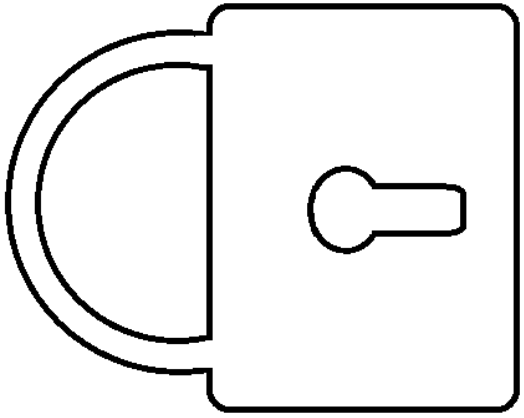


Odborná príručka pre učiteľa

Podporná literatúra pre didaktiku informačnej bezpečnosti, pre 5 ročník ZŠ.

Marek Zeman

Odborná príručka pre učiteľa

Podporná literatúra pre didaktiku informačnej bezpečnosti

pre 5 ročník ZŠ.

Mgr. Marek Zeman, PhD., CRISC

Odborná príručka pre učiteľa bola vytvorená ako odborný podklad pre výučbu informačnej bezpečnosti pre 5. ročník.

Cieľom vytvorenia tejto príručky je poskytnutie informácii o jednotlivých kapitolách informačnej bezpečnosti, podľa tém, ako boli vybrané pre Didaktiku informačnej bezpečnosti pre 5 ročník pod záštitou združení Asociácia Kybernetickej Bezpečnosti a Preventista.sk. Zároveň je publikácia určená širokej verejnosti, jej sekundárny cieľ je zvyšovanie bezpečnostného povedomia a vytvorenie referenčného zdroja pre ďalšie odborné spracovávanie tém.

Publikácia je rozdelená na päť kapitol. Prvá kapitola je venovaná Politike čistého stola, popisuje výhody ak je politika dodržiavaná a prináša možné zneužitia, ktoré nedodržiavanie umožňuje. Druhá kapitola sa venuje prenasledovaniu s využitím dát, ktoré sú prístupné v kybernetickom priestore: Cyberstalking (kybernetické šikanovanie). Definuje, čo je kybernetické šikanovanie, ako ho rozoznať a spôsoby, ako sa ochrániť pred prenasledovateľom (stalkerom). Nasledujúca kapitola ponúka zoznam liniek detskej pomoci, ktoré sú dostupné pre deti v rámci Slovenskej republiky v roku 2019. V rámci článku sú prezentované témy, ktoré deti alebo rodičia nahlasovali na linky detskej pomoci. Predposledná kapitola je venovaná téme Sociálneho inžinierstva na popísanie tvrdých a mäkkých techník, ktoré používajú útočníci. Zároveň kapitola rozpracováva jednotlivé typy útokov a podrobne sa venuje technikám komunikácie na klienta. Posledná kapitola popisuje Phishing a jeho jednotlivé hlavné podoby. V rámci rozpracovania témy Phishingu sú podrobne prezentované prístupy, ktoré využívajú útočníci pri komunikácii s obeťou.

Verím, že táto príručka vám priblíži prostredie kybernetickej aj informačnej bezpečnosti a dokáže vysvetliť všetky zákutia jednotlivých metodických prístupov a útokov, s ktorými sa stretávame v dennom živote.

Autor

10.11.2019 Bratislava

Obsah

Dôvody a spôsob ochrany dát technikou politiky čistého stola

1. Téma, ktorú kapitola prináša:

Politika čistého stola (Clean desk policy)

2. Okruhy, ktoré vysvetľuje

Politika čistého stola, výhody politiky, zameranie, dopady na dodržiavanie, typy únikov a zničenia dát a spôsoby ochrany dát.

3. Definícia

Politika čistého stola je nástroj, ktorý zabezpečí, že všetky citlivé materiály budú na stole len po dobu, kedy sú využívané a ich použitie je pod kontrolou. Následne budú zo stola odstránené a uschované alebo zničené, ak ich potreba pominula. Táto technika je jedna z najsilnejších stratégií pri zvyšovaní bezpečnosti pri práci s dátami.

3.1 Priblíženie technológii, ktoré sa témy týkajú (napr. mobil, email,...)

Politika čistého stola je technika, ktorá ochraňuje rovnako fyzický materiál ako sú tlačené dokumenty, knižky, zošity, tak aj technológie spojené s nosičmi informácii. Silnou stránkou techniky je, že citlivé informácie sú k dispozícii iba počas doby, počas ktorej sa dáta spracovávajú, následne sú uschované na bezpečné miesto.

Metodika sa zameriava na

- Ochrana informácii (náhodným prečítaním, zničením,)
- Ochrana osobných údajov

Cieľom politiky čistého stola je vytvorenie takého prostredia, ktoré zabezpečí ochranu dát a infraštruktúry pri zachovaní plného prístupu a využiteľnosti jednotlivých prostriedkov a všetkých nevyhnutných dát.

Útoky sú delené podľa úmyslu, pri ktorom bol spáchaný prečin:

- Úmyselné poškodenie
- Neúmyselné poškodenie (náhodné poškodenie)

Bezpečnostné požiadavky vytvárajú prostredie na:

- Ochranu informácií, ochranu času na obnovenie informácii a ochranu investícii.
- Zabezpečujú zhodu s bezpečnostnými štandardami v prípade firiem.
- Ochraňujú pred náhodným prečítaním (upratovačka, kolega, ...).
- Ochraňujú pred cieleným prečítaním (konkurent, priemyselná špionáž).

Implementovanie politiky čistého stola zvyšuje produktivitu:

- Voľným miestom na stole je vytvorené miesto použiteľné na prácu.
- Znižuje sa možnosť prepínania medzi rôznymi úlohami človekom.
- Ľahšie sú definované a dodržiavané priority úloh.
- Obmedzené je nedôležité vyhľadávanie v dokumentoch.

4 Bezpečnostné odporúčania

Všetky bezpečnostné odporúčania sa zameriavajú na ochranu pracovných prostriedkov, ktoré sú na stole k dispozícii. Či už ide o firemné, osobné alebo školské údaje. Vo firme sa zameriavajú primárne na ochranu priemyselného vlastníctva a osobných údajov a ochranu pred porušením jednotlivých sektorových zákonov. Ochrana v domácnosti sa zameriava nielen na samotnú ochranu pred stratou alebo zneužitím, ale aj pred poškodením, či už úmyselným alebo náhodným. V domácnosti je nevyhnutné používať politiku čistého stola z dôvodu ochrany firemných údajov ak sú spracovávané v domácnosti. Avšak citlivé údaje sú používané a aj vytvárané aj samotnými členmi domácnosti. Citlivé údaje sú významné svojou jedinečnosťou samotných údajov, či nosičmi, ktoré údaje obsahujú alebo kde sú zapísané, pričom ich stratu by bolo zdĺhavé nahradiť. Napríklad dedičské rozhodnutie, zmluva na dom, domáca úloha vypracovaná na pracovnom liste.

Na ochranu takýchto údajov je vhodné dodržiavať tieto odporúčania. Odporúčania sú delené podľa zložitosti a dôležitosti na celkovú ochranu.

4.1 minimálne

Dokumenty s citlivými údajmi sú na stole len počas doby, počas ktorej sú spracovávané. Počítače sú uzamknuté, ak sa nepoužívajú a po skončené práce musia byť vypnuté. Po skončení práce sú všetky citlivé údaje uschované na bezpečné miesto podľa miery citlivosti (trezor, skriňa, školská taška).
Dokumenty s citlivými údajmi sa do koša môžu odložiť len zničené, aby sa nedali prečítať (rozstrihané, roztrhané, zoskartované (min stupeň skartovania 2),...)

Po skončení práce s citlivými údajmi musí byť pracovný stôl uprataný.

4.2 základné

Dátové nosiče (CD, DVD, USB,...), ktoré ochraňujú citlivé dokumenty nesmú byť voľne prístupné.

Heslá nesmú byť ponechané/zapísané na prístupnom mieste napr. „žltá lepka“ (Obrázok č.1). Citlivé dokumenty sa nesmú ponechávať na tlačiarni, po vytlačení je vhodné ich zobrať z tlačiarne na ďalšie spracovanie. Tabule a flip-charty s dôvernými alebo citlivými údajmi by mali byť po skončené práce zmazané. Zariadenia pre ukladanie dát ako sú CD disky, USB disky a prenosné pevné disky musia byť po skončené práce uschované na bezpečné miesto.

4.3 expertné

Na stole nesmú byť osobné veci ak ich prítomnosť nie je kvôli spracovaniu údajov z týchto vecí. Doska stola musí byť viditeľná. Stôl má obsahovať len veci nevyhnutné ku splneniu úlohy. Vytvorte si pravidelný režim na upratovanie stola.

5 Popis útokov pri nedodržiavaní politiky čistého stola

Politika čistého stola nie je obyčajne priamo spojená s kybernetickou bezpečnosťou. Je to nevyhnutný nástroj pri riadení informačnej bezpečnosti. Pokrýva všetky oblasti, od kybernetickej, cez fyzickú reprezentáciu informácii až po procesnú časť informačnej bezpečnosti.

5.1 Riziká, ktoré odstraňuje implementácia politiky čistého stola

- Priame zničenie infraštruktúry a dát
    - zaliatie kávou,
    - pád na zem,
    - zničenie infraštruktúry náhodne (napr. stane sa súčasťou detskej hry)
    - neodborne sa vypnutie systému,
    - strata dát (napr. dôležitý chat, obchodné dokumenty, projekt,...)
- Prezradenie dát a dokumentov
    - osobné dáta
        - Napr. zdravotná dokumentácia, dáta z občianskeho preukazu, dokumenty popisujúce stav osobných financií, dokumenty o prechode do iného mesta a školy, ...
    - rodinné

        - napr. majetkový stav rodiny, prekvapenie pre mamu,...
    - firemné
        - hrozba: upratovačka alebo údržbár majú stály prístup k nechráneným dokumentom na stole, nasadený zamestnanec na priemyselnú špionáž,...
- Na stole sú dáta, ktoré nesmú byť zničené.
    - Neodborná manipulácia
        - napr. poškodenie jedlom, neznalosť ovládania zariadení, nepozornosť,...
    - Rodinné hrozby
        - Detské hry: dieťa si sadne za rozpracovaný stôl a nakreslí si bábiku v autíčku, práca na inej úlohe, pri ktorej sa zničia dokumenty položené na stole,...
    - Rýchle upratovanie
        - Upratovanie veľkého, neprehľadného množstva dokumentov prináša vysoké nebezpečenstvo zničenia alebo vyhodenia dôležitého dokumentu z dôvodu nejasnej priority, neznalosti dokumentu a jeho určenia alebo zníženej koncentrácie upratujúcej osoby.
- Na stole sú veci, ktoré nesmú byť odcudzené
    - Dátové nosiče
        - opustený USB s citlivými údajmi, CD, DVD, prenosný disk,...
    - Všeobecné, osobné dokumenty
        - žiacka knižka, nezábudník, pracovný dekrét,...
    - Elektronické zariadenia
        - notebook, telefón,...
    - Jedinečné originály dokumentov s dopadom na majetok
        - akcie na doručiteľa,

6 Záver

Problém implementovania Politiky čistého stola sme rozšírili nielen na firemné prostredie, ale aj na domácnosti. Dôvodom rozšírenia je to, že v domácnostiach sa tiež spracovávajú dokumenty s údajmi s vysokou citlivosťou. Vo všeobecnosti existuje rozdiel v potrebe ochrany citlivých dát medzi domácnosťami a firmami. Vyššia potreba ochrany dát a jej silnejšie formy sa implementujú v rámci firiem, v porovnaní s ochranou dát s podobným charakterom v priestoroch domácností. Nižšia miera ochrany v rámci domácností vyplýva hlavne z vyššej miery dôvery v rámci jednotlivých členov v domácnosti a zároveň z lepšej kontroly pohybu cudzích osôb.

Pre obe prostredia prezradenie alebo zničenie dát môže mať fatálny dopad na ďalšiu existenciu a zdravý, finančný potenciál. Niektoré straty sú často náhodné v zmysle, že nastanú pri malej nepozornosti alebo krátkodobej neprítomnosti počas práce. Dopad býva zásadný od straty dôvery až po problém s finančným dopadom (strata dokladu o nadobudnutí majetku, finančný postih od zamestnávateľa,...) alebo postihnutie v škole (pokarhanie, poznámka, zlá známka). Obeť je často náhodná a strata je nečakaná.

Dodržiavanie politiky čistého stola znižuje stres a chaos a zvyšuje produktivitu a zľahčuje dodržiavanie termínov. Implementovaním politiky čistého stola je uložený pevný základ, na ktorom je možné vystavať bezpečné prostredie pripravené plniť aj najťažšie úlohy.

