UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA

FILOZOFICKÁ FAKULTA

SYSTÉM NA ZVYŠOVANIE BEZPEČNOSTNÉHO POVEDOMIA

2020 **KatarínaREGECIOVÁ**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA

FILOZOFICKÁ FAKULTA

SYSTÉM NA ZVYŠOVANIE BEZPEČNOSTNÉHO POVEDOMIA

BAKALÁRSKA PRÁCA

Študijný program:	**Britské a americké štúdiá** - Informatika
Vedúci diplomovej práce:	MSc. Terézia Mézešová
Konzultant diplomovej práce: (nepovinný)	**RNDr. JUDr. Pavol Sokol,** PhD.

Košice2020 **KatarínaREGECIOVÁ**

Poďakovanie

Ďakujem vedúcej mojej bakalárskej práce MSc. Terézie Mézešovej za pomoc, odborné rady, pripomienky a branstorming pri jednotlivých častiach práce. Taktiež ďakujem konzultantovi práce JUDr. RNDr. Pavlovi Sokolovi za pripomienky.

Abstrakt v štátnom jazyku

Informácie sú dnes jednou z najcennejších komodít na trhu. Ich majiteľovi môžu slúžiť, ale taktiež môžu spôsobiť problémy a to nie len majiteľovi, ale celej organizácií či krajine. Avšak najslabším článkom pri ochrane informácií je človek. Jeho neopatrnosť alebo neznalosť môže viesť k úniku informácií. Preto je táto práca zameraná práve na návrh a vývoj systému, ktorý by mal ľudí naučiť ako chrániť dôležité informácie. Smerov, na ktoré by sa dalo zamerať, je mnoho. Preto sme vybrali len tri z nich, ktoré sú jednoducho implementovateľné v akomkoľvek pracovnom prostredí. Nie sú závislé ani od spôsobu akým inštitúcia uchováva informácie a ani od systémov, ktoré využívajú. V každej kapitole tak predkladáme úvod do problému a následný návrh a implementáciu systému, ktorý by mal slúžiť na vzdelávanie používateľov v danej oblasti.

Kľúčové slová:*informačná bezpečnosť, pravidlá čistého stola, phishingové emaily, heslá*

Abstrakt v cudzom jazyku

Now, information is currently one of the most valuable commodities on the market. It can serve its owner. However, it can generate complications not only for its owner but for the whole organization or country as well. Nevertheless, the weakest link in protecting information is a man. His unawareness and ignorance can lead to information leakage. Thus, this thesis is focused on the design and development of a system that should educate people on how to protect important information. There are many dimensions on which we could focus on. Therefore, we have selected three of them which can be easily implemented in any work environment. They are not dependent on how the company handles the information nor the system they use. In each chapter, we provide the introduction to the issue and, subsequently, the design and implementation of the system, which aims to educate the users in this direction.

Keywords: *information security, clean desk policy, phishing emails, passwords*

Obsah

Úvod

Ak sa pozrieme späť približne o 30 rokov, bezpečnostné problémy spojené s počítačmi tak, ako ich ponímame dnes, takmer neexistovali. A to najmä kvôli ich malej škále využitia a tiež malému počtu ľudí, ktorí s počítačmi vedeli pracovať [1]. Dnes je situácia iná. Technológie nám umožňujú byť produktívnejší. Sú pre nás už neoddeliteľnou súčasťou nášho súkromného aj pracovného života. Všetko, čo potrebujeme máme na klik ďaleko [1]. Zároveň to znamená, že pri odcudzení telefónu alebo notebooku, všetky naše informácie sú len na klik ďaleko od útočníka.

Na druhej strane informačná bezpečnosť siaha až do dôb druhej svetovej vojny a využitia počítačov v tomto období. Potreba chrániť fyzickú lokalitu, hardvér a softvér. Začalo sa zavádzať niekoľko úrovní bezpečnosti a ochrany týchto informácií. Potreba národnej ochrany viedla ku komplexnejším a technologicky sofistikovanejším spôsobom ochrany [2].

Médiá a spoločnosť venujú viac pozornosti útokom, za ktorými stoja hackeri a môžu tak za únik informácií obviňovať nedostatočnú kyber ochranu alebo chybu v ochrannom systéme. Na druhej strane, únikom, ktoré boli zapríčinené zlyhaním ľudského faktora sa nevenuje toľko pozornosti. Spoločnosť tak ostáva v nevedomosti o tom, koľko útokov je tak spôsobených človekom a že ohrozenie je bližšie ako sa zdá [3].

Vo väčšine týchto prípadov bola chyba človeka neúmyselná alebo z nevedomosti. Preto je dôležité vzdelanie v tejto oblasti. Aj keď mnoho organizácií a firiem robí pravidelné školenia o bezpečnosti, realita je taká, že sú to len prednášky, z ktorých si účastníci odnesú len minimum informácií. Preto je naším cieľom nájsť efektívnejší spôsob vzdelávania v oblasti informačnej bezpečnosti.

MichelPrince v roku 2004 vypracoval štúdiu [4] o aktívnom učení. Vo svojej práci sledoval spôsob vyučovania na univerzite, teda pracoval s dospelými ľuďmi. Výsledkom štúdie je fakt, že si študenti z prednášok odniesli viac, ak boli súčasťou prednášok aktivity pre študentov. Preto sme sa rozhodli vytvoriť aplikácie a hry, ktoré by sprostredkovali používateľom informácie o bezpečnosti.

Informačná bezpečnosť sama o sebe je veľmi obšírna téma, ktorá zahŕňa množstvo smerov, ktorými sa dá uberať. Pri výbere okruhov budeme nadväzovať na už existujúcu prácu [5], ktorá je zameraná na heslá a phishingové emaily. Okrem toho pridáme ďalšiu

kapitolu o pravidlách čistého stola, pretože sú to pravidlá, ktoré sa dajú využiť v akomkoľvek pracovnom prostredí.

Táto práca sa skladá z 3 kapitol. V prvej kapitole popisujeme pravidlá čistého stola. V úvode vysvetľujeme prečo sú tieto pravidlá dôležité, následne predstavujeme konkrétne pravidlá, s ktorými budeme pracovať. Po tomto prichádza návrh samotného systému. Táto časť bližšie predstavuje aj jednotlivé rozhodnutia týkajúce sa funkcionality systému. Na záver obsahuje technický popis toho, ako samotná aplikácia funguje a ako je možné ju rozširovať.

Druhá kapitola je zameraná na phishingové správy. Kapitola začína popisom phishingových emailov a vysvetlením prečo sú nebezpečné. Taktiež sa pozrieme na to ako rozpoznať phishingový email. Následne kapitola pokračuje návrhom webovej aplikácie, samotnou implementáciou a vysvetlením ako aplikácia funguje. Taktiež uvádza ukážku zdrojového kódu, ktorá ukazuje funkciu na zvýraznenie častí emailu.

Posledná kapitola sa zameriava na heslá a na to ako vytvoriť silné heslá. Rovnako predstavuje návrh hry, ktorá má používateľom ukázať dôležitosť používania silných hesiel. Kapitola končí technickou implementáciou hry.

1 Pravidlá čistého stola

Ochrana informácií začína ešte predtým ako sa zapne počítač a pokračuje aj po tom ako sa vypne. Informačná bezpečnosť je zameraná na ochranu údajov, online aj offline. Množstvo informácií sa nachádza mimo počítača, na pracovnom stole a je dôležité tieto informácie chrániť.

V posledných rokoch, počítačové a sieťové technológie spôsobili nebývanú zmenu v tvorbe, uchovávaní, distribúcii a prístupu k dokumentom [6]. Na druhej strane preferencia ľudí pre papier ako nástroj čítania a uchovávania informácií naznačuje, že papier tak skoro z digitálnej éry nevymizne [6]. Z tohto dôvodu je potrebné orientovať ochranu aj na tieto zdroje a informácie a to zaisťujú Pravidlá čistého stola.

"Účelom týchto pravidiel je zaviesť minimálne požiadavky na udržanie čistého stola - citlivé údaje o zamestnancoch, duševné vlastníctvo, informácie o zákazníkoch a predajcoch sú v uzamykateľných priestoroch a mimo dosahu[7]*"*. Je to jedna z najhlavnejších stratégií, ktoré by sa mali uplatňovať pri snahe znížiť riziko úniku informácií z pracoviska. Taktiež je kompatibilná s normou ISO 27001/17799 [8].
Okrem iného majú tieto pravidlá aj ďalšie vedľajšie výhody [9]:

- Šetria čas a peniaze - Priemerný zamestnanec strávi hľadaním informácií 2,5 hodiny denne. *"Ak predpokladáme, že znalosti zamestnancov vo vašej firme zarobia $80,000 ročne, organizácia s 1000 zamestnancami stratí približne $2,5 milióna dolárov ročne na neschopnosti efektívne hľadať a znovu nadobudnúť informácie*[9]*"*.
- Vytvárajú dobrý dojem - Upratený pracovný priestor vzbudzuje u návštevníkov dojem efektívnosti a organizovanosti.
- Odrádzajú zvedavé oči - Keďže informácie nie sú ponechávané na viditeľných miestach, znižujú riziko, že niekto zahliadne informáciu, ku ktorej by inak nemal prístup.
- Znižujú stres - Keď je všetko na svojom mieste, zamestnanci sa môžu sústrediť viac na prácu a menej času venujú hľadaniu informácií.

1.1 Pravidlá

Rôzne zdroje majú zväčša prispôsobené pravidlá čistého stola pre konkrétnu organizáciu, preto vychádzame z pravidiel, ktoré sa často opakujú a sú aplikovateľné nezávisle od pracoviska. Prvým využitým zdrojom bol dokument od spoločnosti

SANS[7], ktorý pripravila pre svojich zamestnancov. SANS je americká výskumná organizácia zameraná na oblasť informačnej bezpečnosti. Okrem toho organizujú v tejto oblasti certifikované kurzy, ktorými každoročne prejde vyše 30 000 ľudí. Druhým dokumentom, s ktorým sme pracovali bol dokument vydaný Českou šípkovou organizáciou [8] ako norma pre všetkých jej členov. Čiže ide o dokument priamo z praxe.

Pravidlá čistého stola

P1. Zamestnanci sú povinní zabezpečiť, aby všetky citlivé alebo dôverné informácie v tlačenej podobe alebo elektronickej forme v ich pracovnej oblasti boli na konci dňa a vtedy, keď sa očakáva sa, že budú na dlhšie obdobie mimo, bezpečne uložené.

Pri dlhšej neprítomnosti pri pracovnom stole nemá zamestnanec prehľad o tom, kto sa pohybuje v jeho okolí, preto je možné, že aj návštevník alebo klient môže zahliadnuť informácie, ktoré nemajú byť voľne prístupné.

P2. Počítače musia byť uzamknuté s heslom, keď je pracovný stôl neobsadený.

Nemáme prehľad o to, kto sa pohybuje po pracovisku, preto by neuzamknutý počítač uľahčil prácu komukoľvek, kto by chcel zneužiť interné informácie spoločnosti.

P3. Všetky citlivé informácie musia byť odstránené z pracoviska a zaistené v zásuvke, keď je stôl neobsadený alebo na konci pracovného dňa.

Na konci pracovnej doby sa môže stať, že po odchode zamestnancov, príde upratovač alebo upratovačka. Väčšinou upratujú aj pracovné stoly, a okrem toho, že sa dostanú k dôverným informáciám, môžu papiere na stole uložiť inak ako boli pôvodne a tak sa môžu informácie aj stratiť.

P4. Skrine obsahujúce citlivé informácie musia byť zatvorené a uzamknuté, keď sa nepoužívajú.

Je potrebné, aby prístup k dôverným informáciám mali len oprávnené osoby, teda ľudia, ktorí majú kľúč od danej skrine.

P5. Heslá nesmú zostať v poznámkach nalepených na počítači alebo pod počítačom, ani nemôžu byť napísané na prístupnom mieste.

