STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 14: Pedagogika, psychologie, sociologie a problematika volného času

SOCIÁLNÍ INŽENÝRSTVÍ (BEZPEČNOST)

Robert Škvařil

Jihomoravský kraj

Veverské Knínice 2018

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 14: Pedagogika, psychologie, sociologie a problematika volného času

SOCIÁLNÍ INŽENÝRSTVÍ (BEZPEČNOST)
SOCIAL ENGINEERING (SECURITY)

Autor: Robert Škvařil

Škola: Gymnázium T. G. Masaryka Zastávka, příspěvková organizace

U Školy 39, Zastávka u Brna 664 84

Kraj: Jihomoravský kraj

Konzultant: Ing. Stratos Zerdaloglu

Veverské Knínice 2018

Prohlášení

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

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

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

Ve Veverských Knínicích dne 31.1.2018 ...…….

Poděkování

Tímto bych chtěl poděkovat panu Ing. Stratosi Zerdaloglu za konzultace ohledně této práce především za umožnění provedení praktické části v budovách Mendelovy univerzity v Brně. V souvislosti s tím bych rovněž rád poděkoval mému spolupracovníkovi Jakubu Hemalovi, který se angažoval při organizování a provádění praktické části. Taktéž bych chtěl poděkovat všem, kteří se, ačkoliv nevědomky, praktického testu zúčastnili.

Díky patří také paní Ing. Ludmile Brestičové, která mi pro moji práci obstarala konzultanta a sama mi v jistých věcech radila.

Dále bych chtěl poděkovat všem, kteří mi vyplnili dotazník na téma sociální inženýrství.

Anotace

Tato práce se zabývá metodami sociálního inženýrství, což jsou metody používané kriminálníky k oklamání uživatelů počítačů. Účelem této práce je seznámit veřejnost s těmito metodami a naučit ji tyto metody rozpoznat a bránit se proti nim. Jednotlivé metody budou v této práci detailně rozebrány a bude objasněn princip jejich fungování. Součástí je také zhodnocení dotazníku a aplikovaného sociálního inženýrství.

Klíčová slova

sociální inženýrství; podvod; phishing; bezpečnost na internetu

Annotation

This work is about social engineering methods that are used by criminals to deceive computer users. The purpose of this work is inform public about this methods and teach the public to recognize these methods and to defend against them. The individual methods of social engineering will be analyzed in this work. It includes questionnaire and aplicated social enginnering evaluation too.

Keywords

social engineering; fraud; phishing; safety on the internet

Obsah

1. ÚVOD

Nápad napsat odbornou práci na téma sociální inženýrství se ve mně zrodil již před dlouhou dobou, kdy jsem na toto téma dělal prezentaci. Jako téma se mi to zdálo vhodné a především zajímavé. Poslední dobou se o sociálním inženýrství stále více hovoří, ale jak jsem vypozoroval, málo kdo opravdu ví, oč vlastně jde. Jelikož jsem sám neměl ucelený názor na tuto problematiku a především jsem postrádal komplexní informace, rozhodl jsem si pomocí SOČ těchto mých nedostatků zbavit.

Původně jsem chtěl tuto práci pojmout jako čistou teorii, která by lidem řekla, co to vlastně to sociální inženýrství je. Jak jsem si však časem uvědomil, to nestačí. Lidé musí vědět, jak aplikované sociální inženýrství poznají, jaké jsou jejich zbraně proti němu, jak mohou používání sociálního inženýrství zamezit. Najednou se tak stalo z poměrně krátkého a výstižného tématu téma poměrně komplexní a složité. Celá vize ještě více nabobtnala, když jsem se rozhodl ověřit si své domněnky a sepsal jsem dotazník. Jeho pomocí jsem si chtěl ověřit, kolik toho lidé o sociálním inženýrství opravdu vědí.

Později se mi naskytla možnost na projektu spolupracovat s Mendelovou univerzitou, což byla nabídka, která se neodmítá. S její pomocí jsme teoretické a z hlediska pravdivosti neověřitelné odpovědi z dotazníku zkusili vyzkoušet v reálných podmínkách na reálných lidech.

Tímto ukončím své vyprávění a shrnu má očekávání, která si od této práce slibuji. Účelem této odborné práce je zjistit povědomí veřejnosti o metodách sociálního inženýrství, objasnit a popsat tyto metody, uvést dobré rady, které pomohou při obraně před sociálním inženýrstvím a také si trochu posvítit na psychiku lidí.

2. SOCIÁLNÍ INŽENÝRSTVÍ

2.1. Popis pojmu, úvod do problematiky

Z hlediska bezpečnosti zastřešuje pojem sociální inženýrství rozsáhlou skupinu metod, které používá člověk zvaný sociální inženýr k dosažení svých cílů.

Tyto metody obecně fungují na principu, kdy se sociální inženýr (dále jen podvodník) snaží vyvolat v oběti pomocí různých triků důvěru, které následně zneužije k získání kýžených informací.

Sociální inženýrství je v největší míře používáno na internetu. Jeho nespornou výhodou je lehká realizovatelnost. Podvodník nemusí umět programovat, či zvládat jiné náročné úkony. Útok zprostředkovaný v režii sociálního inženýrství totiž oproti tzv. crackingu míří na lidský faktor, namísto faktoru softwarového. Útočník tedy není nucen vyhledávat různé zranitelnosti a způsoby, jak jich zneužít. Stačí mu pouze odhadnout vhodnou oběť, která je neostražitá a vůči sociotechnice náchylná.[1]

3. Metody

3.1. Pretexting

3.1.1. Definice

- Podvodné jednání, při kterém útočník využívá částečně pravdivý příběh, kterým se snaží získat důvěru oběti, a následně chtěné informace.[2]
- Pravdivé části jsou zpravidla ty, které je oběť schopna si ověřit, nebo je již zná.
- Lživé části zahrnují informace, které se nedají z pohledu oběti ověřit jednoduchou cestou. Tyto části příběhu také obsahují prosby mířené na oběť.

3.1.2. Způsoby použití

- Pretexting se řadí mezi metody používané v reálných situacích. Většinou se používá telefonicky, kdy se útočník vydává za důvěryhodnou osobu a na základě jistých, většinou smyšlených skutečností žádá o dané informace. Dále se používá při osobním setkání s obětí.[3] V tomto případě se útočník většinou za důvěryhodnou osobu nevydává, nýbrž se na ni odvolává. K jiné situaci nastává v tzv. korporátní sféře, kdy je útok cílen na velké společnosti. Útočník zde využívá faktu, že se všichni zaměstnanci osobně neznají, a není tak problém se za některého z nich vydávat. Při osobním setkání také poměrně často účinkuje útočník sám za sebe, bez uvádění kohokoliv dalšího.

3.1.3. Princip fungování

Psychologické hledisko

- V případě telefonické formy má útočník výhodu především v tom, že jej druhá strana pouze slyší. Pokud tedy umí napodobit hlas člověka, za něhož se vydává, může telefonát působit legitimně, a to i navzdory tomu, že útočník zpravidla volá z cizího telefonního čísla. Tuto výhodu však útočník ztrácí, pokud se s obětí setká osobně. Za této situace většinou uvádí pravdivé informace, které oběť buď zná, nebo si je lehce ověří. Na základě těchto informací vzbuzuje v oběti důvěru. Oběť následně ztrácí obavy a ostražitost, a v mnohých případech útočníkovi sdělí informace, které chce vědět.

3.1.4. Modelová situace

Telefonní pretexting

- Této metody většinou podvodníci využívají prostřednictvím různých průzkumů a anket. Nejprve se oběti ptají na zpravidla nevinné otázky a současně se pokoušejí navodit příjemnou, přátelskou atmosféru. Když si

jsou jisti, že jim oběť věří, začnou se dotazovat na citlivější otázky, na které by člověk za normálních okolností nikomu cizímu odpověď neposkytl.

- **Osobní pretexting**
  - Tento druh podvodu cílí spíše než na běžné lidi na již zmíněnou korporátní sféru. Podvodník většinou navštíví jím zvolené oddělení a vydává se za zaměstnance oddělení jiného. Nejčastěji vybírá oddělení takové, které není příliš v kontaktu s oddělením, na nějž touto metodou útočí. Oběť si většinou pouze ověří existenci zaměstnance uvedeného jména ve firemním systému a v případě, že jej najde, jedná dále s podvodníkem jako se svým kolegou a žádané informace mu předá.

3.2. Baiting

3.2.1. Definice

- Podvodná metoda, při níž útočník vsází na zvědavost oběti.
- Oproti pretextingu v tomto druhu útoku nevystupuje útočník osobně.
- Obvykle bývá použita na předem vybranou osobu. Díky tomu může být útok přizpůsoben na míru, čímž se zvýší jeho šance na úspěch.

3.2.2. Způsoby použití

- Baiting jako takový se vyskytuje ve dvou základních podobách. První formou je standardní baiting, při kterém zanechá útočník na předem zvoleném místě paměťové médium, které má vyvolat v oběti zvědavost.[4] Druhou formou je mnohem rozšířenější clickbaiting, který naopak probíhá prostřednictvím internetu. Princip fungování je stejný, jako v případě standardního baitingu. Nevyskytuje se zde však fyzický nosič, ale hypertextový odkaz, který svádí k otevření pomocí nevšedního, popřípadě exotického titulku.[5]
- Standardní baiting není používán v takové míře, jako například phishing. Neboť je značně nákladný. Útočník musí investovat do datového média a především do přípravy škodlivého softwaru, které na médium umístí. Dalším úskalím této metody je složitá ověřitelnost úspěšnosti útoku. Útočník totiž v průběhu útoku nehraje žádnou roli. Tím pádem ztrácí nad průběhem kontrolu. Tento nedostatek se ve většině případů řeší navržením škodlivého programu takovým stylem, aby při svém spuštění útočníka informoval.

3.2.3. Princip fungování

○ Informatické hledisko

- Co se standardního baitingu týče, nezastupitelnou roli zde hraje paměťové médium připojitelné k počítači. Nejčastěji se jedná o DVD, či CD, méně často o USB flash disk, či disketu. Obsahem takového média je škodlivý spustitelný soubor a skript autorun.inf, který umožní jeho automatické spuštění. Po připojení takového média dochází v největší míře k infikování hostitelského systému, nebo k odcizení uživatelských dat.
- Clickbaitingový odkaz obvykle oběti neposkytne informaci, kterou na první pohled nabízel. Většinou se jedná o weby, které jsou přeplněny reklamními bannery, v horším případě návštěvníka přesměrují jinam, nebo se mu pomocí škodlivých skriptů pokusí infikovat počítač. Nezřídka kdy je společně s clickbaitingem používána jiná metoda sociálního inženýrství.

○ Psychologické hledisko

- V obou případech útočník využívá zvědavosti, což je vlastnost, kterou v různé míře má každý člověk. Médium, ať už se jedná o fyzický nosič, nebo hypertextový odkaz, obsahuje na první pohled viditelnou informaci, která lidskou zvědavost zvyšuje.
- Fyzické nosiče jsou tedy nejčastěji popsány nějakým lákavým popiskem, například „WINDOWS 7 PROFESSIONAL“. Oběť s největší pravděpodobností ví, co to Windows 7 je, a také ví, že se jedná o placený produkt. Díky vidině, že může vlastnit placený produkt zcela zdarma si médium vezme.
- V situacích, kdy útočník využívá clickbaiting hraje největší roli titulek odkazu a styl, kterým je napsán. Obvykle je v titulku uvedena informace, kterou oběť nikde jinde neviděla a je pro ni tedy něčím speciálním.

3.2.4. Modelová situace

○ Standardní baiting

- Útočník nechá infikované médium odložené v blízkosti místa, kolem kterého se vyhlédnutá oběť intenzivně pohybuje. Jelikož se jedná o útok cílený, podvodník vhodně zvolil popisek média, který vyvolá zvýšený zájem. Oběť nález spustí prostřednictvím svého osobního počítače, čímž dojde k naplnění záměru útočníka.

- **Clickbaiting**
  - Tato forma útoku se nejčastěji vyskytuje na sociálních sítích. Typický je příspěvek pochybné stránky obsahující odkaz na údajný článek o zákulisí života některé celebrity, případně senzace ze světa techniky, či zvířectva. Po otevření odkazu se návštěvník dostane jinam, než očekával.

3.3. Tailgating

3.3.1. Definice

- Podvodná metoda, jejímž prostřednictvím je útočníkovi umožněno vstoupit do míst, která jsou určena pouze autorizovaným osobám.[6]

3.3.2. Způsoby použití

- Díky principu, na kterém tato metoda funguje je nemožné ji použít v kyberprostoru, je tedy úzce spjata s realitou. Možnosti využití jsou však poměrně omezené, neboť většina nepřístupných areálů je nějakým způsobem střežena. Této metody útočník využívá v případě, že chce získat větší množství dat, než je u podobných podvodů běžné, nebo v případech, kdy se snaží ukořistit nějaký fyzický předmět. Může ji také využít v případě, že má zájem o více druhů dat, které by mu nebyla schopna vydat jedna osoba.

3.3.3. Princip fungování

- **Psychologické hledisko**
  - Stejně jako ostatní metody sociálního inženýrství, i tailgating se snaží vyvolat u oběti důvěru. V tomto případě dosáhne útočník této mety pomocí napodobování jisté skupiny lidí, a to ať už stylem oblékání, nebo chování. Typicky se jedná o servisní techniky, případně zaměstnance přepravních služeb. Takto přestrojený útočník je mnohdy úmyslně vpuštěn do areálu samotnými zaměstnanci, případně vnikne dovnitř společně s příchozím zaměstnancem. Důvěra v útočníka je způsobena v největší míře tím, že se podobní lidé v areálu často vyskytují. Zaměstnanci mu díky tomu nevěnují takovou pozornost, jakou by měli. Díky těmto aspektům se šance na odhalení podvodníka zmenšují.

3.3.4. Modelové situace

- Spíše než ze seriózních médií je o tomto druhu podvodného jednání slyšet v akčních filmech, kde však není samotný pojem tailgating používán. Podvodník se většinou převlékne za zaměstnance bezpečnostní agentury střežící nějakou

instituci. Do ní následně v tomto převleku vnikne a nejčastěji odcizí finanční obnos.

- Reálně je tato podvodná metoda nejčastěji používána soukromými detektivy, kteří s její pomocí přichází do styku s daty, která jsou nezbytná pro úspěšné rozřešení případu, a zároveň která by jim standardní cestou nebyla přístupná.

3.4. Quid pro quo

3.4.1. Definice

- Název v překladu z latiny znamená doslovně „něco za něco“.
- Při aplikaci této metody se útočník snaží naleznout v jím zvolené instituci nespokojeného zaměstnance, který by byl útočníkovi ochotný za nějakou službu předat žádané informace.[7]

3.4.2. Způsoby použití

- Způsobů využití této metody je mnoho – quid pro quo lze využít jak po telefonu nebo internetu, tak i osobně. Nejčastěji je kvůli své časové nenáročnosti a nízké šanci odhalení podvodníka používána telefonická varianta.
- Quid pro quo nenalézá přílišné uplatnění, neboť je pro útočníka poměrně těžké vyhledat nespokojeného zaměstnance. Spousta lidí je navíc při různých žádostech po telefonu ostražitá, což také významně snižuje účinnost této metody. Jako adekvátní náhrada se ujal především telefonní pretexting.
- Existují dvě skupiny útočníků. Do první skupiny řadíme útočníky, kteří za předání dat opravdu zaměstnanci pomohou. Druhá skupina útočníků nechce zaměstnanci pomoci, nýbrž se tak pouze tvářit. Tato sorta útočníků vybízí pracovníky k jistým úkonům, které však namísto vyřešení problému infikují počítač malwarem, jenž odcizí uživatelská data.

3.4.3. Princip fungování

Psychologické hledisko

- Útočník při tomto útoku využívá aktuálního negativního rozpoložení zaměstnance určité instituce. Velice ochotně mu nabídne pomoc s řešením problému. Nespokojený zaměstnanec je rád, že na vyřešení jeho pracovních problémů má alespoň někdo zájem a takovému člověku tzv. „za odměnu“ žádaná data mnohdy předá.

3.4.4. Modelová situace

- Nejtypičtější situací je s největší pravděpodobností problém zaměstnance se softwarovým vybavením počítače, na který firemní technici nereagují dostatečně rychle, popřípadě vůbec. Jelikož je v zájmu zaměstnance se problému co nejdříve zbavit, mnohdy se uchýlí i k aplikování rad poskytnutých neznámým člověkem.

3.5. Phishing

3.5.1. Definice

- Jako phishing označujeme útok prováděný prostřednictvím internetové sítě mající za úkol získat od oběti útočníkem chtěné informace.[8]

3.5.2. Způsoby použití

Phishing, jakožto nejpoužívanější metoda sociálního inženýrství se vyskytuje na internetu v několika instancích.

- **Podvodná webová stránka / emailová zpráva**
  - Jedná se o nejčastěji kombinované metody phishingu, které si jdou takzvaně „ruku v ruce“. Phishingová stránka může existovat samostatně, email nikoliv. Jeho účel není připravit příjemce o data, ale zprostředkovat uživateli přístup na podvodnou stránku.
  - Počáteční fází je napodobení emailové zprávy důvěryhodné organizace a záměna hypertextových odkazů z originálních na podvodné. Takovýto email nabádá příjemce k otevření zmíněného odkazu, čímž dojde k uskutečnění záměru útočníka.
- **Kombinace s Cross-site scripting (XSS)**
  - Útok typu XSS se sám o sobě nedá řadit do kategorie sociálního inženýrství, neboť se jedná o zneužití bezpečnostně neošetřeného skriptu zakomponovaného ve zdrojovém kódu stránky.
  - V kombinaci s phishingem útočník naruší a upraví zdrojový kód stránky podle svých nekalých potřeb.