7. Obrazová príloha

Obrázok č.1: Ukážka nevhodného uchovávania hesiel

Sociálne siete priniesli nový typ útokov: Cyberstalking

1. Téma, ktorú kapitola prináša: Cyberstallking

CyberStalking: Správanie, ktoré má znaky abnormálneho záujmu o konkrétnu osobu. Popisuje jednotlivé formy Cyberstalkingu a ochranu pred nimi.

Vo forenznej psychológii je Cyberstalking považovaný za špecifický variant agresie. [3]

2. Okruhy, ktoré vysvetľuje

Cyberstalking alebo kybernetické šikanovanie (niekedy kyberšikanovanie) je opakované, systematické a dlhodobé sledovanie osoby pomocou elektronických médií, ktoré často prerastie do fyzického prenasledovania a obťažovania. Prenasledovateľ (*stalker*) dlhodobo prenasleduje konkrétnu osobu, zbiera o nej informácie a následne nadväzuje s obeťou a jej okolím kontakt. Existuje niekoľko spôsobov ochrany, ktoré v závislosti od stavu a intenzity útoku sa menia od základného odmietania komunikácie so *stalkerom* až po kontakt orgánov činných v trestnom konaní.

Cyberstalking vedie k závažnému zníženiu kvality života obete. [2]

3. Definície

Stalking (prenasledovanie) je dlhodobé známe abnormálne prejavovanie záujmu o konkrétnu osobu, ktorého prejavy sú nad rámec bežného záujmu. Prejavuje sa získavaním všetkých údajov o konkrétnej osobe a kontaktovaním osoby, ktoré prerastá postupne do obťažovania a zároveň narúša obeti súkromie. Kybernetického šikanovanie je podkategória prenasledovania, ktoré rozširuje fyzické prenasledovanie na kybernetický priestor pri zneužívaní vlastností a možností kybernetického priestoru. Hlavnou črtou, ktorá charakterizuje využívanie kybernetického šikanovania je anonymita internetu a veľký rozsah informácii. Obe črty útočníkovi umožňujú lepšie spoznať a priblížiť sa k obeti pri zachovaní vysokej miery anonymity.

V prvej fáze prenasledovateľ zbiera o zverenej osobe všetky dostupné údaje pomocou elektronických médií od sociálnych sietí, cez komunitné a komunikačné skupiny, až po verejné databanky (napr. *https://www.katasterportal.sk*, www.orsr.sk, http://www.zrsr.sk, ...). V ďalšej fáze sa snaží prenasledovateľ priblížiť k obeti priamo alebo pomocou okolia, pričom ju obťažuje , narúša jej súkromie, dokonca môže vzbudzovať strach. Kyberšikanovanie postupne prerastá do závislosti na samotnom zbieraní dát o konkrétnom človeku. Cieľom býva samotné naplnenie závislosti alebo bližší vzťah s obeťou alebo negatívny finančný dopad na obeť. Obeť sa dostáva do nežiadúcich situácii, keď sú jej osobné údaje a osobné údaje jej blízkych osôb verejne prezentované alebo zneužívané na ďalšie získavanie údajov, či nadviazanie komunikácie.

Často sa objavuje nadväzovanie kontaktov *stalkera* (prenasledovateľa) s okruhom blízkych ľudí obete a postavením *stalkera* sa do polohy obete, aby manipuláciou stiahol blízky okruh ľudí obete na svoju stranu. Týmto správaním sa vytvára zložitá sieť kontaktov a poloprávd a klamstiev. Niekedy sa takýto typ kybernetického šikanovania označuje *stalking by proxy*.

Existuje špeciálna forma kybernetického šikanovania na zakázku, v tomto prípade kyber-stalker zbiera o obeti údaje na objednávku a odovzdáva ich následne tretej osobe. Tento spôsob je bežný pre politickú a priemyselnú realitu (napr. z dôvodu odstavenia konkurencie).

Fázy kybernetického šikanovania

- Získavanie všetkých dostupných údajov bez vedomia obete alebo stretnutia s obeťou.
- Približovanie sa k obeti, sledovanie a často aj dokumentovanie stretnutí.
- Psychický nátlak
    - zverejňovanie údajov, napr. súkromných detailov, osobných detailov s intímnym charakterom,
    - objednávanie tovarov a služieb na adresu obete,
    - ničenie majetku.
- Fyzický kontakt (klopanie na dvere, zvonenie, časté „náhodné“ stretnutia).

Rozdelenie stalkerov

- známy človek (spolupracovník, kamarát, spolužiak),
- neznámy človek (kyber-stalker, osoba s ktorou sa poznáte len sprostredkovane).

Negatívne prejavy a formy kybernetického šikanovania

- demonštrovanie moci fyzickou blízkosťou,
- vyhrážanie sa obeti,
- aplikácia vyhrážok,
- manipulácia okolia obete (*stalker* sa v tomto prípade vydáva za obeť),
- poškodzovanie dobrého mena obete.

Delenie stalkerov [4]

- Uctievač - snaží sa o intímny vzťah s idealizovanou obeťou, hľadá dôkazy o láske, ktoré aj nachádza. Ak si uvedomí pravdu, vzniká riziko agresie.
- Neobratný nápadník – stalkingom vyrovnáva frustráciu z interpersonálnych vzťahov. Správa sa majetnícky, bez empatie, ide mu o seba.
- Ublížený útočník – obeť je prostriedok na naplnenie túžby po pomste, obeť je náhodná a predstavuje odplatu za prežité krivdy.
- Sexuálny útočník – občasná forma, útočníkovým cieľom je sexuálne uspokojenie, anonymita zvyšuje pôžitok *stalkera* z útoku.

Odporúčanie: So stalkerom a s jeho aktivitami je nevyhnutné skoncovať čo najskôr po odhalení a zabrániť tak možnosti prerastenia kybernetického prenasledovania do závažného trestného činu.

3.1 Bezpečnostné pohľad

Odporúčania pre zaručenie bezpečnosti obete je nevyhnutné vytvárať a stavať na základe odbúrania anonymity útočníka, pochopenia útoku a vytvorenia formy najlepšej ochrany.

3.2 Základné bezpečnostné odporúčania

Základné bezpečnostné opatrenia na ochranu proti kybernetickému šikanovaniu sú zamerané na minimalizáciu údajov na internete o konkrétnej osobe, sprístupnenie týchto údajov len obmedzenej skupine známych osôb a vzájomnému informovaniu o abnormálnych prejavoch záujmu o niektorú osobu v skupine. Cieľom je neprezrádzať citlivé údaje širokému okruhu ľudí a rýchle rozoznanie potenciálneho útočníka.

Zdieľanie informácii na sociálnych sieťach je potrebné obmedziť len na minimálnu skupinu dobre známych adresátov. Napr. správy od neznámeho krásneho mladého chlapca (milé, láskyplné, imponujúce) pre mladé dievča, môžu pochádzať od úplne iného človeka, pretože internet zabezpečuje anonymitu.

Okruh blízkych známych by mal poznať správanie konkrétneho človeka a mal by vedieť rozoznať na základe tohto správania prejavy útočníka. Zároveň je nevyhnutné vytvoriť prostredie na zdieľanie informácii medzi známymi osobami o abnormálnych prejavoch záujmu niektorej osoby.

3.4 Expertné bezpečnostné odporúčania - trestný zákon

V prípade, že sa nedarí zamedziť kybernetickému šikanovaniu zo strany obete je nevyhnutné, aby sa obeť obrátila na orgány činné v trestnom konaní. V kontexte zákona poznáme a vieme uplatniť pojem: nebezpečné prenasledovanie.

Nebezpečné prenasledovanie (§ 360a): Kto iného dlhodobo prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že a) sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe, b) vyhľadáva jeho osobnú blízkosť alebo ho sleduje, c) ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli) zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu, alebo e) ho inak obmedzuje v jeho obvyklom spôsobe života, potrestá sa odňatím slobody...

Objektívna stránka citovaného trestného činu spočíva v dlhodobom prenasledovaní, ktoré je spôsobilé vzbudiť u iného obavu o jeho život alebo zdravie, život alebo zdravie seba, či blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života. Zo subjektívnej stránky trestného činu sa vyžaduje jeho úmyselné zavinenie. Z aplikačnej praxe sa pri citovanom trestnom čine je nevyhnutné zaoberať sa posúdením a vyhodnotením pojmových znakov: dlhodobo, dôvodná obava a podstatný spôsob zhoršenia kvality života.

4 Obranné postupy

Obrana proti kybernetickému šikanovaniu je zložitá. Internet zabezpečuje útočníkovi anonymitu. Nevýhodou je, že z rovnakého dôvodu je pre obeť neznámy samotný začiatok útoku. Pri kybernetickom šikanovaní alebo podobných formách prenasledovania prevencia v zásade neexistuje. Páchateľom môže byť ktokoľvek a spúšťačom môže byť čokoľvek. Obranné postupy je možné aplikovať až následné pre riešenie konkrétneho kybernetického šikanovania. Na prevenciu kybernetického šikanovania môžeme využiť kontrolovanie informácii, ktoré zverejňujeme o sebe a včasnú vzájomnú informovanosť v rámci komunity, ktoré sme popísali v kapitole 3.2.

4.1 Základné obranné postupy

Dôležité je ako rozoznať kybernetické šikanovanie, existuje niekoľko návodov. Jedna z možností je uvedomiť si a rozoznať jednotlivé fázy ktorých sme popísali v kapitole 3.Každá fáza je naviazaná na nevyhnutný krok a tým je identifikácia obete. Obeť sa identifikuje tým, že chovanie prenasledovateľa u nej vyvoláva obavy, o seba (o zdravie, o život), o blízkych, alebo o majetok. V takomto prípade je najdôležitejšie *veriť svojim inštinktom* a silná podpora okolia obete.

Silným negatívnym prvkom správania okolia obete je to, že okolie nerozumie obeti, nerozumie všetkým formám a dopadom útokov, preto sa snaží situáciu potlačiť a žiada ignorovanie prenasledovateľa samotnou obeťou. Toto správanie okolia je veľmi nebezpečné a prináša okrem uvoľňovania priestoru pre prenasledovateľa aj závažný problém zneistenia obete a následného zmierlivého, defenzívneho vystupovania obete, ktoré môže viac podporiť aktivity prenasledovateľa.

4.2 Best practice (zlatá stredná cesta z pohľadu bezpečnosti)

Ochrana pred kybernetickým šikanovaním [1]

- Dajte vedieť prenasledovateľovi, že o neho nestojíte, ale len raz a práve raz.
- Príklady:
    - Nemám záujem s Vami o vzťah, viac ma nekontaktujte.
    - Nevolajte, nepíšte mi, nekontaktujte ma žiadnym spôsobom.
    - Nekontaktujte ma, ak to urobíte znovu alebo sa objavíte v mojom dome zavolám políciu.
    - Nehovor viac čo som robila včera alebo moje údaje pred spolužiakmi, ak to urobíš, budem to riešiť s triednou učiteľkou.
- Nekomunikujte so stalkerom.
    - Ak vám stalker zavolá, zložte ihneď ako ho spoznáte, bez prejavu emócii.
    - Ak viete, že volajúci je stalker, nedvíhajte telefón.
- Nestretávajte sa so stalkerom.
- Dokumentujte si všetky prejavy obťažovania.
    - Ukladajte si telefonáty, správy, odkazy, vyhrážky.
- Rozprávajte sa o vašej situácii s priateľmi a blízkymi.
- Meňte svoje správanie v závislosti od prenasledovania.
- Uvažujte nielen nad tým, čo sa stalo, ale pripravte sa aj na ďalšie kroky prenasledovateľa.

- Zmeňte svoje návyky a pravidelnosti v správaní, ako je napr. cesta do školy, do práce, obchody, ktoré navštevujete.
- Nebuďte osamote, a to nielen z dôvodu vašej bezpečnosti, ale aj pre prípad svedectva, ktoré by mohlo potvrdiť správanie útočníka.
- Dôsledne kontrolujte a sledujte svoju internetovú komunikáciu, najmä však
    - sociálne siete ,
    - emailove kontá,
    - uverejňovanie fotografií.
- Nahlasujte útoky na polícii, aby boli zdokumentované aj úradne.
- Podajte trestné oznámenie, ak sa naplní dôvod podania.
- Noste so sebou mobilný telefón pre prípad potreby zavolania pomoci.
- Využite sociálne poradenstvo a linky pomoci.
- *Žite ďalej svoj život!, ak využijete kompromisy pri boji s prenasledovateľom, je len na Vás aké si vyberiete*.