Je veľmi dobré, ak sú citlivé a dôverné informácie zaheslované, ale v prípade, že je heslo voľne prístupné je to len malý krôčik navyše pre kohokoľvek, kto sa snaží dostať k daným záznamom.Zviran a Haga robili prieskum [10], v ktorom sa účastníkovpýtali aký spôsob na zapamätanie si a prácu s heslami využívali. Až 35%

z nich si heslá zapisovalo na papier a mali ich odložené v peňaženke, zápisníku alebo kalendári.

P6. Výtlačky obsahujúce citlivé informácie by mali byť okamžite vyzdvihnuté z tlačiarne.

Na dané dokumenty sa môže jednoducho zabudnúť a ľahko sa tak dostanú do nepovolaných rúk.

P7. Zamestnanci by mali citlivé dokumenty skartovať, ak tieto dokumenty už nie sú potrebné.

To, že je dokument v koši neznamená, že je bezpečne odstránený. Za správne zlikvidovanie sa považuje skartovanie. Je tak zložitejšie pospájať celý papier dokopy, aby si z neho ktokoľvek vytiahol informácie, ktoré môže potenciálne zneužiť.

P8. Tabule obsahujúce citlivé informácie by sa mali zmazať.

Know-how, obchodný model, nové projekty, detaily o projektoch alebo produktoch sú taktiež citlivé informácie, ktoré môžu spoločnosť, firmu, či organizáciu stáť nemalé peniaze.

P9. Pamäťové zariadenia, ako CDROM, DVD alebo USB, považujte za citlivé a zaistite ich v uzamknutej zásuvke.

Úložiská obsahujúce dôverné informácie nesmú byť voľne prístupné, preto je potrebné ich zabezpečiť zámkom a kľúč dať len osobám oprávneným s týmito údajmi narábať.

1.2 Webové rozhranie

Pravidlá čistého stola boli mnohokrát spísané a uverejnené pre zamestnancov spoločnosti. Napriek tomu sa často stáva, že ich zamestnanci stále porušujú. Preto si vyberáme interaktívnu cestu ako naučiť ľudí tieto pravidlá. Podľa Daleho kužeľa skúseností [11] si ľudia zapamätajú len 10% z toho čo prečítajú, ale 30% z toho, čo vidia a až 90% z toho, čo robia. To je pre nás hlavnou motiváciou k vytvoreniu aplikácie, v ktorej si môžu používatelia precvičiť identifikáciu pravidiel.

Ako prostriedok na sprostredkovanie aplikácie využívame internet, najmä kvôli jeho dostupnosti. Program by sa dal previesť aj na mobilnú aplikáciu alebo hru na počítač, no jednou z motivácií na začiatku bola možnosť využiť výsledný produkt ako pomôcku pri školeniach. Webová aplikácia má oproti tej mobilnej a počítačovej tu výhodu, že práca s ňou nie je závislá od množstva voľného úložného priestoru

v zariadení, ale len od pripojenia na internet. Navyše je možné stránku stiahnuť do počítača a školiteľ ju môže distribuovať na USB kľúči.

Pri rozhodovaní ako ukončiť program máme niekoľko možností. Prvou je nechať hráča klikať na objekty a po každom kliku vypísať, či bol správny alebo nie. Program by sa ukončil, aký by hráč našiel všetky pravidlá. Táto situácia však nemusí nastať. Nie je isté, že hráč bude schopný identifikovať všetky porušenia pravidiel a táto neschopnosť by ho mohla odradiť od pokračovania v hre. Taktiež by sa mohlo stať, že by hráč klikal na náhodné objekty bez uváženia.

Druhá možnosť, pre ktorú sme sa napokon rozhodli, je vložiť do programu časovač. Po otvorení stránky sa zobrazí obrázok, hráč má teda možnosť prezrieť si objekty po celý čas, kým je stránka aktívna a porozmýšľať o tom, čo môžu byť nebezpečné. Keď bude mať pocit, že je pripravený spustiť časomieru, stlačí tlačidlo "Poďme na to". Následne sa spustí odpočítavanie, ktoré je aj vizuálne znázornené. Časovač odrátava 10 sekúnd, tento čas je možné zmeniť. Po uplynutí časomiery program automaticky vyhodnotí nájdené a nenájdené pravidlá. Hráč tak dostane spätnú väzbu vždy. Môže si pozrieť, ktoré pravidlá sa mu podarilo nájsť a ktoré nenašiel a na tie sa v ďalšej hre zamerať.

Oba použité obrázky sú navrhnuté tak, aby obsahovali niekoľko vyššie spomenutých pravidiel, ale taktiež predmety, ktoré slúžia na zmätenie návštevníka. Cieľom tohto cvičenia je, aby návštevník bol schopný identifikovať predmety, ktoré sú hrozbou pre bezpečnosť informácií, no tiež, aby bol schopný identifikovať, čo k týmto hrozbám nepatrí. Vyhodnotenie sa následne skladá zo 4 častí:

- pravidlá, ktoré sú obsiahnuté v obrázku a ktoré boli nájdené hráčom (hráč na ne klikol)
- predmety, ktoré slúžia na zmätenie, ale hráča nezmiatli (neklikol na ne)
- predmety, ktoré slúžia na zmätenie a hráč na ne klikol
- pravidlá, ktoré sú obsiahnuté v obrázku, no hráč ich nenašiel (neklikol na predmet)

Vyhodnotenie obsahuje len kľúčové slová, ktoré popisujú pravidlo, ktoré je porušené. Aplikácia totiž primárne slúži na precvičenie si znalostí, dodatočné opakovanie a upevňovanie vedomostí. Všetky vymenované pravidlá sú spomenuté vyššie v práci a rovnako ich návštevník stránky môže nájsť na webe CSIRT tímu UPJŠ [12].

Oba obrázky vychádzajú z vyššie uvedených pravidiel. Ako už bolo spomínané, rôzne zdroje sa môžu v jednotlivých pravidlách líšiť a tak aj vytváranie ilustračných obrázkov pre každý rad pravidiel je odlišné. Základom je v danom pravidle nájsť objekt, ktorého sa pravidlo týka. Napríklad, ak pravidlo hovorí o tom, že po opustený pracovného miesta nesmú byť na obrazovke počítača otvorené žiadne dokumenty, objektom v tomto pravidle je obrazovka počítača. Pravidlo zväčša hovoria o tom, kde sa má alebo nemá objekt nachádzať alebo v akom má alebo nemá byť stave. V prípade tohto príkladu je to, že na obrazovke nesmú byť otvorené dokumenty. V ilustrácii pravidlo znázorníme jeho porušením, teda do obrázka vložíme obrazovku počítača, ktorá má viditeľne otvorený dokument.

Obrázok by nemal obsahovať len porušenia pravidiel. Mal by obsahovať aj predmety, ktoré používateľa zmätú. To sa dá dosiahnuť dvoma spôsobmi. Prvý je ten, že do obrázka bude vložený predmet, ktorý je objektom v pravidlách, s ktorými pracujeme, ale je v stave, že neporušuje žiadne pravidlo. V práci so spomínaným príkladom by to mohol byť monitor počítača, ktorý je tmavý. Značí, že počítač je vypnutý a neporušuje tak žiadne pravidlo. Druhým spôsobom je, že sa do obrázka vložia predmety, ktoré vôbec nie sú v zozname pravidiel spomínané, napr. nápoje, jedlo, okuliare, časopisy.

Na obrázkoch je možné jednotlivé pravidlá ilustrovať rôzne. Napríklad pravidlo P1 je možné znázorniť dokumentmi položenými na viditeľnom mieste. Dokumenty by mali byť označené nápisom „tajné“, „dôležité“, „dôverné“, aby boli odlíšiteľné od čistých papierov do tlačiarne alebo obyčajných novín. Na ilustrovanie pravidla P2 je možné do obrázka doplniť stolný počítač alebo notebook, na ktorom budú otvorené aplikácie alebo dokumenty. Spôsob zobrazenia pravidla P3 môže byť dvojaký. Buď môže byť zobrazené dokumentmi na pracovnom stole ako pravidlo P1, alebo otvorenou zásuvkou. Otvorenou skriňou, skrinkou alebo nezaisteným sejfom je možné ilustrovať pravidlo P4. Ďalším pravidlom, ktoré sa dá zobraziť je pravidlo P5 týkajúce sa hesiel. Tie je možné ponechať na akom ktokoľvek viditeľnom mieste, napríklad na poznámkovom lepiacom papieriku nalepenom na monitore. Pravidlo P6 hovorí o tom, že v tlačiarňach nesmú stať dokumenty, preto je najlepšie ilustrovať toto pravidlo práve tlačiarňou, v ktorej sú stále dokumenty. Zároveň je možné použiť prázdnu tlačiareň, bez dokumentov, ako mätúci objekt. Pravidlo P7 je možné ilustrovať viditeľnými dokumentmi v koši alebo pokrčený papier na stole alebo v okolí. Rovnako ako pri pravidle P1 je potrebné, aby papiere boli označené ako "tajné" alebo "dôverné". Pravidlo P8 sa okrem tabúľ týka aj

násteniek, preto je možné použiť jeden z týchto dvoch objektov na obrázku. Na tabuli alebo nástenke by mali byť ilustračne nejaké informácie, ktoré by črtali, že môže ísť o dôverné informácie. Ak je na tabuli nápis „Všetko najlepšie k narodeninám“, môžete ju použiť ako mätúci objekt. Ak by tam bol nápis „Nový produkt“, „Obchodná stratégia“ alebo obrázok ilustračnej mapy, už by to porušovalo pravidlo. Na znázornenie posledného pravidla P9 je vhodné umiestniť jedno alebo viac zo spomínaných pamäťových médií na viditeľné miesto., napr. na pracovný stôl.

1.3 Technická implementácia

Na pozadí tejto miniaplikácie je spolupráca HTML dokumentu a programu v jazyku JavaScript. HTML dokument obsahuje okrem úvodných textov a päty aj dve obrázkové mapy. Každá mapa obsahuje vyznačené predmety reagujúce na myšku. Pri prejdení myšou na objekt sa zmení kurzor a oblasť sa vizuálne vyznačí. Pri kliku myšky sa zavolá funkcia z JavaScriptu`pridajPredmet`, ktorej parametrami sú id mapy a alternatívny názov predmetu.

V JavaScripte sú pripravené prázdne polia, ktoré sa plnia práve vo funkcii `pridajPredmet`. Každá mapa má určené pole, s ktorým pracuje, preto sa pri behu programu zaplní len jedno z dvoch pripravených polí.

Na začiatku scriptu je pre každú mapu určené, ktoré predmety sú pravidlami, ktoré je potrebné nájsť a ktoré sú predmety určené na zmietnutie návštevníka. Samotné vyhodnotenie prebieha funkciou nazvanou “Vyhodnotenie”, do ktorej ako parametre vstupujú pole s pravidlami, pole s predmetmi na zmätenie a pole s predmetmi, ktoré boli zakliknuté hráčom. V tomto bode prebieha porovnanie všetkých troch polí výsledok sa ukladá do 4 polí, podľa vyhodnotenia spomínaného vyššie.

Ukážka zdr. kódu 1. Vyhodnotenie kliknutých objektov

```
functionvyhodnotenie (alloptions_arr, incorrect_arr, clicked_arr){
var alloptions = new Set(alloptions_arr);
var incorrect = new Set(incorrect_arr);
var clicked = new Set(clicked_arr);
    let correct = new Set([...alloptions].filter(x => !incorrect.has(x)));
    let notclicked = new Set([...alloptions].filter(x => !clicked.has(x)));
    true_positives = new Set([...clicked].filter(x =>correct.has(x)));
    false_positives = new Set([...clicked.filter(x =>incorrect.has(x)));
    false_negatices = new Set([...notclicked].filter(x =>correct.has(x)));
    true_negatives = new Set([...notclicked].filter(x =>incorrect.has(x)));
}
```

Samotné vyhodnotenie sa vypíše funkciou `zobrazVysledky`, ktorá ich zobrazuje farebne odlíšené a s ikonami, aby pritiahli pozornosť. Aplikácia je opakovateľná, po opätovnom zobrazení/načítaní stránky sa všetky výsledky vynulujú a hráč môže aplikáciou spustiť znova. Program obsahuje dva obrázky, no na stránke sa vždy objaví len jeden. O to sa stará kúsok JavaScript kódu na začiatku html dokumentu, ktorý zobrazí mapu 1 alebo mapu 2 podľa toho v akom čase (sekunde) bola stránka otvorená. Hráč tak teda môže otestovať svoje znalosti na dvoch rôznych obrázkoch.

