly, bi-weekly, monthly, or annual)</i>
Email templates	✓	✓ <i>(Optional)</i>
Site templates	✓	✓
Email delivery		✓ <i>(Optional)</i>
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
"Fully undetected" links/logs		✓

Obrázek 16: Rozdíly mezi phishing kitem a PhaaS (14)

Popularita Phishing-as-a-Service (PhaaS) vzrůstá, dnes je laťka pro vstup do kyberkriminality razantně nižší než předtím. Dají se zakoupit phishing nástroje/balíčky (většinou v ZIP souboru), které zahrnují např. vytvoření emailového útoku, databázi „terčových“ uživatelů, šablony pro emaily známých značek atp. Předplatit tyto služby se dá za nízkou cenu 50 dolarů měsíčně. Cena mnoha těchto nástrojů se více než zdvojnásobila kvůli vysoké poptávce.

Na začátku roku 2021 se objevil nástroj jmenující se Logokit, který umí postavit phishing stránky v reálném čase (bylo detekováno více než 700 domén).



Obrázek 17: Příklad implementace LogoKit phishing kitu (15)

3.6 Útoky podporované státem

Už z názvu je patrné, že existují útočníci, kteří jsou přímo zaměstnáni v armádě a vládních orgánech státu. Útočníci, kteří jsou na ten útok sami, je jejich hlavním cílem finanční zisk a musí se skrývat před státem. Útočníci placení státem se nemusí bát jakéhokoliv postihu. Tito lidé jsou nepřímo placeni státem (=> je lehčí odepřít, že daný stát měl s útokem něco společného), mají mnohem větší volnost, více možností, jak s útokem vynaložit.

V roce 2020 Twitter čelil koordinovanému útoku, který dovolil těmto státem podporovaným útočnickům převzít kontrolu nad obrovskými Twitter účty (Elon Musk, Jeff Bezos, Barack Obama, atd.), které odesílaly příspěvky na transakce kryptoměn, přesněji řečeno Bitcoin.



Obrázek 18: Jeden příspěvek na Twitteru poslaný hackerem přes účet Baracka Obamy (16)

Je řečeno, že skupina útočníků cílila sociální inženýrství na zaměstnance Twitteru => dostali dostatečnou administraci posílat příspěvky přes velké osoby.

Google skupina pro analýzu hrozeb dokonce identifikovala hackery ze Severní Koreje pod pretextem blogerů kybernetické bezpečnosti, jež cílili bezpečnostní výzkumníky na stránce LinkedIn a Twitteru.

4 Nové komunikační platformy

V této době každý z nás využívá komunikační platformy, ať se už jedná o sociální sítě, instant messaging aplikace atp. Jde vlastně o jakoukoliv platformu či aplikaci, přes kterou se dá spojit s jednou nebo více osobami přes celý svět.

Toho právě využívají sociální inženýři. Podvody na sociálních platformách se stávají čím dál tím více populárními. Důvodem je nadměrné zveřejňování a sdělování osobních informací, které útočník může využít proti danému uživateli (např. pro rychlé vybudování důvěry). Zrovna tito uživatelé, i když si to moc neuvědomují, jsou největšími oběťmi těchto útoků.

Podvodníků na sociálních sítích existuje mnoho a pokud si nebudeme dávat pozor, může to poškodit nejen nás, ale i naše blízké či firmu. Způsobů, jak provést podvod, existuje nespočet, proto bych chtěl uvést pár nejrozšířenějších technik sociálních inženýrů týkajících se sociálních sítí.

4.1 Phishing na sociálních sítích

Pojem phishing jsme si už vysvětlovali v předchozích kapitolách a jeho význam se i v tomto směru nezměnil. Za změnu můžeme považovat pouze prostředí, ve kterém se phishing vyskytuje, ale i tak je to dost obecné. Útoky se mohou lišit podle použité komunikační platformy a ve které z aplikací se útok nachází.

4.1.1 Clickbait Phishing

Jedná se o jakýkoliv příspěvek, falešnou reklamu na Facebooku, Instagramu nebo Twitteru, či velice krátká videa na těchto platformách s poutavým, šokujícím názvem, často s obrázkem, který chce po uživateli, aby kliknul.



Obrázek 19: Příklad Clickbait phishingu (17)

Narozdíl od metody Baitingu se tato metoda snaží navnadit nejenom jednoho člověka, ale celou škálu lidí. Tato technika by se dala navýšit nabouráním se do účtu s velkým sledováním, nebo působit jako někdo známý, např. účet bulvárního média, které zrovna sdílí poslední šokující článek.

4.1.2 Podvodné Inzeráty na sociálních sítích

Skoro to samé jako Clickbait phishing, ale jedná se o reklamy automaticky generované (v dnešní době zakomponované do listu příspěvků, kdy každý 4. – 6. příspěvek je reklama, nebo mimo příspěvek na levé nebo pravé straně obrazovky, v chat aplikaci jako zpráva atd.) na základě našich osobních informací o nás.

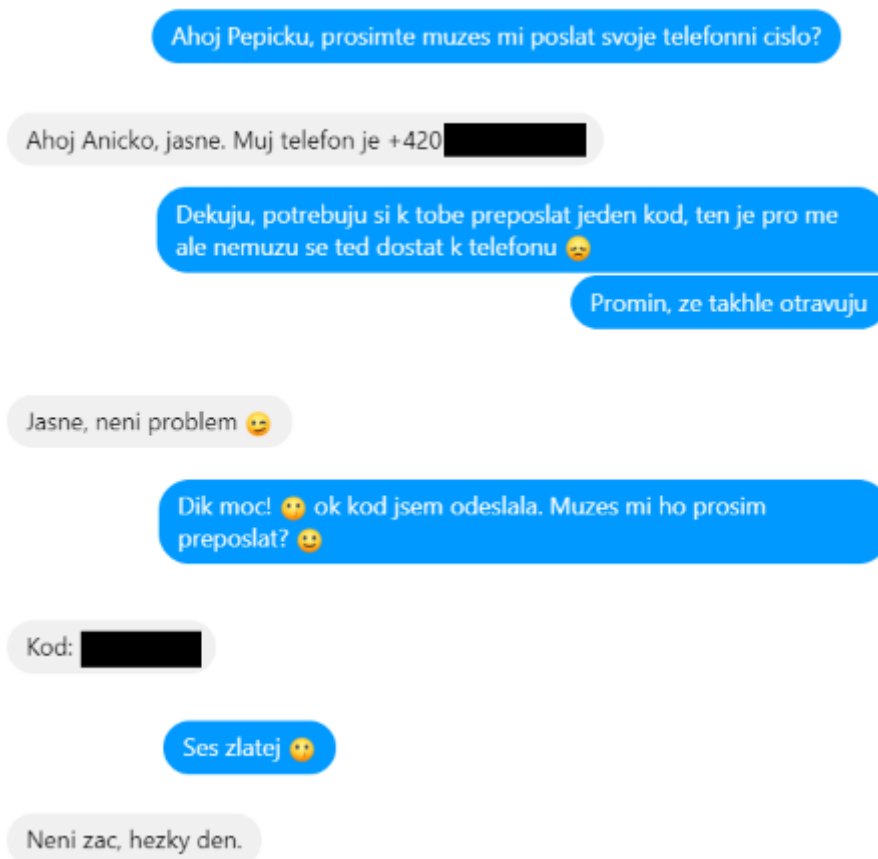


Obrázek 20: Modelový příklad podvodných inzerátů na soc. sítích (18)

Sociální inženýři mohou působit jako známá značka, jakási žhavá novinka, kterou všichni potřebují, nebo inzerát na COVID-19 očkování, které byly velice efektivní před vyvinutím prvních dávek.