5 Spôsoby útokov

Stalking sa dá charakterizovať, ako zlovoľné, úmyselné a systematické prenasledovanie a obťažovanie inej osoby, ktoré u obeti znižuje kvalitu života a ohrozuje jej bezpečnosť. Pri stalkingu obeť cíti strach, nervozitu, obťažovanie a nebezpečenstvo. [6]

Prenasledovatelia využívajú rôzne možnosti stretávania sa s obeťou. Cieľom je získavať všetky možé údaje o obeti, alebo nadväzovať komunikáciu. Spôsoby prenasledovania obete stalkermi/ prenasledovateľmi, resp. stalkeri pri prenasledovaní môžu:

- Kontaktovať kolegov a blízkych obete.
- Bez prestania kontaktovať obeť.
- Ukazovať sa obeti.
- Chodiť a čakať pri dome obete.
- Pozývať sa ku Vám domov.
- Poškodzovať majetok.
- Hacknúť WiFi sieť a sledovať komunikáciu obete.
- Vypnúť elektrickú energiu, internet pre obeť.
- Posieľať darčeky.
- Inštalovať kamery a monitorovať obeť.
- Sledovať obeť pomocou GPS, SpyWare alebo sociálnych médií.
- Hacknúť sa do účtov obete.

- Zdieľať súkromné obrázky, videá a komunikáciu obete.
- Filmovať a fotografovať obeť bez súhlasu.

6 Deti ako cieľ kybernetického šikanovania

Kybernetické šikanovanie je v súčasnosti stále ešte relatívne nový prístup prenasledovania s veľkou možnosťou variability a rozvoja. Často sa stávajú obeťou nielen dospelé osoby, ale aj žiaci a učitelia. Medzi deťmi sa prejavuje prenasledovanie hlavne pri riešení problémov so vzťahmi (chlapec dieťa ale aj medzi kamarátkami a kamarátmi). Často si kybernetickí prenasledovatelia hľadajú obete za prežité krivdy.

Štandardom sa stáva kybernetické šikanovania vo forme hry vo virtuálnom priestore. Pri hraní hier jednotlivec alebo skupina hráčov sa v takomto prípade zameria na obeť a pomocou komunikačnej platformy hry získavajú údaje, nadväzujú komunikáciu a vytvárajú tlak na obeť. Samotný zápal z hry podčiarkuje a zvýrazňuje využívanie komunikácie s obeťou. V takomto prípade hrozí nebezpečenstvo prerastenia nevinného záujmu do kybernetického šikanovania.

6.1 pohľad psychológa vzhľadom na útočníka

V prípadoch, keď ide o premyslenú činnosť, ktorej motív je uvedomovaný, stalking páchajú najmä jedinci s poruchami osobnosti. Najčastejšie ide o osobnosti s disociálnymi, paranoidnými, narcistickými, schizoidnými, obsedantnými či emočne nestabilnými charakteristikami. Väčšinou krátkodobo sa stalking môže objaviť ako reakcia na prežitý závažný životný stres (najčastejšie rozchod/rozvod) aj u osôb, ktoré netrpia žiadnou diagnostikovateľnou psychickou poruchou. [5]

Cyberstalking však niektorí stalkeri definovali ako kreatívnu činnosť, ktorá ich napĺňa a sami seba ako zvedavých a ambicióznych ľudí. [7]

6.2 ako rozoznať obeť?

Obeťou môže byť ktokoľvek, kto vyhodnotí správanie prenasledovateľa subjektívne ako obťažujúce, či ohrozujúce. Kybernetické šikanovanie má negatívny vplyv na sociálny a profesionálny život, kumuluje negatívne pocity z dôsledkov správanie útočníka. Často sa stáva, že okolie obete nerozumie obeti a nechápe jej pocitom. Dôsledok môže byť depresia, pocit bezmocnosti, sebaobviňovanie, úzkostné vzťahy.

Dôsledky kybernetického prenasledovania:

- psychické problémy,
- problémy v škole (zhoršený prospech, psychosomatické problémy..),
- stres, depresie, úzkosť, poruchy spánku,
- sociálne problémy (odmietanie kolektívu, nedôvera k ľudom a sociálnu izolácia),
- fyzické ujmy – útoky na osobu, ublíženie na zdraví.

Záver

Nové technológie prinášajú skvalitnenie života ale aj nové hrozby. Prenasledovanie je vlastné ľudstvu už stáročia, technológie ho umožnili preniesť do virtuálneho priestoru. Prenasledovateľom zároveň množstvo údajov v internete a anonymita umožňuje lepšie cielenie útoku.

Téma kybernetického šikanovania je komplexná a každý útok je nevyhnutné analyzovať a vyhodnocovať samostatne. Rozoznať, že útok, prenasledovanie začalo a ktoré jednotlivé formy a akým spôsobom sú využívané je veľmi zložité a často nemožné. Samotná obeť si často nechce pripustiť, že je prenasledovaná. Útočník môže byť z rozličného prostredia od úplného neznámeho až po blízkeho človeka. Stáva sa, že ak je útočník blízka osoba, samotná blízkosť útočníka obmedzuje správnosť, razantnosť a adresnosť odpovedí zo strany obete. Z týchto dôvodov je veľmi ťažké voliť správne formy ochrany a zamedzenia útoku a obrany obete. Pri voľbe jednotlivých krokov je neustále potrebné mať na pamäti samotnú obeť, udržanie psychickej pohody obete, spoločenské a pracovné postavenie a aj samotnú ochranu obete.

Každé kybernetické šikanovanie je možné obmedziť alebo odraziť za predpokladu, že sa nebojíme podniknúť jednotlivé kroky aj za cenu krátkodobého zníženia svojho komfortu alebo komfortu blízkeho okolia. Nevyhnutným predpokladom je nebáť sa podniknúť jednotlivé kroky na prevenciu kybernetického šikanovania.

Zdroj

[1]https://eduworld.sk/cd/beata-tancsakova/5979/stalking--nekonecne-prenasledovanie-ktore-nici-zivot (15.06.2019)

[2] http://www.psychiatriapreprax.sk/index.php?page=pdf_view&pdf_id=7422&magazine_id=2 (15.06.2019)

[3] Čírtková Ľ. Moderní psychológie pro právníky. 1. vyd. Praha,Czech Republic: Grada Publishing; 2008.

[4] Mullen PE, Pathé M, Purcell R, et al. Study of Stalkers. Am J Psychiatry. 1999;156(8):1244–1249.

[5] http://www.psychiatriapreprax.sk/index.php?page=pdf_view&pdf_id=7422&magazine_id=2 (30.06.2019)

[6] http://www.pravnelisty.sk/clanky/a554-stalking-trestny-cin-nebezpecneho-prenasledovania (30.06.2019)

[7] https://fici.sme.sk/c/20833286/rozhovor-s-kyberstalkerkou-sledovat-sa-da-aj-ludi-ktori-nie-su-na-socialnych-sietach.html (30.06.2019)

Ako použiť linky detskej pomoci?

1. Téma, ktorú kapitola prináša

Zoznam a spôsob použitia liniek detskej pomoci.

2. Okruhy, ktoré vysvetľuje

Úloha liniek detskej pomoci je riešiť kritické situácie, do ktorých sa deti dostávajú. Linky na ochranu detí sú voľne k dispozícii. Pri využívaní je nevyhnutné poznať jednotlivé zamerania liniek, spôsoby kontaktu, rozumieť dôvodom, kedy kontaktovať a identifikovať spôsoby komunikácie s linkami.

Cieľom nie je nahradzovať úlohu rodičov alebo riešiť problémy, ktoré sa stali na verejnosti. Cieľom je pomôcť deťom a rodičom, keď si nevedia rady a odstrániť pasívny prístup ku problémom. Prevencia pasívneho prístupu a prekročenie rozšírenie okruhu riešenia vlastných problémov mimo vlastnej osoby a nad rámec vlastného záujmov, vie zásadne ochrániť ľudí vo Vašom okolí. Významným cieľom sa javí postavenie liniek v úlohe partnera pri riešení problému alebo pri jednoduchom vypočutí a porozumení problému.

Nemenej dôležitým cieľom je rozoznanie páchania trestnej činnosti. Úlohou liniek je v prípade identifikovania, že volajúcemu hrozí nebezpečenstvo, upovedomiť o tom záchranné zložky a požiadať ich o pomoc.

3. Definície

Úlohou liniek na ochranu detí je pomáhať deťom a rodičom, ktorí sa ocitnú v situácii, s ktorou si nevedia rady a nevidia východisko. Na linky sa môžu obracať deti, rodičia, dospelí, pedagógovia, zdravotníci.

Zameranie liniek:

- Prevencia nežiadúcich javov
- Hľadanie riešenia v krízových situáciách

Pre dieťa aj dospelých je veľmi dôležité sledovať a všímať si svoje okolie, či sa nemení správanie jednotlivca a ak, tak akým spôsobom. Častým indikátorom je utiahnutie do seba, poruchy spánku, problémy s komunikáciou.

4, Príklady využitia liniek

Potreba komunikovať s linkami, ktoré sú určené pre detskú pomoc, sa dá rozdeliť nasledovne:

Pohľad dieťaťa:

- Osobné
    - Vzťahy
        - Sme tri nerozlučné kamarátky, strašne ma rozčuľuje, že Janka a Marka sa viac navzájom objímajú a smejú, ako so mnou.
        - Bojím sa vystupovať pred ostatnými a komunikovať s novými ľuďmi.
    - Láska
        - Stretli sme sa s chalanom, dotýkali a spali pri sebe, viac sa neozval, ľúbi ma?
        - Sused tretiak je zaľúbený do mňa ôsmačky, čo s tým?
    - Sex
        - Moja sestra sa vyzývavo oblieka a nahlas masturbuje, čo mám robiť?,
    - Depresia
        - Mám 13 rokov a výrazné ochlpenie.
        - Dostal som sólovú 3jku zo zemepisu, naši o tom nevedia, otec ma asi zabije.
        - Čo je zmysel života? Pretože moja budúcnosť je len negatívna.
        - Pred písomkou som v strašnom strese a robím hlúpe chyby, ja však nie som hlúpy!
    - Osamelosť
        - Som lezba a všetci sa mi vyhýbajú.
        - Môj brat sa prestal so mnou rozprávať, už to trvá 15 dní.
        - Nikto nechce so mnou ísť do mesta počas Silvestrovskej noci.
    - Sebadôvera
        - Mám malé prsia.
        - Hanbím sa za postavu.
        - Prezliekanie na telesnej je nočná mora, mám vždy najhoršie spodné prádlo.
    - Závislosť
        - Začal som fajčiť, viem že to je zlé, ale neviem s tým skončiť, upokojuje ma to.
        - Idem na chatu, spolužiaci tam budú mať marišku, ako sa jej dá vyhnúť?

- Zdravie
  - Prehrávam boj s anorexiou, dá sa to vlastne vyhrať?
  - Prvý menzes, čo mám robiť?!
  - Veľa sa potím, a strašne to smrdí, existuje nejaké riešenie?
  - Môžem spať s podprsenkou?
  - Asi mám zlomený prst, ale ak mi dajú sadru, nepôjdem na sústredenie, nechcem to prezradiť.
  - Moje nohy vyzerajú hrozne, na každej nohe mám zrastené dva prsty, čo s tým?
- Zneužívanie
  - Pri prezliekaní na telesnej mi pán učiteľ veľmi pomáha a mne sa to nepáči.
- Škola
  - Mám problémy s učiteľkou.
  - Spolužiaci sú na mňa odporní.
  - Záchody sú špinavé a ja sa ich bojím používať,
  - O čom mám komunikovať so spolužiakmi v triede? Neviem nájsť témy.
- Šikanovanie
  - ubližovanie, bitka, urážanie, znevažovanie,
  - Stále mi schovávajú veci na telesnej a potom ich polonahá musím hľadať.
  - Moje kamarátky sa so mnou prestali rozprávať a zakazujú to aj tým, čo sa so mnou rozprávať chcú.
  - Mám problém s nadváhou, v škole je to ťažké, rozmýšľam nad samovraždou.
- Problém s napĺňaniami požiadaviek
  - rodičov, učiteľov, starý rodič,
  - Strašne rada behám, ale žiaden iný šport ma nezaujíma.
- Problém so zapájaním sa do kolektívu
  - Dievčatá, ako zvládate Veľkú noc? Ja ju nenávidím.
  - Môj spolu sediaci v lavici často smrdí.
  - Spolužiak mi kupuje rôzne veci, nechce so mnou chodiť, robí to zo slušnosti a mne nedovolí nič kúpiť, ako sa mu odvďačiť tak, aby sa neurazil?