V Ukážke zdr. kódu 2 je časť kódu, ktorá zabezpečuje striedanie obrázkov na základe času, kedy bola stránka otvorená. Aktuálne je program nastavený na dva obrázky, v tomto prípade stačí použiť funkciu if. Je možné kód rozšíriť o viac obrázkov, no v tom prípade bude potrebné zmeniť funkciu na switch ako je to znázornené v Ukážke zdr. kódu 3.

Ukážka zdr. kódu 2. Striedanie 2 obrázkov

```
if((new Date()).getSeconds() % 2 == 0){
    $('.map_2').hide();
}else{
    $('.map_1').hide();
}
```

Ukážka zdr. kódu 3. Striedanie **n** počtu obrázkov.

```
var zvysok = new Date().getSeconds() % n;
var z = zvysok.toString();
switch (z) {
    case "0":
       $('.map_1').hide();
       …
       $('.map_n').hide();
    …
    case "n" :
       $('.map_1').hide();
       …
       $('.map_(n-1)').hide();
}
```

Pridávanie nových obrázkov sa skladá z niekoľkých krokov. V prvom rade je potrebné zmeniť vyššie uvedené striedanie obrázkov. Následne v HTML dokumente

treba pridať časomieru, ktorá sa zobrazí na stránke s novým obrázkom. Nato je potrebné pridať samotnú mapu v tvare nižšie uvedeného kódu.

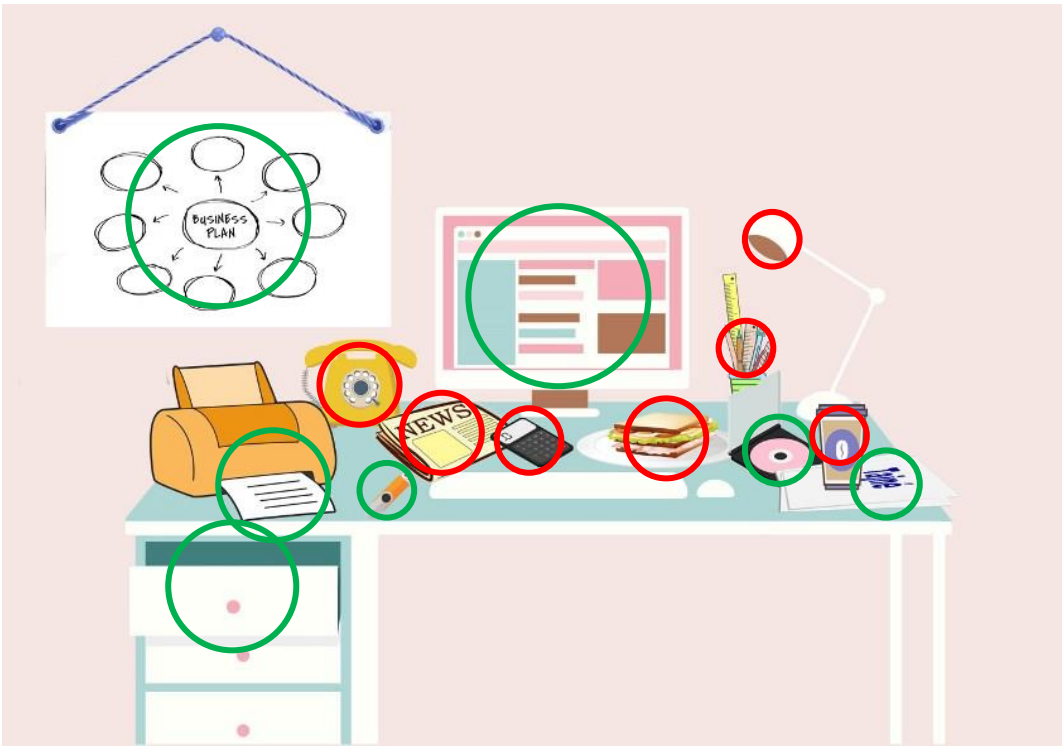
Ukážka zdr. kódu 4. Vytváranie mapy

```
<articleclass="map_n">
    <div class="imginfo"><span></span></div>
    <imgsrc="názov_obrázka.formát" alt="Fotografia pracovného stola"
usemap="#workplace" class="map" width="840" height="588">
    <mapname="workplace">
      <areashape="..." coords="..." onclick="pridajPredmet(n,
'názov_predmetu')" id="x" alt="názov_predmetu"
onmousehover="this.style.cursor = 'pointer'>
      ...
    </map>
</article>
```

Následne je potrebné v JavaScript dokumente pridať polia `klikatelne_n` a `nespravne_n`, do ktorých sa ako hodnoty vkladajú názvy predmetov z vytváranej mapy. Do poľa `klikatelne_n`sa radia predmety, ktoré porušujú pravidlá. Do poľa `nespravne_n`patria, predmety určené na zmätenie používateľa. V tom istom dokumente je potrebné pridať do funkcií `casovac`, `countdown`, `pridajPredmet` a kontrola spracovanie novej mapy. Inými slovami, skopírovať časť kódu a upraviť v nej číslovanie, aby korešpondovalo s novou pridanou mapou.

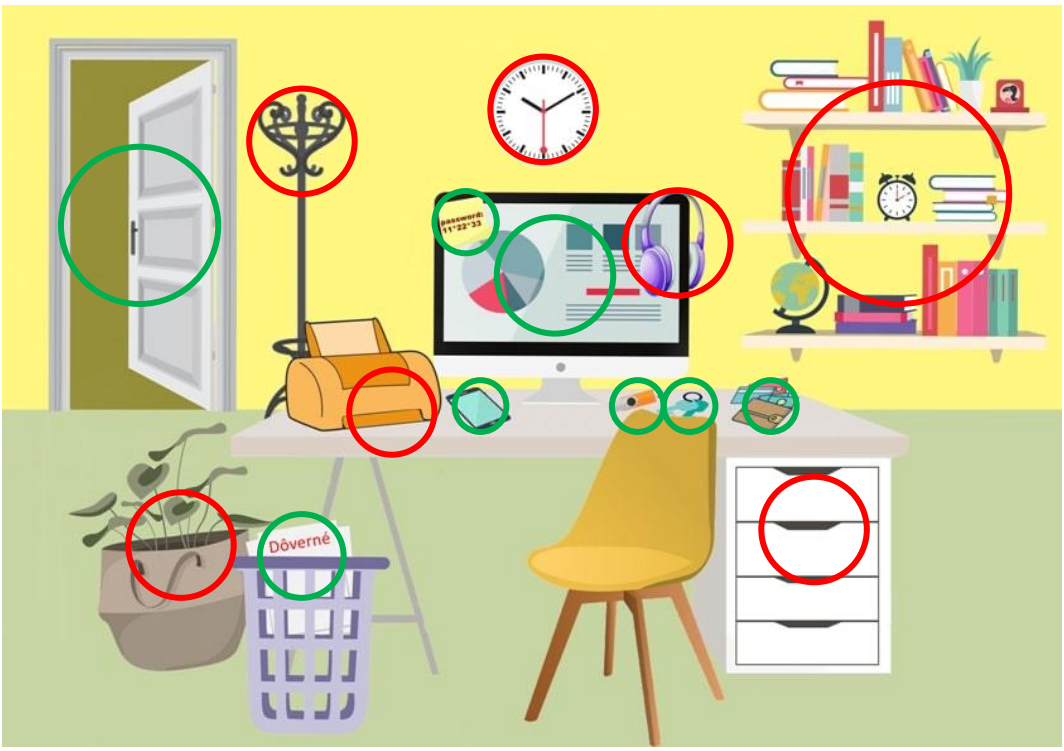
1.4 Obrázky v aplikácií

Prvým pridaným obrázkom je Obr. 1, na ktorom sú zvýraznené predmety, na ktoré môže používateľ klikať. Zeleným kruhom sú označené predmety, ktoré porušujú pravidlá. Teda tie, ktoré by mal používateľ nájsť a označiť. Červenou sú označené predmety, ktoré slúžia na zmätenie. V tomto prípade by na nich užívateľ kliknúť nemal.



Obrázok 1. Zásady 1 - obrázok v aplikácii

Druhým obrázkom je Obr. 2. Na ňom sú rovnakým spôsobom zvýraznené predmety, ktoré porušujú pravidlá a tie, ktoré sú určené len na zmätenie používateľa.



Obrázok 2. Zásady 2 - obrázok v aplikácii

2 Phishingové emaily

Od októbra 2013 do decembra 2016 FBI vyšetrila viac než 22 000 phishingových útokov zameraných na podniky v Spojených štátoch amerických. Celková strata sa vyšplhala na 1,6 miliardy dolárov, teda približne 500 miliónov dolárov ročne [13]. V roku 2019 FBI zaznamenalo 23 775 sťažností na Business Email Compromise útoky, ktoré viedli k stratám viac ako 1,7 miliardy dolárov [14]. BEC útoky využívajú napodobnenú emailovú adresu alebo webovú doménu, ktorá sa javí ako od spoločnosti alebo jednotlivca, s ktorým obeť spolupracuje.

Podľa Donna Gregoryho, šéfa IC3 (FBI - Internet Crime Complaint Center), rok 2019 nebol významný novými metódami vo využívaní podvodných emailov a správ, ale vo vylepšovaní techniky a tak je náročnejšie všímať si červené vlajky [14]. Phishing sa vyvinul z jednoducho konštruovaných okamžitých správ na vytvorenie komplexnej podvodnej stránky, ktorá od užívateľa žiada osobné informácie [15]. Už je celkom bežné, že pri útokoch funguje deľba práce a trh. Existujú aj programy, ktoré dokážu vytvoriť kópie stránok, ktoré chce útočník zneužiť [16]. Tým pádom aj útočníci majú uľahčenú prácu a je tak pre nich jednoduchšie vytvoriť dôveryhodne vyzerajúcu správu.

Phishing sa vyvinul vo veľmi prepracovanú metódy získavania citlivých údajov. Tento pojem vo všeobecnosti označuje klamlivý email poslaný ľuďom s cieľom získania osobných informácií. V užšom slova zmysle je to kriminálna aktivita, ktorá využíva princípy sociálneho inžinierstva s cieľom získať citlivé informácie ako prihlasovacie meno a heslo, tým, že príjemcovi správy podvrhne falošnú verziu stránky, ktorú bežne navštevuje a pozná [15].

Vzhľadom na spôsob získavania informácií - email - sa môže jednoducho stať, že sa bude zamieňať za iný pojem. To, s čím sa najčastejšie stretávame v našich mailových schránkach sú spamy. Spam, na rozdiel od phishingu, je nevyžiadaný, hromadne rozposielaný email, napríklad zo sociálnej siete. Zväčša je reklamného charakteru, je veľmi jednoduché ho rozoznať od ostatných správ.

Spoofing je technika, pri ktorej sa útočník tvári skrýva za identitu dôveryhodnej osoby alebo inštitúcie [16]. Niečo podobné poznáme aj pod pojmom catfishing, no pri tomto sa môže útočník skrývať aj za neexistujúcou, ním vytvorenou osobou a jeho hlavným zámerom je vlákať obeť do vzťahu [17]. A v neposlednom rade pharming je metóda presmerovania webovej stránky internet bankingu na iný server.

Kompozícia správy môže byť rôzna. Niektoré správy sú pripravované pre väčšie publikum, obsah môže byť pomerne všeobecný. Napríklad, známe maily od nigérijského princa, ktorý ponúka peňažnú odmenu za možnosť transferovať peniaze prostredníctvom bankového konta obete. K týmto mailom však patria aj tie, ktoré sa zdajú byť z banky a upozorňujú na zmeny v systéme, v obchodných podmienkach alebo upozorňujú na chybu či útok a s touto zámienkou žiadajú od obete údaje o bankovom konte alebo dokonca prihlasovacie údaje do internet bankingu [18]. Z tohto dôvodu v dnešnej dobe je prihlasovanie do internet bankingu dvojstupňové.