3.5.3. Princip fungování

- **Informatické hledisko**
  - Phishing, jakožto podvodná webová stránka je webová stránka vytvořená pomocí značkovacího jazyka HTML, případně CSS, která bývá nezřídka kdy obohacena o skripty jazyka JavaScript, či PHP. Základním rysem podvodné

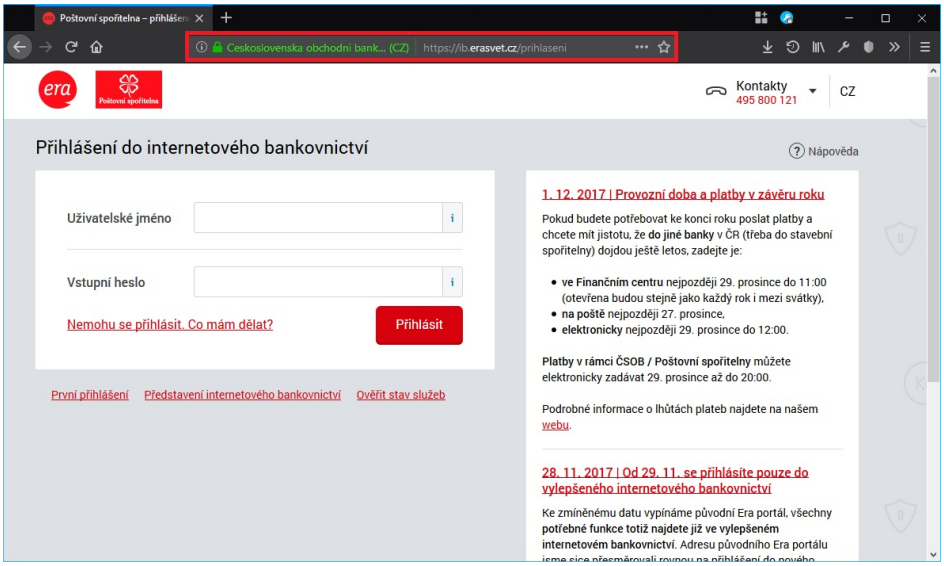
phishingové stránky je podobnost jejího vzhledu s originální webovou stránku, za kterou se podvodná stránka vydává. Míra podobnosti je závislá na schopnostech sociálního inženýra, který ji vytvořil.

- Stejná pravidla platí i pro samotný phishingový email, v jehož případě se však skripty jazyka JavaScript téměř nepoužívají. Použití skriptů jazyka PHP je vyloučeno, neboť to neumožňuje poštovní server.
- Dáváme-li phishing do spojitosti s XSS, jedná se o rozdílný typ útoku. V tomto případě se návštěvník opravdu nachází na legitimních webových stránkách dané instituce. Pro úspěšné vykonání tohoto útoku je nezbytné, aby webová stránka obsahovala bezpečnostně neošetřený skript, většinou s příponou .js, nebo .php. Pomocí takto zneužitého skriptu útočník zabuduje do zdrojového kódu nadbytečný objekt, který bude např. zachytávat stisknuté klávesy, přesměruje legitimní web na web podvržený, nebo nahradí přihlašovací formuláře svými formuláři.[9]

- **Psychologické hledisko**
  - Shodnost podvodné phishingové a originální stránky vyvolává v návštěvníkovi pocit, že je opravdu na legitimním webu. Nachází se v prostředí, které je mu důvěrně známé a kterému důvěřuje. Tím ztrácí zábrany a obavy z toho, že své údaje předává do špatných rukou.

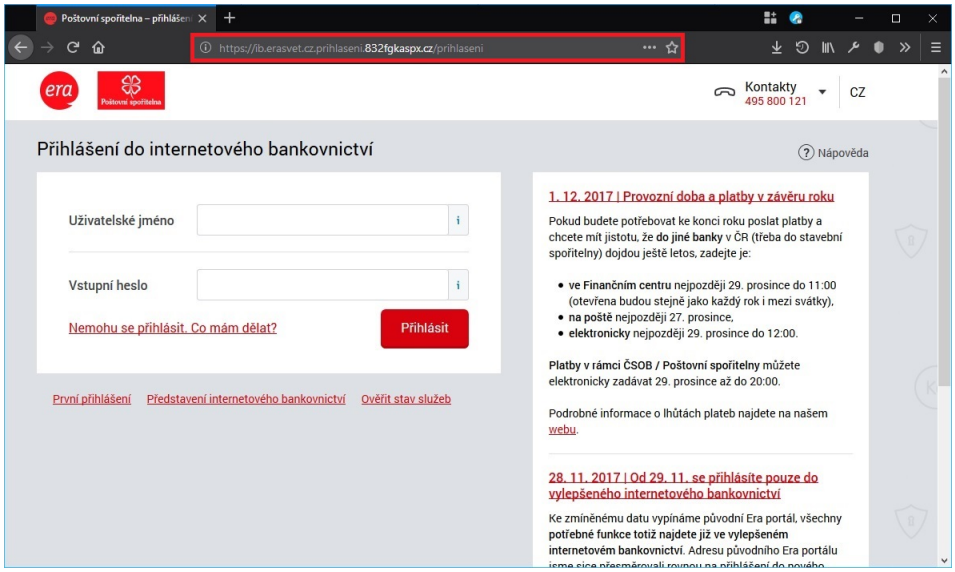
3.5.4. Modelová situace

- Typickou ukázkou phishingu v praxi je emailová zpráva vydávající se ve většině případů za oznámení banky. Ve zprávě je uživatel převážně informován o jistých nesrovnalostech, které se týkají jeho bankovního konta.
- Na následujícím snímku obrazovky je k vidění legitimní web banky Poštovní spořitelny. Z adresního řádku je patrné, že je web zabezpečený protokolem HTTPS a ověřený důvěryhodnou certifikační autoritou. Z adresního řádku dále jasně vyplývá, že se uživatel opravdu nachází na webu banky.



Obr. 1.: Legitimní stránka internetového bankovnictví Poštovní spořitelny

- Na následujícím screenshotu je k vidění webová stránka, která je s webovou stránkou zobrazenou výše naprosto identická. Zásadní rozdíl je však v obsahu adresního řádku. V tomto případě web používá pouze nezabezpečený protokol HTTP, přes který se všechna komunikace přijímá i odesílá nešifrovaně. Je tedy jednoduše vysledovatelná. Největší roli zde hraje adresa webu. Na první pohled se zdá, že se jedná o identickou adresu, avšak pokud si ji prohlédnete pozorně, zjistíte, že se web nenachází na doméně erasvet.cz, ale na doméně 832fgkapsx.cz, která rozhodně nespadá pod banku.



Obr. 2.: Podvodná stránka vydávající se za internetové bankovnictví Poštovní spořitelny

4. Metody sociálního inženýrství praktikované na reálných osobách

4.1. Vyjádření ohledně legálnosti vyzkoušených podvodů

Veškeré z níže uvedených útoků byly provedeny v prostorách Mendelovy univerzity v Brně za plného vědomí vedení, které s námi jednotlivé útoky konzultovalo a schvalovalo. Z právního hlediska se tedy nejedná o sociální inženýrství použité za účelem poškození cizí osoby, nýbrž jako bezpečnostní prověrka nejmenovaného pracoviště.

Na základě dohody o mlčenlivosti uzavřené mezi mou osobou a Mendelovou univerzitou došlo z bezpečnostních důvodů k nahrazení reálných jmen osob a názvů ústavů za jména a názvy smyšlené.

Při sestavování scénářů jednotlivých podvodů jsme čerpali informace pouze z veřejně dostupných zdrojů. Nevěděli jsme tedy navíc žádnou informaci, ke které by pravý útočník neměl přístup. Jednotlivé podvody tedy probíhaly za reálných podmínek, které jsou k dispozici každému sociálnímu inženýrovi.

Následující kapitola rozhodně nemá v úmyslu někomu radit při vykonávání podvodných praktik sociálního inženýrství.

4.2. Telefonní pretexting

4.2.1. Metodika

- Předmětem tohoto sociotechnického pokusu bylo zavolání na předem vybrané telefonní číslo a vydávání se za jinou osobu s cílem získání citlivých dat, která by za standardních podmínek nebyla přístupná.

4.2.2. Průběh

- Z mého osobního mobilního telefonu jsem zavolal do kanceláře paní Jarmily Veselé, která pracuje na Mendelově univerzitě jakožto pracovnice informačních systémů. Představil jsem se jí jako Mgr. Oldřich Černý, PhD. a požádal jsem ji o nadiktování osobního příplatku slečny Bc. Anežky Horákové. Svou žádost jsem podložil tvrzením, že mi byl z důvodu neznámé chyby odmítnut přístup do informačního systému SAP. Dále jsem podotknul, že jsem v časové tísni, neboť spěchám s jistými dokumenty, které mimo jiné zahrnují i onen osobní příplatek za paní kvestorkou. Paní Veselá nepožadovala z mojí strany jakoukoliv další identifikaci a žádaná data mi začala vyhledávat. Během vyhledávání mne požádala o upřesnění charakteru příplatků. Na její žádost jsem jí jednoduše odvětil, že mi tuto informaci paní kvestorka neupřesnila a že tedy stačí, když mi sdělí pouze osobní příplatky, bez jakýchkoliv odměn a bonusů. Poté mi bylo sděleno, že osobní příplatek slečny Bc. Anežky Horákové činí 11 800 Kč.

4.2.3. Vyhodnocení

- Veškeré aspekty a předpoklady, které jsme si při vytváření scénáře tohoto útoku stanovily byly splněny.
- Po celou dobu telefonátu přispíval k úspěšnosti fakt, že jsem k paní Veselé promlouval sebevědomým hlasem, ze kterého bylo patrné, že řeším akutní situaci. V kombinaci s oznámením, že spěchám za paní kvestorkou tyto dva faktory velice přispěly k tomu, že se mne paní Veselá nepokoušela nijak dál identifikovat.

4.3. Pretexting v kombinaci s podvodným emailem

4.3.1. Metodika

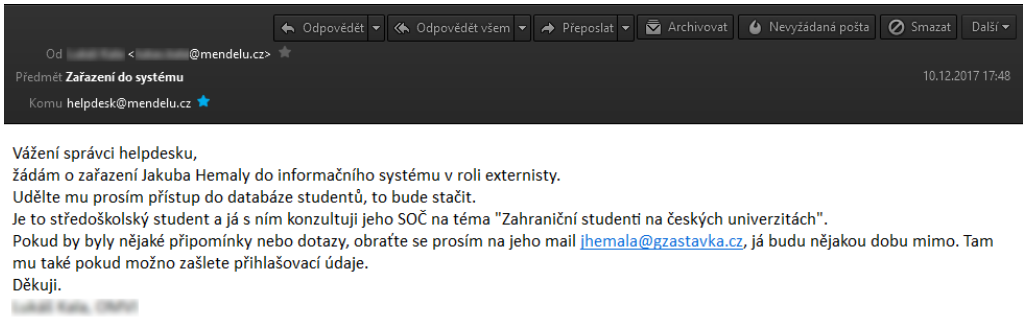
- Tento podvod si kladl za cíl umožnit mému spolupracovníkovi Jakubu Hemalovi legitimní přístup do informačního systému Mendelovy univerzity pomocí účtu externisty, který mu měl být za pomoci pretextingu oficiálně zřízen.
- Z důvodu nedostatečnosti pretextingové fáze byla následně použita podvodná emailová zpráva, která oběť utvrdila v Jakubově zdánlivé důvěryhodnosti.

4.3.2. Průběh

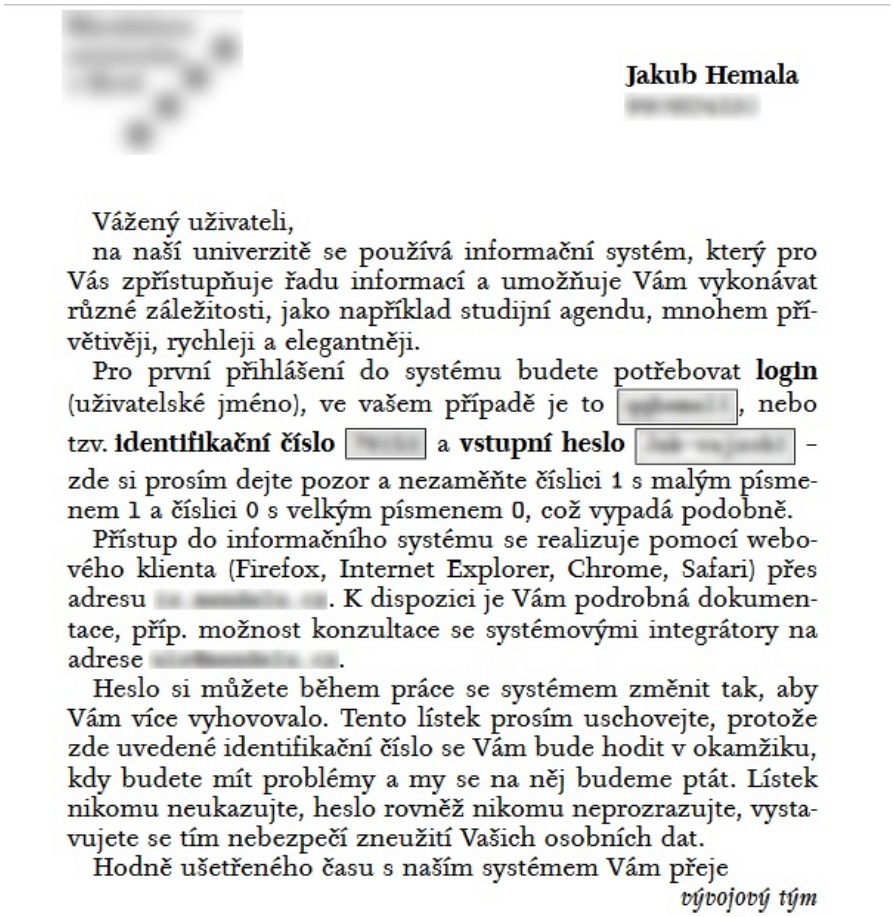
- Jakub se infiltroval společně se mnou (viz. kapitola Pretexting v kombinaci s tailgatingem) do uzavřeného sektoru kanceláří Ústavu matematických věd (UMV), kde navštívil tamního zaměstnance, pana Radka Novotného. Představil se jako Jakub Hemala, student gymnázia, který pracuje na středoškolské odborné práci na téma „Zahraniční studenti na českých univerzitách“. Jako důvod návštěvy uvedl žádost vedoucího oddělení studentských odborů (OSO) Martina Bílka o vytvoření profilu externisty v univerzitním informačním systému, který je pro jeho práci důležitý. Pan Novotný, však řekl, že nelze vytvořit uživatelský profil pouze na základě slovní domluvy. Jakubovi následně detailně popsal způsob, jakým se žádost o vytvoření profilu podává.
- Na základě zjištěných informací byl následně na helpdesk zaslán podvodný email tvářící se jako email zaslaný panem Bílkem. Tento email obsahoval písemnou žádost o zařazení do systému. Zároveň byla ve zprávě uvedena informace, že bude pan Bílek delší dobu nedostupný, ať se tedy v případě jakýchkoliv dotazů obrací na email Jakuba Hemaly. Tím jsme zajistili, že případná odpověď nepoputuje do schránky pana Bílka. Veškerá zbývající komunikace, tedy předání jména a rodného čísla, nebo předání přihlašovacích údajů probíhala už přes osobní email Jakuba Hemaly, který již nebylo třeba jakkoliv maskovat.

4.3.3. Vyhodnocení

- V tomto případě byla oběť poměrně obezřetná a značně lpěla na stanovených zásadách, což razantně snížilo účinnost pretextingové fáze. Pretexting sám o sobě se tedy v tomto případě neosvědčil. Po použití podvodného emailu se však situace změnila. Důležitá byla posloupnost provedených operací. V pretextingové fázi, ačkoliv neúspěšné, se pan Novotný setkal s žadatelem o profil osobně, což je pro podvodníka rozhodně lepší, než když se o něm dozví pouze prostřednictvím emailu.



Obr. 3.: Falešná zpráva žádající o zařazení Jakuba Hemaly do systému



Obr. 4.: Potvrzení o zařazení Jakuba Hemaly do univerzitního systému

4.4. Pretexting v kombinaci s tailgatingem

4.4.1. Metodika

- Předmětem této sociální praktiky bylo vzbuzení důvěryhodnosti u pracovníků ústavu a následná infiltrace do prostor, které nejsou za normálních podmínek člověku, který v ústavu nepracuje přístupné. Za cíl jsme si stanovili odcizení libovolného předmětu a získání administrátorských práv k libovolnému počítači.

4.4.2. Průběh

- Vstoupil jsem do veřejné části Ústavu matematických věd (UMV), přes kterou jsem se dostal k internímu sektoru kanceláří, kam mají přístup pouze zaměstnanci oddělení. Po chvíli stání u dveří přišel zevnitř sektoru člověk, který se mne zeptal, co potřebuji. Využil jsem metody tailgatingu a představil jsem se mu jako student, který potřebuje nutně mluvit s vedoucím oddělení, panem Kučerou. Bylo mi řečeno, že vedoucí zde momentálně není (což jsem si dopředu zjistil) a požádal jsem tedy alespoň o audienci u sekretářky, načež jsem byl vpuštěn dovnitř.

- V kanceláři jsem se paní sekretářce představil jako student pracující na středoškolské odborné práci na téma „Zahraniční studenti na českých univerzitách“. Dodal jsem, že jsem již úspěšně navštívil Masarykovu univerzitu v Brně a že Mendelova univerzita je poslední, která mi zbývá. Jako svého konzultanta jsem uvedl pana Martina Bílka, který je na univerzitě zaměstnán jako vedoucí oddělení studentských odborů (OSO). Dále jsem uvedl, že mě pan Bílek posílá s prosbou na pana Kučeru, zda-li by byl ochoten nám pro naši konzultaci propůjčit místní počítačovou učebnu. Jelikož zde pan Kučera nebyl, požádal jsem o to paní sekretářku. Ta si nejprve ověřila, zda-li nějaký pan Martin Bílek opravdu pracuje jako vedoucí mnou uvedeného oddělení a po zjištění, že tomu tak opravdu je náš rozhovor pokračoval. Na dotaz, kdy pan Bílek dorazí jsem jí odvětil, že by tu měl být nejpozději do půl hodiny. Celá situace se jí zdála zvláštní v tom, že člověk z OSO žádá o konzultaci v budově UMV. Věc však nadále neprověřovala a učebnu mi odemkla, načež mne tam nechala naprosto bez dozoru.