- Rodina
    - Týranie
        - Mama je šikanovaná a bitá otcom alkoholikom.
    - Hádky
        - Doma sa rodičia sústavne hádajú a ja sa potom bojím.
        - Chcem ísť na jarnú lyžovačku s kamošmi a rodičia ma nechcú pustiť, vždy, keď to otvorím, doma je hádka.
    - domáce násilie
        - Minula som peniaze určené na školský výlet na telefón, ako to povedať doma?
        - Ležím doma s chrípkou, nudím sa a nič sa mi nechce, keď sa však nebudem učiť, mama ma zbije.
    - zneužívanie
    - problém s financiami
        - Rodina ledva prežíva od výplaty ku výplate,
    - Neporozumenie si
        - Psychiatrička mi povedala, že trpím depresívnou poruchou, povedala som mame, že sa cítim zle, ale ona ma odmieta.
- Kamaráti
    - To isté, čo pri osobnej kategórii vztiahnuté na kamaráta,
    - Uzatvorenie spolužiaka (vztiahnutie sa do seba a ustávanie, viaznutie komunikácie),
    - Problém s omamnými a psychotropnými látkami.

Pohľad rodiča/dospelého:

- Dieťa sa uzavrelo, zhoršilo prospech, prestalo komunikovať s okolím.
- Sociálne zmeny:
    - nezaopatrené dieťa, opustené a túlajúce sa po večeroch,
    - Ruch u susedov: napr. krik dospelých a detský plač
- Konzultovanie správania detí a starostlivosti o deti.
- Dopad rozvodu rodičov na dieťa.
- Problémy v rodine, v škole a ich dopad na dieťa a hľadanie riešenia.
- Problémy s výchovou dieťaťa.

Kedy nevolať

- Nuda
- Hra
- Zábava

Prečo nevolať, ak nemám problém?

- Blokovanie linky môže ovplyvniť životy iných

5 Zoznam liniek

Linky dôvery pre deti

Detská linka záchrany 0800 123 232, 0800 121 212, 0820 434 343
Linka detskej istoty, LDI - UNICEF 116 111
Linka detskej dôvery 0800 117 878
Linka detskej dôvery - LIENKA 0800 112 878
Linka detskej pomoci 0800 100 444
Linka dôvery Košice 055/ 622 2323, 055/ 644 1155
Linka dôvery Prešov 051/ 7731 000

Psychologické poradne

Linka dôvery nezábudka 0850 11 10 22
Linka nádeje 055/ 644 11 55

Linky pomoci proti násiliu

Ambulantné krízové stredisko 0800 500 500
Linka pomoci obetiam násilia 0850 111 321
Linka pre nezvestné a sexuálne zneužívané deti 116 000
Pomoc ohrozeným deťom 02/ 62 24 78 77

Všetky linky na Slovensku: https://www.zdravie.sk/clanok/27634/telefonicke-linky-pomoci

5.1 Minimálne bezpečnostné odporúčanie

Linky sa nesmú zneužívať na hranie alebo zábavu, pretože slúžia na záchranu ohrozených detí.

6 Pohľad na obete

Obete reagujú na deje, v ktorých participujú ale aj na aktuálnu situáciu v spoločnosti. V prípade prázdnin sa orientujú komunikácie na trávenie voľného času a stretávanie s kamarátmi a riešenie problémov pri záujmoch. Deti sa zameriavajú nielen na svoje osobné problémy, ale aj problémy v rodine a problémy kamarátov. Napríklad v prípade významných sviatkov sa orientuje komunikácia na osamelosť.

Sociálny inžiniering, útok s veľkým dopadom

1. Téma, ktorú kapitola prináša

Sociálne inžinierstvo je spôsob manipulácie ľudí a účelom neoprávneného získania určitej informácie.

2. Okruhy, ktoré vysvetľuje

Zameranie sociálneho inžinierstva na napadnutie a zneužitie základných osobnostných nastavení človeka.

3. Základné predpoklady:

Sociálne inžinierstvo sú systematicky používané vedomosti ľudského chovania a umenia presviedčať, aby užívateľ urobil to, čo by za normálnych okolností, pri dodržiavaní všetkých bezpečnostných pravidiel nikdy neurobil. Tým sú samotným ľudským faktorom prelomené technologické a organizačné bezpečnostné opatrenia a je umožnený kybernetický útok.[1]

Sociálne inžinierstvo je jedným z najnebezpečnejších spôsobov útoku, napriek tomu, že nevyžaduje veľké technické zručnosti, je zamerané na človeka. Hacker využíva inteligenciu a znalosť osobnosti človeka. Hlavné ciele využívania sociálneho inžinierstva je možné kategorizovať nasledovne:

- Spáchanie podvodu,
- Obohatenie sa,
- Narušenie systému alebo siete,
- Priemyselná špionáž,
- Krádež identity,
- Pomsta,

Vhodnými cieľmi sa javia veľké firmy s významným dopadom na obyvateľstvo, ako sú: operátori (internetu a telefonickí), finančné inštitúcie, vládne a vojenské agentúry, nemocnice.

Výhoda útoku je v jednoduchom prístupe k veľmi dobre ochráneným informáciám. Napr. namiesto zložitého prieniku do dobre zabezpečeného systému, hacker zatelefonuje vhodnej osobe a vypýta si prístupové oprávnenia. Základný kameň na naštartovanie útoku sociálnym inžinierstvom je vzbudenie dôvery. Pred samotným útokom si útočník zistí potrebné informácie o obeti prostredníctvom verejne dostupných zdrojov (sociálne siete, blogy, firemné stránky, tlačové správy, webové komunity, reporty, konferencie,...). Prípadne sa snaží dostať do jednotlivých objektov a získať údaje priamo z objektov odpozorovaním, prezeraním košov, náhodným alebo cieleným ukradnutím. Nasleduje analýza a príprava útoku. Cieľom útoku je zneužitie slabín obete, kam patrí nízke bezpečnostné povedomie, nepoznanie interných pravidiel organizácie, ochota pomáhať, možnosť umiestňovania citlivých informácii na sociálne média.

Techniky sa delia

- Tvrdé – využívajú ľudskú slabosť, labilnosť, frustráciu, pomstychtivosť , škodoradosť, závisť.
- Mäkké – zakladajúce sa na zneužití ľudskej dôverčivosti

Sociálne inžinierstvo sa delí

- Fyzické: prechádzanie cez kancelárie a prehľadávať stoly, odpadky, zabudnuté telefóny,..
- Virtuálne: kontaktovanie potenciálnych obetí vzdialene (telefón, sms, email) a získavanie osobných dát.

Popis útoku technikami sociálneho inžinierstva:

- Zhromažďovanie informácii
- Budovanie vzťahov a dôvery
- Využitie dôvery
- Realizácia a zneužitie

Počas útoku pomocou sociálneho inžinierstva sa využívajú vlastnosti ľudí, ktoré sú pokladané za dobré vlastnosti, napríklad:

- Dôvernosť
- Ľútosť
- Láskavosť
- Zvedavosť
- Ochota pomáhať

3.1 Priblíženie jednotlivých útokov

Trashing

Je to metóda založená na prehľadávaní odpadkových košov a získania citlivých informácii z dokumentov alebo zabudnutých, či starých dátových nosičov (USB, CD, starý mobil).

Pretexting

Pretexting je spôsob manipulácie obete s tým, že útočník skontaktuje obeť a zahrnie ju informáciami, pričom časť informácie je pravdivá a overiteľná a druhá časť klamlivá. Informácie, ktoré obeť dostáva sú presne adresované a ich súslednosť je kontrolovaná útočníkom. Cieľom je presvedčiť obeť o legitímnosti požiadaviek alebo o opravu nepravdivých informácii s cieľom získať presné, citlivé informácie. Technika útokmi narába s technikami rétoriky. Je využívaná nielen útočníkmi, ale aj súkromnými detektívmi a v bežnej životnej a školskej praxi. Na implementáciu je potrebná príprava a zozbieranie vhodných informácii, sú známe prípady, keď nebolo potrebné vedieť priveľa údajov, stačilo využívať autoritatívny tón a presvedčivý obsah konverzácie. Útok je presne cielený so zameraním na konkrétneho človeka alebo malú skupinu ľudí a cieľom je získanie konkrétnych informácii.

Phishing

Podvodná technika, ktorá využíva internetové prostriedky na získavanie citlivých údajov ako sú heslá, čísla kariet, osobné údaje. Princípom je dostať adresátovi podvodnú správu s cieľom vymámenia citlivých údajov, častom sa ako odosielateľ vydáva samotná firma, ktorej klienti sú terčom útoku. Phishing je orientovaný primárne na klienta firmy, nie na firmu samotnú. Príprava útoku je jednoduchá a útok je vedený plošne na všetky dostupné kontakty s malou mierou správneho smerovania komunikácie, v prípade zasiahnutia dôverčivej obete sa počíta s vysokým ziskom.

IVR phishing

Útočníci vytvoria falošný odpovedací telefónny automat, s podobnou štruktúrou ako konkrétna firma (napríklad odpovedajúca služba finančnej organizácie). Automat je vystavený na podobnom čísle ako originálna inštitúcia a obeť je vyzvaná na zavolanie do banky na priložené telefónne číslo. Počas komunikácie sú od obete vylákané prihlasovacie údaje a následne zneužité. Príprava útoku je zložitá, následne záleží na výbere obete, na ktorú bude vedená komunikácia, útok sa využíva len vo veľmi špecifických prípadoch.

Spear phishing

Útočník vytvára komunikácie prostredníctvom elektronických komunikačných prostriedkov a vydáva sa za dôveryhodnú osobu. Útočník sa vydáva za prepravné spoločnosti, finančné inštitúcie, či iné dôveryhodné organizácie (ako napríklad pošta), posiela adresné emaily sc ieľom zasiahnuť klienta a potenciálnu obeť, vmanipulovať ju do stavu, že prezradí citlivé údaje. Všetky informácie v emaile musia byť uveriteľné a napísané a doručené spôsobom, ktorý je používaný organizáciou. Často ide o priamy útok s cieľom zmanipulovať obeť do poslania peňazí na určené konto (*CEO fraud – spear phishing*, pri ktorom sa útočník vydáva za riaditeľa firmy a manipuluje obeť do poslania peňazí na konkrétny účet). Útok s veľkým dopadom je, keď obeť vmanipuluje útočník k inštalácii, či spusteniu vírusu na zariadení organizácie. V tomto prípade ide útočníkovi o získanie prístupu na pracovnú stanicu alebo to robí s cieľom urobiť organizácii čo najväčšiu škodu, napríklad zašifrovaním pracovných diskov. Útok je orientovaný na úzku skupinu potenciálnych obetí. Úspešnosť útoku závisí od dôverčivosti obete.

Baiting

Útočník nechá záznamové médium (CD, DVD, USB) na mieste, kde ho obeť ľahko nájde, využije zvedavosť obete, ktorá toto médium vloží do svojho počítača a nakazí ho nežiadúcim kódom. Nežiadúci kód sa automaticky snaží prihlásiť do internetu. Cieľom útočníka je získať prístup do počítačovej siete. Príprava útoku je stredne zložitá, útok je vedený plošne na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie. Správna funkcia závisí od bezpečnostnej ochrany počítačového prostredia konkrétnej firmy (ak sa vírus nespustí z USB, nebude útok fungovať).

Quid pro quo (niečo za niečo)

Útočník zistí telefónne čísla spoločnosti a začne telefonovať na všetkým potenciálnym obetiam, pričom sa tvári ako technická podpora a pýta sa, ako vie pomôcť zamestnancovi. S vysokou pravdepodobnosťou nájde zamestnanca, ktorému sa nedostáva pomoc a preto rád pomôže technickej pomoci/útočníkovi spustením programu alebo špeciálnou akciou v informačnom systéme organizácie. Príprava útoku je stredne zložitá, útok je vedený na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie, používajú sa techniky rétoriky.

Watering holes

Jedno z technicky zložitejších foriem sociálneho inžinierstva. Podmienkou je vytipovať si vhodný typ obetí, následne nájsť webovú stránku s vysokou mierou dôvery pre danú skupinu

a infikovať / kompromitovať webovú stránku vírusom. Využíva sa hlavne technika „drive-by download“, t.j. technika stiahnutia víru bez potreby alebo len s minimálnou potrebou interakcie s obeťou. Príprava útoku je stredne zložitá, útok je vedený plošne na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie. Úspešnosť útoku závisí od bezpečnostnej ochrany počítačového prostredia konkrétnej firmy (ak sa vírus nespustí z WEBu, nebude útok fungovať).

Reverzné sociálne inžinierstvo

Štandardné sociálne inžinierstvo znamená kontakt útočníka s obeťou, reverzné sociálne inžinierstvo vytvára podmienky tak, aby obete vyhľadali útočníka. Cieľom je zmanipulovať obeť tak, aby sama pokladala útočníka za osobu z dôveryhodnej organizácie a vie pomôcť s problémom, ktorý sám útočník vytvoril. V tomto prípade obeť úplne dôveruje útočníkovi a preto je náchylná na poskytnutie akýchkoľvek dôverných údajov.