Druhý typ phishing te tzv. spear-phishing, kedy je správa "šitá na mieru" konkrétnej osobe. Vtedy mu predchádza získavanie údajov o obeti. Email pôsobí, že ho odoslala osoba alebo organizácia, ktorú obeť pozná. Teda je väčšia pravdepodobnosť, že sa obeť nechá zlákať a poskytne svoje osobné údaje útočníkovi. V tomto type sú väčšinou obeťami politici, zamestnanci na vysokých pozíciách či dokonca riaditelia firiem [19]. Takáto správa potom ohrozuje už nie len osobu, ktorej bola doručená, ale celú firmu či organizáciu.

2.1 Ako rozpoznať phishingový email?

Spôsoby získavania informácií sú dnes veľmi prepracované, preto rozoznať phishingový email môže byť náročné. No nie nemožné. Vzhľadom na to, že ohrozený je v podstate každý, kto ma emailovú schránku, tejto téme sa venujú aj populárne webové portály. Všetky návody sa v niečom odlišujú, ale často sa stáva, že sa niektoré body opakujú alebo sú len parafrázované. Stáva sa však aj to, že s vývinom nových taktík niektoré už niektoré tipy nie sú spoľahlivé. Ako príklad môžeme uviesť HTTPS protokoly. HTTPS protokol sa od HTTP odlišuje bezpečnostným certifikátom SSL (Secure Socket Layer) a bol tak synonymom bezpečnosti. Avšak podľa Anti-Phishing Working Group, Ins [US] v prvej štvrtine roka 2019 až 58%phishingových stránok malo SSL certifikát [20].

Ako je teda možné chrániť sa pred phishingovým útokom? Nižšie je uvedených pár tipov, ktoré sú často opakované, vybraté z troch hlavných zdrojov [21-23].

Žiadanie dôverných informácií prostredníctvom emailu

Prvý bod sa nachádza a zároveň nenachádza v samotnej správe. Je dôležité si uvedomiť, že legitímne spoločnosti nežiadajú od svojich klientov dôverné informácie prostredníctvom emailu.

Verejná doména

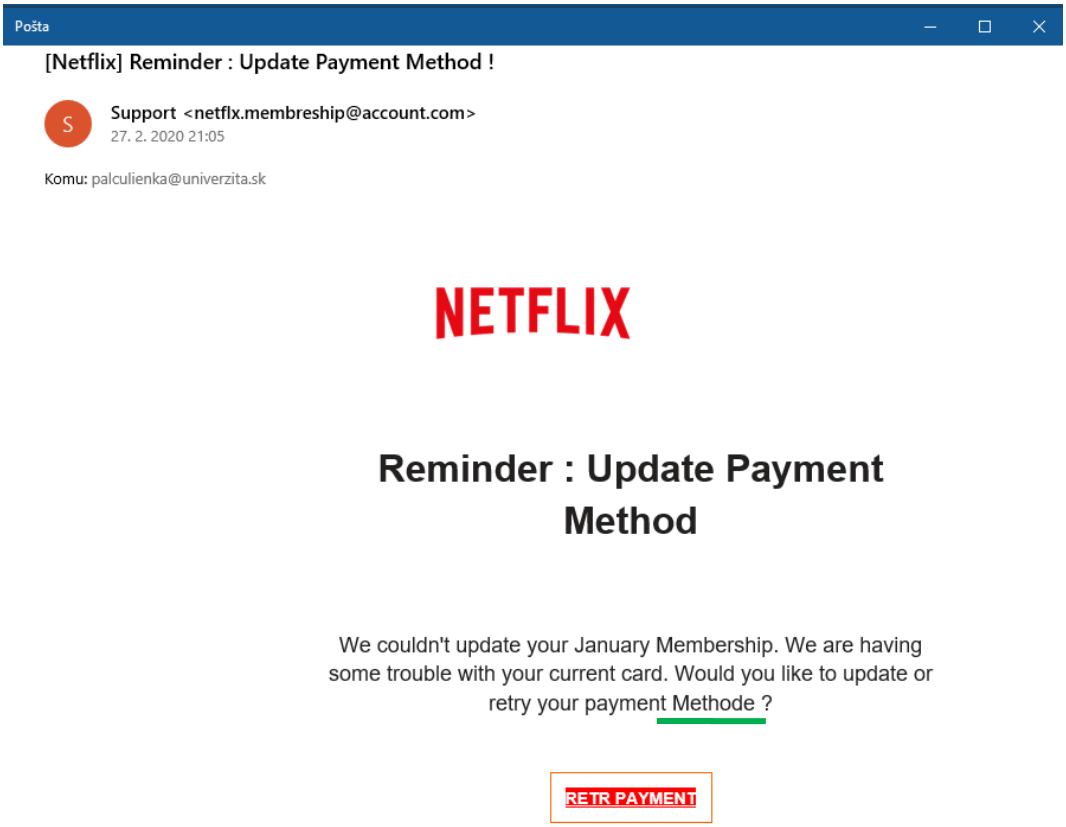
Pochádza email z verejnej emailovej domény? Ak áno, v takom prípade nie je veľmi dôveryhodný. Väčšie spoločnosti a podniky majú svoje domény. Teda je vysoko nepravdepodobné, že by mohol niekomu prísť email, žiadajúci čitateľa o jeho prihlásenie do internet bankingu odoslaný z emailovej adresy ktorá končí "@gmail.com", preto je potrebné si všímať emailovú adresu odosielateľa.

Preklepy v adrese

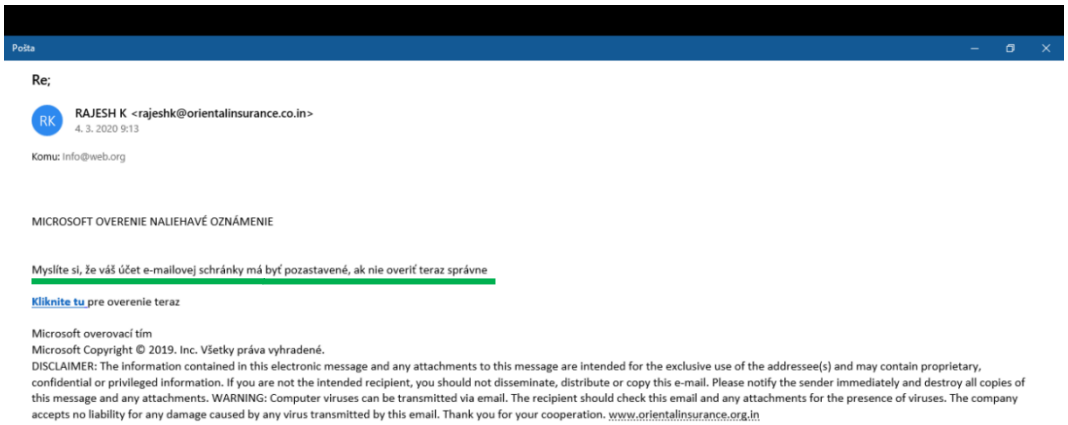
V nadväznosti na predchádzajúci bod, je potrebné všímať si adresu pozorne. Môže sa totiž zdať, že sa nápadne podobá na adresu alebo doménu, ktorú poznáme, no obsahuje menší preklep. Vzhľadom na to, že domény sa dajú kúpiť u registrátora domén a jedinou podmienkou je, že každá doména je unikátna, existuje možnosť, že sa doména emailovej adresy odosielateľa podobá, na inú známu adresu.

Chyby v texte

Pozornosť na gramatiku by sme mali zamerať aj v tele správy. Ak sa v ňom nachádzajú gramatické chyby, mali by sme zvýšiť pozornosť. Tieto chyby tam nie sú nepozornosťou hackera. Bolo by ťažké uveriť, že človek, ktorý stojí za takto prepracovaným projektom by mal takéto veľké medzery v gramatike. Môže to byť zámerné, pretože je vysoko pravdepodobné, že ľudia, ktorí si menej všímajú takéto mýlky v správe samotnej, budú menej pozornejší voči všetkým červeným vlajkám, ktoré sa môžu vyskytnúť. Podľa spoločnosti ESET však ani toto už dnes nie je pravidlom, mnohí útočníci dnes využívajú služby profesionálnych prekladateľov [23]. Z tohto dôvodu je lepšie zamerať sa skôr na chyby v štruktúre vety ako v chybách v jednotlivých slovách.



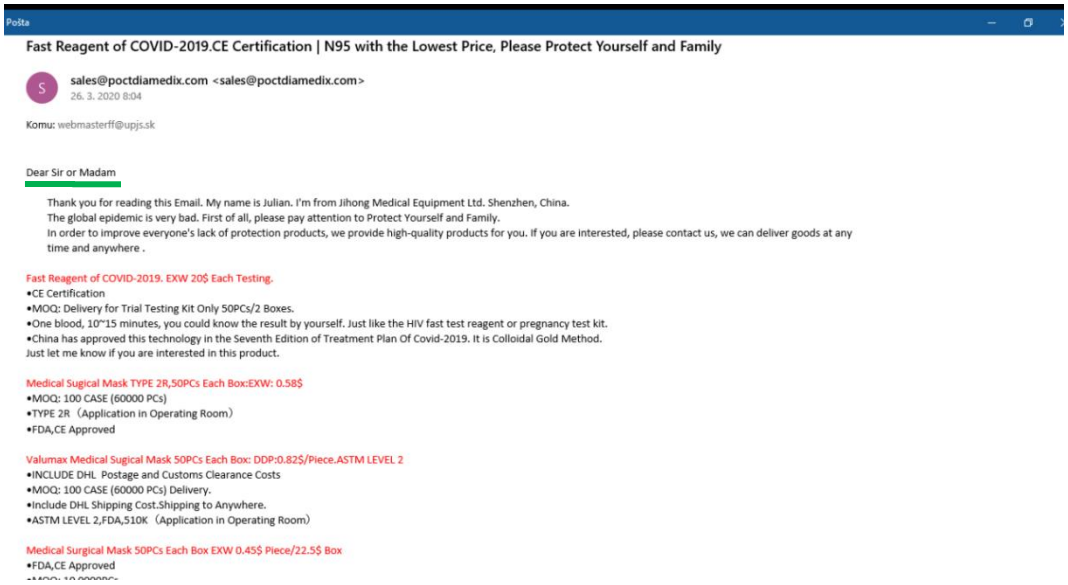
Obrázok 3. Ukážka - chyba v texte



Obrázok 4. Ukážka - Chyba v texte

Všeobecné oslovenie

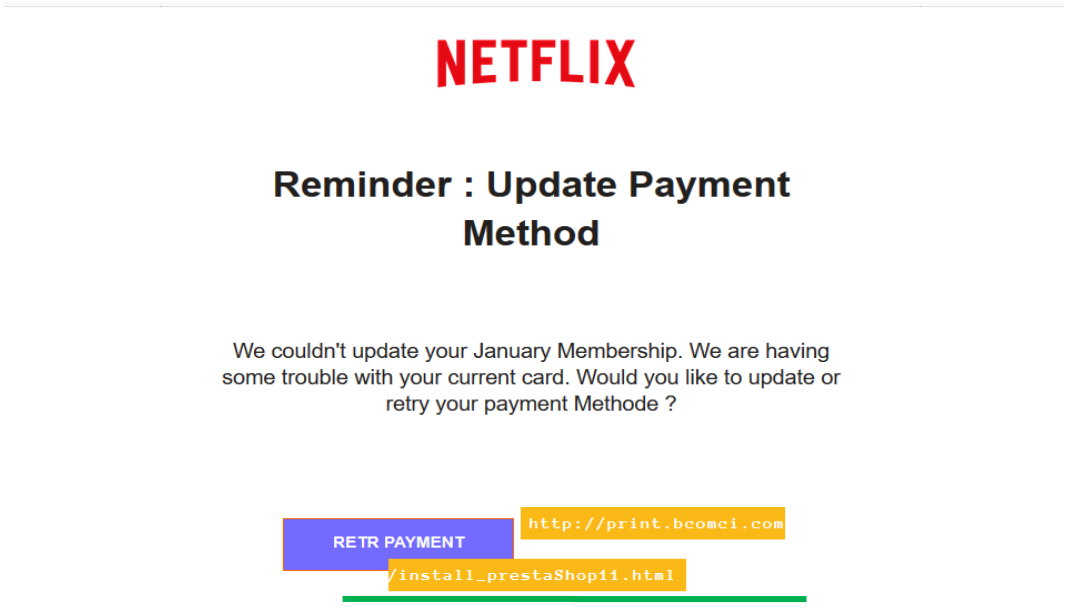
V obsahu samotnej správy môže byť ukazovateľom aj oslovenie. Ak by spoločnosť žiadala od niekoho špecifické informácie, oslovila by klienta priamo menom, nie “Vážený zákazník, ...”