- V učebně se nacházelo několik řad stolů vybavených počítači s operačním systémem Microsoft Windows 10, monitory, routery a další počítačová technika. Jakožto cíl svého útoku jsem si zvolil počítač, na který nebylo od dveří, které zůstaly otevřené, příliš vidět. Spustil jsem jej a místo z pevného disku jsem nabootoval z instalačního USB flash disku systému Windows 10, který jsem si s sebou přinesl. Pomocí možností usnadnění jsem spustil příkazový řádek s právy administrátora a zaměnil jsem systémový soubor *utilman.exe* nacházející se v umístění *%windir%/System32/* za soubor *cmd.exe*, který se nacházel ve stejné

složce. Počítač jsem následně restartoval a standardně nabootoval do operačního systému. Na přihlašovací obrazovce jsem klikl na ikonu nástrojů usnadnění, načež se mi zapříčiněním mé předchozí aktivity namísto okna pro výběr usnadňujícího nástroje spustil příkazový řádek. Jelikož jsem v tu chvíli nebyl přihlášen jako žádný uživatel, příkazový řádek se spustil se systémovými právy, čímž mi bylo umožněno vykonávat příkazy, které nejsou pro standardního uživatele povoleny. Pomocí příkazu *net user* jsem změnil heslo administrátorského účtu, do kterého jsem se následně přihlásil. Ve složce *%appdata%* jsem založil složku s názvem Brestcom a v ní soubor *gotcha.txt,* který obsahoval informaci o napadení počítače technikami sociálního inženýrství. Počítač jsem poté vypnul.

- Cestou z učebny jsem odcizil žlutý ethernetový kabel, který jsem schoval do útrob své bundy. Cestou ven jsem jsi všiml několika otevřených, avšak prázdných kanceláří. Na chodbě jsem nechal pohozené DVD (viz. následující kapitola) a sektor jsem opustil.

4.4.3. Vyhodnocení

- První fáze tailgatingu, tedy vstup do uzavřeného sektoru vyšla i navzdory tomu, že jsem nebyl v přestrojení. Zaměstnanec pravděpodobně neměl důvod mi nevěřit, že nejsem student a tak mu nic nebránilo v puštění mé osoby do areálu.

- V pretextingové fázi bylo patrné typické kombinování pravdivých a lživých informací. Paní sekretářka špatně vyhodnotila, které z mnou vyřčených informací si má před mým vpuštěním do učebny ověřit. Tento fakt jsem bral v potaz a při výběru lživých informací jsem se jím řídil. Zajímavé je, že se vzniklá situace zdála paní sekretářce podezřelá, nicméně pro její důkladnější ověření neudělal zhola nic.

- Druhá fáze tailgatingu, což bylo napadnutí počítače se obešla bez jakýchkoliv zádrhelů. To mne překvapilo, neboť jsem alespoň minimální potíže očekával. S počítačem jsem nic závažného neprovedl, jak je však z průběhu celé akce zřejmé, kdybych chtěl, mohl jsem s počítačem spáchat cokoliv, například jej infikovat spywarem.

- Otevřené kanceláře, které jsou bez jakéhokoliv dozoru jsou nežádoucí jev. Samozřejmě, v tomto případě se jedná o uzavřené pracoviště, jehož zaměstnanci se mezi sebou znají a důvěřují si. Je však potřeba si uvědomit, že když je do takovéhoto pracoviště vpuštěna cizí osoba, jako tomu bylo v našem případě, je nutné bezpečnostní zásady posunout o několik úrovní výše.

4.5. Baiting

4.5.1. Metodika

- Předmětem tohoto pokusu bylo zanechání infikovaného DVD na místě, v němž se vyhlédnutá oběť frekventovaně pohybuje.

4.5.2. Průběh

- Pomocí počítače jsem na DVD vypálil společně s ikonou a konfiguračním souborem autorun.inf také dávkový soubor Databaze.bat. Tento soubor obsahující skript pro vytvoření složky ve zvoleném umístění se měl díky vhodnému nastavení souboru autorun.inf po vsunutí DVD do počítače automaticky spustit.

- Při odchodu z uzavřeného pracoviště, viz. kapitola Pretexting v kombinaci s tailgatingem, jsem toto DVD s popiskem „*DATABÁZE FRRMS*“ nechal odložené na chodbě.

4.5.3. Vyhodnocení

- Při provádění tohoto druhu sociálního inženýrství je velice důležitá volba vhodného popisku média. Ten musí v potenciální oběti vzbudit zvědavost. V tomto případě však byl popisek zvolen špatně. Při jeho vymýšlení jsme předpokládali, že zaměstnance ústavu zaujme, což však byla chybná domněnka. DVD našla paní sekretářka, která jej založila do poličky mezi ostatní disky, aniž by jej předtím spustila.

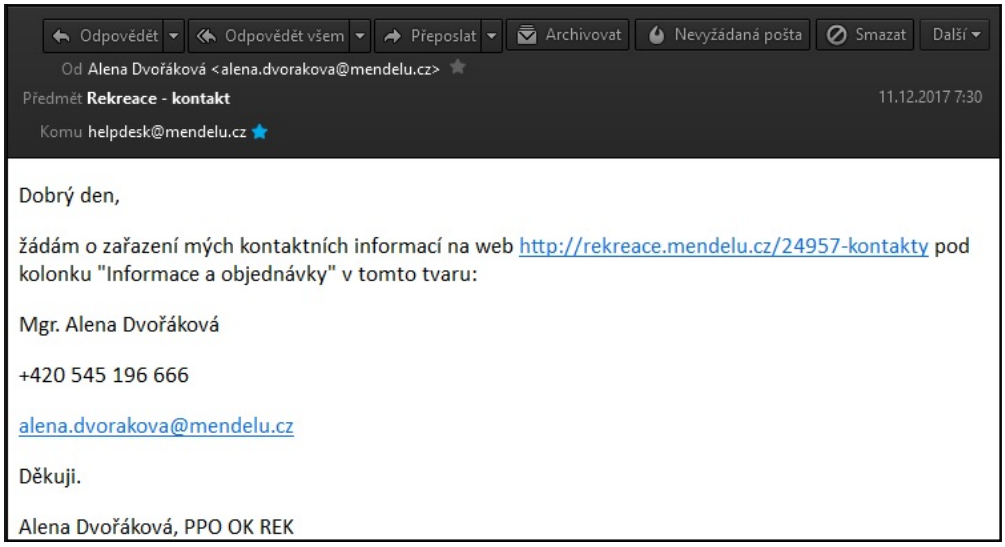
4.6. Podvodný email

4.6.1. Metodika

- Předmětem tohoto pokusu bylo odeslání žádosti na helpdesk jakožto autorizovaná a důvěryhodná osoba. Cílem bylo zařazení paní Mgr. Aleny Dvořákové jako kontaktní osoby na web rekreace.mendelu.cz.

4.6.2. Průběh

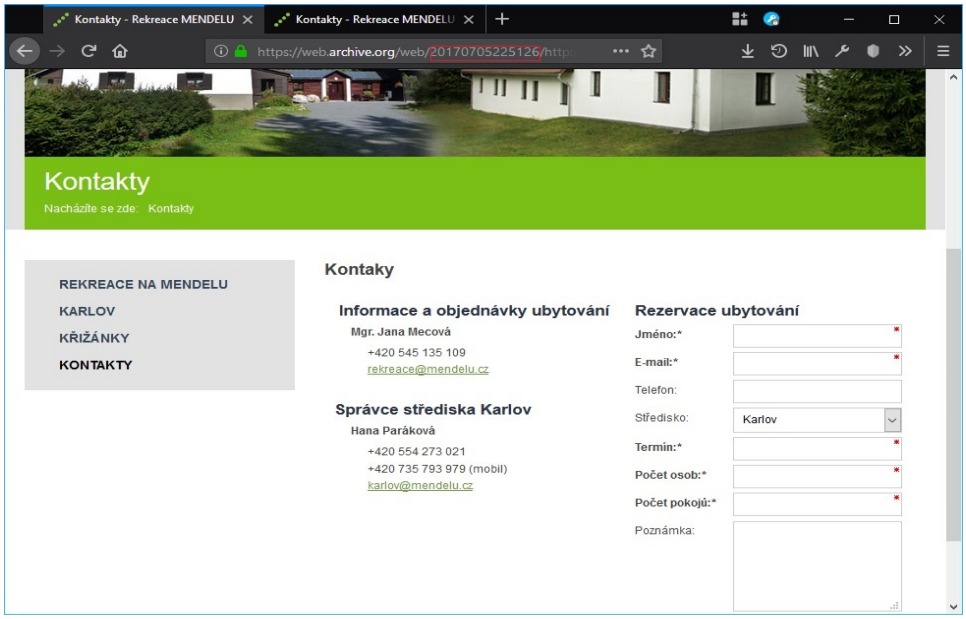
- Pomocí poštovního klienta Mozilla Thunderbird jsem napsal požadavek na adresu helpdesk@mendelu.cz ve tvaru viz. obrázek níže. Odeslání probíhalo z emailové adresy, jejíž jsem vlastníkem. Program Thunderbird však umožňuje poupravit hlavičku zprávy tak, že se příjemci zobrazí jiná adresa, než je pravá adresa odesílatele. Tímto způsobem jsem adresu odesílatele změnil na alena.dvorakova@mendelu.cz a takto poupravený email jsem odeslal.



Obr. 5.: Podvodný email se žádostí o zařazení mezi kontakty

○ Vyhodnocení

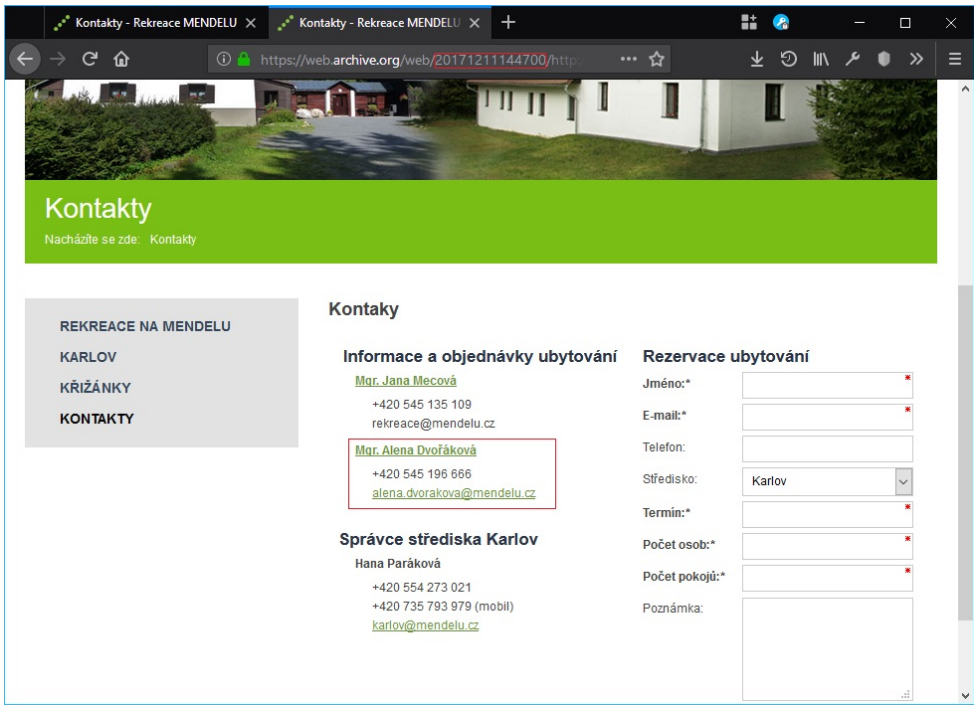
- Během několika následujících dní jsme pravidelně kontrolovali odkaz, na němž mělo dojít ke změně obsahu. Dva dny po odeslání byly kontaktní informace pozměněny tím, že byl mezi ně přidán kontakt na paní Dvořákovou. Z tohoto faktu jsme vyvodili závěr, že byl pokus úspěšný.



Obr. 6.: Webové stránky rekreace před přijetím podvodného požadavku

- Nezastupitelnou roli hraje v tomto druhu podvodu emailová adresa odesílatele. Za situace, že by byla zanechána původní adresa, v tomto případě ingenieur@post.cz, bylo by na první pohled zřejmé, že se jedná o neoprávněný a podvodný požadavek. Většina lidí si není vědoma faktu,

že se dá hlavička emailové zprávy zaměnit. Pokud tedy vidí známou emailovou adresu, zprávě automaticky důvěřují.



Obr. 7.: Webové stránky rekreace po schválení podvodného požadavku

4.7. Zhodnocení praktické části

Praktickou část jsem se rozhodl uskutečnit z toho důvodu, abych zjistil, jaká je reálná situace ve společnosti. Výhoda oproti dotazníku, který byl taktéž proveden je zřejmá. V případě reálného testování, které je provedeno v utajení nemají respondenti, dají-li se tak v této situaci nazvat, možnost jakkoliv úmyslně ovlivnit výsledky. Naopak nevýhodou je pouze malý počet lidí, na které se dá tento způsob průzkumu aplikovat. Tento nedostatek se tedy pokouší kompenzovat právě již zmíněný dotazník.

Prvotní očekávání z celého testování v reálných podmínkách bylo takové, že se nám nepodaří úspěšně provést ani polovinu našich pokusů. Proti nám stál také fakt, že lidé, na kterých byly naše pokusy ozkoušeny se poměrně dobře orientují v oblasti IT, která problematiku sociálního inženýrství zahrnuje.

Navzdory těmto očekáváním dopadlo celé testování naprosto odlišně. Z mého osobního hlediska jsem s výsledky spokojen. To z toho důvodu, že se mi vydařilo něco, co jsem dlouho plánoval a do detailu vymýšlel. Podívám-li se však na výsledky jakožto autor této práce a někdo, kdo se problematikou sociálního inženýrství dlouhodobě zabývá, toto mé nadšení rázem mizí.

Výsledky reálného testování jsou z mého pohledu naprosto nedostatečné. V době, kdy se sociální inženýrství používá v takové míře, jako je tomu dnes, by mělo být povědomí o něm znatelně větší, než jaké bylo prokázáno testováním.

Přínos praktické části je jasný. Poskytla mi data, která by bylo jinak poměrně těžké obstarat. Kromě toho však přispěla k improvizaci zabezpečení v rámci Mendelovy univerzity, které po našich úspěšných pokusech proběhlo.

5. Dotazník na téma sociální inženýrství

5.1. Vyjádření ohledně objektivity výsledků

Ačkoliv úvodní text, který byl k dotazníku přiložen, žádal o pokud možno maximální spontánnost, není možné s jistotou tvrdit, že respondenti odpovídali opravdu způsobem, o jaký jsem je prostřednictvím zmíněného textu žádal.

Díky psychologickým poznatkům víme, že si velké množství lidí není schopno připustit možnost, že by mohli chybovat. Takovíto jedinci vědí, jak za dané situace. Mnohdy však zareagují způsobem, který je v dané chvíli naprosto nevhodné použít. Díky neověřitelnosti spontánnosti jednotlivých odpovědí nelze výsledky dotazníku brát jako odraz společnosti, což ostatně potvrdí jejich srovnání s daty získanými při praktické části práce, v níž jsme praktiky sociálního inženýrství zkoušeli na existujících osobách.

5.2. Účel a parametry dotazníku

Smysl dotazníku spočíval ve zjištění povědomí veřejnosti, tj. lidí různého vzdělání a věku, o praktikách sociálního inženýrství, a především zjištění spontánních reakcí lidí konfrontovaných praktikami sociálního inženýrství.

V průvodním textu, který byl k dotazníku přiložen byli respondenti informováni o účelu dotazníku a především o způsobu, jakým bude s jimi vyplněnými daty nakládáno. Důležitou součástí tohoto textu byla žádost o co možná nejspontánnější odpovědi. Respondenti byli upozorněni, že veškerá vložená data budou zaznamenána v anonymní podobně a nebude možné skrze jejich analýzu totožnost respondenta odhalit. Tuto informaci jsem považoval za důležitou z toho důvodu, že by mohli mít někteří tázaní obavy ze zneužití vyplněných údajů ve spojitosti s jejich osobou.

Šíření dotazníku bylo uskutečněno především prostřednictvím internetu, respektive sociální sítě Facebook. Tam jsem dotazník sdílel na svém osobním profilu, na třídní skupině a na stránce, kterou prostřednictvím této sítě provozuji. Na šíření dotazníku měla dále významný podíl Ing. Ludmila Brestičová, která o dotazníku informovala nemalý počet studentů a také lektory z cizích škol.

V poslední řadě jsem o dotazníku informoval respondenty osobně, přímým kontaktem s nimi.

Dotazníku se zúčastnilo celkově 91 fyzických osob.

5.3. Výsledky a zhodnocení

V této podkapitole budou rozebrány jednotlivé otázky dotazníku, u nichž bude uvedeno zastoupení správných a špatných možností, odůvodnění jejich správnosti, případně nesprávnosti a především zhodnocení výsledků.

○ Vlastními slovy popište pojem „sociální inženýrství“. Pokuste se popsat princip jeho fungování a důvody, proč jej lidé používají.

Tato teoretická otázka byla jakýmsi základním kamenem tohoto dotazníku. Jejím účelem bylo zjistit, jestli je mezi veřejností pojem sociální inženýrství rozšířený, a v případě, že je, měla otázka dále zjistit, co všechno o tomto pojmu lidé vědí.

■ Výsledky

- Ze souhrnu odpovědí všech respondentů vyplynulo, že je pojem sociální inženýrství mezi lidmi téměř neznámý.

  Respondentů, kteří uvedli, že neznají význam pojmu, popř. odpověděli špatně bylo **69** z **91.**

- Správných odpovědí, které definovaly sociální inženýrství jako manipulaci s lidmi za účelem získání informací, či nějakou podobnou formulací se stejným významem bylo **13** z **91**.