Príprava útoku je veľmi zložitá, následne záleží na výbere obete, na ktorú bude vedená komunikácia, útok sa využíva len vo veľmi špecifických prípadoch.

Podvodné lotérie

Sú to lotérie, najmä „vyskakovacie“ okná, kde sa aplikuje útok na dôverčivosť obete. Útočník ponúkne výhru (napr. nový mobilný telefón alebo notebook), obeť sa musí prihlásiť do systému pomocou svojich pravých údajov, poprípade zaplatiť kartou účastnícky poplatok. Útočník týmto spôsobom získa prístup k osobným aj platobným dátam.

Lotérie sa prenášajú v súčasnosti do sociálnych médií a orientujú sa hlavne na obete z radov detí a ľudí s nízkym bezpečnostným povedomím. Príprava útoku je veľmi zložitá, úspešnosť závisí od spôsobu komunikácie s obeťou. Útok s rozšírením sociálnych sietí sa objavuje stále častejšie. V prípade sociálnych sietí je technická náročnosť prevedenia útoku veľmi nízka, k útoku je potrebná len anonymná adresa na sociálnej sieti.

4 Bezpečnostné odporúčania

Neexistuje komplexná, priama ochrana pred jednotlivými typmi útokov. Ochrana sa zameriava na ochranu technického perimetra, tak, aby sa zabránilo prieniku škodlivého kódu do vnútra organizácie. Hlavnou ochranou je sústavné zvyšovanie bezpečnostného povedomia členov organizácie a jednotlivcov a nastavením pravidiel a procesov v prípade členov organizácie. V prípade útoku by mala každá potenciálna obeť vedieť, kam a komu sa má ozvať, v prípade pochybností pri komunikácii s externou osobou.

4.1 minimálne bezpečnostné opatrenia

Technická ochrana

- Používať len overený softvér s povoleným certifikátom.
- Používať len autorizované (známe zariadenia).
- Mať aktualizovaný antivírusový softvér, spamové filtre a posledné záplaty.
- Blokovanie neautorizovaných zariadení.
- Používanie len bezpečných sietí na pripojenie počítača a mobilných zariadení.

Procesná ochrana

- Sústavné zvyšovanie bezpečnostného povedomia dotknutých osôb.
- Rýchle, správne nahlasovanie hrozby pri útokoch typu Phishing a Spear phishing.
- Pripraviť vo firme bezpečnostné procesy na riadenie správania zamestnancov a nastavenie základnej úrovne bezpečnosti.
- Pripraviť a implementovať proces Incident menežmentu aj so zaučením pracovníkov na identifikovanie hrozby a rýchlom a správnom nahlásení hrozby.

4.2 základné

Nevyhnutným prostriedkom pre zabezpečenie ochrany je zadefinovanie kritických aktív a informácii v organizácii. Tieto údaje budú vstupnými informáciami pre vytvorenie komplexnej analýzy rizík. Na základe tejto analýzy je nevyhnutné implementovať ochranné technické prvky do prostredia a vytvoriť vzdelávaciu aktivitu, aby zamestnanci chápali dôležitosť aktív a informácii a spôsob ich ochrany, musia vedieť rozoznať útok a reagovať na útok.

5 Psychologické faktory

V prípade útoku systémom Sociálneho inžinierstva je veľmi dôležité rozprávať s obeťou psychologické postupy, ktoré zjednodušia nájdenie si cesty k obeti. Jednotlivé prístupy je nevyhnutné poznať, aby obeť mohla identifikovať prípadné použitie techniky.

Silný afekt

Ak obeť cíti silný hnev, alebo je prekvapená, rozrušená, či v panike, bude s menšou pravdepodobnosťou rozmýšľať o prezentovaných argumentoch. Afekt sa spúšťa vyslovením výroku, ktorý spustí príval emócii. Na tejto istej báze funguje kontrafaktuálne myslenie, v tomto prípade obeti je ponúknutá veľká výhra, následne obeť riskuje skutočný tovar, pričom ignoruje myšlienku, že pravdepodobnosť výhry je minimálna.

Preťaženie

Útočník rýchlo za sebou odovzdá veľa informácii naraz, pričom zahltí obeť a tá nevie rozlíšiť mylné predpoklady od presvedčivých banalít a postaví sa do polohy, radšej absorbuje informáciu, akoby ju vyhodnotila. Rovnako funguje argumentácia z nečakanej perspektívy. Obeť potrebuje čas na vytvorenie argumentácie, ktorý sa obeti nedostáva. Má veľa informácii, nedostatok argumentov a je ochotná prijať aj argumenty, ktoré by normálne odmietla.

Opätovanie

Opätovanie alebo reciprocita – útočník presvedčí obeť, že jej niečo dal a vyžaduje spätne vrátenú vec. Obeť často nevie rozlíšiť alebo nerozlišuje, že dar bol vynútený a že vrátená vec je oveľa hodnotnejšia. Vo firemnom svete je to nastavenie: ak niekto zatelefonuje a požiada o pomoc s problémom volajúci mu ochotne pomôže, dokonca je k tomu firmou nabádaný, potom je náchylný poskytnúť citlivé informácie ako poďakovanie za pomoc. Využíva to hlavne inverzné sociálne inžinierstvo. Druhý prístup: ak majú obeť aj útočník vážne požiadavky a útočník ustúpi, obeť bude mať tendenciu ustúpiť tiež. Útočníkovi stačí vytvoriť viac ako jednu požiadavku.

Klamlivé vzťahy

Útočník nadviaže kontakt s obeťou, ak komunikáciu nastaví tak, aby obeť uverila, že má s útočníkom podobné vlastnosti bude cítiť silný element komunikovať a jednať s útočníkom kladne a dôverovať mu bez opodstatneného dôvodu. Iným spôsobom je odhaľovanie obeti útočníkom svojho vnútorného nastavenia , prerozdelenie „tajných“ informácii, či diskutovanie o nepriateľoch. V oboch prípadoch je obeť rovnako náchylná prezrádzať citlivé informácie.

Rozšírenie zodpovednosti a morálne povinnosti

Obeť je vmanipulovaná, že svojou činnosťou a rozhodovaním ovplyvní úspech, či zlyhanie spoločnosti. Alebo zamestnanec, ktorý volá vie ovplyvniť zotrvanie v spoločnosti. V týchto prípadoch je pre obeť veľmi ťažké urobiť akékoľvek rozhodnutie a zamestnanec sa poddá útočníkovi.

Často je útok rozšírený o morálne povinnosti, t.j. útočník, ktorý volá robí niečo pre záchranu obete, preto obeť pomáha útočníkovi, často sa chce vyhnúť pocitu viny.

Autorita

Útočník sa vydáva za vysoko postavenú osobu, ak obeť nevyužije overenie útočníka alebo ak overenie nie je k dispozícii, bude útočník považovaný za kompetentnú osobu, ktorá môže získať citlivé údaje.

Bezúhonnosť a dôslednosť

Zamestnanci majú sklon pokračovať v práci na pracovisku aj keď majú podozrenie, že požiadavka nie je oprávnená. Ľudia majú tendenciu veriť ostatným, ak rozprávajú o svojich skutočných názoroch a rozhodnutiach, tendencia je primárne založená na ich čestnosti a vyjadrovaní pocitov.

Záver

Sociálne inžinierstvo je veľmi efektívnym nástrojom na získavanie citlivých informácii. Jeho najsilnejšou stránkou je zavádzanie prvkov, ktoré majú pôvod v psychológii do informačnej bezpečnosti. Takéto prepájanie rôznorodých oblastí je pre bežného človeka veľmi zložité správne vyhodnotiť. Zameranie útoku je na ľudí a je závislé výlučne od ľudí, budúcich obetí. Veľkým nebezpečenstvom je rôznorodosť útokov, od plošného útoku až po útoky na skupiny a jednotlivcov. Často sa pri útoku využívajú obranné prístupy jednotlivca a organizácie v prospech útočníkov. Podstatou útoku je využitie manipulačných techník útočníkom. Tieto techniky oscilujú od implementovania psychologických techník, po fyzické manipulatívne techniky, nie nezvyčajná je žiadosť o informácie od krásneho, múdreho, milého, mladého človeka.

Najlepšou obranou sa v súčasnosti javí využívať starodávnu múdrosť: „Dôveruj, ale preveruj.“ V prípade, že sú len trochu rozpoznané prvky sociálneho inžinierstva potenciálnou obeťou, mala by potenciálna obeť nastaviť komunikáciu do módu preverovania informácii a skontrolovania kontaktu nezávislou cestou. Nechýbať by Vám mala rozvaha, spomalenie pri odpovedaní a premýšľanie nad každou novou žiadosťou. Nebojte sa odložiť odpovede o niekoľko hodín. Každý útok je možné odraziť, sociálne inžinierstvo nevynímajúc, potrebné je len uchovať si rozvahu a „zdravý, sedliacky“ rozum a nadhľad.

Literatúra

[1] Rak, R. – Kummer, R. 2007. Informační hrozby v letech 2007-2017. In: Magazín Security, 2007, č. 1, s. 2 – 5.

Identifikácia útoku a ochrana pred útokmi typu Phishing

1. Téma, ktorú kapitola prináša

Informáciu o technike podvodného, neoprávneného získavania prístupu k údajom: Phishing. Technika je založená na podvodnej komunikácií s obeťou s cieľom získania citlivých údajov (osobných, bankových,firemných,...) od obetí. Počas phishingu útočník zvyčajne podvrhne falošný priestor, kde následne sa snaží zaviesť obeť a zozbierať citlivé údaje od obete alebo ju donútiť stiahnúť softvér na počítač obete.

2. Okruhy, ktoré vysvetľuje

Popis Phishingu a aj jeho špecifických typov útokov ako sú: Phishing, Spear Phishing, CEO fraud, Vishing, Smishing. Približuje spôsoby útoku, možnosti rozoznania útoku. Definuje dopady útoku. Navrhuje spôsoby ochrany pred útokom.

3. Definície

Phisnig je nebezpečný, lebo je jednoduché vykonateľný, pričom je možné využiť také formy útoku, ktoré nevyžadujú hlboké programovacie zručnosti. Nebezpečenstvo je o to väčšie, o čo viac útočníci využívajú prvky sociálneho inžinierstva a o čo presnejšie zasiahnu záujmy a postoje obete.

Phishing je druh podvodného konania, ktorým podvodníci sa snažia získať prístup k citlivým informáciam. Najčastejšie sú to prihlasovacie údaje (napr. do sociálnych sietí, elektronického prístupu do finančného domu, prihlasovacie údaje do zdravotnej poisťovne,...), citlivé informácie, ktoré sa dajú ďalej zneužiť alebo speňažiť (napr. špecifické osobné, firemné, údaje z karty, priamy zisk). Phishing využíva slabé stránky obeti. Útočníci sa snažia cielene navodiť situáciu dôvery alebo nájsť slabú stránku obete na ktorú zatlačia a tým získajú vysokú mieru angažovanosti obete.

3.1 Popis útoku

Prvým krokom je vytvorenie falošnej správy, najčastejšie je touto správou email. Cieľom falošnej správy je navodiť u obeti pocit, že musí niečo vykonať na svoju ochranu v rámci

konkrétnej webovej služby. Toto konanie sa dá naplniť buď priamym vyplnením dotazníka v tele správy alebo presmerovaním pomocou weboveho odkazu v správe na podvrhnutú webovú stránku. Následne je podvrhnutá správa distribuovaná plošne na všetky získané adresy alebo cielene.

Druhým krokom je vytvorenie podvrhnutej webovej stránke. V tomto prípade sa používajú sva spôsoby: buď je podvrhnutá webová stránka je podobná originálu alebo je vytvorená tak, aby podporila tlak na slabú stránku obete a tým vytvorila potrebu odpovede zo strany obete. Podvrhnutá webová stránka je vytvorená na akejkoľvek existujúcej webovej doméne, nezávisle od napadnutého subjektu. Často je vytvorený na doméne podstrom s podobnými názvami, ako je meno stránky, ktorú útočník kopíroval (napr. najlepšie.bankovanie.*dokonalékvetyzababku.sk*). Útočník zneužíva dĺžku zobrazenia adresy v internetovom prehliadači, ktorá je obmedzená a obeť ak nekontroluje adresu stránky nespozoruje, že adresa v prehliadači patrí podvrhnutej doméne.

Phishingova komunikácia je väčšinou posielaná na všetky adresy bez rozdielu, ktoré sú útočníkovi k dispozícii. V takomto prípade počet nehrá rolu, pretože posielanie vo virtuálnom priestore je lacné a rýchle, obete, ktoré nemajú prístup k službe, na ktorú je komunikácia smerovaná sa niekam nebudú hlásiť a žiadne údaje vyplňovať.