4.1.3 Ukradení identity

Pojednáváme o útočnickovi, který si na základě informací o dané osobě vytvoří profil identický jejího profilu nebo profilu příbuzného té osoby. Poté uživatel je kontaktován účtem „příbuzného“, který na první pohled vypadá, že to je on (uživatel by si mohl usmyslet, že „příbuzný“ má nový účet, nebo si ho omylem smazal z přátel, může se stát cokoliv). Při psaní v chatovací aplikaci se snaží získat důvěru uživatele k poslání důležitých informací. Bud', aby klikl na neznámý odkaz, stáhl malware, nebo za pomoci m-platby, který stále je populárním podvodem v ČR, kdy podvodník žádá o přeposlání kódu.

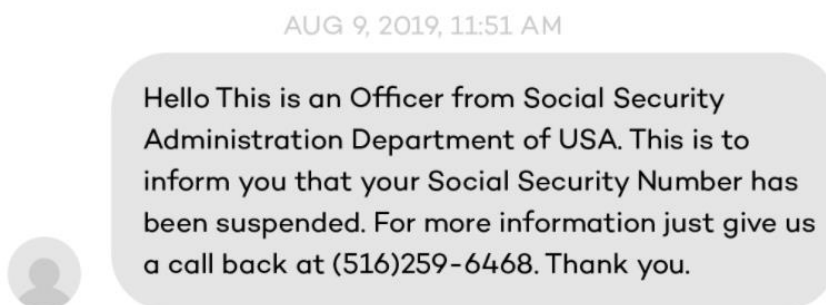


Obrázek 21: Příklad podvodu s m-platbou (19)

Ukradení identity se nemusí přímo týkat příbuzných, může do toho zapadat i pretext nějaké zdravotní péče, nějaké neznámé osoby, která se zeptá, jestli jste tohle vy (tedy odkaz na falešnou stránku). Může se jednat o jakoukoliv zprávu přes insta-messaging aplikace.

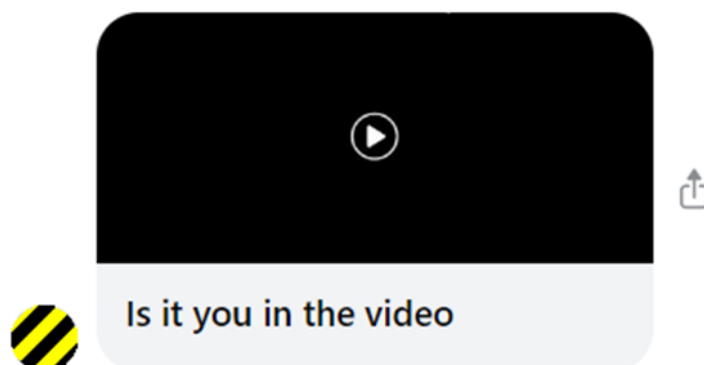
Pro příklad tyto „metody“ se nazývají:

1. Healthcare scam (podvod o zdravotní péči)



Obrázek 22: Příklad podvodu zdravotní péče (20)

2. „Is this you?“ scam (podvod „Jsi tohle ty?“).



Obrázek 23: Příklad "Is this you?" podvodu, vypadá to jako video, jenže se jedná o odkaz na falešnou stránku útočníka (21)

4.2 Láska na internetu aneb Catfishing

Tento typ podvodu je od ostatních podvodů odlišný tím, že sociální inženýr parazituje na lidské potřebě a snaží se emočně navázat na uživatele. Kvůli prohlubování vztahu útočník získává jakousi formu kontroly nad uživatelem. Při větší náklonnosti si podvodník může průběžně navyšovat nároky na finanční obnos, posílat zamilované zprávy a komplimenty (v nějakém normálním časovém intervalu). Dělá to tak dlouho, dokud si to uživatel může dovolit. Poté útočník odřízne veškerou komunikaci s uživatelem a vyhledá někoho dalšího.



Obrázek 24: Příklad lásky na internetu (Romance scam) (22)

Útočníci se vydávají za neznámou osobu s hezkým profilem, který na první pohled nevypadá falešně, slouží k navázání vztahu s uživatelem => Catfishing. Vyhlízejí si hlavně matky samoživitelky, případně ženy ve středním věku. Tyto osoby jsou zranitelné, protože například matky samoživitelky jsou nějakou dobu bez partnera a nemají to jednoduché => skvělý terč pro sociální inženýry.

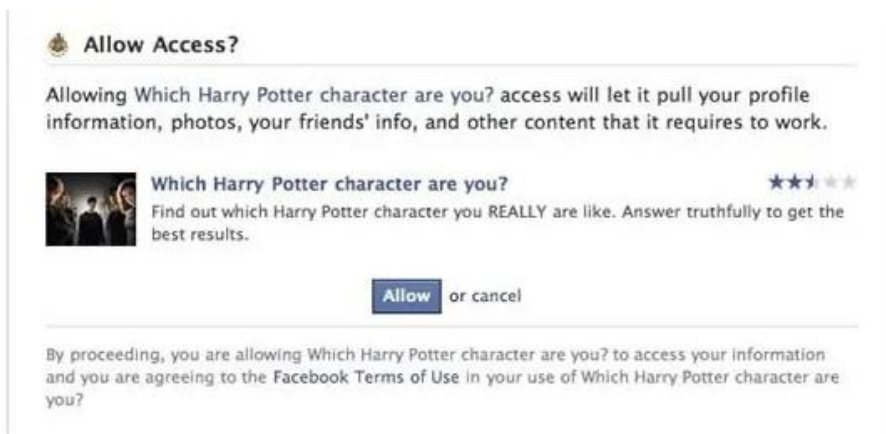
Samo o sobě se jedná o obzvláště krutý podvod.

4.3 Kvízy

Vcelku populární aktivita (bývá na Facebooku, ale i na jiných stránkách). Kdo by si nechtěl zjistit, jaká postava z Avengers je, jaký je jeho nejoblíbenější mazlíček atp.

Nesmíte se ale nechat zmást, i když se jedná o jaksi nevinou záležitost, sociální inženýři ji mohou využít k získání vašich dat, k instalaci malwaru atp.

„V případě, že je kvíz legitimní, jsou o nás beztak sbírány osobní údaje, které mohou být použity pro cílenou reklamu. Nejlepším způsobem, jak se proti potenciálním podvodům bránit, je prostě tyto kvízy nedělat.“ (19)



Obrázek 25: Příklad povolení kvízu na Facebooku (23)

Mnoho těchto kvízů vás informuje o podmínkách, se kterými musíte souhlasit. Je to potom na vás, jestli chcete, aby k vašim datům měly přístup programy z třetích stran, přesněji řečeno např. přístup k uživatelským údajům, seznamu přátel, telefonnímu číslu, emailové adrese atd.

5 Stanovení organizačních pravidel pro školení zaměstnanců

V každé organizaci by měl být pracovník odpovídající za nakládání s osobními údaji a kybernetickou bezpečností.