- Zbývající odpovědi, kterých bylo **9** z **91** byly ve většině případů nedostatečné. V těchto případech respondenti často místo komplexní odpovědi uváděli aspekty sociálního inženýrství, např. že se jedná o podvodné jednání. Druhou skupinou těchto odpovědí byly odpovědi správné, k nimž však byly přidány nepravdivé informace.

■ Zhodnocení

Výsledky, které vzešly z této otázky se v dnešní době dají považovat za alarmující. Sociální inženýrství se stále více stává rozšířeným společenským jevem a lidé by o něm měli být informováni. Navzdory tomu však z výsledků vyplynulo, že tato problematika není mezi lidmi příliš známá.

Průzkumy antivirové společnosti Bitdefender, LLC. zjistily, že v roce 2015 byla uživateli otevřena třetina odeslaných podvodných emailů. 15 %

podvodných zpráv splnilo svůj účel, neboť uživatel otevřel phishingový odkaz, nebo v horším případě uložil a spustil soubor zaslaný jako přílohu.

○ Vlastními slovy popište, co je to phishing.

Druhá otázka se zabývala problematikou phishingu především z důvodu, že se jedná o dnes nejpoužívanější metodu sociálního inženýrství. Většina uživatelů emailových služeb se v životě minimálně jednou setkala s podvodnou zprávou žádající o vyplnění osobních informací, na základě čehož byla zvolena otázka právě na tuto podvodnou metodu.

■ Výsledky

- Míra úspěšnosti respondentů byla v případě této otázky ještě nižší, než tomu bylo v případě otázky první.

  Respondentů, kteří uvedli, že neznají význam pojmu, popř. odpověděli špatně bylo **75** z **91**.

- Správných odpovědí bylo v poměru k částečně správným odpovědím méně, než tomu bylo u první otázky.

  Správných odpovědí, které definovaly phishing jako podvodnou metodu určenou k získávání informací fungující na základě podobnosti podvodné webové stránky s originální stránkou, či nějakou podobnou formulací se stejným významem bylo **7** z **91**.

- Zbývající odpovědi, kterých bylo **10** z **91** většinou pojem phishing příliš zobecnily, čímž majoritně definovaly sociální inženýrství jako takové.

■ Zhodnocení

Znalost phishingu jako pojmu je mezi lidmi ještě nižší, než tomu bylo u sociálního inženýrství. To však neznamená, že je tato praktika mezi lidmi neznámá. Lidí ji znají ze zkušenosti, avšak nedokáží k ní přiřadit název.

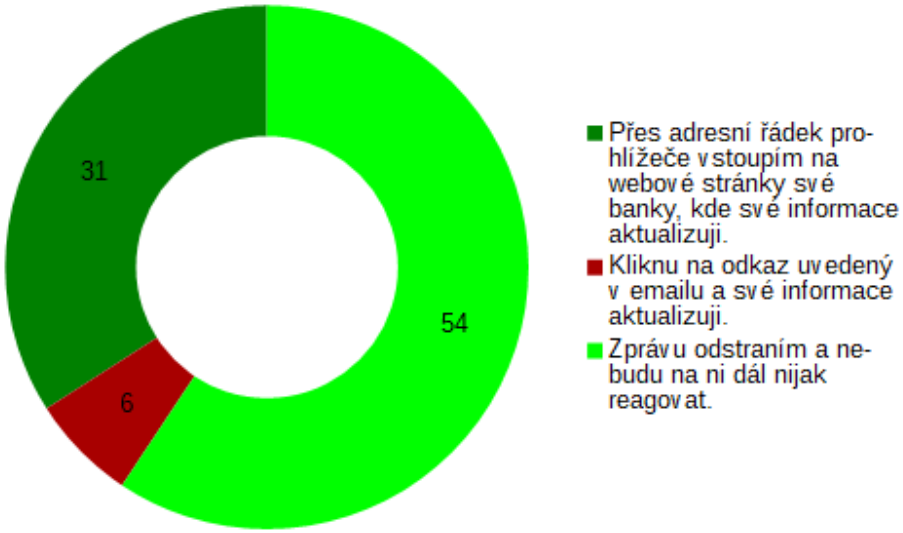
○ Do emailu vám dojde zpráva, která vás vybízí k lepšímu zabezpečení vašeho konta. Ve zprávě je hlavička a logo banky, zpráva pochází z legitimní emailové adresy. Spolu s informacemi je ve zprávě uvedený odkaz, na němž máte své informace aktualizovat. Jak budete postupovat?

■ Nabídnuté možnosti

- Zprávu odstraním a nebudu na ni dál nijak reagovat.
- Kliknu na odkaz uvedený v emailu a své informace aktualizuji.

- Přes adresní řádek prohlížeče vstoupím na webové stránky své banky, kde své informace aktualizuji.

■ Výsledky



Graf 1.: Odpovědi respondentů k otázce zabezpečení internetového bankovnictví

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Přes adresní řádek prohlížeče vstoupím na webové stránky své banky, kde své informace aktualizuji.**

  Tato možnost je **správná.**

  V případě, že vás libovolná instituce požádá o takovýto, nebo podobný úkon, je nejvhodnější na její web vstoupit přímým napsáním odkazu do adresního řádku. Tím získáte jistotu, že jste se opravdu dostali na web instituce.

- **Kliknu na odkaz uvedený v emailu a své informace aktualizuji.**

  Tato možnost je **špatná**.

  Značkovací jazyk HTML umožňuje vytvořit hypertextový odkaz z jakéhokoliv textu, čehož podvodníci využívají. Uvedený odkaz, ačkoliv se tváří jako odkaz na web instituce většinou vede na web, který jej pouze napodobuje.

- **Zprávu odstraním a nebudu na ni dál nijak reagovat.**

  Tato možnost je **správná**.

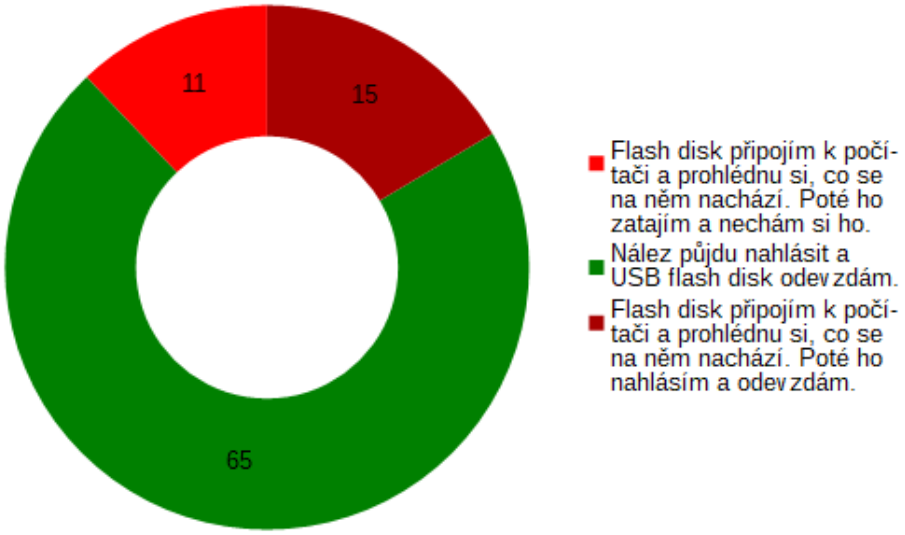
  V případě této možnosti nedojde ze strany uživatele k vyhovění požadavků uvedených ve zprávě. Tím se automaticky tento útok stane neúspěšným. Je však si potřeba uvědomit, že zpráva může být pravá a v případě nevyhovění požadavků se může uživatel potýkat s následky.

○ Na chodbě, v místě svého pracoviště, naleznete pohozený neznámý USB flash disk. Co s ním uděláte?

■ Nabídnuté možnosti

- Flash disk připojím k počítači a prohlédnu si, co se na něm nachází. Poté ho zatajím a nechám si ho.
- Nález půjdu nahlásit a USB flash disk odevzdám.
- Flash disk připojím k počítači a prohlédnu si, co se na něm nachází. Poté ho nahlásím a odevzdám.

■ Výsledky



Graf 2.: Odpovědi respondentů k otázce nalezeného USB flash disku

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Flash disk připojím k počítači a prohlédnu si, co se na něm nachází. Poté ho zatajím a nechám si ho.**

  Tato možnost je **špatná.**

  V případě tohoto útoku nejde útočníkovi o to, zda-li si datové médium necháte, nebo ne. Principiálně se tento útok zakládá na zvědavosti nálezce. Po připojení datového média k počítači dojde k automatickému spuštění škodlivého kódu, díky čemuž je útočník schopen odcizit uložená data

- **Nález půjdu nahlásit a USB flash disk odevzdám.**

  Tato možnost je **správná.**

  Nalezené médium není vaším majetkem a tudíž byste neměli zkoumat, co se na něm nachází. Tuto situaci mohu přirovnat k odemčenému cizímu autu zaparkovanému na parkovišti – také by jste se pravděpodobně nedívali dovnitř, co v něm jeho majitel má. Pokud se budete řídit touto zásadou, vyhnete se infikování vašeho počítače.

- **Flash disk připojím k počítači a prohlédnu si, co se na něm nachází. Poté ho nahlásím a odevzdám.**

  Tato možnost je **špatná.**

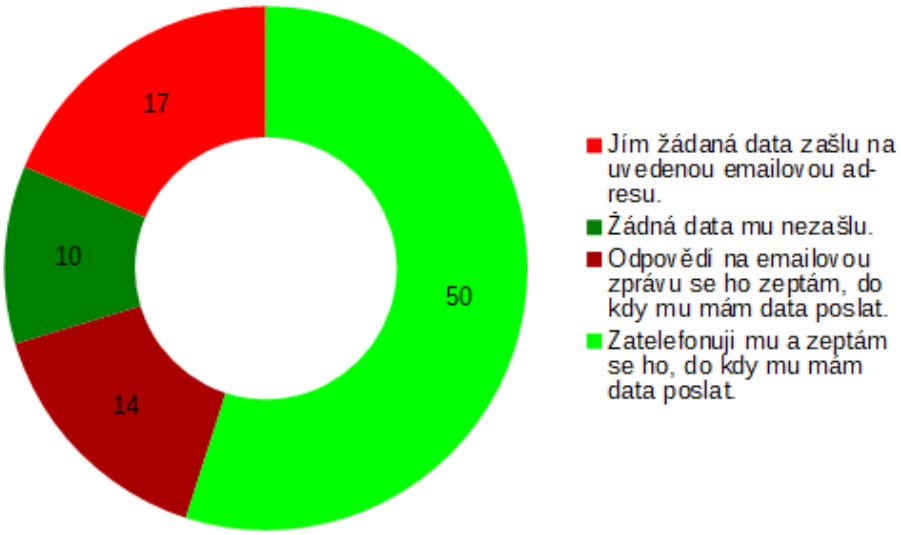
  Je chvályhodné, že chcete nálezce flash disk nahlásit, ale pokud médium připojí k počítače, nastane situace popsaná u předchozí možnosti. Jak již bylo zmíněno, útočníkovi nezáleží na tom, jestli si oběť nález nechá, ale na tom, zda jej připojí k PC.

○ **Na váš email vám dojde zpráva z emailové adresy vašeho nadřízeného, v níž vás váš nadřízený žádá o zaslání jím zvolených dat na uvedenou emailovou adresu. Jak zareagujete?**

■ **Nabídnuté možnosti**

- Jím žádaná data zašlu na uvedenou emailovou adresu.
- Žádná data mu nezašlu.
- Odpovědí na emailovou zprávu se ho zeptám, do kdy mu mám data poslat.
- Zatelefonuji mu a zeptám se ho, do kdy mu mám data poslat.

■ Výsledky



Graf 3.: Odpovědi respondentů k otázce zaslání dat nadřízenému

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Jím žádaná data zašlu na uvedenou emailovou adresu.**

  Tato možnost je **špatná.**

  Emailová adresa se dá poměrně lehce zfalšovat, při aplikování standardního postupu otevírání emailových zpráv tedy není obyčejný uživatel schopen podvod rozpoznat. V tomto případě je nejlepší kontaktovat nadřízeného osobně, či telefonicky, neboť máte jistotu, že jednáte opravdu s ním.

- **Žádná data mu nezašlu.**

  Tato možnost je **správná.**

  Z hlediska ochrany před sociálním inženýrstvím tato možnost správná je, reálná situace však zahrnuje i hlediska jiná. Z tohoto důvodu tuto možnost nemohu nedoporučit, neboť v případě, že by byla zpráva legitimní by mohl být člověk při jejím ignorování nějakým způsobem sankcionován.

- **Odpovědí na emailovou zprávu se ho zeptám, do kdy mu mám data poslat.**

  Tato možnost je **špatná.**

  Stejně tak, jako hlavička emailu, tj. adresa zobrazená v poli odesílatele, se dá stejně jednoduše i zaměnit adresa pro odpověď. Pokud se tedy uživatel rozhodne na email odpovědět a nebude příliš pozorný, odešle data na emailovou adresu podvodníka.

- **Zatelefonuji mu a zeptám se ho, do kdy mu mám data poslat.**

  Tato možnost je **správná**.

  Při aplikování této možnosti dojde k ověření legitimity zprávy způsobem, který nemůže podvodník jakkoliv narušit. Telefonní číslo zfalšovat nejde, takže máte jistotu, že opravdu voláte svému nadřízenému.

○ **Na váš telefon vám zavolá člověk, který se představí jako zaměstnanec úřadu a informuje vás o tom, že se z databáze úřadu ztratily softwarovou chybou informace o vaší osobě a zároveň vás o tyto informace požádá. Mezi tyto informace zahrneme rodné číslo; datum, rok a místo narození; jména případných dětí; adresu trvalého bydliště; telefonní číslo; emailovou adresu; číslo občanského průkazu. Co volajícímu řeknete?**

■ **Nabídnuté možnosti**

- Informuji ho o tom, že půjdu tuto záležitost osobně vyřešit na úřad.
- Zeptám se ho na další informace, požádám ho o detailnější legitimaci, a až poté mu údaje předám.
- Ztrátu dat budu považovat za chybu úřadu a pracovníkovi řeknu, ať se data pokusí obnovit, nebo si je sežene z jiných zdrojů.
- Veškeré jím vyžadované informace mu sdělím.

■ Výsledky

Graf 4.: Odpovědi respondentů k otázce telefonické žádosti z úřadu

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Informuji ho o tom, že půjdu tuto záležitost osobně vyřešit na úřad.**

  Tato možnost je **správná.**

  Kritické situace podobné té, která je uvedena v otázce se ze zásady řeší osobně na některé z poboček dané instituce, případně na zmíněném úřadě.

- **Zeptám se ho na další informace, požádám ho o detailnější legitimaci, a až poté mu údaje předám.**

  Tato možnost je **špatná.**

  Snaha o detailnější legitimaci je záslužná, avšak je třeba si uvědomit, v jaké situaci je o ni požádáno. V případě telefonátu nelze volající osobu jakkoliv detailně ověřit, neboť není schopna předložit jakýkoliv doklad, či oprávnění.

- **Ztrátu dat budu považovat za chybu úřadu a pracovníkovi řeknu, ať se data pokusí obnovit, nebo si je sežene z jiných zdrojů.**

  Tato možnost je **špatná.**

  Při volbě této možnosti sice nedošlo k vyzrazení jakýchkoliv údajů, avšak je také špatná. Na vině jsou v tomto případě nedostatečné přesvědčovací

schopnosti volajícího, kterými nebyl potenciální oběť schopen obalamutit. Zároveň je z jednání vyhlédnuté oběti patrné, že jedná v rozhořčení. Byl-li by tedy podvodník ve svém oboru zběhlejší, úspěch by se zajisté dostavil.

- **Veškeré jím vyžadované informace mu sdělím.**

  Tato možnost je **špatná.**

  Při telefonické žádosti neexistuje žádná záruka, že člověk opravdu hovoří s autorizovanou osobou. Tuto skutečnost také nelze po telefonu jakkoliv ověřit, zejména pokud se jedná o zmíněného zaměstnance úřadu. Je tedy nebezpečné touto formou komukoliv předávat citlivé informace.

○ **Přes hypertextový odkaz vstoupíte na webové stránky vašeho internetového bankovnictví. Co uděláte jako první?**

■ **Nabídnuté možnosti**

- Vyplním přihlašovací formuláře a přihlásím se.
- Zkontroluji, zda-li se v adresním řádku vyskytuje zelený zámek, popř. nápis Zabezpečeno.
- Stránku si prohlédnu a ujistím se, že jsem opravdu na webu banky.
- Zkontroluji adresu uvedenou v adresním řádku.

■ Výsledky

Graf 5.: Odpovědi respondentů k otázce přihlašování do internetového bankovnictví

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Vyplním přihlašovací formuláře a přihlásím se.**

  Tato možnost je **špatná.**

  Uživatele v tomto případě naprosto nezajímá, kde se ocitl. Otevřel odkaz u něhož usoudil, že patří bance a spoléhá se na to, že se na webu banky opravdu nachází. Jak jsem již uvedl výše jazyk HTML umožňuje vytvořit hypertextový odkaz z jakéhokoliv textu. A to je v tomto případě kámen úrazu.

- **Zkontroluji, zda-li se v adresním řádku vyskytuje zelený zámek, popř. nápis Zabezpečeno.**

  Tato možnost je **špatná.**

  Při přihlašování se ke kterékoliv online službě je potřeba, aby bylo spojení mezi uživatelem a serverem zabezpečeno protokolem HTTPS, které se v adresním řádku vyznačuje zeleným zámkem. Nesmíme však zapomínat, že stejně jako pravý web může být takto zabezpečen i web podvodný. Pokud tedy návštěvník nezkontroluje obsah adresního řádku, opět si nemůže být jist tím, kde se nachází.

- **Stránku si prohlédnu a ujistím se, že jsem opravdu na webu banky.**

  Tato možnost je **špatná.**

  Základním principem phishingu je co nejkvalitnější napodobení originální stránky. Pokud je podvodná stránka vytvořena precizně, může být na první pohled velmi obtížné rozeznat ji od originálu. Tento způsob ověření je tedy nedostatečný.