Obrázok 5. Ukážka - Všeobecné oslovenie

Linky a presmerovanie

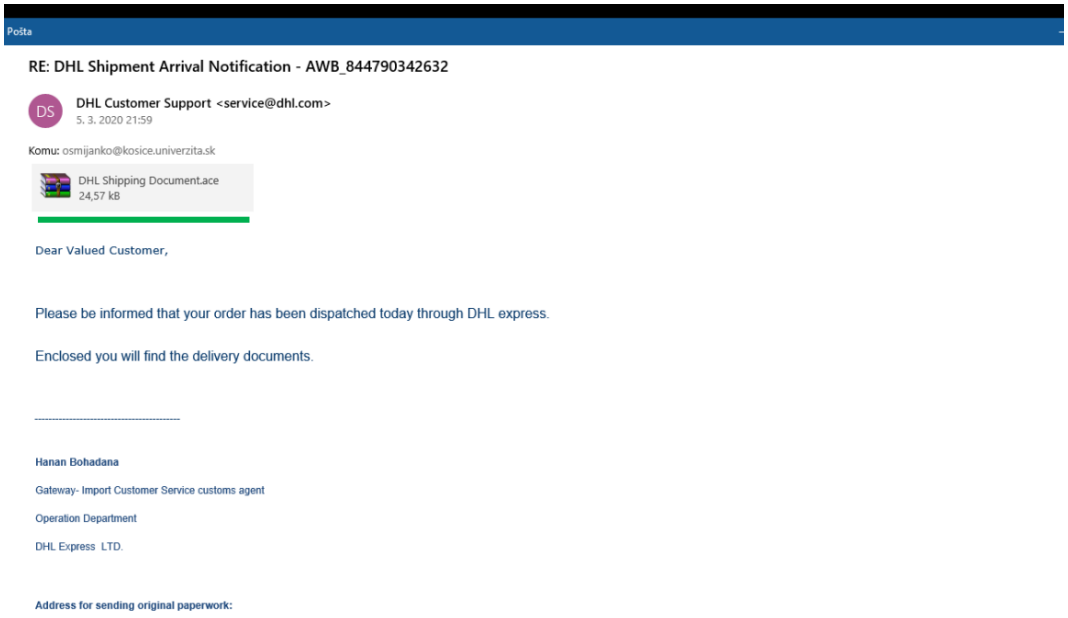
Môže sa stať, že telo emailu obsahuje linky, ktoré majú príjemcu niekam presmerovať. Väčšinou sú tieto linky zamaskované ako tlačidlo nachádzajúce sa v tele správy. Okrem toho, že tieto linky môžu požadovať klientovo prihlásenie, adresa na ktorú smeruje sa veľmi pravdepodobne nebude zhodovať s webovou stránkou inštitúcie.



Obrázok 6. Ukážka - Linky a presmerovanie

Prílohy v emaile

Email obsahuje prílohu. Nie je to nič nezvyčajné, množstvo správ, ktoré sa odosielajú a prijímajú obsahujú prílohu. Zbystriť pozornosť by sme mali, ak súbor končí príponou *.exe alebo *.zip. Tieto sú tie najčastejšie posielané a najnebezpečnejšie. Nenápadnejšie môže byť maskovanie prílohy príponou *.pdf. Zoberme si príklad ak príjemcovi príde email s prílohou nazvanou "Faktúra.pdf". je prirodzené, že príjemca na ňu zo zvedavosti klikne, aj keď si všimne, že faktúra môže byť pre niekoho iného môže byť už neskoro. Malvér sa už sťahuje do zariadenia klienta. Mnoho zariadení má však antivírusovú ochranu, preto ak vyskočí ochranné okno s podozrením na vírus, netreba ho ignorovať. Základné pravidlo, ktoré tu platí, je otvárať len prílohy, ktoré očakávame. V opačnom prípade je lepšie preventívne kontaktovať odosielateľa mailu nejakým alternatívnym spôsobom, napríklad telefonicky, a overiť si bezpečnosť prílohy.

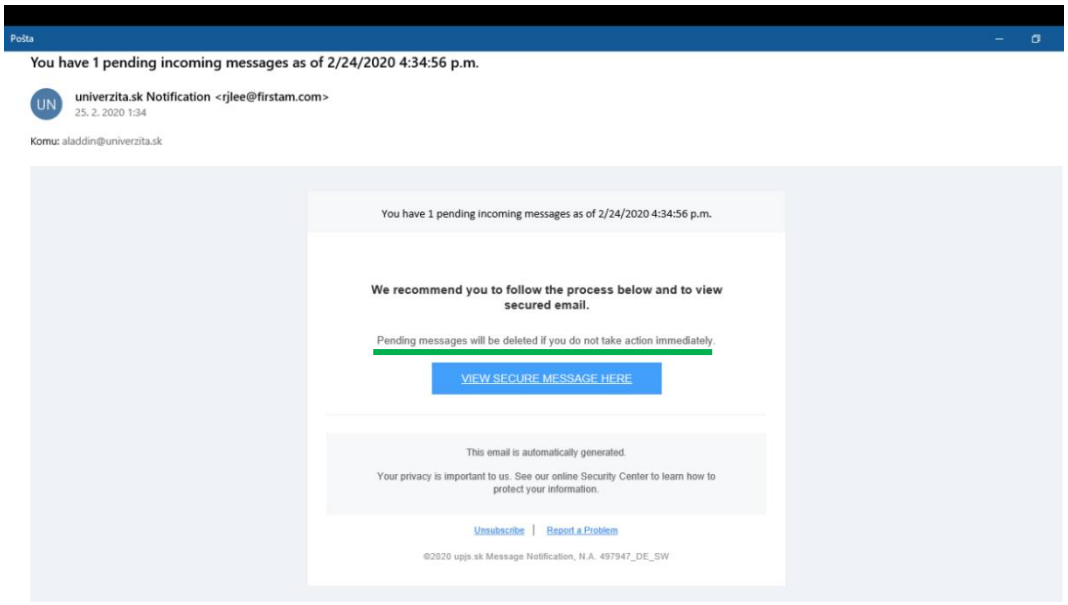


Obrázok 7. Ukážka - Prílohy v maile

Vzbudenie urgencie

Posledným z tých základných tipov je, že email vzbudzuje urgenciu. Útočníci sú si vedomí toho, že väčšina z nás odkladá všetko na poslednú chvíľu s tým, že sa o to postaráme neskôr. Sú si vedomí toho, že čím dlhšie s niečím budeme čakať, tým viac nepresností v maile si môžeme všimnúť. Preto sa snažia vytvoriť pocit naliehavosti, no spoločnosti, ktorých služby bežne využíva množstvo klientov, napríklad Netflix,

Windows, PayPal poskytujú služby, ktoré sú pravidelné využívané, preto je nepravdepodobné, že by poslali email, ktorý si vyžaduje klientovu okamžitú pozornosť. Netýka sa to len striktne mailov od veľkých spoločností. Útočníci si sú vedomí toho, že ak niekomu z nás pošle šéf alebo riaditeľ email, ktorý vyžaduje našu okamžitú pozornosť, môže pre dekoráciu dodať, že na tom závisí stav spoločnosti, pustíme z rúk všetko na čom momentálne pracujeme a okamžite vybavíme daný email. Tu vzniká pre útočníka aj ďalšia výhoda v tom, že aj keď email vyzerá podozrivo, väčšina z nás by kvôli nemu nešla konfrontovať svojho šéfa, ale radšej by sa postarali o čokoľvek, čo žiada.



Obrázok 8 Ukážka - Vzbudenie urgencie

Prevencia

Najúčinnejším liekom je prevencia, preto aj tu platí, že riziku z phishingových správ sa dá predísť vzdelaním v danej oblasti.

Nahlásenie phishingového emailu

Posledný bod je o tom, čo robiť ak sa k nám dostane podozrivý email. V tomto štádiu je najlepšie priamo kontaktovať "odosielateľa". Teda ak je ako odosielateľ správy uvedená banka, kontaktovať priamo banku a spýtať sa na konkrétny email a nahlásiť ho.

2.2 Webová aplikácia

Phishingové útoky sú úspešne preto, že ich princíp je založený na sociálnom inžinierstve. Hlavným spôsobom, ktorý sa využíva je psychológia. Preto identifikácia phishingovej správy nie je tak rovnako implementovateľná ako spamy. Správy sú príliš rôznorodé a ako bolo už vyššie spomínané, mnoho pomôcok sa ukrýva medzi riadkami textu.

Z tohto dôvodu sme sa zameriavame na vzdelanie človeka ako na najlepšiu ochranu. "*Nezáleží na tom koľko firewallov, šifrovacích softvérov, certifikátov alebo dvojstupňových autentifikačných mechanizmov má organizácia, pokiaľ človek sediaci nad klávesnicou sa nachytá na pshishing* [18]*"*.

Pripravujeme jednoduchú webovú aplikáciu, na ktorej si môže hráč prejsť niekoľkými skutočnými phishingovými správami. V bezpečnom prostredí tak príde do kontaktu s potenciálnou hrozbou. Hráč musí rozhodnúť o správe, ktorú práve vidí, či je phishing alebo legitímna správa. V rozhodovaní si môže pomôcť nápoveďami, ktoré mu zvýraznia čo je potrebné si všimnúť.

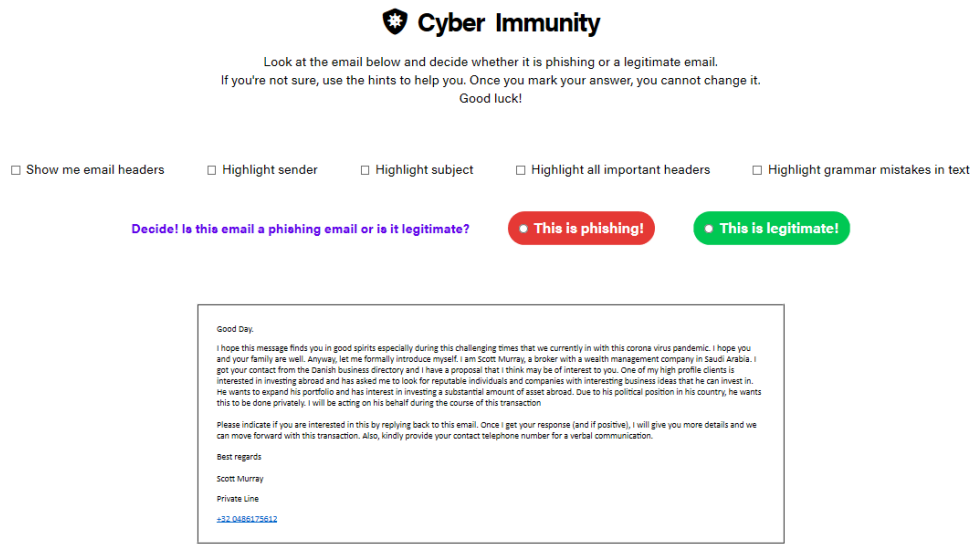
Úvodná stránka obsahuje krátky text o tom, prečo je phishing nebezpečný. Upozorňuje na to, že už to nie je len jednoduchý email a rozpoznať správu môže byť náročná výzva. V skratke oznamuje, že správa môže často obsahovať link, ktorý presmeruje užívateľa na podvodnú stránku alebo obsahuje možnosť stiahnuť si malvér.