5.1 GDPR

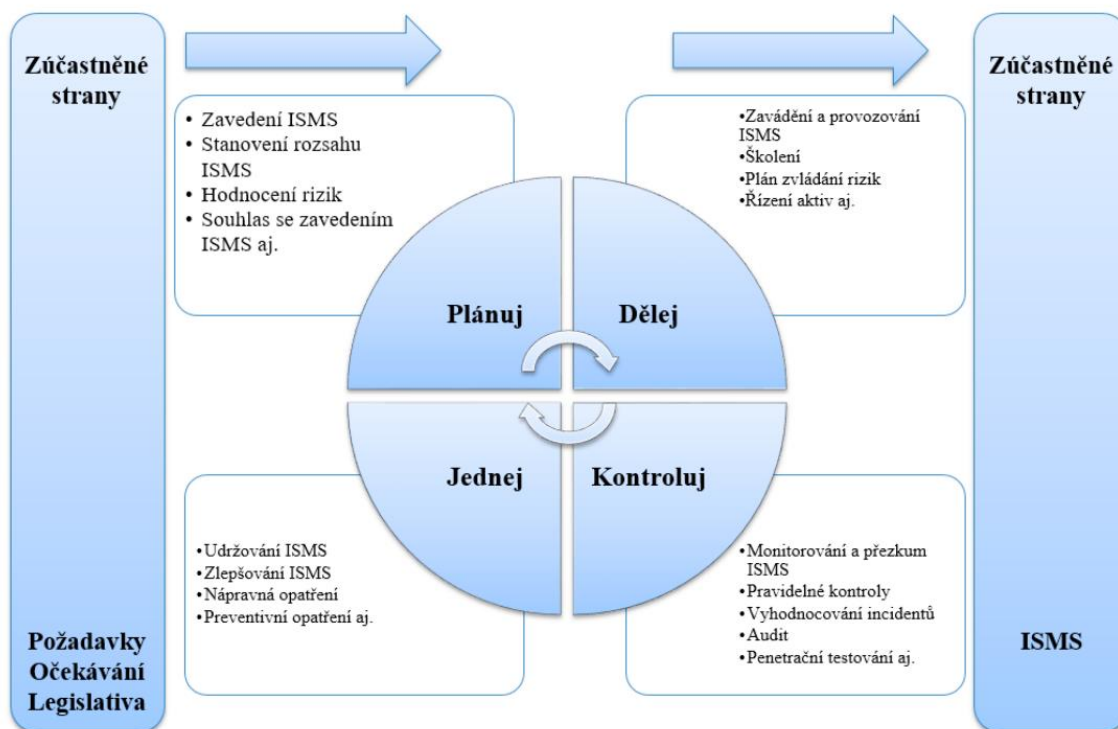
Jedná se o právní předpis, nařízení EU, které stanovuje pravidla pro shromažďování, zpracování a ochranu osobních údajů osob žijících v EU. Jeho účelem je vytvořit soubor standardizovaných zákonů, aby občan EU věděl, jak je s jeho daty naloženo. Tato pravidla se týkají každého, kdo shromažďuje nebo/a zpracovává data, dokonce i pro společnosti, firmy nebo instituce sídlící mimo EU, které zpracovávají data občanů EU.

5.2 PDCA

Cyklus zabývající se opakování základních činností: Plan-Do-Check-Act (Plánuj-Dělej-Kontroluj-Jednej). Je jedním ze základních manažerských principů spočívajících v postupném zlepšování kvality procesů, služeb, dat, výrobků atp.

V rámci kybernetické bezpečnosti lze aplikovat varianta OPDCA => rozšiřuje cyklus o fázi Observe (Pozoruj) předcházející fázi plánování.

Tento cyklus (a některé jeho varianty) je možno aplikovat např. na všechny procesy ISMS (Information Security Management System => systém řízení bezpečnosti informací). Často se zobrazuje jako nekonečný kruh.



Obrázek 26: Příklad modelu PDCA (24)

6 Ochrana před kybernetickými útoky

V předešlých kapitolách, podkapitolách a příkladech bylo naznačeno, jak se proti takovým útokům bránit, ale ne natolik podrobně, a ne u všech příkladů, že by to stačilo pro plné vyjádření, jak se bránit proti sociálním inženýrům.

Jednoho dne se pokusy o sociální inženýrství objeví, ať se jedná o zaměstnance firmy, či jiné osoby (např. vytváření videa na Youtube nebo streaming) bez ohledu na to, jaké jsou bezpečnostní opatření.

Proto bychom si měli říci doporučené postupy a zároveň si říci, kde se mohou vyskytovat nebezpečná místa v uvedených případech.

6.1 Doporučené postupy ochrany před sociálním inženýrstvím

Mezi jednotlivé postupy/tipy patří:

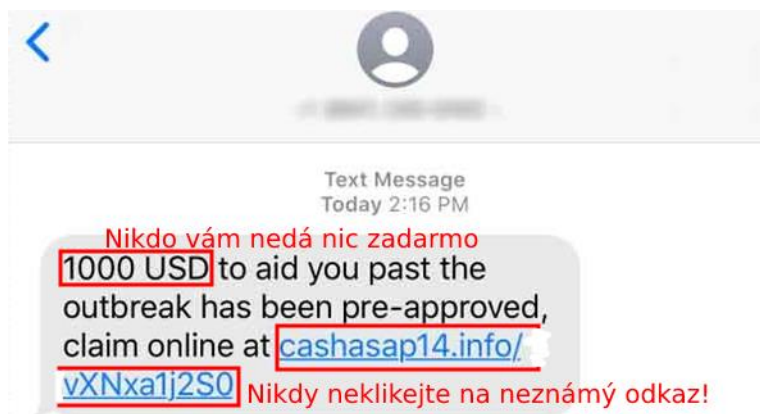
1. Pozastavte se a zamyslete se, než kliknete na přílohu v emailu, odkaz na stránku, stahování/aktualizování atd. Sociální inženýři si pohrávají s vašimi emocemi – strach, chamtivost, empatie (vcítění), naléhavost, autorita => nenechte se rozhodit, nejdříve se rozmyslete, než začnete jednat.
2. Nikdy nikomu nesdělujte své osobní nebo firemní informace, pokud nejsou všeobecně známé nebo osoba má oprávnění takové informace znát.
3. Když si nejste jistí, ověřte si to. To znamená vyhledejte identitu profilu, oprávnění ke sdílení, mobilní číslo atd.
4. Pokud dostanete email/zprávu od známé osoby/firmy, která po vás vyžaduje něco neobvyklého, kontaktujte ji přes telefon nebo osobně, jestli to byla doopravdy ona, kdo zprávu poslal.
5. Mějte dvou/multifázovou autentizaci (2FA/MFA => použití lepší technologie 2FA => Google Authenticator).
6. Udržujte svůj antivirus, emailové filtry a firewally, provádějte rutinní aktualizace pro opravu zranitelností aplikací/systému.
7. Důkladně si prohlédněte webovou adresu, jestli začíná „https“, a dávejte si pozor na weby se „http“ na začátku („s“ je klíčem, znamená „Secure“ (Bezpečný)).

6.2 Příklady nesrovnalostí útoků

Mnoho těchto útoků má vždy schovanou nějakou nesrovnalost, někdy je jich víc, někdy méně.