- **Zkontroluji adresu uvedenou v adresním řádku.**

  Tato možnost je **správná.**

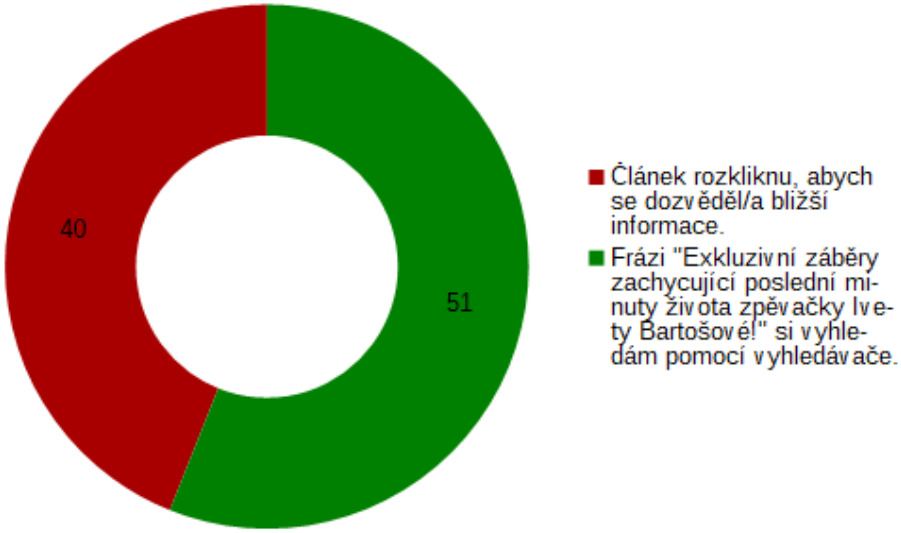
  Z odkazu uvedeného v adresním řádku je vždy poznat, kde se uživatel opravdu nachází. Tento údaj je možné pozměnit pouze pomocí velice sofistikovaného DNS útoku, který je však složitě proveditelný a nespadá do kategorie sociálního inženýrství. Společně se správnou adresou by se měl v adresním řádku zobrazovat i zelený zámek, jehož přítomnost zamezí odposlechnutí odeslaných údajů v průběhu jejich odesílání.

○ **Na hlavní stránce vašeho facebookového profilu se vám zobrazí odkaz na článek, v jehož titulku bude psáno: „Exkluzivní záběry zachycující poslední minuty života zpěvačky Ivety Bartošové!“. Jaká bude vaše reakce?**

■ **Nabídnuté možnosti**

- Frázi "Exkluzivní záběry zachycující poslední minuty života zpěvačky Ivety Bartošové!" si vyhledám pomocí vyhledávače.
- Článek rozkliknu, abych se dozvěděl/a bližší informace.

■ Výsledky



Graf 6.: Odpovědi respondentů k otázce zajímavého titulku článku

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Frázi „Exkluzivní záběry zachycující poslední minuty života zpěvačky Ivety Bartošové!“ si vyhledám pomocí vyhledávače.**

  Tato možnost je **správná.**

  V titulku clickbaitingového odkazu se zpravidla vyskytují vysoce nepravděpodobné informace. Pokud odkaz u uživatele svým titulkem vyvolá zájem, měl by si uvedenou frázi před otevřením odkazu vyhledat a zjistit, zda-li se článek na toto téma vyskytuje i na dalších webech.

- **Článek rozkliknu, abych se dozvěděl/a bližší informace.**

  Tato možnost je **špatná.**

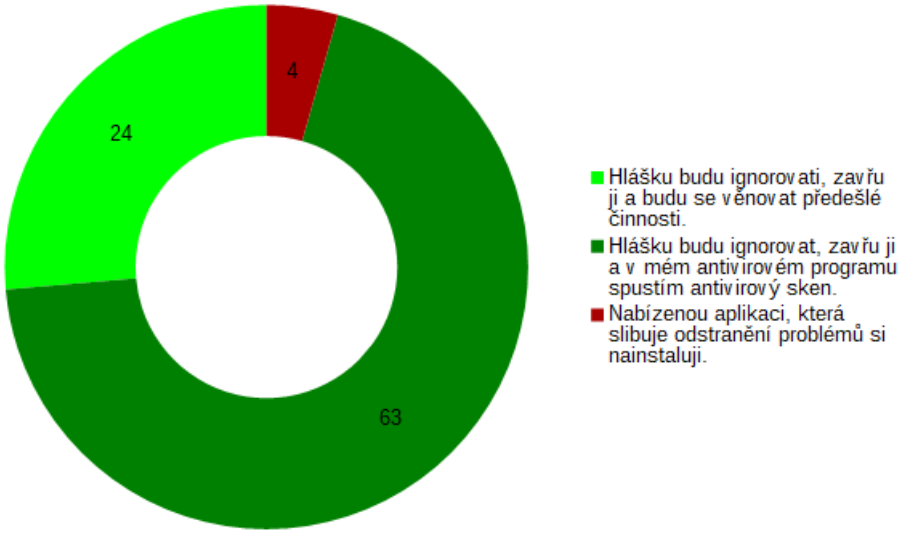
  Otevřením odkazu dojde k naplnění podvodníkových cílů. Titulek sice uváděl jistou informaci, avšak návštěvník nemůže vědět, zda-li se uvedená informace na webu nachází.

- **Na vašem mobilním telefonu se vám zobrazí zpráva, která vás informuje o aktuálním stavu vašeho zařízení. Zpráva vás informuje o zaneseném vnitřním úložišti a o čtyřech virech, které se ve vašem mobilu nacházejí. Současně vám nabídne aplikaci, která vaše problémy vyřeší. Nabídka aplikace však bude časově omezena na dvě minuty, poté přestane platit. Jak zareagujete?**

  ■ **Nabídnuté možnosti**

  - Hlášku budu ignorovati, zavřu ji a budu se věnovat předešlé činnosti.
  - Hlášku budu ignorovat, zavřu ji a v mém antivirovém programu spustím antivirový sken.
  - Nabízenou aplikaci, která slibuje odstranění problémů si nainstaluji.

  ■ **Výsledky**



Graf 7.: Odpovědi respondentů k otázce upozornění o zavirovaném telefonu

  ■ **Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností**

  - **Hlášku budu ignorovati, zavřu ji a budu se věnovat předešlé činnosti.**

    Tato možnost je **správná.**

    Touto akcí zamezí uživatel nakažení systému nebezpečnou aplikací. Poměrně často se však tato podvodná oznámení zobrazují prostřednictvím jiné škodlivé aplikace na již infikovaném telefonu. Jelikož uživatel po

zavření hlášky neprovede žádnou další akci, nezjistí, jak na tom jeho telefon co se nákazy týče opravdu je.

- **Hlášku budu ignorovat, zavřu ji a v mém antivirovém programu spustím antivirový sken.**

  Tato možnost je **správná.**

  Stejně jako v předchozím případě je útočníkovi znemožněno nainstalovat škodlivou aplikaci. Provedením antivirového skenu navíc uživatel zjistí opravdový stav jeho telefonu a v případě výskytu infekce může zasáhnout.

- **Nabízenou aplikaci, která slibuje odstranění problémů si nainstaluji.**

  Tato možnost je **špatná.**

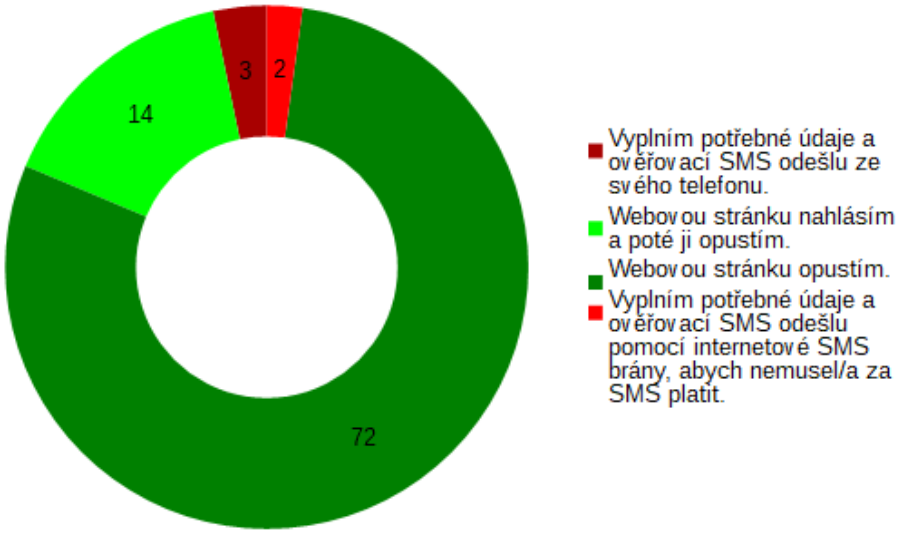
  V tomto případě si uživatel s největší pravděpodobností do svého smartphonu nainstaluje škodlivou aplikaci. Při surfování prostřednictvím mobilního telefonu nesmí uživatel zapomínat na skutečnost, že má telefon zabezpečen jím vybraným antivirovým řešením, které vždy upozorňuje prostřednictvím svojí aplikace, ne webového prohlížeče, jak je tomu v případě podvodných oznámení.

○ **Ve vašem webovém prohlížeči se vám zobrazí banner, který vás informuje o výhře notebooku IBM Thinkpad T1100. Po rozkliknutí banneru se vám na obrazovce zobrazí stránka, která vás vybízí k vyplnění vašich kontaktních informací. Dále vás žádá o odeslání kontrolního kódu na dané telefonní číslo. To vše s příslibem získání onoho notebooku. Jak se zachováte?**

■ **Nabídnuté možnosti**

- Vyplním potřebné údaje a ověřovací SMS odešlu ze svého telefonu.
- Webovou stránku nahlásím a poté ji opustím.
- Webovou stránku opustím.
- Vyplním potřebné údaje a ověřovací SMS odešlu pomocí internetové SMS brány, abych nemusel/a za SMS platit.

■ Výsledky



Graf 8.: Odpovědi respondentů k otázce výherního banneru

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Vyplním potřebné údaje a ověřovací SMS odešlu ze svého telefonu.**

  Tato možnost je **špatná.**

  Při odeslání těchto údajů z telefonního čísla získá útočník kromě obětí uvedených informací také finanční obnos, kterým byla financováno zaslání prémiové SMS.

- **Webovou stránku nahlásím a poté ji opustím.**

  Tato možnost je **správná.**

  Opuštění webové stránky je v tomto případě nejlepším řešením. Jejím nahlášením se navíc dostane do systému vyhledávačů a antivirových společností, které začnou své uživatele při návštěvě tohoto webu upozorňovat na nebezpečí, které se na něm skrývá. Díky tomu se životnost takovéto stránky rapidně sníží.

- **Webovou stránku opustím.**

  Tato možnost je **správná.**

  Opustí-li návštěvník webovou stránku bez toho, aniž by přes ni odeslal jakékoliv údaje, zmaří tím zájem útočníka. Jelikož však stránku

nenahlásí, nebude zařazena do databází a o to delší dobu může zkoušet obalamutit další surfaře.

- **Vyplním potřebné údaje a ověřovací SMS odešlu pomocí internetové SMS brány, abych nemusel/a za SMS platit.**

  Tato možnost je **špatná**.

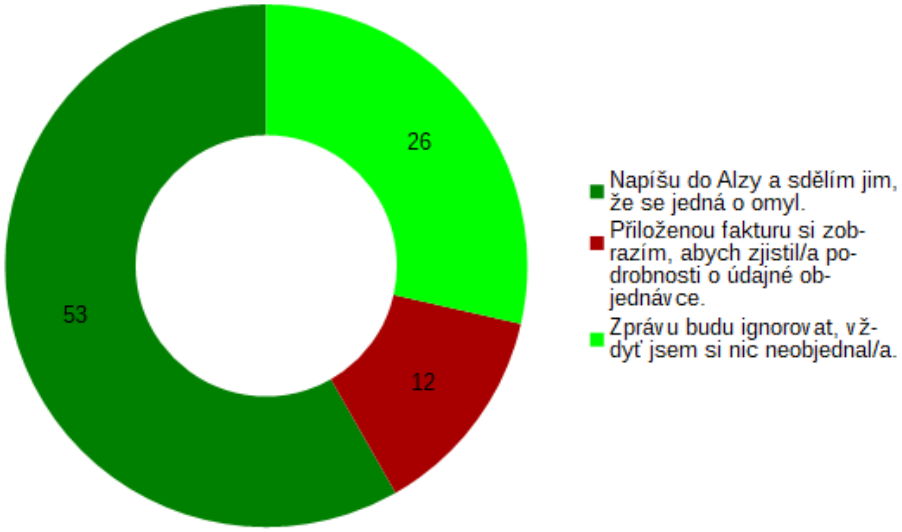
  Toto řešení se dá označit za elegantní díky faktu, že se návštěvník šikovně vyhne nutnosti platit za prémiovou SMS. Navzdory tomu však přesto dojde k vyzrazení kontaktních údajů, které jsou obecně považovány za soukromé.

○ **Do vaší emailové schránky vám přijde zpráva, v níž vám Alza posílá ve formátu PDF fakturu k plazmové televizi, kterou jste si však neobjednali. Jak se zprávou naložíte?**

■ **Nabídnuté možnosti**

- Napíšu do Alzy a sdělím jim, že se jedná o omyl.
- Přiloženou fakturu si zobrazím, abych zjistil/a podrobnosti o údajné objednávce.
- Zprávu budu ignorovat, vždyť jsem si nic neobjednal/a.

■ Výsledky



Graf 9.: Odpovědi respondentů k otázce faktury z Alzy

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Napíšu do Alzy a sdělím jim, že se jedná o omyl.**

  Tato možnost je **správná.**

  Informováním Alzy o této skutečnosti napomůže uživatel ve vyřešení celé situace. V případě, že se nejednalo o omyl, ale o podvod může díky jeho zprávě Alza proti podvodníkovi zasáhnout. Samozřejmě, nedojde-li ke spuštění přílohy, nebudou podvodníkova očekávání naplněna.

- **Přiloženou fakturu si zobrazím, abych zjistil/a podrobnosti o údajné objednávce.**

  Tato možnost je **špatná**.

  Otevírání neznámé přílohy není bezpečné za žádné situace, obzvlášť, pokud se jedná o spustitelné soubory, tj. např. .com, .bat, .exe, nebo o soubory dokumentů, mezi které řadíme např. .docx, .pdf, .xlsx, .odt a podobné. Otevření takového souboru vede ke spuštění škodlivého kódu, který může způsobit cokoliv, ať už se jedná o zcizení dat, nebo zašifrování disku.

- **Zprávu budu ignorovat, vždyť jsem si nic neobjednal/a.**

  Tato možnost je **správná.**

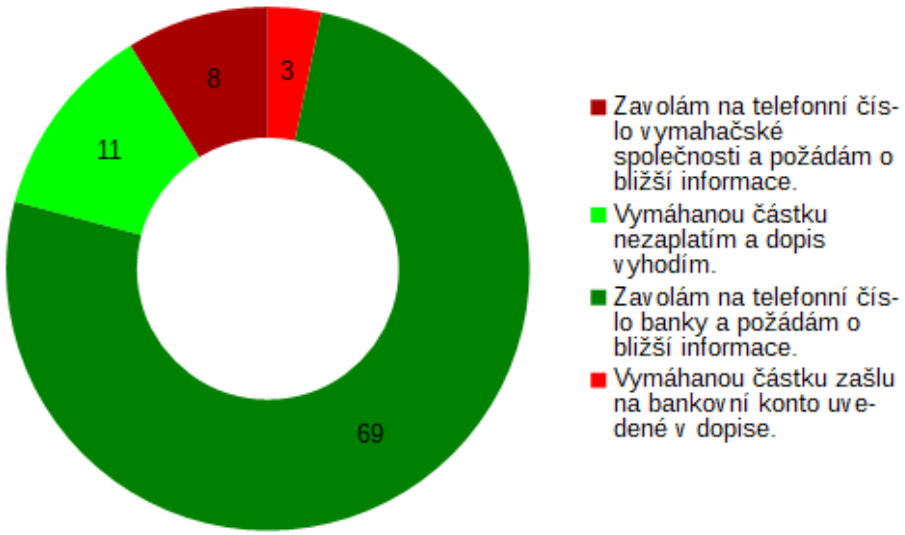
  Zvolí-li uživatel tuto možnost, vyvaruje se infekci svého počítače. Žádným způsobem však nezasáhne proti nekalému jednání podvodníka, který bude moci své praktiky dále zkoušet na další uživatele.

○ **Do poštovní schránky vám přijde dopis od vymahačské společnosti najaté vaší bankou, která chce splatit dluh ve výši 1004 Kč, který vznikl neplacením poplatků za vedení účtu. Jak budete postupovat?**

■ **Nabídnuté možnosti**

- Zavolám na telefonní číslo vymahačské společnosti a požádám o bližší informace.
- Vymáhanou částku nezaplatím a dopis vyhodím.
- Zavolám na telefonní číslo banky a požádám o bližší informace.
- Vymáhanou částku zašlu na bankovní konto uvedené v dopise.

■ **Výsledky**



Graf 10.: Odpovědi respondentů k otázce dopisu od vymahačské společnosti

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Zavolám na telefonní číslo vymahačské společnosti a požádám o bližší informace.**

  Tato možnost je **špatná.**

  Příjemce netuší, zda-li je žádost o zaplacení částky opravdu podána bankou. Pokud je dopis podvržený, bude podvržené taktéž telefonní číslo. V případě, že na něj domnělý dlužník zavolá, bude pravděpodobně komunikovat přímo s podvodníkem, který mu všechny otázky potvrdí. Přesvědčený člověk poté částku zašle.

- **Vymáhanou částku nezaplatím a dopis vyhodím.**

  Tato možnost je **správná.**

  O správné jednání se jedná v případě, že byl dopis podvržený. Phishing použitý ve formě dopisu se na příjemce neosvědčil a útočník tak žádné peníze nezíská. V případě, že je dopis pravý by však mohlo dojít k situace, že by se dluh vyšplhal do ještě vyšších částek. Je proto vhodné si pravost dopisu ověřit, nejlépe zavoláním do banky.