Často sa na phishingový útok využíva komunikácia cez sociálne siete, či už prostredníctvom konkrétnych riadených správ alebo pomocou klamlivých kampaní vedených v sociálnych sieťach. V prípade, ak sa využíva ako nosič informácie osobná správa, využíva sa neoficiálne a skomolené meno známej osobnosti alebo v prípade presne zacielených útokov sa využíva ukradnuté konto konkrétneho človeka. Zaujímavosť o samotnú kampane sa zvyšuje tým, že ponúka zaujímavú výhru pri poslaní osobných údajov alebo platby. Významným problémom pri ochrane útokov cez sociálne stránky je odstraňovanie phishingovej kampane. Kampaň na sociálnych sieťach je obmedzovaná na adresátov a ich osobné preferencie a nie je možné ju vyvolať na obrazovku. Z tohto dôvodu je veľmi zložité sa k jednotlivým kampaniam dostať.

3.2 Analýza phishingových útokov

Príklad navodenia dôvery:

- Firma alebo finančný dom stratila údaje o klientoch, pošle vám správu so žiadosťou o vyplnenie
    - v prípade, že túto správu dostane klient, ktorý dôveruje konkrétnej firme, nerozmýšľa nad obsahom správy a jeho nereálnosťou, ale vykoná požiadavku. Nereálnosť správy je schovaná v statuse, že firma, ktorá je závislá od

osobných údajov klientov má niekoľko úrovní ochrany a je prakticky nemožné, aby prišla o klientske údaje (*Obrázok č. 1*). Ďalším dôvodom býva aktualizovanie bezpečnostných nastavení konkrétnej organizácie a nevyhnutnosť znovu obnovenia prihlasovacích údajov.

- Váš známy pošle správu pomocou emailu alebo cez sociálne siete a varuje Vás pred nebezpečenstvom, proti ktorému sa dá obrániť iba prihlásením sa na konkrétnu stránku a vyplnením údajov.
    - v takomto prípade je útok zamierený na využitie dôvery klienta v konkrétneho človeka. Útoku zvyčajne predchádza napadnutie a získanie dát od konkrétneho používateľa a zneužitie jeho údajov (napr. počítač klienta, emailový klient, sociálne siete klienta,...). Následne sú tieto údaje zneužité na podvodnú komunikáciu s ďalšími potenciálnymi obeťami. V prípade emailovej komunikácie sa často využíva forma podvrhnutia adresy a následné presmerovanie komunikácie na webovú stránku, nezávislú od pôvodného odosielateľa (*Obrázok č. 2*).

Tlak na sociálne cítenie obete:

- Obeť potrebuje rýchlo poslať peniaze do inej krajiny, pretože je v sociálnej tiesni, alebo je iba krátkodobo v meste, kde sa nachádza finančná inštitúcia, z ktorej je možné vybrať peniaze.
    - tieto správy pôsobia na sociálne cítenie, ale zároveň aj na zlepšenie finančného postavenia obete, pretože za preposlanie peňazí obeť získava aj možnosť získať percentuálnu odmenu z preposlanej sumy. Častým je prevod dedičstva cez účet obete, alebo preposlanie peňazí do exotickej krajiny ako Nigéria (Nigeria SCAM). Na presvedčenie obete sa používajú prvky sociálneho útoku ako tlak na čas, sociálne cítenie obete (žiada chudobný človek, matka,...) a zisk obete (môže si časť peňazí ponechať). Tento útok je veľmi nebezpečný, pretože peniaze pochádzajú z trestnej činnosti a zapojením sa do preposielania sa obeť zároveň stáva členom organizovanej skupiny, ktorý zároveň získa neoprávnené obohatenie z trestnej činnosti (*Obrázok č. 3*).

      Nebezpečenstvo spočíva v dvoch rovinách:

        - Zapojením do organizovanej trestnej činnosti obeť je zodpovedná a súdne trestateľná a sadzby sú vyššie, pričom práve obeť je ľahko identifikovateľná.
        - Vymáhanie od poškodených sa javí v tomto prípade ako významná vec, pretože obeť je jediné známe ohnivko v organizovanom zločine

a preto sa od obete nárokujú všetky škody, či straty ktoré sú s touto činnosťou spojené.

- Organizovaná skupina získa zapojením obete všetky informácie o obeti a preto je možné obeť ďalej vydierať.

Vytvorenie tlaku na obeť

- Útočník vytvorí tlak na obeť, napríklad prostredníctvom navodenia pocitu, že správu poslala vyššia, nadradená autorita. V takomto prípade sa útočník pripravuje aj niekoľko týždňov, získava údaje o firme a konkrétnych osobách a jednotlivých závislostiach. Príklad: vlastník firmy pošle príkaz na zaplatenie na konkrétny účet účtovníčke. V tomto prípade účtovníčka ako podriadená, ak je takýto spôsob posielania príkazov prirodzený môže podľahnúť klamu a zaplatiť na podvrhnutý účet. Peniaze po prevode sú okamžite vybrané z účtu v cieľovej banke, preto je skoro nemožné získať peniaze späť (Obrázok č. 4).

3.3 Popis útokov a technológii, ktoré sa Phishingu týkajú

Smishing – patrí do kategórie phishingových útokov, vykonaných pomocou SMSkových správ. V rámci správy je uložená (väčšinou skrátená) linka, ktorá odkazuje na stránku, kde útočník sa snaží získať podvodné informácie. SMS využíva symboliku urgencie ako je výkričník, často s podvrhnutého čísla, aby sa správa javila ako odoslaná konkrétnou organizáciu alebo osobou (*Obrázok č. 5*).

Vishing – technika založená na útoku cez telefón. Buď je podvrhnuté falošné číslo, napríklad ako číslo Call centra konkrétnej firmy, pričom podvrhnuté číslo je presmerované na útočníka, ktorý sa snaží vymámiť od obete citlivé údaje. Niekedy je útok vedený zo strany útočníka, ktorý sa snaží vyvolať dojem, že volá dôveryhodná organizácia.

Phishing - podvodná technika, ktorá využíva internetové prostriedky na získavanie citlivých údajov ako sú heslá, čísla kariet, osobné údaje. Princípom je dostať adresátovi podvodnú správu s cieľom vymámenia citlivých údajov, častom sa ako odosielateľ vydáva samotná firma, ktorej klienti sú terčom útoku. Phishing je orientovaný primárne na klienta firmy, nie na firmu samotnú. Príprava útoku je jednoduchá a útok je vedený plošne na všetky dostupné kontakty s malou mierou správneho smerovania komunikácie, v prípade zasiahnutia dôverčivej obete sa počíta s vysokým ziskom.

Spear phishing – je skupina útokov, ktorá vyžaduje dlhodobejšiu analýzu prostredia konkrétnej firmy a následne je na klientov spustená cielená phishingova kamaň. Pôvodne boli správy rozosielane plošne na klientov, v súčasnosti sa dá na základe analýzy komunikácie

firmy na klientov a ďalších štatistických veličín nasmerovať útok presne na konkrétnych zamestnancov, študentov alebo klientov danej organizácie od nadriadeného. Príkladom je správa, ktorá vyzerá ako preposlaná od nadriadeného s úlohou, ktorú treba okamžite vykonať. Iným príkladom môže byť správa zaslaná na na triedu konkrétnej triednej učiteľky, ktorá bude vyžadovať rýchle zaslanie konkrétnych osobných informácii. (*Obrázok č. 6*).

Whalling - je obmedzenie phishingového útoku na konkrétnych ľudí špecifickej organizácie, resp. vo vysokom menežmente. Útočníci si pripravia organizačnú štruktúru špecifickej organizácie, pomocou ďalších metód sociálneho inžinierstva ako je Vishing sa snažia dostať k presnejším informáciam, zároveň sa snažia odchytiť správu z firmy, aby sa naučili písať správy presne v štandardoch a rozmeroch firmy (*Obrázok č. 7*).

CEO fraud - v tomto prípade ide o špecifickú implementáciu Whallingu, kde autorom podvrhnutej, falošnej správy sa javí byť CEO špecifickej organizácie (*Obrázok č. 8*).

Špeciálne útoky

Tabnabbing - tento prístup vyžaduje spojenie dvoch prístupov exploitu stránky konkrétnej organizácie a phishingového útoku. Obsahuje upravenie stránky konkrétnej organizácie alebo vytvorenie vírusu, tak aby sa pri prihlasovaní na konkrétnu stránku organizácie objavilo okno, ktoré imituje okno organizácie, ktoré vyžiada od obete prihlasovacie údaje. Útok využíva nepozornosť obete a možnosť internetových prehliadačov, prepísať načítaný obsah na stránke dlho po načítaní.

Evil twin - útok je založený na vytvorení WiFi siete a donútení presmerovania komunikácie cez túto WiFi sieť. Cieľom je analyzovať sieť a získavať z komunikácie citlivé údaje, poväčšine vhodné na ďalšiu komunikáciu a prihlasovanie pod identitou obete.

Pharming - útok je založený na vytvorení kópie webovej stránky a presmerovaní verejného DNS záznamu originálnej stránky na podvrhnutú kópiu. Cieľom je vytvoriť novú stránku, ktorá sa veľmi podobá na originál, pričom podvrhnutá stránka má za úlohu zhromažďovať citlivé dáta od klientov. Pre klienta je veľmi zložité zistiť, že ide o podvrhnutú stránku, pretože do prehliadača zadá správnu adresu požadovanej organizácie. Útok vyžaduje veľkú znalosť ako napadnúť a prestaviť verejný DNS server, ktorý je štandardne pod veľkou kontrolou, zároveň je orientovaný na menšiu geografickú oblasť

3.4 Identifikovanie phishingu

Čo si všímať na phishingovej správe?

1. Všeobecné oslovenie, z ktorého vyplýva, že útočník nepozná obeť (napr. Vážený klient)
2. Správa vyžaduje osobné alebo bankové údaje (dáta z karty, meno/heslo)
3. Neštandardná komunikácia, komunikácia, ktorú konkrétny odosielateľ nikdy neviedol a takúto správu ani neposiela. Snaží sa získať dáta od obete, ktoré by daná firma nikdy si nepýtala.
4. Pocit naliehavosti alebo výhodná ponuka – phishingový útok prebieha rádovo v dňoch, je nevyhnutné aby sa prípadná obeť zapojila v prvých dňoch útoku.
5. Neštandardná doména – doména na kde sa vypĺňajú údaje nepatrí konkrétnemu odosielateľovi alebo je len vzdialene podobná aleo obsahuje preklepy. Kontrolujte správnosť URL adries navštevovaných adries.
6. Častým javom je zlá jazyková úroveň spôsobená nekvalitou internetových prekladačov.

V prípade, že si nie ste istí, že konkrétna správa je phishingová, kontaktujte adresáta a opýtajte sa, či je to žiadosť, ktorú poslal. Nepoužívajte možnosť Odpovedať/Reply na správu, ktorú ste dostali, kontakt získajte na oficiálnych webových stránkach, aby kontakt nebol nadviazaný s útočníkom. Obozretnosť je nadôležitejšia pri prvotnom rozoznávaní phishingového útoku.

4 Ochrana pred phishingom

Základná ochrana pred phishingom je zamyslenie sa nad úlohou, ktorú bola poslaná cez elektronický kanál. Vždy je nevyhnutné zvážiť jej rozumovú existenciu a opodstatnenosť. Vyhýbajte sa klikaniu na odkazy v neznámych správach. Za týmito adresami môžu byť ukryté vírusy, ktoré vytvoria backdoor v systéme a útočníci následne môžu cez tieto programy riadiť útok z vnútra firmy. Útočníci využívajú populárne skrátené názvy domén, na zakrytie útoku. Pri kliknutí, okrem získania údajov, útočníci zároveň sa snažia napadnúť počítač obete. Výhodou je, že niektoré súčasné prehliadače v súčasnosti majú antiphishingovu ochranu a upozornia príjemcu správy na phishing. Na osobné stránky, ktoré obsahujú citlivé informácie nevstupujte z cudzích a nezabezpečených zariadení.

4.1 Vyššia ochrana pred phishingom

Zabezpečenie konkrétnej Webovej stránky je ochránené bezpečnostným certifikátom, ktorý musí patriť odosielateľovi, skontrolujte, overte vlastníka certifikátu. Majte antivírus

s kontrolou emailového klienta a rozšírením o ochranu pred phishingom (*antiphishing solution*). Výhodou je, že antivírus s takýmto rozšírením analyzuje podstatnosť emailu a požiadavky v ňom na Vás a zároveň overuje, či takýto phishingový email niekde inde na svete už nezaútočil.