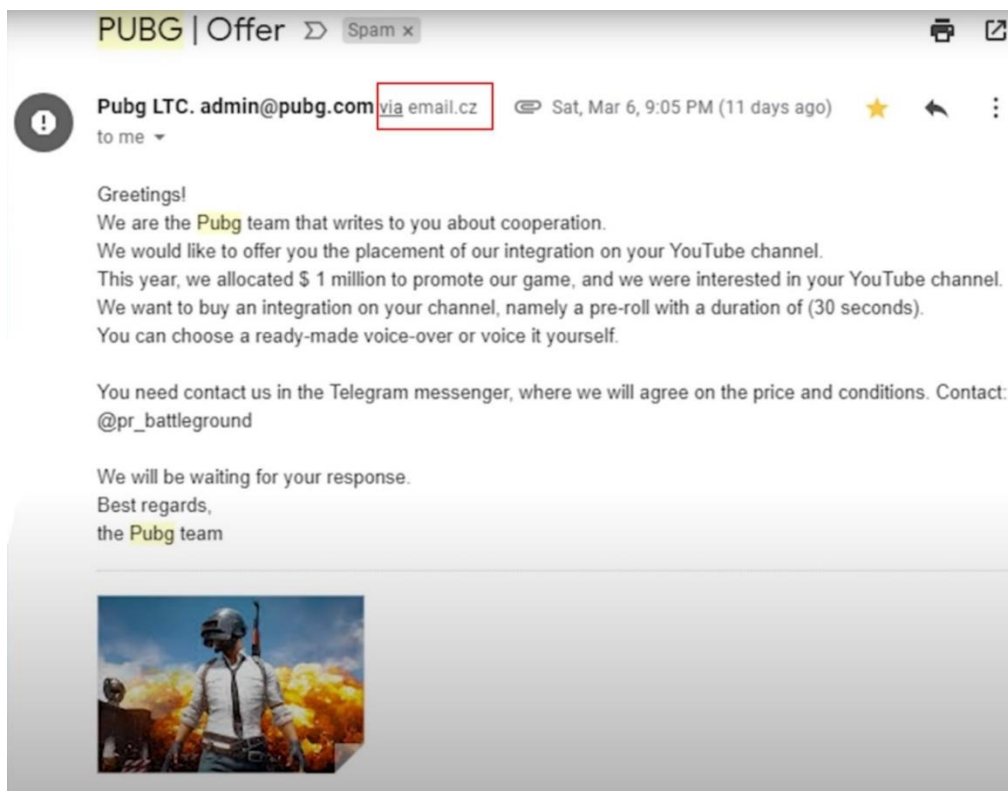
Mezi nejčastější patří:

1. Zní to až moc dobře, aby to byla pravda.



Obrázek 27: Příklad textové zprávy (Smishing) (4)

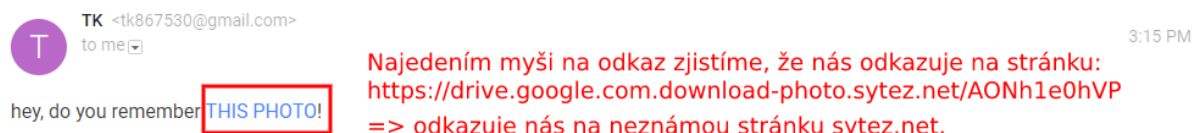
2. Mimika legitimního emailu



Obrázek 28: Vypadá téměř legitimně, jenže tento email byl poslán kompletně jinou službou (25)

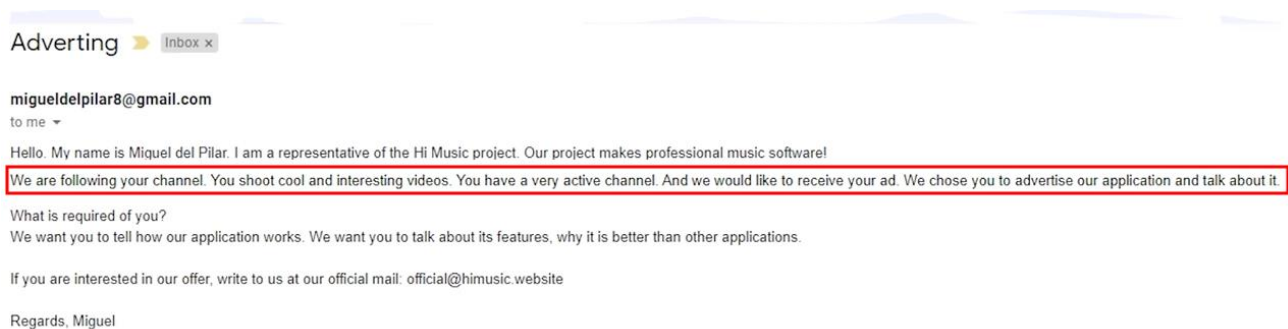
Email se také může lišit jedním písmenkem od legitimního emailu, a/nebo jméno emailu neodpovídá podpisu v obsahu emailu.

3. Odkaz na webovou stránku vypadá podivně (nemá „s“ v https, doména směřuje, kam nemá, doména má písmenko navíc atd).



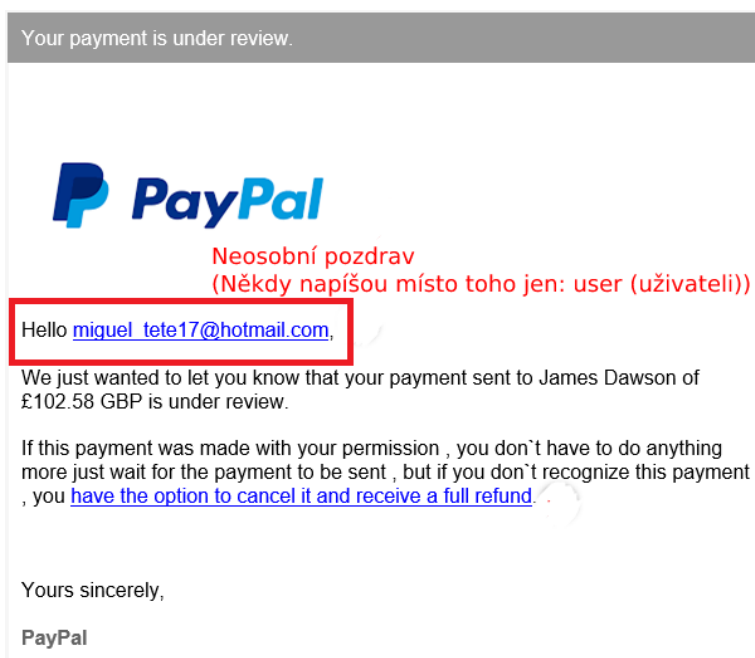
Obrázek 29: Modelový příklad (26)

4. Špatný překlad, téměř nečitelné.