- **Zavolám na telefonní číslo banky a požádám o bližší informace.**

  Tato možnost je **správná.**

  Není-li si příjemce pravostí dopisu zcela jist, je vhodné, když zavolá na číslo banky uvedené na jejich oficiálních webových stránkách. Získá tím informace z první ruky a společně s nimi jistotu, že je dopis pravý, případně podvržený.

- **Vymáhanou částku zašlu na bankovní konto uvedené v dopise.**

  Tato možnost je **špatná.**

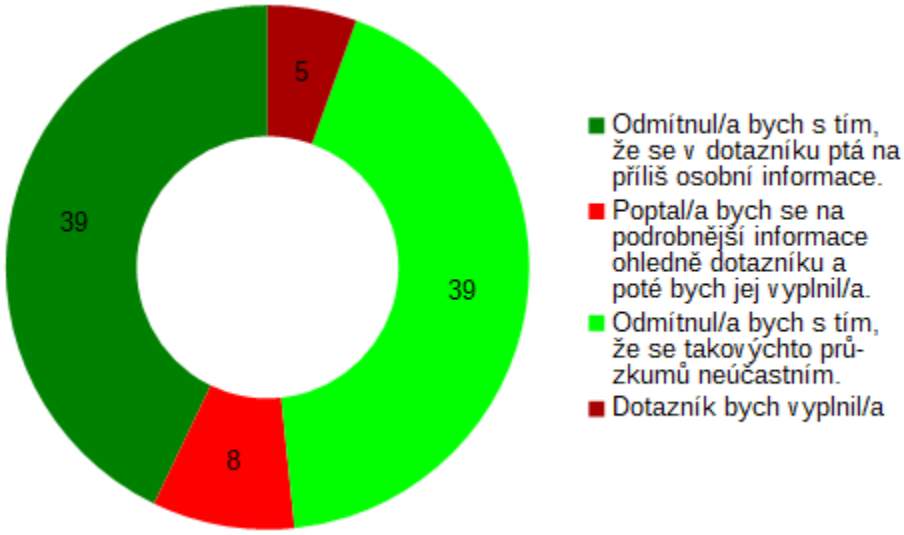
  Ze strany příjemce není v tomto případě žádná snaha o ověření pravosti vzniklé situace. Díky tomu ulehčí podvodníkovi práci tím, že nezavolá na telefonní číslo uvedené v dopise, a podvodník tak získá uvedenou částku téměř bez námahy.

- **Na ulici vás zastaví člověk, který se vám představí jako zaměstnanec nějaké organizace, s prosbou o vyplnění dotazníku týkajícího se prázdnin. Naleznete v něm otázky typu kam a kdy jedete na dovolenou; jak dlouho bude vaše dovolená trvat; zda-li cestujete raději do zahraničí, či po tuzemsku; jak byste ohodnotili ubytovací zařízení, které jste doposud navštívili; atp. Za odměnu byste dostali přívěsek na klíče. Jak byste zareagovali? Byli byste ochotni dotazník vyplnit, či nikoliv? Odpověď odůvodněte.**

  - **Nabídnuté možnosti**

    - Odmítnul/a bych s tím, že se v dotazníku ptá na příliš osobní informace.
    - Poptal/a bych se na podrobnější informace ohledně dotazníku a poté bych jej vyplnil/a.
    - Odmítnul/a bych s tím, že se takovýchto průzkumů neúčastním.
    - Dotazník bych vyplnil/a.

  - **Výsledky**



Graf 11.: Odpovědi respondentů k otázce pouličního dotazníku

■ Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností

- **Odmítnul/a bych s tím, že se v dotazníku ptá na příliš osobní informace.**

  Tato možnost je **správná.**

  Veřejné dotazníky obsahující otázky týkající-se ožehavých témat, jako je například toto, byl měl každý zásadně odmítnout. Při zamyšlení se nad smyslem takového dotazníku je těžké dojít ke smysluplnému závěru. Zároveň není jasné, do jaké úrovně je dotazník anonymní a jak je s informacemi dále nakládáno.

- **Poptal/a bych se na podrobnější informace ohledně dotazníku a poté bych jej vyplnil/a.**

  Tato možnost je **špatná.**

  V každém případě se zmíněné informace považují soukromé, není tedy vhodné je sdělovat komukoliv cizímu. Pokud je tazatel zkušený sociální inženýr, nebude pro něj těžké přesvědčit kolemjdoucího o „své pravdě“. Během tohoto rozhovoru může z nic netušící oběti získat i nějaké informace navíc.

- **Odmítnul/a bych s tím, že se takovýchto průzkumů neúčastním.**

  Tato možnost je **správná.**

  Další správná možnost, avšak tentokrát si tázaný neuvědomuje cennost informací, které po něm tazatel žádá. Před vyplněním dotazníku ho chrání pouze princip, který si sám stanovil.

- **Dotazník bych vyplnil/a.**

  Tato možnost je **špatná.**

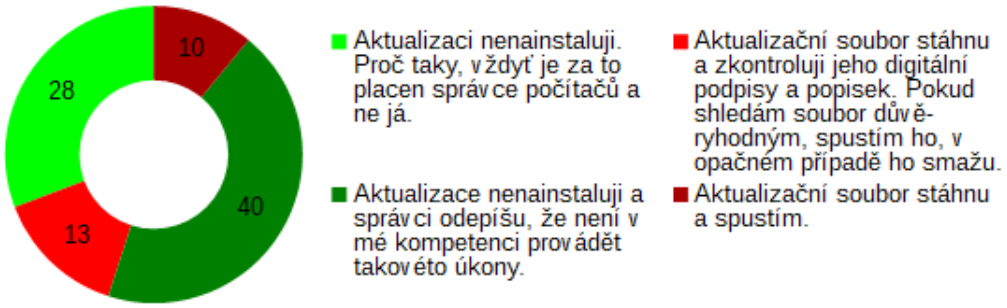
  Kolemjdoucího nezajímají detailnější informace, co se dotazníku týče. Zároveň mu nedělá problém sdělit cizí osobě informace, které po něm žádá, případně si neuvědomuje jejich hodnotu.

- **Na email vám dojde zpráva od správce firemní počítačové sítě, v níž vás žádá o instalaci kritické aktualizace, která je pro váš pracovní počítač nezbytná. Soubor s aktualizacemi najdete v příloze. Jak s touto zprávou naložíte?**

  ■ **Nabídnuté možnosti**

  - Aktualizaci nenainstaluji. Proč taky, vždyť je za to placen správce počítačů a ne já.
  - Aktualizační soubor stáhnu a zkontroluji jeho digitální podpisy a popisek. Pokud shledám soubor důvěryhodným, spustím ho, v opačném případě ho smažu.
  - Aktualizace nenainstaluji a správci odepíšu, že není v mé kompetenci provádět takovéto úkony.
  - Aktualizační soubor stáhnu a spustím.

  ■ **Výsledky**



Graf 12.: Odpovědi respondentů k otázce žádosti o aktualizaci systému

  ■ **Odůvodnění správnosti, nebo nesprávnosti jednotlivých možností**

  - **Aktualizaci nenainstaluji. Proč taky, vždyť je za to placen správce počítačů a ne já.**

    Tato možnost je **správná.**

Každý zaměstnanec by si měl uvědomit, že v instituci, která jej zaměstnává plní určitou roli, která obnáší své povinnosti a kompetence. Tyto kompetence by neměl překračovat jednak proto, že to není součásti náplně jeho práce a také proto, že za to není zaplacen. Pokud nemá v náplni práce instalaci aktualizací, je důležité, aby tuto práci nevykonával, a to i navzdory tomu, že jej o to správce počítačů požádá.

- **Aktualizační soubor stáhnu a zkontroluji jeho digitální podpisy a popisek. Pokud shledám soubor důvěryhodným, spustím ho, v opačném případě ho smažu.**

  Tato možnost je **špatná.**

  Digitální podpis souboru je vydáván společností, která daný soubor vytvořila. Tento podpis stvrzuje pravost onoho souboru. Pomocí některých sofistikovaných metod se však i tento podpis dá zfalšovat. Ověření pravosti digitálního podpisu však není uživatel počítače mající k dispozici standardní softwarovou výbavu schopen. Proto je vhodné se řídit poučkou, která byla uvedena u předchozí možnosti.

- **Aktualizace nenainstaluji a správci odepíšu, že není v mé kompetenci provádět takovéto úkony.**

  Tato možnost je **správná.**

  Pro tento případ platí poučka uvedená u první zmíněné možnosti, tj. „Aktualizaci nenainstaluji. Proč taky, vždyť je za to placen správce počítačů a ne já.“ Tím, že zaměstnanec správce počítačů nejlépe po telefonu kontaktuje a sdělí mu, že aktualizaci nemůže nainstalovat, správce bude s touto skutečností počítat a zařídí se podle ní.

- **Aktualizační soubor stáhnu a spustím.**

  Tato možnost je **špatná.**

  Jak již bylo několikrát zmíněno, technologie, na níž pracuje email má své vady, které umožňují změnit adresu odesílatele – zaměstnanec tedy nemá jistotu, že zprávu psal opravdu správce. Do tohoto pokusu je navíc zakomponována spustitelná příloha, jejíž obsah je stejně neznámý, jako identita odesílatele.

5.4. Zhodnocení výsledků dotazníku

Ačkoliv většina respondentů neměla tušení o významu základních pojmů této problematiky, v uvedených situacích by, soudě dle odpovědí, obstála taktéž většina. Z mého pohledu se jedná o chvályhodný výsledek.

Na druhou stranu, není jednoznačně prokazatelné, zda respondenti odpovídali opravdu tak, jak jsem je o to žádal. Přestože jim byla zaručena naprostá anonymita, mohli někteří záměrně odpovídat jiným, než požadovaným způsobem. Dále je také možné, že ačkoliv respondenti své reakce na dané situace znali, odmítli si je z důvodu jejich nesprávnosti připustit a tak odpovídali jinak. Tyto faktory významně ovlivňují objektivitu a vypovídající hodnotu dotazníku. Výsledky dotazníku je tedy nutné brát s rezervou a nelze je považovat za obraz společnosti.

5.5. Srovnání vybraných výsledků s daty získanými v reálném testování

Přestože byly výsledky dotazníku vyhodnoceny velice kladně, při jejich srovnání s výsledky získanými při reálném testování vzniklo mnoho nesrovnalostí.

Předpokládal jsem, že si budou obě skupiny výsledků velice podobné. Jak se však ukázalo, reálné testy dopadly naprosto katastrofálně, kdy nám většina útoků hladce prošla.

Toto srovnání je poměrně lehce napadnutelné, neboť dotazník vyplnilo 91 respondentů a jednotlivých podvodných zkoušek se účastnila zpravidla jedna osoba. Dá se tedy namítnout, že zrovna tato osoba patří do menšinové skupiny respondentů, kteří odpověděli špatně.

Důvodem tohoto srovnání je však vzdělání prakticky testovaných osob. Tito lidé mají všichni do jednoho vysokoškolské vzdělání obohacené o znalost IT, která je při jejich práci nutná. Dle těchto informací soudě jsem předpokládal, že mají násobně větší šanci v testech uspět, než jakou by měli například respondenti studující základní školu.

Vědomím této skutečnosti docházím k závěru, že někteří z respondentů nevyplňovali dotazník podle pokynů, které jsem uvedl, čímž ovlivnili vypovídající hodnotu dotazníku.

■ Telefonní pretexting versus „telefonát z úřadu“

V případě zmíněné otázky zabývající se domnělým telefonátem z úřadu byla úspěšnost poměrně vysoká. Některou ze správných možností zvolily více než 2 třetiny respondentů.

Naopak v případě reálného testování vyhověla oběť veškerým požadavkům a to bez jakéhokoliv ověřování vzniklé situace.

- **Baiting versus odstavec „pohozená flashka“**

  V případě tohoto pokusu je shodnost výsledků nejvyšší. Respondenti by podle jejich odpovědí nalezené médium nahlásili bez toho, aniž by jej spustili.

  Ke stejnému výsledku došlo i v případě praktického testování, kdy bylo nalezené DVD umístěno do kanceláře mezi ostatní DVD bez toho, aniž by bylo spuštěno.

- **Podvodný email versus „zpráva od nadřízeného“**

  Uvedená otázka se zabývala problematikou emailu žádajícího jistá pracovní data. Jednu ze správných možností si v případě této otázky vybraly jako svou reakci necelé dvě třetiny všech respondentů.

  V případě podvodného emailu, jehož prostřednictvím jsme žádali o zařazení paní Dvořákové do položky Rekreace jsme se však setkali s úspěchem.

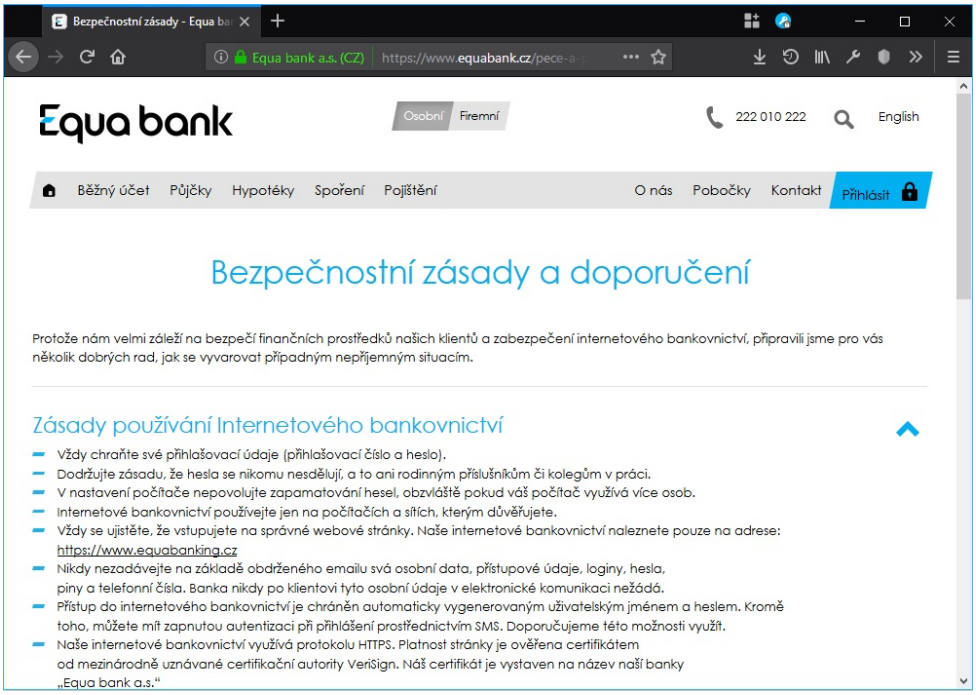
6. Obrana před metodami sociálního inženýrství

6.1. V reálném světě

6.1.1. Objasnění rozdílu mezi standardně a nestandardně řešenou situací

Za standardní postup řešení dané situace považujeme takový postup, který je všeobecně používaný a uváděný jako správný. Takovýto postup je dán zákonem, etickými kodexy, nebo v našem případě nejčastěji nějakou organizací, či institucí.

Vyžaduje-li nějaká instituce vykonávání úkonů, které by v případě nesprávného provedení mohly jakýmkoliv způsobem ohrozit klienta této instituce, je vhodné vydat doporučené zásady v provádění dané operace. Zjednodušeně řečeno, každá instituce by měla mít své bezpečnostní zásady, kterými by se měli její klienti řídit. Díky tomu jsou schopni předejít mnohým problémům.



Obr.8.: Bezpečnostní zásady a doporučení bankovní společnosti Equa Bank a.s.

Zdroj: EQUA BANK A.S.: Bezpečnostní zásady a doporučení. https://www.equabank.cz/pece-a-podpora/bezpecnostni-zasady

Za nestandardní postup se obecně považuje postup takový, který neodpovídá daným bezpečnostním zásadám.

6.1.2. Techniky, jejichž pomocí se dá podvodné jednání odhalit

Znalost zmíněných bezpečnostních zásad by měla být samozřejmostí. Díky jejich znalosti je člověk v určitých situacích schopen reagovat správně, ačkoliv jej druhá strana vybízí ke zvolení jiného postupu.

Dalším aspektem ochrany před sociálním inženýrstvím je lidová poučka znějící „důvěřuj, ale prověřuj“. Je potřeba počítat s tím, že ne každý má dobré úmysly. V případě i sebemenších pochybností o jakékoliv nastalé situaci je vhodné se ptát na detaily a otázky, které mohou případného podvodníka zaskočit. Uznávám však, že výběr těchto otázek nemusí být lehký.

6.1.3. Způsoby zakročení proti sociálním inženýrům

Za situace, kdy člověk vyhodnotí danou situaci jako podvodnou je vhodné o tomto činu někoho informovat.

Za vhodnou možnost se dá považovat informování Policie České republiky, která se na člověka, který se o podvod pokoušel více zaměří. V případě, že by jej přistihla při vykonávání podobné činnosti, by jej mohla odvést na policejní stanici k výslechu, čímž by zabránila dalším snahám o podvod.

Další vhodnou variantou je přímé kontaktování instituce, za jejíhož zaměstnance se podvodník vydával. Ta poté o těchto podvodných snahách informuje své klienty, případně i policii, která může této informaci přikládat vyšší váhu než v případě, že by ji ohlásil jednotlivec.

6.2. V kyberprostoru

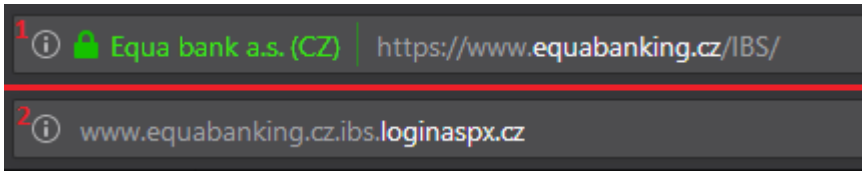
6.2.1. Znaky definující podvodnou stránku

- **Falešná adresa**

Doména, na níž se originální webová stránka nachází je ve vlastnictví příslušné instituce. Podvodník tedy není na tuto doméno schopen nahrát svůj vlastní podvodný web.