Samotná stránka so správou je zobrazená na Obrázku 1 Implementácia tohto testu je prístupná na stránke *cyber-immunity.online*. Vo vrchnej časti stránky je vysvetlenie ako s aplikáciou pracovať. Pod textom sa nachádzajú checkboxy s nápoveďami. Najčastejšie využívané pomôcky sú:

- `Show me email headers` - zobrazí všetky hlavičky, ktoré email zobrazuje.
- `Highlight sender`- Emailová adresa odosielateľa môže napomôcť k rozhodovaniu. Obsahuje hneď niekoľko indícií:
    - meno pred @ obsahuje preklepy
    - použitý verejný webový klient (email z banky prišiel z adresy `*@gmail.com`)
    - v doméne (za zavináčom) je preklep (`@netflx.com` namiesto `@netflix.com`)

- odosielateľ sa nezhoduje s emailovou adresou v hlavičke emailu Reply-To

- `Highlight subject` - slúži na pomoc zaradenia emailu, napríklad ak subject začína RE:, teda ako odpoveď na email, ktorý vlastne neexistuje
- `Highlight all important headers` - email obsahuje niekoľko hlavičiek, táto pomôcka zvýrazní odosielateľa, predmet a prijímateľa správy
- `Highlight links` - práve tie môžu byť kľúčové pri odhalení správy.
- `Highlight grammar mistakes in text` - táto pomôcka nie je aplikovateľná pri všetkých správach a ako bolo vyššie uvedené, už nie vždy je tento bod upozornením podvodnej správy, stále sú však správy, pri ktorých gramatika odhalí, či je správa legitímna



Obrázok 9 Ukážka rozhrania zo cyber-immunity.online

Hneď po rozhodnutí (kliknutí na odpoveď) dostáva hráč spätnú väzbu. Ak správu identifikoval správne, či už ako phishing alebo legitímnu, otvorí sa mu stránka s oznámením a možnosťou pokračovať na ďalšiu správu. V prípade, že správa bola identifikovaná nesprávne, dostane sa hráč na stránku, na ktorej je pripravený krátky scenár s akými následkami by sa mohol v reálnom živote stretnúť pri takejto chybe.

Pri každej správe je dôležité stále myslieť na to, že sú emaily, ktoré treba vybaviť, nie je možné ignorovať každú správu ako phishing. Aj označenie legitímnej správy môže mať negatívne dôsledky.

Pri phishingovej správe, ktorá bola označená za legitímnu sa hráčovi takisto zobrazí stránka s upozorňujúca na jeho následky konania. Pre každý email vytvárame scenár, čo by sa mohlo stať, ak by sa používateľ nechal nachytať na phishing.

Prvý email bol od brokera zo Saudskej Arábie, ktorý má klienta túžiaceho po investícií do zahraničných podnikov. V emaily žiada len o spätnú väzbu, či má príjemca záujem o takúto formu spolupráce. V tomto prípade riziko nastane až keď sa príjemca rozhodne spolupracovať. Negatívny scenár, ku ktorému by táto situácia mohla viesť je, že daný broker ponúkne príjemcovi vysokú sumu peňazí, no na začiatku bude žiadať od príjemcu, aby mu poslal malú čiastku peňazí na jeho účet a tak by prišiel o svoje peniaze úplne, pretože broker by mu dohodnutú investíciu neposlal.

Ďalšie dva zo scenárov zameriavajú pozornosť na opatrnosť pri nakupovaní. Hráč dostal mail o výhodnej cene kvalitných masiek chrániacich pred vírusom Covid-19. Linka, na ktor smerujú tlačidlá v správe, začína amazon-medical-mask.... čím môže nepozorného užívateľa zmiasť, že ide o stránku amazon.com. Pri kliknutí na email sa môže zobraziť stránka podobná prihlasovacej stránke Amazonu, ale nie je tomu tak. Po zadaní prihlasovacích údajov získa útočník prihlasovacie meno a heslo do Amazon účtu obete.

Posledný email upozorňoval používateľov na možnosť nákupu potravín online. Pozornosť užívateľa upriamoval na tlačidlá, ktoré by mali o tejto možnosti povedať používateľovi viac. Situácia, ktorú volíme ako negatívny scenár, je upozornenie o tom, že bol práve infikovaný ransomvérom a všetky jeho súbory boli zašifrované. Za kľúč odšifrovanie si útočníci pýtajú čiastku okolo 500€.

Dôvod prečo sme sa rozhodli zakomponovať tieto hodnotiace stránky je, aby hráči získali skúsenosť alebo aspoň skúsenosti blízky pocit, že sa dostali do ohrozenia. Navyše je to forma averzného podmieňovania, kde negatívna reakcia, napríklad trest, vedie k zníženiu pravdepodobnosti, že sa bude opakovať správanie, ktoré túto reakciu vyvolalo [24]. V našom prípade je touto negatívnou reakciu práve hodnotiaca stránka, ktorá sa objaví, ak používateľ nesprávne identifikuje dôveryhodnosť správy.

Aplikácia obsahuje niekoľko mailov. Pôvodný nápad bol rozdeliť ich do určitých levelov a ich náročnosť by sa zvyšovala. Nie je však možné jednoznačne porovnať dva

maily a povedať, ktorý je viac phishingový alebo ťažšie identifikovateľný. Tiež by sme nemohli rozhodnúť, do ktorej úrovne by bolo možné zaradiť legitímne správy. Preto sme od tohto nápadu upúšťame. Všetky správy sú tak považované za rovnocenné.

Hru je možné opakovať, ale správy sa nemenia. Každý email je jedinečný, preto je potrebné každý analyzovať samostatne a vyznačiť jeho možné indikátory. Z tohto dôvodu aplikácia obsahuje len obmedzený počet správ. Na druhej strane je program otvorený rozšíreniam. Pridávanie nových správ zahŕňa celý priečinok stránok a scenárov, ktoré je potrebné vziať do úvahy. Samotná správa je len jeden HTML súbor, v ktorom sa dajú pridávať položky na zvýraznenie. Funkcionalita pre často opakované zvýraznenia a pomôcky je pripravená v JavaScripte.

Pri práci pracujeme so skutočnými emailami. Každý email však obsahuje informácie, ktoré by mohli jednoznačne identifikovať príjemcu správy. Bez súhlasu so spracovaním osobných údajov tak akákoľvek práca s týmito emailami porušuje GDPR [25]. Ako riešenie sa naskytá anonymizácia, avšak nadmerná anonymizácia môže znehodnotiť údaje, ktoré sú predmetom skúmania, čo môže viesť k nesprávnym výsledkom [26]. Údaje, ktoré budeme anonymizovať sú emailová adresa príjemcu a IP adresa. Emailovú adresu, kvôli tomu, že spravidla každá emailová adresa musí byť jedinečná. Väčšina inštitúcií dokonca využíva na vytváranie emailových schránok zaužívané pravidlá ako použitie mena a priezviska zamestnanca. Kvôli tomu je možné jednoznačne identifikovať komu emailová adresa patrí. Druhým údajom je IP adresa. Napriek tomu, že práva na jednoznačnú identifikáciu osoby pomocou IP adresy má len Poskytovateľ Internetových Služieb, identifikácia je možná a z toho dôvodu sme sa rozhodli anonymizovať aj tento údaj. Ako spôsob anonymizácie využívame substitúciu. Emailovú adresu príjemcu nahrádzame adresou cinderella.charming@upjs.sk. IP adresu sme nahrádzali náhodnými číslami z rozsahu 0-255, aby výsledná adresa vyzerala ako skutočná IP adresa.

2.3 Technická implementácia

Na začiatku procesu máme niekoľko podvodných správ. V každej správe sa zameriavame na hlavičku aj na telo. Pred začatím je nutné sa zamyslieť, ktoré informácie zobraziť a ako ich čo najlepšie ukázať. Pre ucelenosť informácií uvedieme celú hlavičku emailu, no kvôli jej veľkosti ju ukážeme používateľovi až keď si ju vyžiada. Inými slovami, až keď zaklikne pomôcku, ktorá mu ukáže časť alebo celú hlavičku.

Aby sme poskytli používateľovi čo najbližší zážitok, snažíme sa zobraziť email tak, ako bol poslaný. To je možné konvertovaním tela textu do formátu HTML, ktorý sme následne vkladáme do dokumentu, v ktorom už bola hlavička a nápovede. Telo HTML dokumentu začína práve nápoveďami.

Ukážka zdr. kódu 5. Pomôcky v dokumente

```
<ul id="hints>
    <li>
      <input type="checkbox" id="show-email-subject" name="show-email-
subject"><labelfor="show-email-subject"> Show email subject</label>
    </li>
</ul>
```

Zvýraznenie nápovede je v jednom spoločnom dokumente pre všetky emaily. Nie je tak potrebné pre každý email vytvárať samostatný dokument s funkcionalitou. Dokument je napísaný v jazyku JavaScript.

Ukážka zdr. kódu 6. Zvýraznenie pomôcok

```
FunctionhighlightSubject(command){
switch(command){
case 1:
$("#email-header").removeClass('hidden');
$('input[type=checkbox][name=show-email-headersall]').prop("checked",
true);
$("#email-header").addClass('highlighted');
break;
case 0:
$("#email-header").removeClass('highlighted');
break;
default:
break;
}
}
```

Vyššie znázornené ukážky kódov sú konkrétne funkcie slúžiace na zvýraznenie predmetu emailovej správy. Zároveň však môžu slúžiť aj ako príklad, keďže takýmto spôsobom je možné zvýrazniť akúkoľvek časť správy. Tým ostáva program otvorený akýmkoľvek doplneniam a prispôsobeniam v tomto smere.

3 Heslá

"*Tak ako sa webová technológia posúva o krok dopredu v iných oblastiach, heslá tvrdohlavo prežívajú a reprodukujú sa s každou novou webstránkou.* [27]" S heslami sa potykáme každý deň. Každý, kto má email, účet v banke alebo na sociálnej sieti si musí prejsť tvorbou hesla. Heslo by malo chrániť informácie o používateľovi, organizácií, financiách, alebo aj súkromné súbory, fotografie, kontakty. Princíp, ako funguje heslo, je jednoduchý. Pozná ho len osoba, ktorá ho vytvárala, teda majiteľ účtu. Heslo je jednofaktorová identifikácia, preto riziko narastá s každou osobou, ktorá pozná heslo.

Používateľ by si mal heslo chrániť, aby ho nikto nezistil, ale je dôležité, aby si heslo pamätal a to je väčšinou na úkor sily hesla. "*Počítačové heslá majú byť tajné. Avšak psychológovia tvrdia, že je možné predpovedať heslo podľa osobnosti používateľa alebo dokonca aj podľa toho, čo majú na ich pracovnom stole ... Podľa nedávnej Britskej štúdie sú heslá často založené na niečom očividnom. Približne 50 percent počítačových používateľov vytvárajú svoje heslá na základe mien rodinných členov, partnerov alebo domácich miláčikov. Tridsať percent sa obrátili k popovej hviezde alebo športovému hrdinovi.* [28]" Problémom je tiež aj to, že používatelia si nemenia heslá často [29].

Na základe rôznych algoritmov prelomenia hesla sú aj rôzne kritéria silného hesla. Napríklad podľa Dr. Wayne C. Summers and Dr. Edward Boswort z Columbus State University sú silné heslá tie, ktoré spĺňajú nasledovné kritéria [29]:

- Obsahuje aspoň 6 znakov.
- Čím dlhšie heslo, tým dlhšie trvá jeho prelomenie.
- Musí obsahovať aspoň 3 z nasledovných: malé písmeno, veľké písmeno, číslica a špeciálny znak. Čím variabilnejšie, tým ťažšie na prelomenie.
- Nepoužívať "slovníkové" slová. To zahŕňa aj slovníky vlastných podstatných mien a cudzojazyčné slovníky. Vyhýbať sa "bežným slovám" s číslicami pripojenými na konci.
- Návrhy dobrých hesiel môžu zahŕňať použitie prvých písmen frázy s vhodne nahraditeľnými písmenami.