Nepoužívate neznáme programy alebo programy, ktoré boli stiahnuté z neznámeho úložiska.

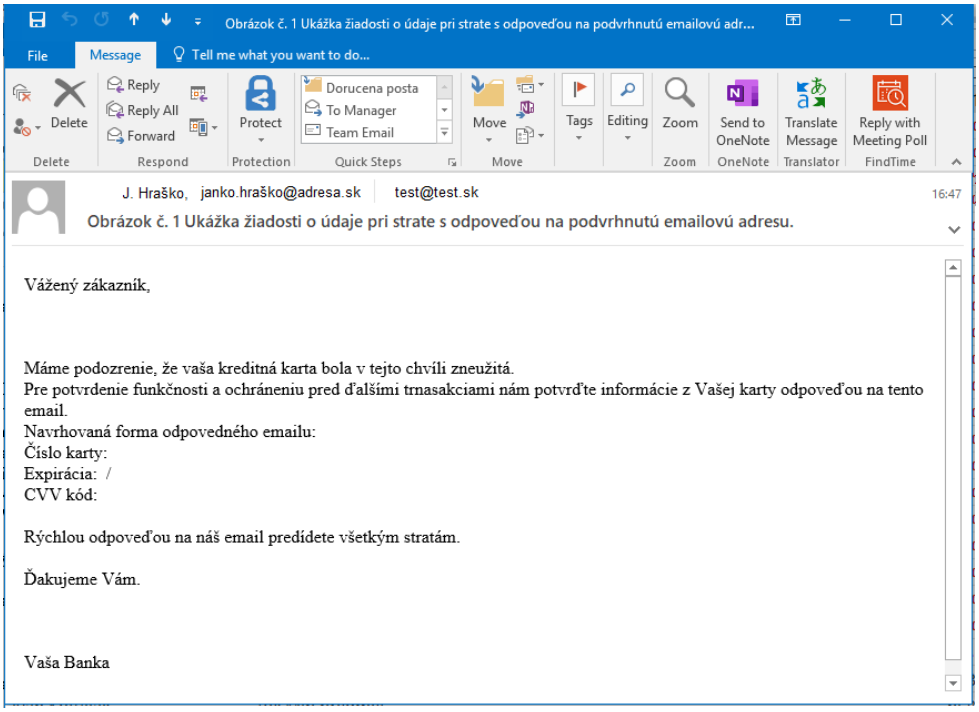
Používajte zdravý sedliacky rozum.

Záver

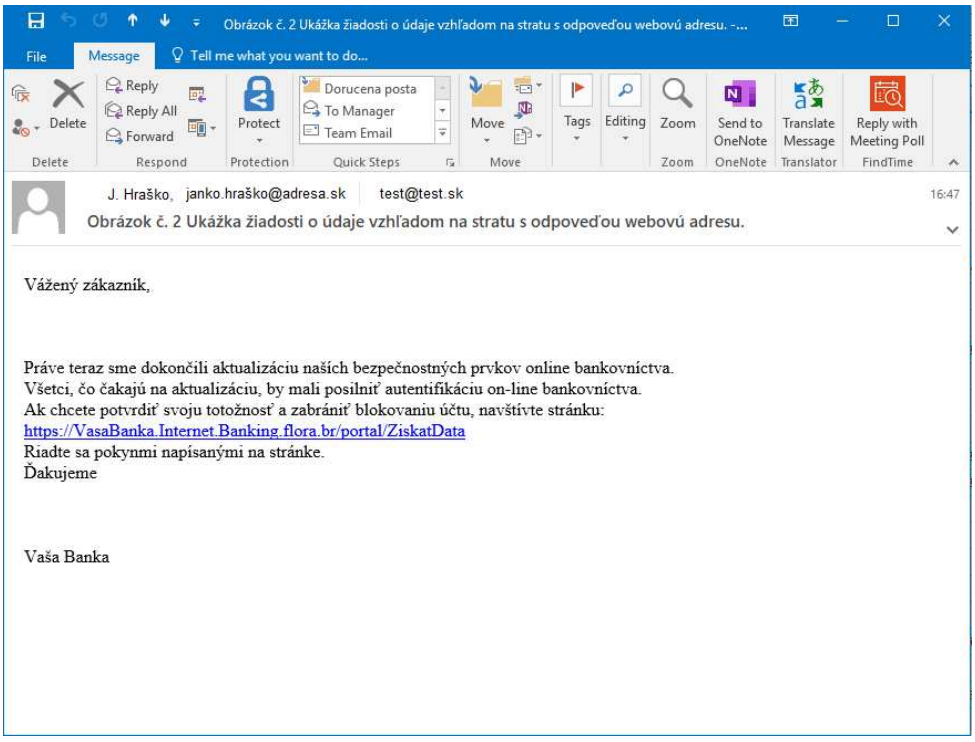
Útočníci stále viac využívajú moderné prostriedky a virtuálny priestor internetu na rozšírenie svojej pôsobnosti a obohatenie sa. Útok je vždy zameraný na konkrétneho človeka, klienta, rodiča a preto aj systém je len taký bezpečný, aký bezpečný a uvedomelý je konkrétny človek. Nebezpečenstvo útokov je o to väčšie, o čo viac sa využívajú viaceré kanály a o čo presnejšie sa zameria útočník na citlivé miesto obete. Citlivé miesto môže mať v každom čase inú podobu, raz to je potreba získania peňazí, obava z hnevu nadriadeného, či ľútosť nad stratou a nešťastím neznámej rodiny.

V dokumente sme popísali jednotlivé typy útokov. Najjednoduchšie riešenie ochrany je útok pochopiť, odhaliť, nevypĺňať a nahlásiť email a stránku ako phishing vo vašom internetovom prehliadači (Obrázok č. 9) a tak následne pomôcť ďalším budúcim obetiam. Boj, resp. ochrana pred phishingom je beh na dlhé trate, pretože phishing ako taký je lacný spôsob útoku a aj pri malej návratnosti, pre útočníkov prináša nemalé zisky.

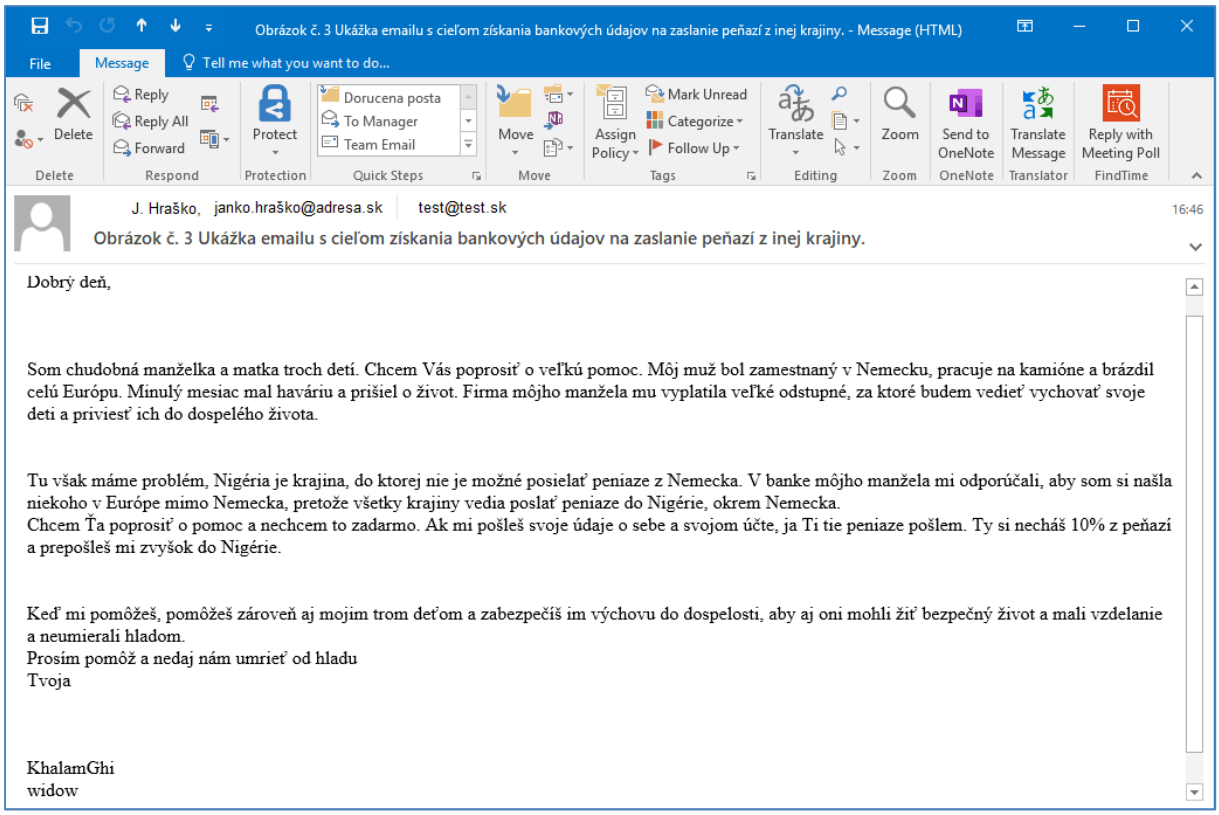
Obrazová príloha



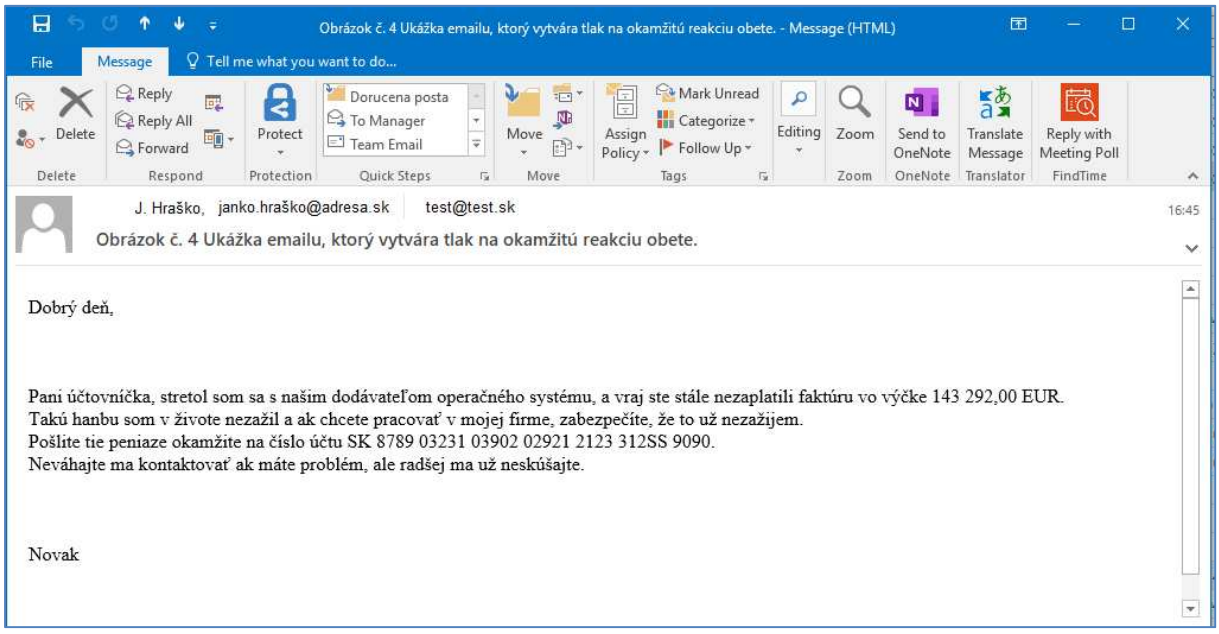
Obrázok č. 1 Ukážka žiadosti o údaje pri strate s odpoveďou na podvrhnutú emailovú adresu.



Obrázok č. 2 Ukážka žiadosti o údaje vzhľadom na stratu s odpoveďou webovú adresu.