Řešením je založení webové stránky, jejíž adresa je podobná originální adrese, a to prostřednictvím některého z webhostingů.

Zná-li návštěvník legitimní adresu webu, ke kterému chce přistoupit, není pro něj těžké podvodný web odhalit.



Obr. 9.: Rozdíl mezi legitimní a podvodnou adresou

Z obrázku je rozdíl mezi oběma adresami zcela patrný. Podvodník spoléhá na to, že bude uživatel číst adresu od začátku. Jak je totiž nepřehlédnutelné, obě adresy začínají stejně. Pozornost je však třeba věnovat části adresy, která je vyznačena odlišnou barvou, než zbytek adresy. Tuto funkcionalitu nabízí webový prohlížeč Mozilla Firefox, který byl použit pro pořízení uvedeného obrázku. Majoritně zastoupený prohlížeč Google Chrome tuto funkcionalitu postrádá. Je tedy nutné adresu zkontrolovat ručně.

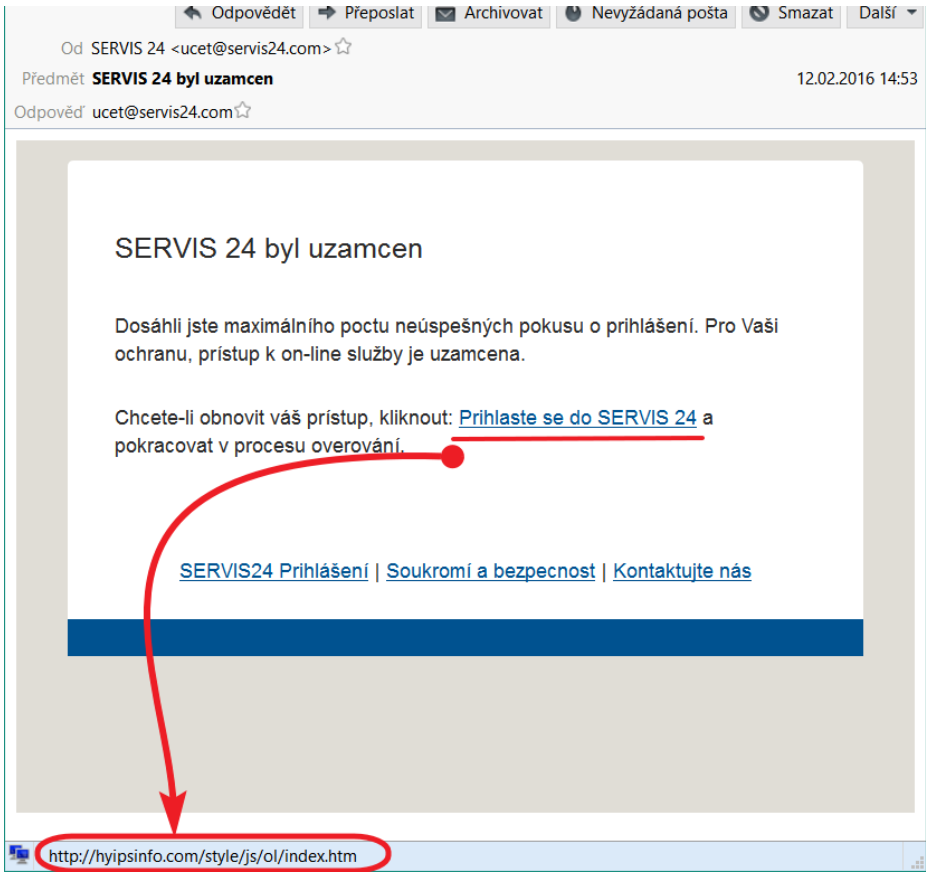
○ Gramatické chyby, cizí jazyk

Phishingové útoky se ve většině případů vyznačují taktéž různými chybami v textu, ať už se jedná o skladbu vět, či gramatické chyby. Je tomu tak z toho důvodu, že většina takovýchto útoků je vedena ze zahraničí. Vytvoření důvěryhodné kopie tedy zabraňuje jazyková bariéra.

V případě webových stránek je situace komplikovanější, neboť poměrně často podvodníci vytvoří kopii struktury originálního webu, včetně textu. Ty jsou tedy ve finále stejné.

Odlišná situace nastává v případě podvodného emailu, kdy nemá útočník pro vytvoření zprávy žádné podklady. Obsah takového emailu je odlišný od legitimní zprávy a tím pádem si jej musí podvodník vymyslet sám.

Další častou variantou je podvodná stránka či zpráva v cizím jazyce. Cizí jazyk sám o sobě je známkou toho, že je něco v nepořádku. To však platí pouze v případě, že legitimní zprávy od napodobované instituce bývaly již dříve doručovány v jazyce používaném podvodníkem.



Obr. 10.: Podvodný email vydávající se za SERVIS24

Zdroj: HOAX.CZ: Servis 24 byl uzamčen. http://www.hoax.cz/phishing/servis-24-byl-uzamcen-20160212/

Z uvedeného screenshotu je jasně patrné, že zpráva postrádá diakritiku. Nejvíce však bije do očí slovosled některých vět, které díky tomu vypadají naprosto nedůvěryhodně.

Text zvýrazněný červenou barvou vizuálně objasňuje princip maskování odkazů. Při najetí na jakýkoliv odkaz, ať už ve webovém prohlížeči, či poštovním klientovi dojde vždy k zobrazení skutečné adresy, na kterou odkaz vede. Většinou je tato adresa ukázána v levém spodním rohu okna.

6.2.2. Možnosti zabraňující šíření phishingu

- **Osvěta a prevence**

Stejně, jak tomu bývá i u dalších rizikových situací, nejlepší zbraní je prevence. Pokud budou lidé schopni phishing rozeznat a eliminovat, nebude pro podvodníky výhodné jej používat. Tato poučka neplatí pouze pro phishing, ale taktéž pro ostatní metody sociálního inženýrství.

○ Nahlášení podvodných úkazů

Do konfrontace s phishingem se uživatel dostává téměř výhradně prostřednictvím webového prohlížeče, v menším zastoupení také pomocí poštovního klienta.

Moderní webové prohlížeče nabízí kromě bezpočtu různých funkcionalit také možnost nahlásit nebezpečný web. Nezáleží na tom, zda-li se jedná o web obsahující malware, nelegální obsah, nebo právě phishing. Nahlášením stránky dojde k jejímu zařazení do blacklistu autora prohlížeče, případně vyhledávače. Zařazení do blacklistu však samozřejmě nezáleží na reportu jednoho člověka. Pro zařazení webu do blacklistu je třeba sesbírat více stížností.

■ Nahlášení nebezpečné stránky v prohlížeči Mozilla Firefox

Do formuláře pro odeslání podvodné stránky se uživatel dostane kliknutím na tlačítko Menu – Nápověda – Nahlásit klamavou stránku...

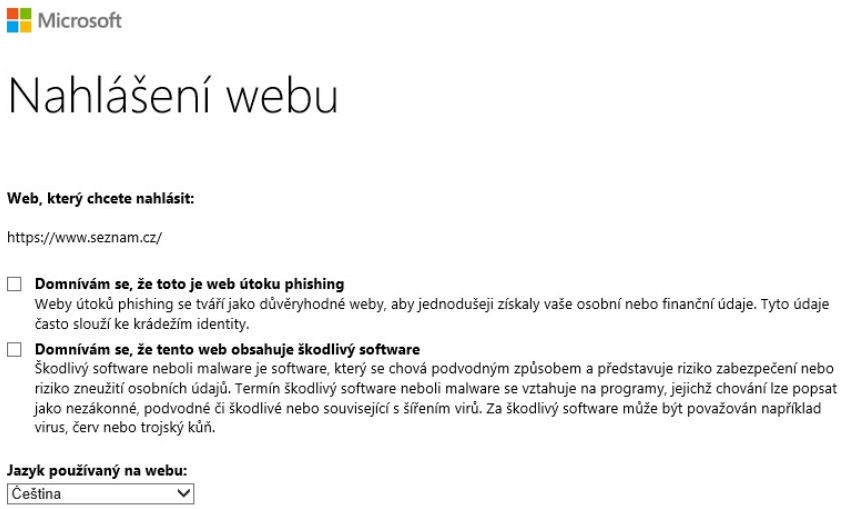
Obr. 11.: Formulář pro ohlášení podvodné stránky v aplikaci Mozilla Firefox

■ Nahlášení nebezpečné stránky v prohlížeči Google Chrome

Prohlížeč Chrome umožňuje skrze své nabídky odeslat pouze zprávu o problému s danou webovou stránkou. Nejefektivnějším řešením je pravděpodobně navštívení webové stránky na adrese https://safebrowsing.google.com/safebrowsing/report_phish/, kde je možné podvodný web nahlásit stejným způsobem, jakým tomu bylo u prohlížeče Firefox.

■ Nahlášení nebezpečné stránky v prohlížeči Internet Explorer

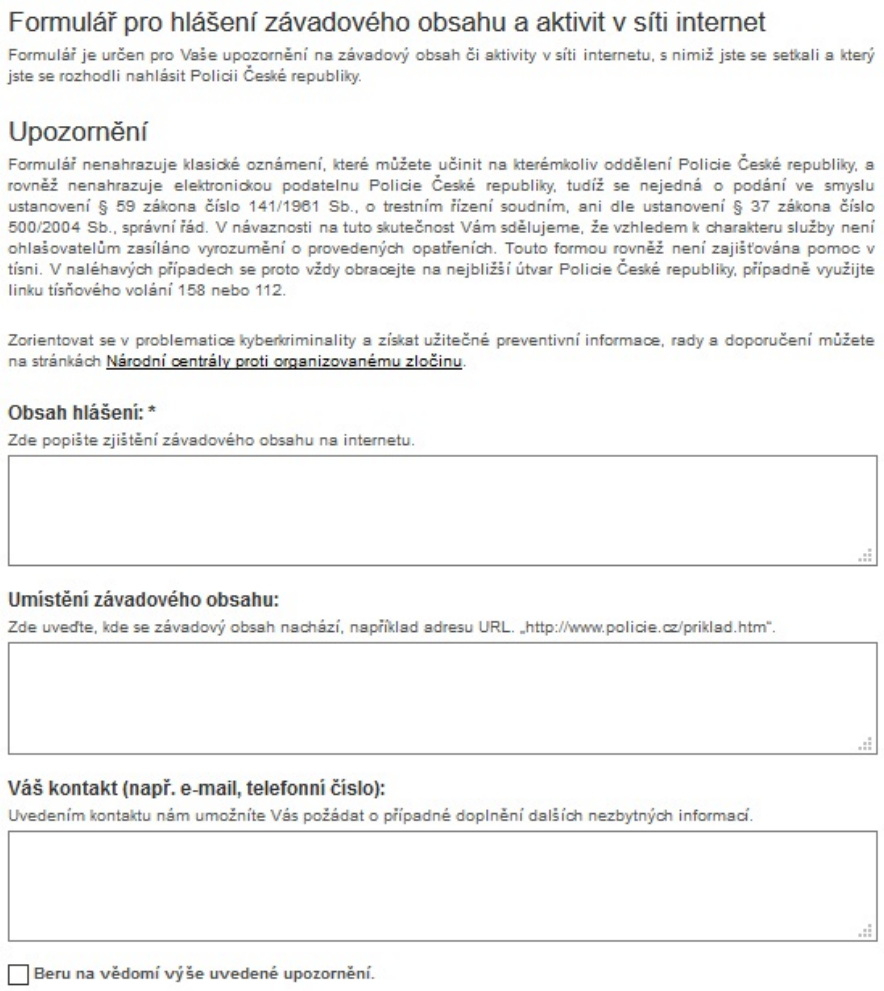
V Internet Exploreru je nahlášení webové stránky umožněno kliknutím na tlačítko Nástroje – Zabezpečení – Ohlásit nebezpečný web. Následuje otevření webu s formulářem, v němž uživatel upřesní svůj problém s webovou stránkou.



Obr. 12.: Formulář pro ohlášení podvodné stránky v aplikaci Internet Explorer

■ Nahlášení nebezpečné stránky Policii ČR

Také Policie České republiky nabízí na svých webových stránkách formulář, který umožňuje uživateli nahlásit obsah, který je proti zákonům a předpisům České republiky. Mezi tento obsah phishing rozhodně patří.



Formulář pro hlášení závadového obsahu a aktivit v síti internet

Formulář je určen pro Vaše upozornění na závadový obsah či aktivity v síti internetu, s nimiž jste se setkali a který jste se rozhodli nahlásit Policii České republiky.

Upozornění

Formulář nenahrazuje klasické oznámení, které můžete učinit na kterémkoliv oddělení Policie České republiky, a rovněž nenahrazuje elektronickou podatelnu Policie České republiky, tudíž se nejedná o podání ve smyslu ustanovení § 59 zákona číslo 141/1961 Sb., o trestním řízení soudním, ani dle ustanovení § 37 zákona číslo 500/2004 Sb., správní řád. V návaznosti na tuto skutečnost Vám sdělujeme, že vzhledem k charakteru služby není ohlašovatelům zasíláno vyrozumění o provedených opatřeních. Touto formou rovněž není zajišťována pomoc v tísni. V naléhavých případech se proto vždy obracejte na nejbližší útvar Policie České republiky, případně využijte linku tísňového volání 158 nebo 112.

Zorientovat se v problematice kyberkriminality a získat užitečné preventivní informace, rady a doporučení můžete na stránkách Národní centrály proti organizovanému zločinu.

Obsah hlášení: *

Zde popište zjištění závadového obsahu na internetu.

Umístění závadového obsahu:

Zde uveďte, kde se závadový obsah nachází, například adresu URL. „http://www.policie.cz/priklad.htm".

Váš kontakt (např. e-mail, telefonní číslo):

Uvedením kontaktu nám umožníte Vás požádat o případné doplnění dalších nezbytných informací.

☐ Beru na vědomí výše uvedené upozornění.

Obr. 13.: Formulář pro nahlášení závadných stránek provozovaný Policií ČR

Zdroj: POLICIE ČR: Formulář pro hlášení závadného obsahu a aktivit v síti Internet. http://aplikace.policie.cz/hotline/

6.2.3. Úspěšnost odhalování phishingu ve webových prohlížečích

NSS Labs je organizací, která pravidelně provádí různé průzkumy týkající se především zabezpečení webových prohlížečů.

Poslední antiphishingový průzkum provedený touto organizací, který se konal v říjnu roku 2017, zahrnul do testování prohlížeče Microsoft Edge,

Google Chrome a Mozilla Firefox, jakožto nejvýznamnější hráče na poli webových prohlížečů.

Při utváření závěrů byly použity empiricky ověřené důkazy, které byly shromažďovány nepřetržitě po dobu 23 dní, po níž probíhalo testování.

Z výsledků NSS Labs vyplynulo, že nejlepší ochranu před phishingem nabízí z testovaných prohlížečů Microsoft Edge – 92,3 %, dále Google Chrome – 74,5 % a v poslední řadě Mozilla Firefox – 61,1 %.[10]

6.2.4. Blokování phishingu pomocí nastavení sítě

Následující popis platí pro operační systém Microsoft Windows, který má mezi desktopovými operačními podíl cirka 89 %.[11] Jedná se tedy o majoritní platformu. Pro Apple Mac OS se zastoupením necelých 8 % nebude srovnání dostupné, neboť nemám k dispozici zařízení s tímto systémem. Zbývajícími systémy se svým téměř nulovým zastoupením na trhu se taktéž zabývat nebudu.

Výhoda použití DNS serveru pro většinu uživatelů spočívá v tom, že jim toto nastavení umožní obejít cenzuru určitých webových stran, které mohou být ze strany poskytovatele internetového připojení blokovány. Další výhodou, která však již souvisí s touto odbornou prací je zvýšené zabezpečení při přistupování k internetu.

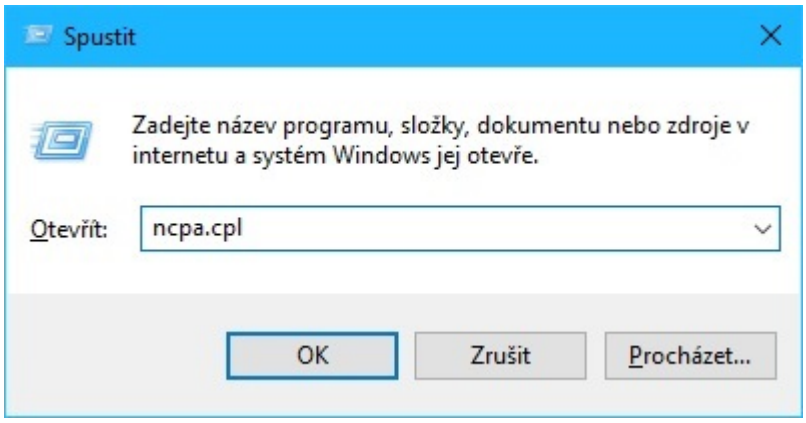
Většina populárních DNS serverů v dnešní době nabízí ochranu komunikace pomocí DNSSEC. Tato technologie zabraňuje podvodníkům pomocí techniky zvané pharming v napadení DNS záznamů. Tím je zajištěna ochrana proti zfalšování adresy zobrazované v adresním řádku.[12] Spousta poskytovatelů internetového připojení však zatím DNSSEC nenasadila. Počítače přistupující na internet přes takovéto DNS servery tedy nejsou vůči pharmingu chráněny.

Některé DNS servery jsou provozovány samotnými antivirovými společnostmi. Tyto servery zabraňují uživateli v navštívení webů, které jsou na blacklistu, tj. weby obsahující malware, nabídky zbraní a drog, podvodné weby apod.

Mezi nejvýznamnější DNS servery patří například Google Public DNS, Norton ConnectSafe, VeriSign Public DNS, Comodo Secure DNS, nebo například DNS server provozovaný správce české národní domény CZ.NIC.