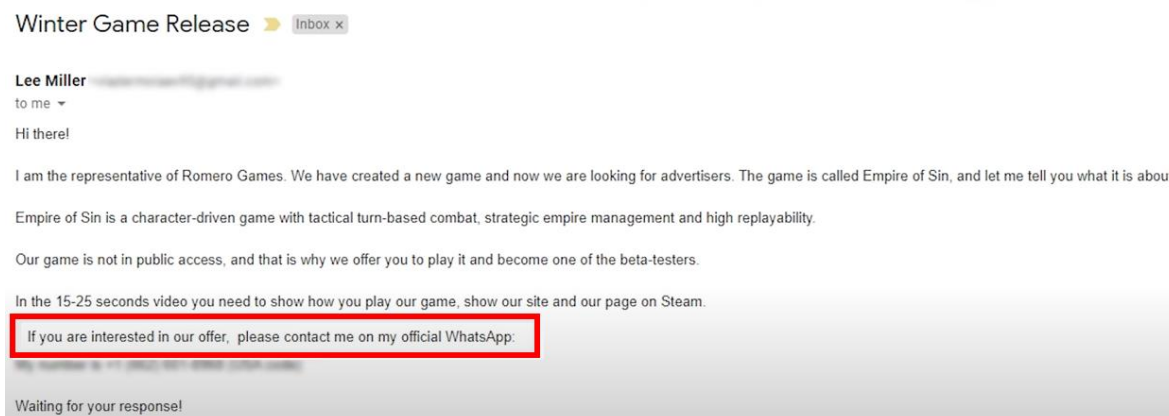
Obrázek 30: Phishing email poslán tvůrci videí na Youtube (25)

5. Naprosto neosobní.



Obrázek 31: Příklad Paypal phishingu (17)

6. Snaží se vás dostat na jiný chatovací systém, než je email



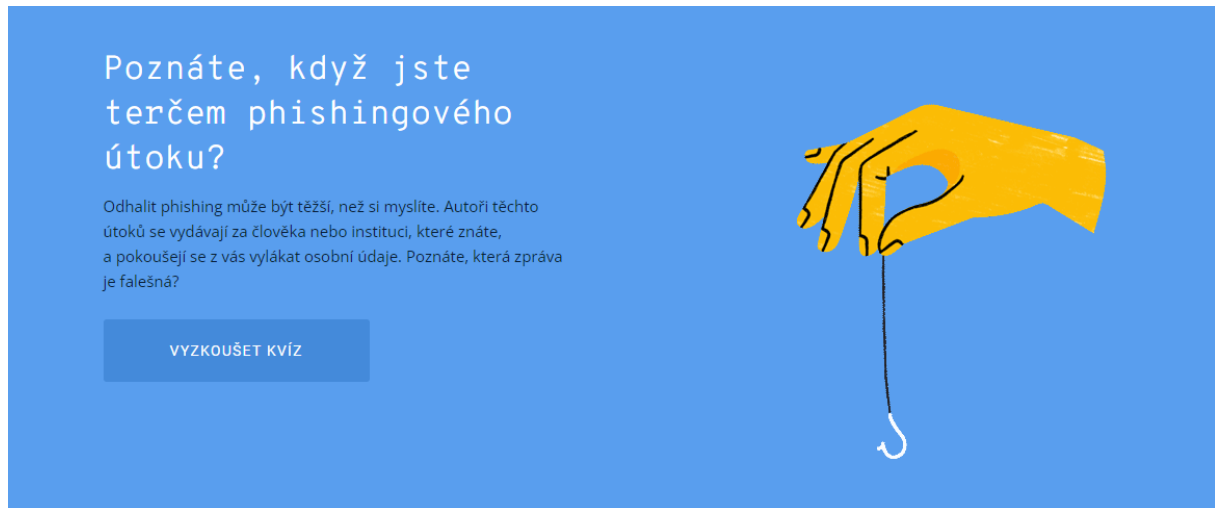
Obrázek 32: Proč si potřebujeme kvůli někomu neznámému stáhnout aplikaci třetích stran pro chat, když máme email? (25)

6.3 Dokážete rozpoznat phishingový útok od normální zprávy?

Google a Youtube mají svůj vlastní phishingový test, který si můžete sami vyzkoušet a zjistit, jak jste na tom s rozpoznáním falešné zprávy od skutečné.

Test je dostupný v češtině a ostatních jazycích.

Odkaz: <https://phishingquiz.withgoogle.com/?hl=cs>



Obrázek 33: Úvodní stránka phishing testu od Googlu (26)

Závěr

V odborné práci se mi podařilo popsat jednotlivé techniky sociálního inženýrství, jako jsou spear phishing, baiting atp, jaké jsou trendy, výskyty (např. na soc. sítích), historie a zároveň jak se chránit před těmito kybernetickými útoky. Hlavním cílem práce bylo sepsat jednotlivé kapitoly a podkapitoly tak, aby toto téma mohl pochopit i někdo, kdo nikdy neslyšel o kyberzločinech v rámci sociálního inženýrství. Dále jsem vytvořil prezentaci jako praktický podklad pro školení zaměstnanců.

Práce trvala přibližně 106 hodin. I přes tento čas nelze plně popsat každou techniku a její výskyty, protože se většinou kombinují navzájem nebo během útoku podvodník může použít techniku jinou, nebo se k nim může vracet atp.

Při psaní této práce jsem se mnoho naučil. Vidím, jak by se tyto metody daly aplikovat na naši školu. Dal by se aplikovat tailgating, příkladem by byl člověk se dvěma taškami a čekal by, jestli by mu někdo otevřel dveře do šatny čipem (popřípadě mu je i student podrží z laskavosti). Nebo dále pretexting. Útočník si vyhledá informace o našem zástupci ředitele školy, který často píše zprávy všem studentům ohledně velké akce, oznámení. Útočník by si mohl vytvořit identitu zástupce a vytvořit přesvědčivý email pro studenty => email phishing. Nebo spear phishing, kdy se přímo zaměří na našeho ředitele a bude působit jako jeden ze sponzorů/soukromých kontaktů, který mu chce nabídnout nějakou dodatečnou službu => Quid Pro Quo (spíše se jedná také o BEC útok).

Kdybych měl psát tuto práci od znova, určitě bych zlepšil téma: „Nové komunikační platformy“. Byl zde hlavně problém s vyhledáním zdrojů týkajících se tohoto tématu, protože veškerá odborná a srozumitelná vysvětlení technik z předešlých témat byla nazývaná „scam“. Každá z těchto technik se může nazývat „scam“, všechno je to podvod. V této kapitole jsem se tedy potýkal s nepřesností zdrojů pro toto téma. Co bych ještě zlepšil, jsou příklady u některých technik/podkapitol a jejich vysvětlení.

Seznam zkratk a odborných výrazů

2FA/MFA

Two/Multi-factor authentication – Dvou/multifázová autentizace – Dodatečná vrstva zabezpečení pro připojení k účtu.