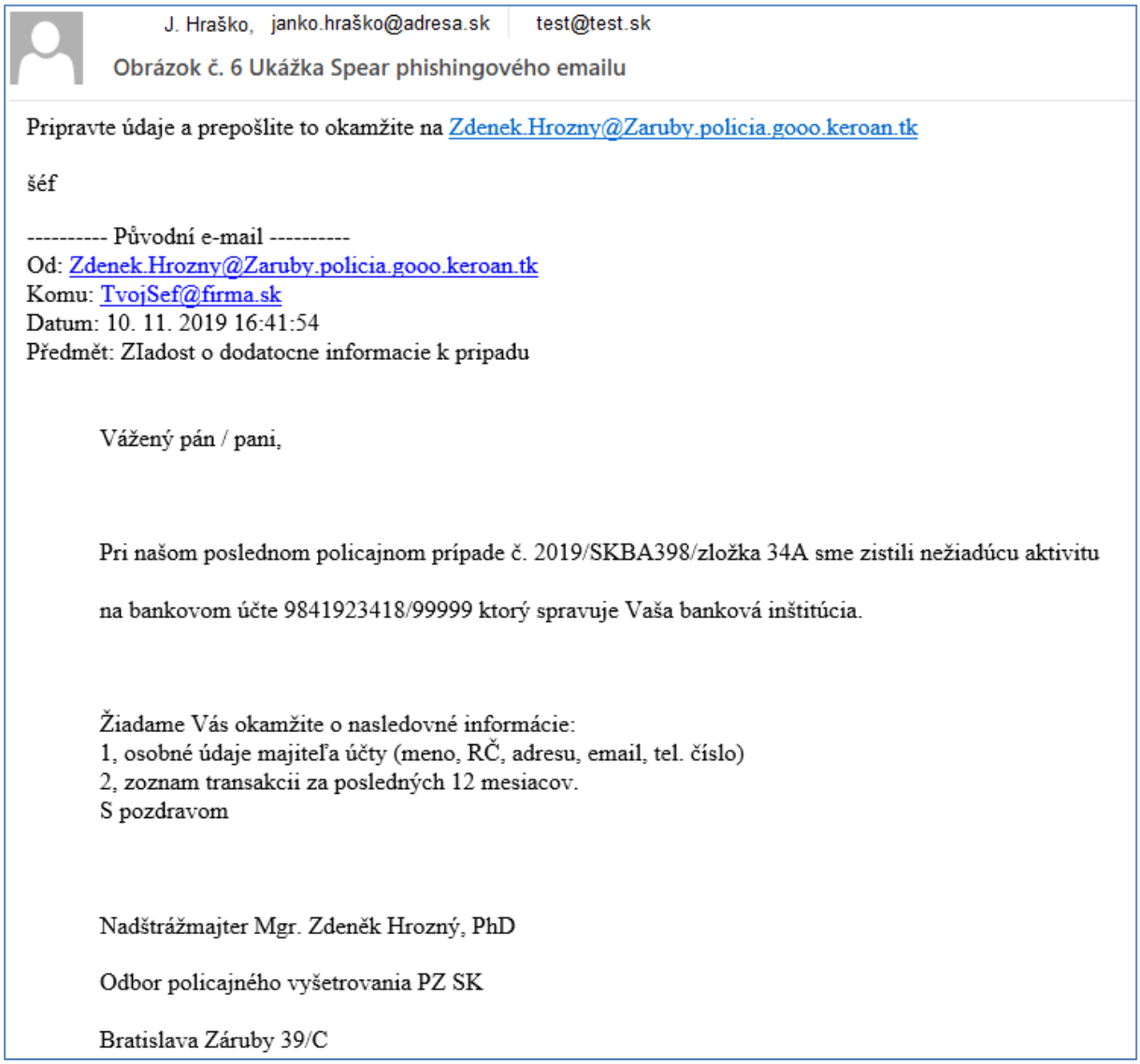
Obrázok č. 3 Ukážka emailu s cieľom získania bankových údajov na zaslanie peňazí z inej krajiny.



Obrázok č. 4 Ukážka emailu, ktorý vytvára tlak na okamžitú reakciu obete.

VAŠA FINANČNÝ ÚSTAV:
Bol zaregistrovaný incident na Vašom účte. Pre overenie incidentu sa nahláte na http://bit.ly/,jd023ekdc a vyplňte nevyhnutné informácie.

Obrázok č. 5 Príklad SMSishingovej správy



J. Hraško, janko.hraško@adresa.sk test@test.sk

Obrázok č. 6 Ukážka Spear phishingového emailu

Pripravte údaje a prepošlite to okamžite na Zdenek.Hrozny@Zaruby.policia.gooo.keroan.tk

šéf

---------- Původní e-mail ----------
Od: Zdenek.Hrozny@Zaruby.policia.gooo.keroan.tk
Komu: TvojSef@firma.sk
Datum: 10. 11. 2019 16:41:54
Předmět: ZIadost o dodatocne informacie k pripadu

Vážený pán / pani,

Pri našom poslednom policajnom prípade č. 2019/SKBA398/zložka 34A sme zistili nežiadúcu aktivitu

na bankovom účte 9841923418/99999 ktorý spravuje Vaša banková inštitúcia.

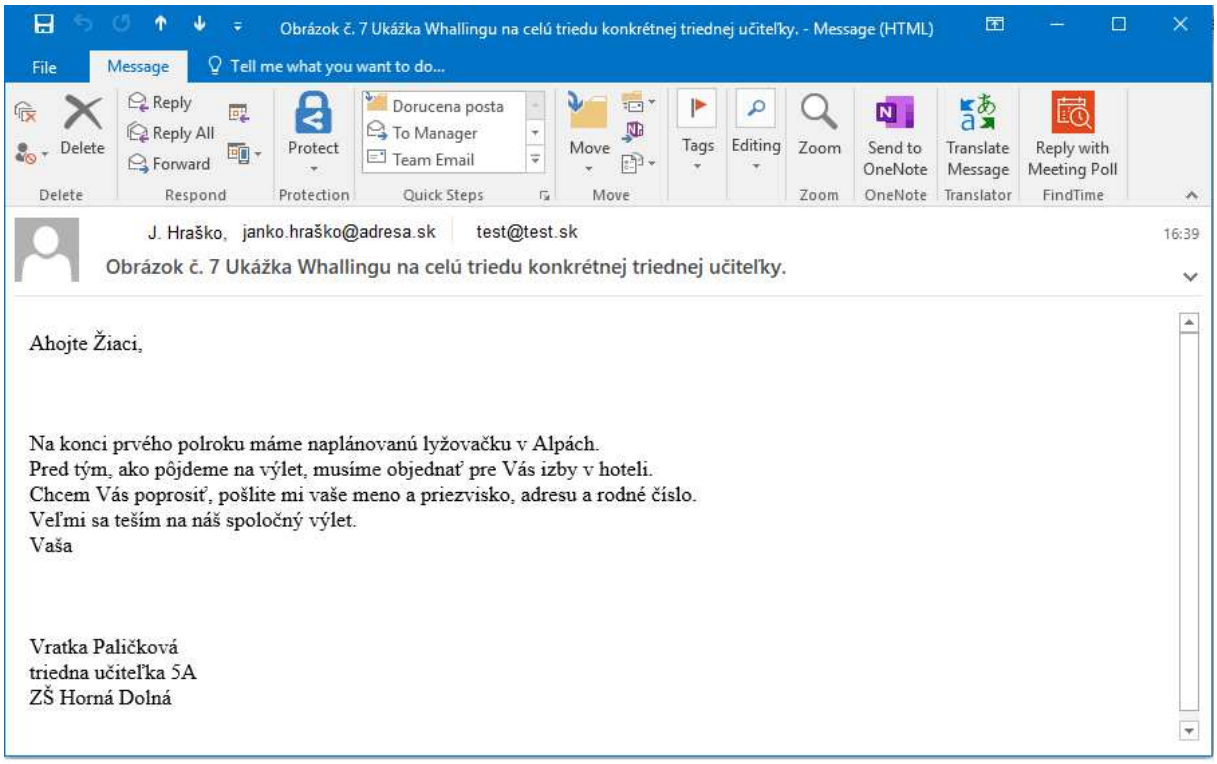
Žiadame Vás okamžite o nasledovné informácie:
1, osobné údaje majiteľa účty (meno, RČ, adresu, email, tel. číslo)
2, zoznam transakcii za posledných 12 mesiacov.
S pozdravom

Nadštrážmajter Mgr. Zdeněk Hrozný, PhD

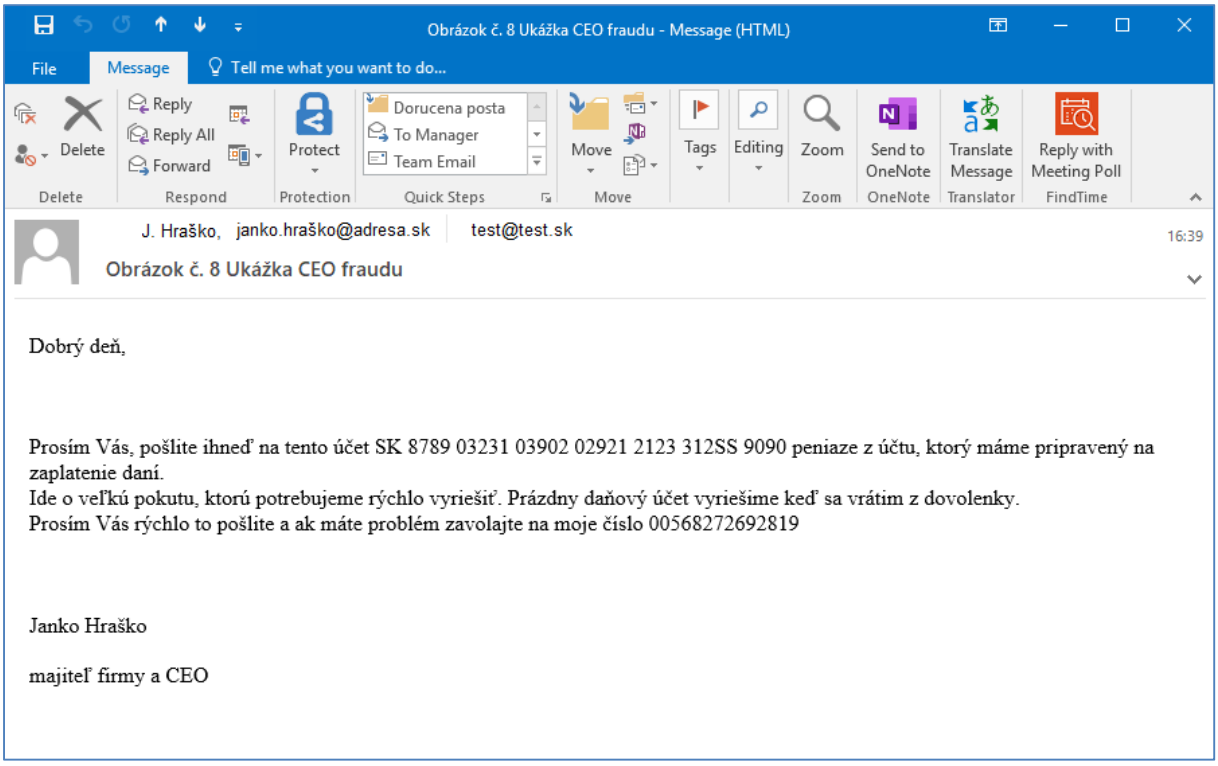
Odbor policajného vyšetrovania PZ SK

Bratislava Záruby 39/C

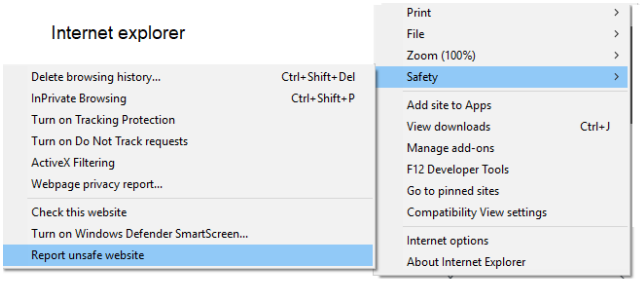
Obrázok č. 6 Ukážka Spear phishingového emailu



Obrázok č. 7 Ukážka Whallingu na celú triedu konkrétnej triednej učiteľky.



Obrázok č. 8 Ukážka CEO fraudu



Mozilla Firefox
https://www.mozilla.org/en-US/about/legal/fraud-report/

Google Chrome
https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

Obrázok č. 9 Ukážky nahlásenia phishingu v troch typoch prehliadačov

Tlačiarne:

LC.print plus s.r.o.

Komenského 9, Lučenec

www.lcprintplus.sk

Odborná príručka pre učiteľa

Podporná literatúra pre didaktiku informačnej bezpečnosti,

pre 5 ročník ZŠ.

Autor: Mgr. Marek Zeman, PhD.

Preventista.sk , 2019

1. vydanie

ISBN: 978-80-972100-2-1

EAN: 9788097210021

OZ Preventista – združenie pre bezpečnosť a prevenciu

Misiou združenia je robiť prevenciu IT kriminality a prispievať ku osvete informačnej bezpečnosti. Základnou komunikačnou platformou združenia OZ Preventista je portál Preventista.sk, kde poskytujeme informácie o jednotlivých oblastiach informačnej bezpečnosti. Portál umožňuje výmenu skúseností, v prevencii zahrňuje všetky úrovne spoločenského života.