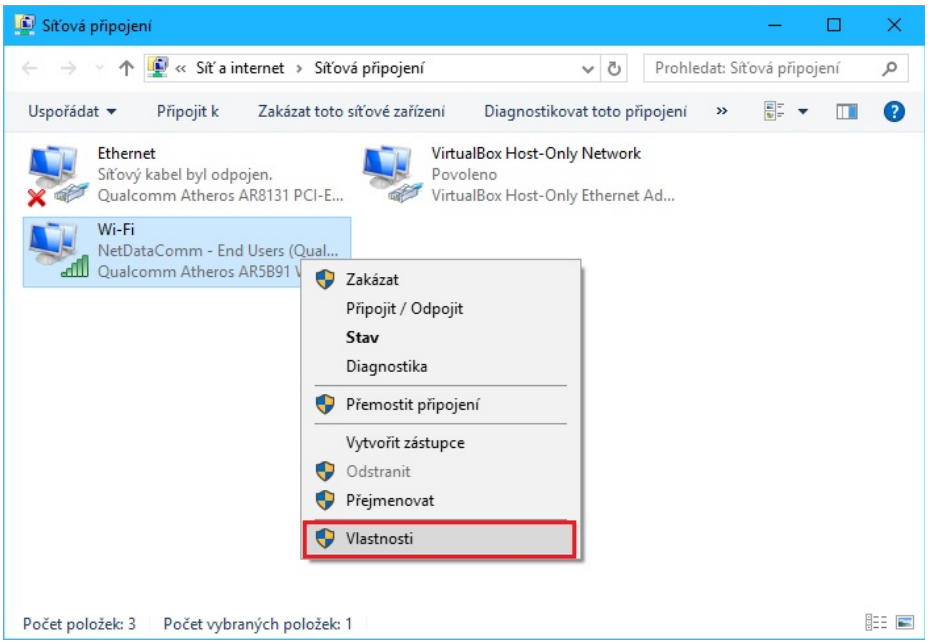
Pomocí níže uvedeného postupu zjistíte, jak přesměrovat přes některý z DNS serverů veškerou komunikaci.

- Stisknutím kombinace kláves *Win* + *R* se otevře dialogové okno Spustit. Zadejte do něj příkaz *ncpa.cpl* a stiskněte OK.



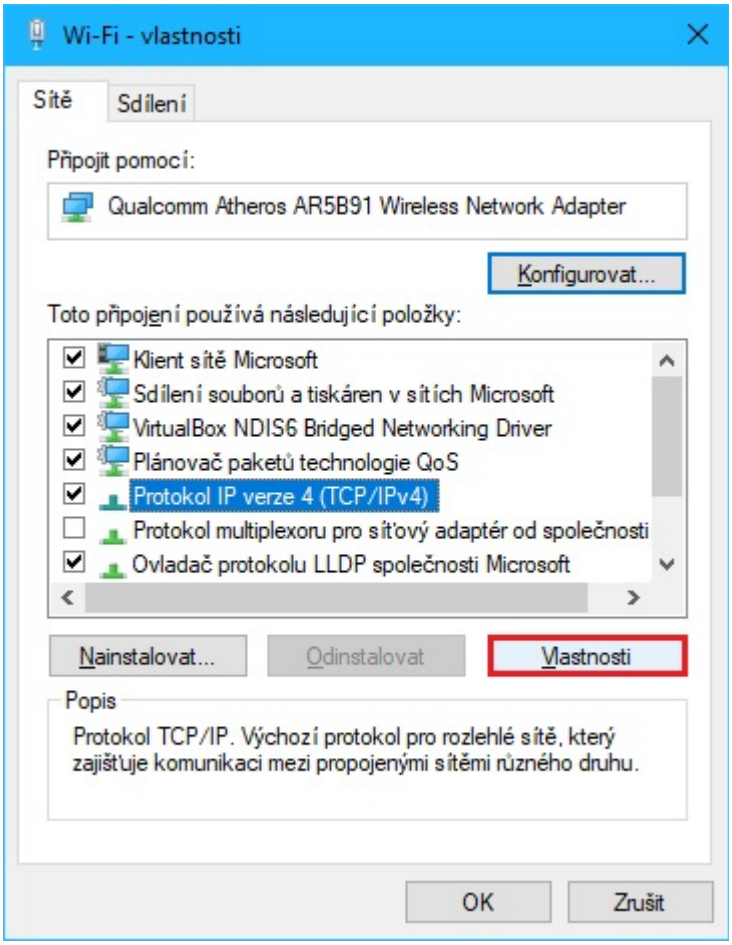
Obr. 14: Dialogové okno s příkazem ncpa.cpl

- V zobrazeném okně zvolte síť, do níž jste připojeni, klikněte na ni pravým tlačítkem myši a zvolte Vlastnosti. Tento krok může v závislosti na typu vašeho uživatelského profilu vyžadovat heslo administrátora.



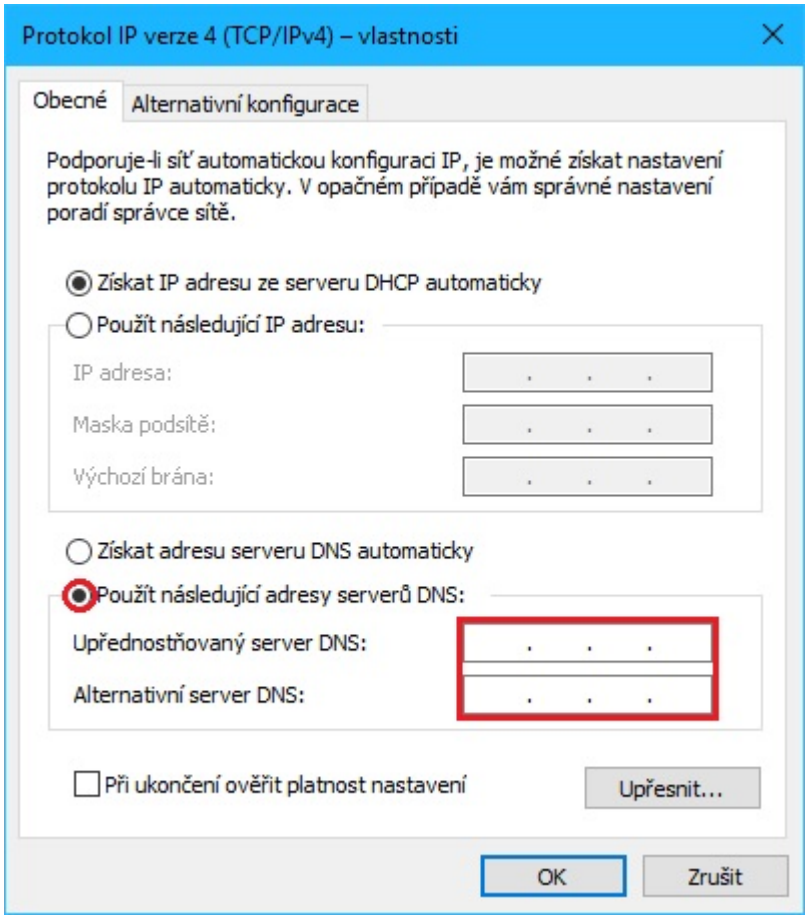
Obr. 15.: Výběr aktuálního síťového připojení

- V nabídce položek označte „Protokol IP verze 4 (TCP/IPv4)“ a klikněte na tlačítko Vlastnosti.



Obr. 16.: Přístup do nastavení protokolu IPv4

- Označte položku „Použít následující adresy serverů DNS“ a do nově zpřístupněných kolonek vyplňte sekundární a primární adresu DNS serveru, který jste zvolili. Tyto adresy jsou uvedeny na webových stránkách jednotlivých DNS serverů.



Obr. 17.: Zadání adres zvoleného DNS serveru

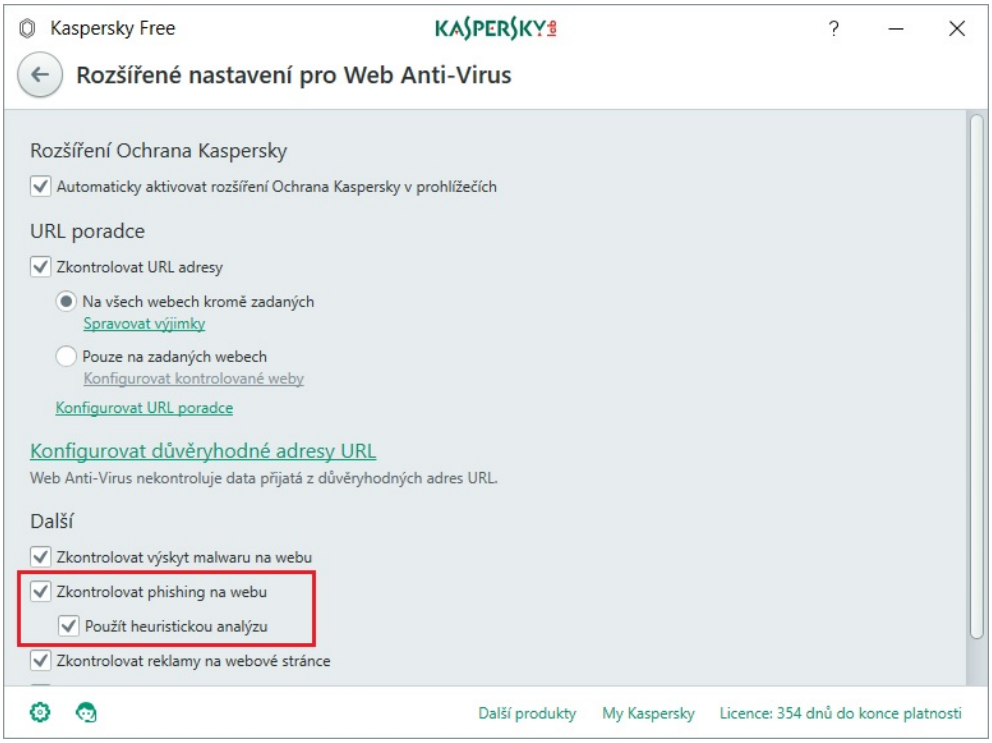
6.2.5. Blokování phishingu prostřednictvím softwaru

○ Antivirový software

Většina dostupných antivirových řešení v sobě má zakomponovaný kromě standardní výbavy také antiphishingový štít.

Tyto štíty většinou fungují na principu databází phishingových webů. Pokud uživatel chráněný touto komponentou navštíví podvodný web, který je v databázi, antivirus mu k němu zablokuje přístup.

Dle posledního měření organizace AV-Comparatives, které proběhlo v červenci roku 2017, měly největší úspěch v blokování phishingu antivirová řešení značek Kaspersky, Avast, Bitdefender a Fortinet.[13]



Obr. 18.: Antiphishingová komponenta antiviru Kaspersky Free

■ Doplněk webového prohlížeče

• Blokátor reklamy

Blokátory reklamy jsou používány stále větším spektrem uživatelů. Na vině je tomu především reklama, která je poslední dobou mnohdy agresivní a obtěžující.

Tato rozšíření prohlížeče fungují stejně tak, jako například antiphishingové komponenty antivirů, tedy na principu databáze. Ty jsou však v tomto případě tvořeny uživatelskou komunitou, která je složena z mnohem více lidí, než-li je tomu například v případě antivirových společností.

Při instalaci blokátoru je uživateli umožněno si vybrat z rozsáhlého množství tzv. filtrů, které blokují pro ně specifické objekty. Některé z filtrů cílí pouze na reklamy, jiné na sledování třetími stranami a jiné například bezpečnost. Samostatné phishingové filtry nejsou dostupné, avšak mnoho phishingových webů je zařazeno v antimalwarových filtrech, které obecně blokují stránky s nebezpečným obsahem.

Pokud je antimalwarový filtr aktivován a uživatel vstoupí na nebezpečnou stránku, která je zahrnuta v databázi, nebude na ni vpuštěn.

Mezi nejpoužívanější blokátory reklamy patří především AdBlock Plus německé firmy Eyeo GmbH., dále pak také uBlock Origin, nebo původní AdBlock.

- **Netcraft Extension**

  Společnost Netcraft Ltd. je autorem stejnojmenného doplňku prohlížeče, jehož primární funkcí je detekce a blokace phishingu. Stejně, jako předchozí metody funguje Netcraft Extension na principu databáze. Ta je tvořena taktéž dobrovolníky, avšak jejich zaměření se týká pouze phishingu.

  Dle nezávislých testů Carnegie-Mellonovy univerzity z roku 2006 byl v té době doplněk Netcraft Extension schopen zablokovat přes 75 % phishingových webů.[14]

  Aktuální statistiky nejsou k dispozici, dá se však předpokládat, že se s masivním nárůstem phishingových útoků účinnost doplňku snížila.

7. ZÁVĚR

Jak výsledky dotazníku ukázaly, lidé, ačkoliv většinou nevědí, že se jedná o sociální inženýrství, jsou proti těmto praktikám poměrně imunní. Což je dobrá zpráva. Jak však říkám jsou to pouze výsledky dotazníku, u kterého není prokazatelné, zda-li jsou pravdivé. O možnosti nepravdivosti odpovědí některých respondentů mě přesvědčuje i fakt, že praktické testování, alespoň co se schopnosti rozpoznat podvodné jednání týče, dopadlo naprosto katastrofálně. Otázka, zda-li tedy lidé sociální inženýrství znají, nebo jeho znalost pouze předstírají, či vůbec neví, oč jde, zůstává i nadále nezodpovězena.

Pro případ, že by jej však neznali tu byla teoretická část, která poměrně detailně popsala různé mechanismy a situace, v nichž se podvodné metody používají. Dále byli lidé seznámeni s možnostmi, jak se proti těmto praktikám bránit. A to jak v realitě, tak i v kyberprostoru.

Ačkoliv jsem v to v prvních chvílích nedoufal, stalo se z této práce poměrně komplexní shrnutí problematiky sociálního inženýrství. Není tedy nutné zdlouhavě hledat všechny možné informace prostřednictvím internetu, či jiných médií. S nadsázkou se tato práce dá označit jako průvodce světem sociálního inženýrství, který své čtenáře naučí tímto světem bez úhony proplouvat.

Kromě podkladu pro tvorbu komplexní příručky čitelné laickou veřejností se dá tato práce využít i mnohými jinými způsoby. Jak již bylo dříve zmíněno, na základě našich pokusů v reálných podmínkách došlo k improvizaci zabezpečení nejmenovaného ústavu Mendelovy univerzity, a to zejména ve směru ochrany osobních údajů. Tato odborná práce má potenciál ukázat různým institucím a organizacím, že i na renomovaném pracovišti si může sociální inženýr přijít na své. V kombinaci s informacemi, které se týkají obrany proti podvodným metodám se dá tato práce považovat za manuál ke zlepšení zabezpečení na pracovištích.

Samotné výsledky dotazníku a testování v reálných podmínkách by mohly zapříčinit zájem různých institucí, které by mohly na základě mnou zjištěných informací pořádat například kurzy, v nichž by byla divákům tato problematika podrobně vysvětlena.

Doufám, že si z této práce všichni její čtenáře něco odnesli, a také doufám, že lidí, kteří naletí na techniky sociálního inženýrství bude do budoucna ubývat.

SEZNAM POUŽITÉ LITERATURY

1. Social engineering (security). In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2017-12-21]. Dostupné z: https://en.wikipedia.org/wiki/Social_engineering_(security)
2. Pretexting. *Security Through Education* [online]. [cit. 2017-12-21]. Dostupné z: https://www.social-engineer.org/framework/influencing-others/pretexting/
3. Pretexting. In: ManagementMania.com [online]. Wilmington (DE) 2011-2017, 26.10.2016 [cit. 21.12.2017]. Dostupné z: https://managementmania.com/cs/pretexting
4. Social Engineering: What is baiting? *Mailfence Blog* [online]. 2017 [cit. 2017-12-21]. Dostupné z: https://blog.mailfence.com/what-is-baiting-in-social-engineering/
5. TIP#551: Co je to clickbait, clickbaiting? *365 tipů* [online]. ČR, 2017 [cit. 2017-12-21]. Dostupné z: https://365tipu.cz/2016/07/04/tip551-co-je-to-clickbait-clickbaiting/
6. 5 Social Engineering Attacks to Watch Out For. Tripwire [online]. 2017 [cit. 2017-12-21]. Dostupné z: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
7. Definition of the Day: Quid Pro Quo Attack. Bank Vault [online]. 2017 [cit. 2017-12-21]. Dostupné z: https://www.bankvaultonline.com/knowledge-base/definition-of-the-day/definition-quid-pro-quo-attack/
8. Phishing. Bezpečný internet [online]. ČR, 2017 [cit. 2017-12-21]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx
9. RAMZAN, Zulfikar. Phishing and Cross-Site Scripting. SYMANTEC CORPORATION. Symantec Connect [online]. ČR, 2017 [cit. 2017-12-21]. Dostupné z: https://www.symantec.com/connect/blogs/phishing-and-cross-site-scripting
10. DHANRAJ, Morgan a Luis ROJO. Web browser security comparative report - Protection Against Phishing [online]. NSS Labs, 2017 [cit. 2017-11-21]. Dostupné z: https://download.microsoft.com/download/E/8/5/E856C533-1B87-4EAC-8EA5-449ED7F7C23E/NSS%20Labs_Web%20Browser%20Security_Phishing_Comparative%20Report.pdf
11. Operating System Market Share. NetMarketShare [online]. 2017 [cit. 2017-12-21]. Dostupné z: https://www.netmarketshare.com/operating-system-market-share.aspx
12. Jak funguje DNSSEC. CZ.NIC [online]. ČR, 2017 [cit. 2017-12-21]. Dostupné z: https://www.dnssec.cz/page/444/jak-funguje-dnssec/
13. Anti-Phishing Certification 2017. *AV-Comparatives* [online]. 2017 [cit. 2017-12-21]. Dostupné z: https://www.av-comparatives.org/anti-phishing-certification-2017/
14. CRANNON, Lorrie, Serge EGELMAN, Jason HONG a Yue ZHANG. Phinding Phish: An Evaluation of Anti-Phishing Toolbars. CARNEGIE MELLON UNIVERSITY.

Cylab.cmu.edu [online]. USA, 2006 [cit. 2017-12-21]. Dostupné z: http://www.cylab.cmu.edu/files/pdfs/tech_reports/cmucylab06018.pdf

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