Seznam obrázků

Obrázek 1: Průběh sociálního inženýrství (1).....	2
Obrázek 2: Speciální příklad amatérského phishingu (přesněji řečeno smishingu), který se nedávno udal na platformě Discord. Někdo ukradnul účet uživatele na serveru, účet poté použil jako „robota“, který všude automaticky přeposílal podvod na Discord Nitro (předplatné pro tuhle platformu s výhodami).....	6
Obrázek 3: Příklad Spear Phishingu (2)	7
Obrázek 4: Příklad Vishingu, útočník se může vydávat za banku a vyžadovat peníze (3) .	8
Obrázek 5: Příklad Smishingu, v téhle zprávě jsou velmi agresivní a pospíchají na uživatele, aby provedl akci (4)	9
Obrázek 6: Příklad Baitingu (5)	9
Obrázek 7: Příklad Pretextu (6).....	10
Obrázek 8: Příklad Tailgatingu (7)	11
Obrázek 9: Příklad Piggybackingu (8).....	12
Obrázek 10: Příklad metody Quid Pro Quo (5)	13
Obrázek 11: Příklad scarewaru (9)	14
Obrázek 12: Příklad Consent Phishingu (10)	16
Obrázek 13: Vysvětlení, jak vlastně SIM Swapping funguje (11).....	17
Obrázek 14: Přehled statistik ztrát z roku 2020 zveřejněno FBI, BEC představoval 37% všech ztrát (12)	18
Obrázek 15: Příklad použití technologie Deepfaku (13).....	19
Obrázek 16: Rozdíly mezi phishing kitem a PhaaS (14)	20
Obrázek 17: Příklad implementace LogoKit phishing kitu (15)	21
Obrázek 18: Jeden příspěvek na Twitteru poslaný hackerem přes účet Baracka Obamy (16).....	22
Obrázek 19: Příklad Clickbait phishingu (17)	24
Obrázek 20: Modelový příklad podvodných inzerátů na soc. sítích (18)	25
Obrázek 21: Příklad podvodu s m-platbou (19).....	26
Obrázek 22: Příklad podvodu zdravotní péče (20)	26
Obrázek 23: Příklad "Is this you?" podvodu, vypadá to jako video, jenže se jedná o odkaz na falešnou stránku útočníka (21).....	27

Obrázek 24: Příklad lásky na internetu (Romance scam) (22)	28
Obrázek 25: Příklad povolení kvízu na Facebooku (23)	29
Obrázek 26: Příklad modelu PDCA (24)	31
Obrázek 27: Příklad textové zprávy (Smishing) (4)	33
Obrázek 28: Vypadá téměř legitimně, jenže tento email byl poslán kompletně jinou službou (25).....	34
Obrázek 29: Modelový příklad (26)	34
Obrázek 30: Phishing email poslán tvůrci videí na Youtube (25)	35
Obrázek 31: Příklad Paypal phishingu (17)	35
Obrázek 32: Proč si potřebujeme kvůli někomu neznámému stáhnout aplikaci třetích stran pro chat, když máme email? (25)	35
Obrázek 33: Úvodní stránka phishing testu od Googlu (26)	36

Použité zdroje

1. **Imperva.** Social Engineering. *Imperva*. [Online] [Citace: 09. 11. 2021.] <https://www.imperva.com/learn/application-security/social-engineering-attack/>.
2. **Trend Micro.** What Are the Different Types of Phishing? *Trend Micro*. [Online] [Citace: 19. 02. 2022.] https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html.
3. **Silent Breach.** Social engineering: Putting people at the heart of cybersecurity. *Silent Breach*. [Online] [Citace: 25. 02. 2020.] <https://silentbreach.com/social-engineering.php>.
4. **IdentityForce.** Coronavirus Fake Websites and Phishing Emails. *IdentityForce*. [Online] 2020. [Citace: 20. 02. 2022.] <https://www.identityforce.com/identity-theft/coronavirus-scams>.
5. **Mitnick Security.** 4 Social Engineering Attack Examples (with Pictures!). *Mitnick Security*. [Online] 10. 05. 2021. [Citace: 19. 02. 2022.] <https://www.mitnicksecurity.com/blog/4-social-engineering-attack-examples>.
6. **MEL.** Cyber Risk Control: Social Engineering. *MEL*. [Online] 10. 02. 2020. [Citace: 25. 02. 2022.] <https://njmel.org/2020/02/cyber-risk-social-engineering/>.
7. **Trustaira Staff.** The Art of Hacking Humans is Social Engineering. *Trustaira*. [Online] 12. 09. 2018. [Citace: 25. 02. 2022.] <https://trustaira.com/art-hacking-humans-social-engineering/>.
8. **BYU.** SOCIAL ENGINEERING. *BYU: Brigham Young University*. [Online] [Citace: 25. 02. 2022.] <https://infosec.byu.edu/social-engineering>.
9. **Bellerue, Michael.** BROWSER SPYWARE INFECTIONS “SCAREWARE”. *Technical Reinforcements*. [Online] 05. 10. 2018. [Citace: 28. 12. 2021.] <https://www.reinforceme.com/tri-october-2018-newsletter/>.
10. **Girling, Agnieszka.** Protecting your remote workforce from application-based attacks like consent phishing. *Microsoft*. [Online] 08. 07. 2020. [Citace: 19. 02. 2022.] <https://www.microsoft.com/security/blog/2020/07/08/protecting-remote-workforce-application-attacks-consent-phishing/>.

11. **ThreatMark Team.** SIM Swap Scams & How to Prevent Them. *ThreatMark*. [Online] 15. 04. 2021. [Citace: 19. 02. 2022.] <https://www.threatmark.com/sim-swap-scams-and-how-to-prevent-them/>.
12. **FBI: IC3.** Internet Crime Report 2020. *ic3.gov*. [Online] 2020. [Citace: 19. 02. 2022.] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
13. **Palmer, Shelly.** The Deepest Deepfake of All. *Shelly Palmer*. [Online] 17. 10. 2021. [Citace: 19. 02. 2022.] <https://www.shellypalmer.com/2021/10/the-deepest-deepfake-of-all/>.
14. **Microsoft 365 Defender Threat Intelligence Team.** Catching the big fish: Analyzing a large-scale phishing-as-a-service operation. *Microsoft*. [Online] 21. 10. 2021. [Citace: 20. 02. 2022.] <https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/>.
15. **Team RISKIQ.** LogoKit: Simple, Effective, and Deceptive. *RISKIQ*. [Online] 27. 01. 2021. [Citace: 27. 02. 2022.] <https://www.riskiq.com/blog/external-threat-management/logokit-phishing/>.
16. **Mitnick Security.** The 2020 Twitter Bitcoin Scam: How it Happened and Key Lessons from Whitehat Hacker Kevin Mitnick. *Mitnick Security*. [Online] 16. 06. 2020. [Citace: 19. 02. 2022.] <https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam>.
17. **Benedict, Goldy.** What to Do If You Click on a Phishing Link – 4 Steps to Minimize Impact. *Private Vault*. [Online] 06. 11. 2019. [Citace: 20. 02. 2022.] <https://www.digitalprivatevault.com/blogs/what-to-do-if-you-click-on-a-phishing-link>.
18. **Faux, Zeke.** How Facebook Helps Shady Advertisers Pollute the Internet. *Bloomberg*. [Online] 27. 03. 2018. [Citace: 25. 02. 2022.] <https://www.bloomberg.com/news/features/2018-03-27/ad-scammers-need-suckers-and-facebook-helps-find-them>.
19. **Fojtík, Martin.** Sociální sítě, nová platforma pro útoky sociálních inženýrů. *hackingLab*. [Online] 31. 11. 2019. [Citace: 19. 02. 2022.] <https://hackinglab.cz/cs/blog/socialni-site-nova-platforma-pro-utoky-socialnich-inzenyru/>.