Ďalšie vlastnosti hesiel zahŕňajú [29]:

- Nepoužívať posledných 5 hesiel. Niektoré spoločnosti odporúčajú vôbec nepoužívať už použité heslá.
- Minimálny vek hesla by mal byť 10 dní.
- Maximálny vek by mal byť 45-60 dní. Toľko by malo totiž trvať hackerovi prelomenie hesla.
- Zabezpečenie limitovaného počtu pokusov na zadanie hesla po 3-5 pokusoch. To by malo odradiť hackerov od skúšania rôznych kombinácií hesiel.
- Nezapisovať si heslá na papier.
- Nezdieľajte heslá.
- Používatelia si musia zmeniť heslo hneď ako majú podozrenie, že heslo môže byť odhalené.
- Používateľský účet by mal byť deaktivovaný po 30 dňovej nečinnosti.
- Počas zadávania hesla nesmie byť heslo viditeľné.
- Ak je na stránke/platforme/sieti predvolené heslo, musí byť zmenené používateľom pre prvým použitím stránky.
- Vzdelávať ostatných používateľom o heslách.

Tieto princípy sa líšia v závislosti od autorov, ale existujú aj iné aspekty, ktoré sa berú do úvahy. Silné heslo by malo byť považované za silné ak naň pozeráme z pohľadu nasledujúcich troch aspektov [30]:

- Metóda založená na útoku meria silu hesla podľa času, ktorý je potrebný na jeho prelomenie. Tento parameter je priamo spojený so spôsobom útoku - hádanie hesla. Využíva práve to, že ľudia sú predvídateľní. Tieto útoky sú najvšeobecnejšie. Spôsob, akým funguje, prelomí veľké množstvo hesiel, zároveň však produkuje aj mnoho nesprávnych možností, čo ho spomaľuje.
- Heuristický spôsob meria silu hesla počtom bitov entropie. Existujú rôzne vzory, podľa ktorých sa meria sila hesla. Napríklad metóda, berie do úvahy počet malých písmen, veľkých písmen, čísel a špeciálnych symbolov. Mohlo by sa zdať, že táto metóda je dostatočná, pretože práve to sú pravidlá, ktoré sa od nás väčšinou vyžadujú pri vytváraní nového hesla. Opak je pravdou. Ukazuje sa, že je stále veľa typov hesiel, na ktoré tento princíp neplatí. Tento prístup označí heslo “David-1982” za silnejšie ako “RpixTsGa” [30].

- Pravdepodobnostná metóda je založená, ako už názov napovedá, na štatistickej pravdepodobnosti hesla. I keď by sa mohlo zdať, že každý užívateľ vytvára heslá náhodne, tento princíp odhaľuje nedostatok náhodnosti pri "náhodných heslách. Odhaľuje princípy podľa akých ľudia vymýšľajú svoje heslá. Teda čím pravdepodobnejšie heslo, tým je slabšie a naopak.

Okrem toho najspoľahlivejším a zároveň najnespoľahlivejším zdrojom hesla sú ľudia samotní. V roku 2015 sa redaktori show Jimmy Kimmel Live vydali na Hollywood Boulevard a pýtali sa ľudí na heslá. Ľubovoľne heslá, ktoré využívajú. V tomto prípade, ak ľudia nepovedali rovno svoje heslo, svoje heslo prezradili po pár otázkach [31]. Rovnaký pokus zopakovali v roku 2017 s podobným výsledkom. Niektorí ľudia si už viac uvedomovali situáciu, ale heslo nakoniec stále prezradili [32]. Treba myslieť na to, že videá sú zostrihané, nedá sa teda pracovať s presnými číslami a porovnávať množstvo ľudí, ktorí heslo prezradiť nechceli. V každom prípade poukazuje to na to, že ľudia sú predsa len najslabším článkom v informačnej bezpečnosti. V roku 2019 pridal Youtubový kanál Cut video [33], kde sa pýtali 100 Američanov na ich heslá. V tomto prípade už boli ľudia opatrnejší, no ku koncu videa je už prestrih na ľudí, ktorí svoje heslo nakoniec vyzradili. V tomto prípade môže počiatočné váhavé správanie spôsobovať aj to, že video je natočené v profesionálnom štúdiu, ľudia sú teda opatrnejší v porovnaní s prvými dvoma videami, ktoré sa odohrávali na ulici.

Aj vyššie uvedené videá sú skutočnosťou prečo je stále potrebné venovať sa heslám a ich ochrane. Tomu ako sa naučiť tvoriť silné heslá sa venuje mnoho populárnych článkov, blogov, videí, no väčšinou len formou vymenovania tipov, ako vytvoriť silné heslo. Informácie, ktoré si každý z nás pasívne uvedomuje.

3.1 Princíp hry

Pravidlá hry Hangman alebo Obesenec spočívajú v tom, že jeden hráč si zvolí slovo alebo frázu, ktorú potom druhý hráč háda po písmenkách. Hádajúci hráč na začiatku vie len počet písmen hádanej frázy. Po jednom písmene sa pýta druhého hráča, či sa dané písmeno nachádza v hádanej fráze.

Ak sa tam dané písmeno nachádza, hráč, ktorý frázu vytváral, ho dopíše na všetky miesta kde sa nachádza. Podľa dohody aj vo všetkých formách. Teda ak sa hádajúci pýta na písmeno A, druhý hráč ho zapíše aj vo forme A, a, Á, á, ä.

Ak sa dané písmeno vo fráze nenachádza, hráč, ktorý frázu zadával, dokreslí na obrázok jednu čiaru. Spravidla hra začína od zeme, pokračuje zvislým stĺpom, horizontálnou latkou, diagonálnou latkou ako opora medzi týmito dvoma. Následne pokračuje ďalšia zvislá latka, povraz, hlava, telo, jedna ruka, druhá ruka, jedna noha, druhá noha. Znova podľa dohody záleží na tom, či bude mať obesený muž tvár alebo nie. V tomto bode, keď je panáčik obesený, hra končí a hádajúci hráč hru prehráva.

Hra sa vyhodnocuje automaticky po každom kole. Spravidla v našej verzii nie je možné prehrať. Hráč ma toľko pokusov koľko potrebuje na uhádnutie hesla. Cieľom nie je odradiť ho od hry prehrou, ale nechať ho uvedomiť si koľko času trávi nad hádaním jednotlivých typov hesiel.

Hra je určená pre jedného hráča. Podľa bežných pravidiel hru Obesenec alebo Hangman hrajú aspoň dvaja hráči, kde jeden vymýšľa slovo a druhý hráč ho háda. V tomto prípade hrá však len jeden hráč s počítačom, ktorý pre hráča pripraví hádané heslo, postupne ho odhaľuje a na konci hru vyhodnocuje.

Ako bolo spomínané vyššie, mnoho článkov a blogov sa venuje téme hesiel, ale zdrojov, ktoré by sa snažili interaktívne naučiť používateľov viac o heslách je málo. Naším cieľom je hravou formou ponúknuť užívateľovi skúsenosť zo strany hackera. Sám teda skúsi uhádnuť niekoľko hesiel a teda sám by si mal uvedomiť, že niektoré typy hesiel je ťažšie prelomiť ako iné.

3.2 Aplikácia

Pôvodný súbor bol prevzatý od užívateľa Youtube od používateľa JoeReisigl [34, 35], ktorý vo svojom videu popisoval ako program funguje a zdieľal ho ako opensource program [34]. Pôvodný program obsahuje niekoľko možností ako hru hrať. Pre jedného hráča alebo multiplayer. Pre jedného hráča ponúka 4 kategórie hry:

- Phrases
- Movies
- Songs
- Challenges

Prvé tri sú tradičný obesenec, kde hráč musí uhádnuť slovo alebo frázu, ktorá sa skrýva a pri každom neúspešnom pokuse posúva obesenca samotného bližšie k smrti. Hra sa považuje za vyhratú, ak hráč odhalí ukryté slovo alebo frázu. Prehrať sa nedá. Hráčovi je umožnené hádať až kým sa mu neminú písmená v abecede. Posledná

kategória funguje na opačnom princípe a to, že skryté je len jedno písmeno abecedy. Hra sa považuje za vyhratú, ak hráč uhádne všetky písmená, ktoré skryté nie sú.

Druhý mód hry je multiplayer. Tento mód je určený pre dvoch hráčov. Najskôr jeden zadá hádané slovo alebo frázu a potom druhý hráč háda podľa rovnakých pravidiel ako v móde single player v prvých troch kategóriách.

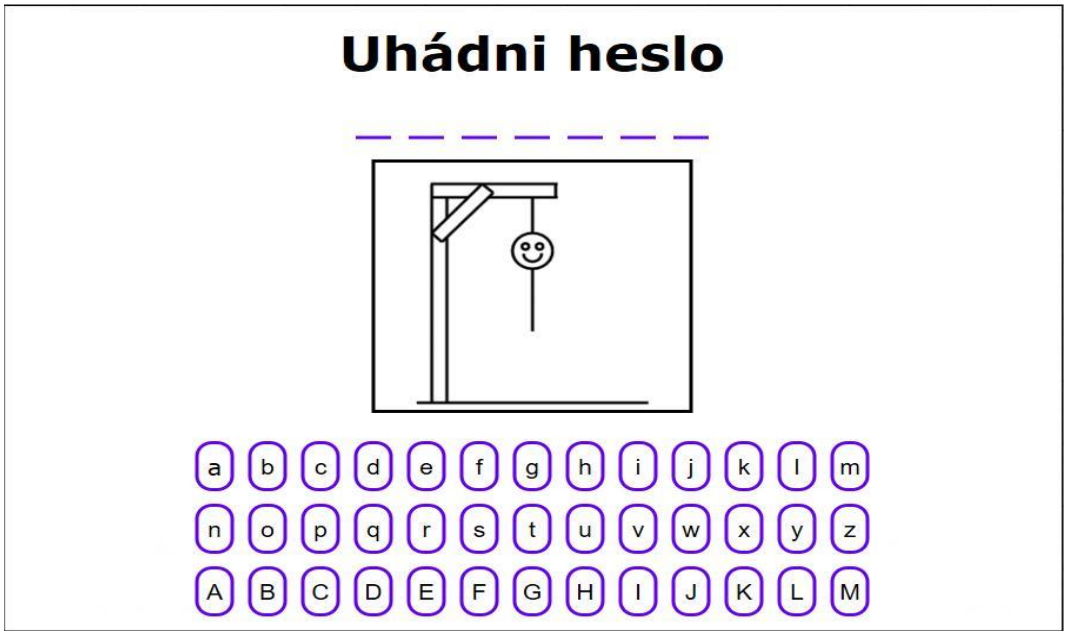
To je základ, s ktorým sme pracujeme a prispôsobujeme našim potrebám. V prvom rade sa musíme rozhodnúť, čo chceme používateľa naučiť a akým spôsobom. Možností je viacero. Jednou z nich je vniesť hráča do pozície útočníka a nechať ho hádať heslá. Náročnosť hesiel by sa zvyšovala každým levelom. Sám by si tak hráč uvedomil, že niektoré heslá je jednoduchšie uhádnuť ako iné.

Úrovne by sa tak odlišovali do seba v náročnosti. V každej úrovni sa generujú heslá, ktoré vyhovujú podmienkam danej úrovne. Zvyšujúcu sa náročnosť si používateľ všimne aj tým, že v rozhraní pribudnú nové tlačidlá - nová abeceda. Na prvej úrovni háda len s písmenami malej abecedy bez diakritiky, na druhej úrovni pracuje už aj s písmenami veľkej abecedy a na poslednej úrovni má pridané aj špeciálne symboly.

3.3 Technická implementácia

Celá hra sa skladá z troch dokumentov. HTML, JavaScript a CSS. Pôvodná hra bola nastavená tak, že pri prepínaní medzi módmi hry nebolo nutné prechádzať na ďalší dokument. V našej verzii hry sa však s každou úrovňou mení používateľské rozhranie a ovplyvňuje sa funkcia generovania hesla, preto každá úroveň je samostatný dokument.