20. **Panda Security.** 10 Social Media Scams and How to Spot Them. *Panda Security*. [Online] 02. 04. 2019. [Citace: 19. 02. 2022.]
<https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/>.
21. **Naked Security.** “Is it you in the video?” – don’t fall for this Messenger scam. *Naked Security*. [Online] 18. 12. 2020. [Citace: 19. 02. 2022.]
<https://nakedsecurity.sophos.com/2020/12/18/is-it-you-in-the-video-dont-fall-for-this-messenger-scam/>.
22. **Griese, Kelly.** Love Hurts: How to Spot a Romance Scam. *IN.gov*. [Online] 12. 02. 2020. [Citace: 19. 02. 2022.]
<https://www.in.gov/sos/indianamoneywise/blog/posts/love-hurts-how-to-spot-a-romance-scam/>.
23. **Komando staff.** Read this before you take a Facebook quiz again. *Komado.com*. [Online] 04. 06. 2017. [Citace: 19. 02. 2022.]
<https://www.komando.com/privacy/read-this-before-you-take-a-facebook-quiz-again/361184/>.
24. **Kolouch, Jan, a další.** *CyberSecurity*. Praha : CZ.NIC, z. s. p. o, 2019. ISBN 978-80-88168-34-8.
25. **Wanderbot Prime.** Scammers Keep Trying To Steal My Channel. *Youtube*. [Online] 21. 03. 2021. [Citace: 19. 02. 2022.]
https://www.youtube.com/watch?v=FGJ8QD8MO6o&t=614s&ab_channel=WanderbotPrime.
26. **Google.** Poznáte, když jste terčem phishingového útoku? *Phishing Quiz*. [Online] [Citace: 25. 02. 2022.] <https://phishingquiz.withgoogle.com/?hl=cs>.
27. **Přispěvatelé Wikipedie.** Sociální inženýrství (bezpečnost). *Wikipedie: Otevřená encyklopedie*. [Online] 08. 08. 2021. [Citace: 07. 11. 2021.]
[https://cs.wikipedia.org/w/index.php?title=Sociální_inženýrství_\(bezpečnost\)&oldid=20344801](https://cs.wikipedia.org/w/index.php?title=Sociální_inženýrství_(bezpečnost)&oldid=20344801).
28. **Wikipedia contributors.** Social engineering (security). *Wikipedia, The Free Encyclopedia*. [Online] 05. 11. 2021. [Citace: 07. 11. 2021.]
[https://en.wikipedia.org/w/index.php?title=Social_engineering_\(security\)&oldid=1053683778](https://en.wikipedia.org/w/index.php?title=Social_engineering_(security)&oldid=1053683778).

29. **Gonzalez, Cynthia.** Top 5 Social Engineering Techniques and How to Prevent Them. *Exabeam*. [Online] 15. 04. 2020. [Citace: 11. 07. 2021.]
<https://www.exabeam.com/information-security/social-engineering/>.
30. **Bersheva, Maya.** 5 nejčastějších metod sociálního inženýrství a způsoby, jak jim předejít. *Kurzy.cz*. [Online] 30. 03. 2021. [Citace: 07. 11. 2021.]
<https://www.kurzy.cz/zpravy/586164-5-nejcastejsich-metod-socialniho-inzenyrstvi-a-zpusoby-jak-jim-predejti/>.
31. **NÚKIB.** Sociální inženýrství. *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost*. [Online] 22. 03. 2016. [Citace: 09. 11. 2021.]
<https://nukib.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/>.
32. **Přispěvatelé Wikipedie.** Sociální inženýrství (společenská věda). *Wikipedie: Otevřená encyklopedie*. [Online] 16. 09. 2021. [Citace: 12. 11. 2021.]
[https://cs.wikipedia.org/w/index.php?title=Soci%C3%A1ln%C3%AD_in%C5%BEn%C3%BDrstv%C3%AD_\(spole%C4%8Densk%C3%A1_v%C4%Bda\)&oldid=20479033](https://cs.wikipedia.org/w/index.php?title=Soci%C3%A1ln%C3%AD_in%C5%BEn%C3%BDrstv%C3%AD_(spole%C4%8Densk%C3%A1_v%C4%Bda)&oldid=20479033).
33. **Carneige Mellon University.** Social Engineering. *CMU: Carneige Mellon University*. [Online] [Citace: 28. 12. 2021.] <https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html>.
34. **paton.** Pojem Baiting. *SCS.ABZ.CZ: Slovník cizích slov*. [Online] [Citace: 26. 12. 2021.]
<https://slovník-cizich-slov.abz.cz/web.php/slovo/baiting>.
35. **Mitnick Security.** The History of Social Engineering. *MitnickSecurity*. [Online] 2020. [Citace: 09. 11. 2021.] <https://www.mitnicksecurity.com/the-history-of-social-engineering>.
36. **Fortinet.** Scareware. *Fortinet*. [Online] [Citace: 28. 12. 2021.]
<https://www.fortinet.com/resources/cyberglossary/scareware>.
37. **Mitnick Security.** 6 Types of Social Engineering Attacks. *MitnickSecurity*. [Online] 05. 04. 2021. [Citace: 28. 12. 2021.] <https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks>.
38. **Forcepoint.** What is Scareware? *Forcepoint*. [Online] [Citace: 28. 12. 2021.]
<https://www.forcepoint.com/cyber-edu/scareware>.

39. **Wikipedia contributors.** Scareware. *Wikipedia, The Free Encyclopedia*. [Online] 21. 12. 2021. [Citace: 28. 12. 2021.]
<https://en.wikipedia.org/w/index.php?title=Scareware&oldid=1061356878>.
40. **Gillis, Alexander S.** scareware. *WhatIs.com / TechTarget*. [Online] 12. 2021. [Citace: 28. 12. 2021.] <https://whatis.techtarget.com/definition/scareware>.
41. **Wikipedia contributors.** Deepfake. *Wikipedia, The Free Encyclopedia*. [Online] 11. 01. 2022. [Citace: 13. 01. 2022.]
<https://en.wikipedia.org/w/index.php?title=Deepfake&oldid=1065010404>.
42. **FBI.** Business Email Compromise . *FBI*. [Online] [Citace: 13. 01. 2022.]
<https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>.
43. **Schmerler, Ben.** 3 BIG TRENDS IN 2020 SOCIAL ENGINEERING (VIDEO). *DP Solutions*. [Online] 21. 08. 2020. [Citace: 13. 01. 2022.]
<https://www.dpsolutions.com/blog/social-engineering-2020>.
44. **Sjouwerman, Stu.** Five Social Engineering Trends to Watch for 2021. *CISO MAG - News and Updates / Cyber Security Magazine*. [Online] 24. 03. 2021. [Citace: 07. 11. 2021.] <https://cisomag.eccouncil.org/5-social-engineering-trends-to-watch-for-2021>.
45. **Chapman, Jack.** Phishing-as-a-Service Brings Cybercrime to the Masses. *CPO Magazine*. [Online] 20. 01. 2022. [Citace: 12. 02. 2022.]
<https://www.cpomagazine.com/cyber-security/phishing-as-a-service-brings-cybercrime-to-the-masses/>.
46. **Dove, Martina.** The Use of Deepfakes in Social Engineering Attacks. *Tripwire*. [Online] 24. 01. 2022. [Citace: 12. 02. 2022.] <https://www.tripwire.com/state-of-security/security-data-protection/use-of-deepfakes-in-social-engineering-attacks/>.
47. **Washington, D.C. FBI National Press Office.** FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics. *FBI*. [Online] 17. 03. 2021. [Citace: 12. 02. 2022.]
<https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics>.