Na Obrázku 10 je uvedený návrh rozhrania. Stránka obsahuje canvas, na ktorom sa vyobrazuje “obesenie”. Pod tým je hádané heslo a nižšie je abeceda, ktorú môže hráč využívať. Tá je nastavená tak, že po kliknutí na písmeno, číslo alebo znak, zmizne, aby nebolo možné kliknúť na jednu položku viackrát.



Obrázok 10 Návrh rozhrania hry Obesenec

Vo vyšších leveloch sa zobrazujú dve abecedy. S veľkými písmenami a malými. Je to dôležitý faktor pri určovaní sily hesla, preto program rozlišuje použitie malých a veľkých písmen. Do najvyššieho levelu je pridaná aj klávesnica so špeciálnymi znakmi. . Tieto znaky boli vybrané zámerne, pretože väčšina z nich sa dá jednoducho nájsť na klávesnici notebooku, stolového počítača, ale aj na mobilnej klávesnici, preto sú vhodné na využitie v heslách. Zároveň pri samotnej implementácií boli niektoré symboly vymazané, pretože sú zároveň špeciálnymi entitami v programovacom jazyku a preto sa program nespúšťal správne.

Každý level je jedinečný. Na začiatku program vygeneruje množinu hesiel podľa kritérií danej úrovne. Ich počet sa dá upraviť v programe. V heslách sa identifikujú ich spoločné znaky a odlišné znaky. Tie, ktoré sú jedinečné pre dané heslo. Tieto úpravy generátora značne ovplyvňujú jeho náhodnosť, preto samotný generátor nie je ideálny na generovanie skutočne náhodných hesiel, no pre potreby tejto hry je dostatočne náhodný.

Kritéria pre jednotlivé úrovne sú:

- Level 1 - obsahuje heslá dĺžky 6 znakov a len malé písmená
- Level 2 - heslá dĺžky 8 znakov, ktoré obsahujú malé aj veľké písmená
- Level 3 - heslá dĺžky 10 znakov obsahujúce malé aj veľké písmená, čísla a špeciálne znaky

Vďaka týmto úpravám je možné opakovať jeden level aj niekoľko krát, bez toho, aby sa množiny hesiel opakovali. Samotné vyhodnotenie tak berie do úvahy vyššie spomenuté kritériá a sleduje či sa hráč približuje k správnej odpovedi. Či využíva písmená a symboly, ktoré sú či už spoločné pre množinu hesiel alebo jedinečné pre dané heslo. Ak klikne na znak, ktorý sa nenachádza v žiadnom hesle v množine, odpoveď je označená ako nesprávna a prikreslí sa ďalšia časť obesenca.

Ako už bolo spomínané, v tejto verzii hry nie jemožné prehrať. Cieľom nie je ukázať hráčovi, že nedokázal uhádnuť nejaké heslo alebo množinu hesiel, ale ukázať mu ako dlho jemu samotnému trvá nájdene správnej odpovede.

Záver

Touto prácou sme sa snažili nájsť efektívnejší spôsob ako ľudí naučiť viac o informačnej bezpečnosti. V práci samotnej sme okrem poznatkov, štúdií a faktov z informačnej bezpečnosti pracovali aj s psychológiou a pedagogikou a skúmali sme formy učenia, ktoré sú efektívnejšie ako prednáška a sú vhodné pre široké spektrum používateľov.

Na začiatku práce bolo potrebné analyzovať jednotlivé hrozby a riziká a vybrať z nich tie, ktorým sa ďalej budeme venovať. V tejto časti sme nadviazali na už existujúcu prácu [5]. V tejto práci autor sa bližšie venuje heslám, sociálnemu inžinierstvu vo všeobecnosti a phishingovým emailom ako forme útokov, ktorá využíva praktiky sociálneho inžinierstva. Navyše sme k tomu pridali pravidlá čistého stola, pretože, rovnako ako vyššie spomenuté, sú relevantné pre každého, kto pracuje v kancelárií a s citlivými údajmi.

Každú z vybraných hrozieb sme podrobnejšie predstavili a popísali prečo je potrebné sa jej venovať. Spomíname aj to ako sa touto témou aktuálne zaoberajú rôzne zdroje a ako k nej pristupujú. Následne predkladáme návrh systému, ktorého cieľom je naučiť ľudí viac o danej téme.

Každé riešenie je jedinečné. V dvoch riešeniach využívame prvky gamifikácie a to hlavne možnosť zvyšovať úroveň a náročnosť hry. Všetky programy sú opakovateľné a otvorené pre ďalšie rozšírenie. Uviedli sme aj návody ako dané aplikácie rozšíriť alebo upraviť pre konkrétne potreby. Motiváciou tejto práce bolo aj to, aby boli výsledné systémy vhodné a dostupné pre verejnosť.

Tvorbe a návrhu jednotlivých aplikácií predchádzalo skúmanie psychologických štúdií o tom, ako sa ľudia učia a akým spôsobom si počas učenia osvoja čo najviac informácií. Našli sme mnoho článkov, vedeckých aj populárnych, ktoré sa zaoberali interaktívnymi aktivitami a ich výsledkami vo vyučovacom procese. Vzhľadom na to, že naša cieľová skupina sú dospelé osoby, museli sme niekoľkokrát uvažovať o iných spôsoboch interakcie.

Táto práca bola zameraná na návrh a vývoj systémov. Ich funkčnosť je podložená teoretickými princípmi z psychológie, no systémy neboli testované verejnosťou. To znamená, že konkrétne výsledky, či sú ako spôsob učenia účinnejšie ako prednášky a spísané materiály, je zatiaľ neznámy. Tu sa naskytá priestor rozšírenie tejto práce a otestovanie daných systémov počas školení o bezpečnosti. Následne porovnať výsledky

oproti školeniam, ktoré nevyužívajú túto formu interakcie. Priestor na zlepšenie poskytuje aj hra, ktorá sa venuje heslám. Na účely tejto práce a ukážky práce systému sme v niektorých bodoch tejto hry zvolili jednoduchší variant. Avšak aplikácia poskytuje priestor pre komplexnejšiu algoritmizáciu vyhodnocovania výsledkov a generovania hesiel pre jednotlivé úrovne.

Zoznam použitej literatúry

1. ANDRESS, J. 2014. Thebasics of informationsecurity: understandingthefundamentals of InfoSec in theory and practice. Syngress, 2014.658s. ISBN: 978-0-12-800744-0
2. WHITMAN, M.E. – MATTORD, H.J. 2012. Principles of InformationSecurity 4.vyd. CengageLearning. 2012. ISBN: 978-1-111-13821-9
3. Humanerroristheprimarycause of most dataleaks. TheDutchlend a helpinghandpointingoutthecauses. https://www.zivver.eu/en/blog/human-error-is-the-cause-primary-cause-of-most-data-leaks (2020-05-16)
4. PRINCE, Michael. Doesactivelearningwork? A review of theresearch. *Journal of engineeringeducation*, 2004, 93.3: 223-231.
5. CHOMIČ, P. 208. Systém na zvyšovanie povedomia v oblasti informačnej bezpečnosti. Košice: UPJŠ. 57s.
6. LIU, Z. 2008. Paper to Digital: Documents in theInformationAge. London: GreenwoodPublishing Group. 2008. 157s. ISBN: 978-1-59158-620-3
7. InformationSecurityPolicyTemplates. SANS Institute. In Sans.org [online] Dostupné na internete: <https://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy>
8. In Czechdarts.org [online]. 2020. [cit. 2020-05-18] Dostupné na internete: <https://www.czechdarts.org/storage/CSO_001_P2_Politika_cisteho_stolu.pdf>
9. 5 Benefits to Having a CleanDeskPolicy – PrivacySense.net. In PrivacySense.net [online]. 2020 [cit. 2020-05-18] Dostupné na internete: <http://www.privacysense.net/clean-desk-policy/>
10. STOBERT, E. – BIDDLE, R. 2015. Expert PasswordManagement. In: International Conference on Passwords. Springer, Cham, 2015. P. 3-20
11. In *Qscience.com* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.qscience.com/docserver/fulltext/qproc/2015/4/qproc.2015.elc2014.6.pdf?expires=1589828514&id=id&accname=guest&checksum=BC7527A26728B44D65CB205467F5D9DD>.
12. https://csirt.upjs.sk/#/navody/
13. MATHEWS, L. Phishing Scams Cost American Businesses Half A Billion Dollars A Year. In *Forbes* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete:

<https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/>.

14. FBI Releases 2019 Internet Crime Report - Merchant Fraud Journal. In *Merchant Fraud Journal* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.merchantfraudjournal.com/fbi-2019-internet-crime-report/>.
15. VAYANSKY, I. – KUMAR, S. 2018. Phishing – challenges and solutions. In Computer Fraud & Security. ISSN: 1361-3723, 2018, roč. 18, č. 1, s 15-20
16. Scams – Spam, Phishing, Spoofing and Pharming | Be in Charge of Your Digital Life | Cybersecurity Awareness Program: Lubbock | TTU. In *Ttu.edu* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.ttu.edu/cybersecurity/lubbock/digital-life/digital-identity/scams-spam-phishing-spoofing-pharming.php>.
17. TEAM, T. What Is Phishing, Spoofing, Ghosting, and Catfishing? - Bark. In *Bark* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.bark.us/blog/phishing-spoofing-ghosting-catfishing/>.
18. HONG, J. The State of Phishing Attacks. In *Dl.acm.org* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://dl.acm.org/doi/pdf/10.1145/2063176.2063197>.
19. https://www.youtube.com/watch?v=PR0c-gJ20kA
20. Phishing Activity Trends Report. In *Docs.apwg.org* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf>.
21. IRWIN, L. 5 ways to detect a phishing email – with examples - IT Governance UK Blog. In *IT Governance UK Blog* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email>.
22. ELLIS, D. 7 Ways to Recognize a Phishing Email: Email Phishing Examples. In *SecurityMetrics* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email>.
23. Ako rozpoznať phishing?. In *Eset.com* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-rozpoznat-phishing/>.
24. ATKINSON, R.L. a.i. 2003. Psychologie. 2.vyd. Praha: Portál, s.r.o. 2003. 751s. ISBN: 978-8-08-560535-8

25. REGULATION, General Data Protection. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ)*, 2016, 59.1-88: 294.
26. EL EMAM, K., DANKAR, F.K. 2008. Protecting Privacy Using k-Anonymity. In: *Journal of the American Medical Informatics Association*, Volume 15, Issue 5, September 2008, Pages 627–637,
27. BONNEAU, J. - HERLEY, C. - OORSCHOT, P. - STAJANO, F. IEEE Xplore Full-Text PDF:. In *Ieeexplore.ieee.org* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6234436>.
28. BROWN, A. 2002. UK Study: Passwords often easy to crack. In CNN.com. Dostupné na internete: http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/
29. SUMMERS, W. - BOSWORTH, E. CNN.com - UK study: Passwords often easy to crack - March 13, 2002. In *Cnn.com* [online]. 2020. [cit. 2020- 05- 18]. Dostupné na internete: <http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/>.
30. GALBALLY, J. – COISEL, I. – SANCHEZ, I. 2017. A New Multimodal Approach for Password Strength Estimation – Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*, 12(12), pp.2829-2844,
31. Jimmy Kimmel Live: *What's Your Password?.* 2015. Dostupné na internete: <https://www.youtube.com/watch?v=opRMrEfAIiI>
32. Jimmy Kimmel Live: *What's Your Password?.* 2017. Dostupné na internete: <https://www.youtube.com/watch?v=UzvPP6_LRHc>
33. Cut: 100 People Tell Us Their Password – Keep it 100 – Cut <https://www.youtube.com/watch?v=xWEEFFnJeIc>
34. Joe Reisigl: How to code a hangman game – HTML, CS, JavaScript (w/ source code) <https://www.youtube.com/watch?v=ZtNyfGyS00M>
35. Hangman: https://drive.google.com/drive/folders/0B4fAjHGILATeNm5pZHhpYnZhaEU