48. **Cluley, Graham.** FBI statistics underline the horrific cost of business email compromise. *Tripwire*. [Online] 18. 03. 2021. [Citace: 12. 02. 2022.] <https://www.tripwire.com/state-of-security/featured/fbi-statistics-underline-horrific-cost-of-business-email-compromise/>.
49. **Vaas, Lisa.** Phishing Costs Nearly Quadrupled Over 6 Years. *Threatpost*. [Online] 17. 08. 2021. [Citace: 12. 02. 2022.] <https://threatpost.com/phishing-costs-quadrupled/168716/>.
50. **Brook, Chris.** Phishing, BEC Scams Netting \$80,000 On Average in 2020. *Digital Guardian*. [Online] 01. 09. 2020. [Citace: 12. 02. 2022.] <https://digitalguardian.com/blog/phishing-bec-scams-netting-80000-average-2020>.
51. **Cimpanu, Catalin.** Lithuanian man pleads guilty to scamming Google and Facebook out of \$123 million. *ZDNet*. [Online] 20. 03. 2019. [Citace: 12. 02. 2022.] <https://www.zdnet.com/article/lithuanian-man-pleads-guilty-to-scamming-google-and-facebook-out-of-123-million/>.
52. **ScienceDaily.** 'Deepfakes' ranked as most serious AI crime threat. *ScienceDaily*. [Online] 04. 08. 2020. [Citace: 12. 02. 2022.] <https://www.sciencedaily.com/releases/2020/08/200804085908.htm>.
53. **Wagenseil, Paul.** Google is forcing people to use 2FA — what that means for you. *Tom's Guide*. [Online] 05. 11. 2021. [Citace: 12. 02. 2022.] <https://www.tomsguide.com/news/google-forcing-2fa-users>.
54. **Wikipedia contributors.** SIM swap scam. *Wikipedia, The Free Encyclopedia*. [Online] 23. 10. 2021. [Citace: 12. 02. 2022.] https://en.wikipedia.org/w/index.php?title=SIM_swap_scam&oldid=1051495915.
55. **Mundell, Michael.** Google Is Making 2FA Mandatory and It's Happening Before 2022. *Antivirus.com*. [Online] 25. 11. 2021. [Citace: 12. 02. 2022.] <https://antivirus.com/2021/11/25/google-is-making-2fa-mandatory-and-its-happening-before-2022/>.
56. **Techquickie.** Don't Trust ANYTHING You See - Deepfakes Explained. *Youtube*. [Online] 01. 11. 2019. [Citace: 11. 02. 2022.] https://www.youtube.com/watch?v=4JNBDwd40is&ab_channel=Techquickie.

57. **iluli by Mike Lamb.** How SIM Swapping Works. *Youtube*. [Online] 31. 08. 2019. [Citace: 12. 02. 2022.] https://www.youtube.com/watch?v=k4UNNKfsjXE&ab_channel=ilulibyMikeLamb.
58. **Novinson, Michael.** Twitter Employees Hacked In ‘Coordinated Social Engineering Attack’. *CRN*. [Online] 16. 07. 2020. [Citace: 12. 02. 2022.] <https://www.crn.com/news/security/twitter-employees-hacked-in-coordinated-social-engineering-attack-?itc=refresh>.
59. **Shead, Sam.** Google says North Korean state hackers are targeting security researchers on social media. *CNBC*. [Online] 26. 01. 2021. [Citace: 12. 02. 2022.] <https://www.cnbc.com/2021/01/26/north-korean-hackers-targeting-security-researchers-on-twitter.html>.
60. **Swinhoe, Dan.** Protecting high-value research data from nation-state attackers. *CSO: United States*. [Online] 06. 07. 2020. [Citace: 12. 02. 2022.] <https://www.csoonline.com/article/3564623/how-to-protect-high-value-research-data-from-aps.html>.
61. **Hernández, Luciano.** What are state-sponsored cyberattacks? *F-Secure*. [Online] 10. 03. 2021. [Citace: 12. 02. 2022.] <https://blog.f-secure.com/what-are-state-sponsored-cyberattacks/>.
62. **salesforce.** What is SaaS? *salesforce.com*. [Online] [Citace: 12. 02. 2022.] <https://www.salesforce.com/in/saas/>.
63. **Certo.** How to protect yourself from scamming text messages. *Certo*. [Online] [Citace: 19. 02. 2022.] <https://www.certosoftware.com/how-to-protect-yourself-from-scamming-text-messages/>.
64. **Fruhlinger, Josh.** Social engineering: Definition, examples, and techniques. *CSO: United States*. [Online] 07. 02. 2022. [Citace: 19. 02. 2022.] <https://www.csoonline.com/article/3648654/social-engineering-definition-examples-and-techniques.html>.
65. **NordVPN.** How to avoid a vishing attack | NordVPN. *Youtube*. [Online] 07. 07. 2020. [Citace: 19. 02. 2022.] https://www.youtube.com/watch?v=6IIW6m72eX8&ab_channel=NordVPN.

66. **Heinbach, Courtney.** 5 Types of Social Engineering Attacks. *Datto*. [Online] 11. 08. 2020. [Citace: 19. 02. 2022.] <https://www.datto.com/blog/5-types-of-social-engineering-attacks>.
67. **Kučera, Petr.** Chcete 2500 korun zdarma od Lidlu a Penny? Pozor na podvod, varují řetězce. *Aktuálně.cz*. [Online] 13. 12. 2016. [Citace: 19. 02. 2022.] <https://zpravy.aktualne.cz/finance/nakupovani/chcete-2500-korun-zdarma-od-lidlu-a-penny-pozor-na-podvod-va/r~070b1e4ec11e11e6977e002590604f2e/>.
68. **Trend Micro.** What Is Social Media Phishing? *Trend Micro*. [Online] [Citace: 19. 02. 2022.] https://www.trendmicro.com/en_vn/what-is/phishing/social-media-phishing.html.
69. **Reinhardtsen, Morten.** Consent phishing – Why you need to act right now. *Ironstone*. [Online] 16. 10. 2020. [Citace: 19. 02. 2022.] <https://www.ironstoneit.com/blog/consent-phishing-why-you-need-to-act-right-now>.
70. **Coinmate.io.** SCAM – can you really double your money? *Coinmate.io*. [Online] 21. 10. 2020. [Citace: 20. 02. 2020.] <https://coinmate.io/blog/en/scam-can-you-really-double-your-money/>.
71. **The Minnesota Attorney General: Keith Ellison.** Social Media Scams. *The Minnesota Attorney General: Keith Ellison*. [Online] [Citace: 20. 02. 2022.] <https://www.ag.state.mn.us/consumer/Publications/SocialMediaScams.asp>.
72. **Proofpoint.** What is Smishing? *Proofpoint*. [Online] [Citace: 20. 02. 2022.] <https://www.proofpoint.com/us/threat-reference/smishing>.
73. **That's NONSENSE.** Facebook “sponsored” posts are clickbait, fake news & scams all in one. *thatsnonsense.com*. [Online] 01. 08. 2017. [Citace: 19. 02. 2022.] <https://www.thatsnonsense.com/facebook-sponsored-posts-clickbait-fake-news-scams-one/>.

A. Seznam přiložených souborů

Na přiloženém datovém nosiči se nacházejí následující soubory a složky:

- Složka MP: obsahuje Word a PDF verzi textové části MP
- Složka SOČ: obsahuje Word a PDF verzi odborné práce
- Prezentace: praktická část MP