

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



Účinky metod sociálneho inžinierstva na rôzne cieľové skupiny

BAKALÁŘSKÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Autor: Lukáš Blaško

Vedoucí bakalářské práce: Mgr. Ing. Tomáš Sigmund, Ph.D.

Praha, květen 2019

Prohlášení

Prohlašuji, že jsem bakalářskou práci „Účinky metod sociálního inženýrstva na různé cílové skupiny” vypracoval samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 30. dubna 2019

.....

Lukáš Blaško

Pod'akovanie

Na tomto mieste by som chcel poďakovať vedúcemu mojej bakalárskej práce Mgr. Ing. Tomášovi Sigmundovi, Ph.D. za odborné vedenie a pomoc počas tvorby práce. Taktiež by som rád poďakoval mojim rodičom a priateľke za pevné nervy a mentálnu podporu v ťažkých chvíľach počas môjho štúdia.

Abstrakt

Informačná bezpečnosť a ochrana osobných údajov sa v dnešnej dobe radia k hlavným témam informačnej spoločnosti. So zabezpečením čo najmenej rizikového správania jednotlivca v súčasnej dobe je úzko spätý pojem sociálne inžinierstvo a sociotechnika.

Cieľom bakalárskej práce je analyzovať rozhodovací proces jednotlivca – zistiť, podľa čoho sa rozhoduje a čo ovplyvňuje jeho rozhodovanie. V teoretickej časti je definovaný pojem sociálne inžinierstvo, jeho metódy, postupy, vlastnosti subjektov, ktoré sociálne inžinierstvo využíva. V praktickej časti je na analyzovanie dôležitosti faktorov rozhodovania použitý dotazníkový prieskum, ktorý sa týka náchylnosti voči sociálnemu inžinierstvu. Na otázky dotazníka odpovedalo platne 203 respondentov, ktorí boli pre účely analýzy výsledkov rozdelení podľa rôznych kritérií do ôsmich rôznych delení.

Výsledky dotazníkového prieskumu sú prezentované formou overenia správnosti vopred stanovených piatich hypotéz, ktoré predpokladajú isté stereotypmi dané správanie skupín jedincov. Záverom bakalárskej práce je určenie miery rizikovosti správania jednotlivých skupín pri rôznych sociotechnických útokoch, resp. miera účinnosti rôznych metód sociálneho inžinierstva na rôzne skupiny jedincov.

S metódami a postupmi sociálneho inžinierstva by sa malo oboznámiť čo najviac osôb, ktorým záleží na bezpečnosti a minimalizácii rizika úniku osobných informácií v súčasnej modernej informačnej spoločnosti.

Kľúčové slová

Sociálne inžinierstvo, sociotechnika, útok, informačná bezpečnosť, manipulácia, ovplyvňovanie.

JEL klasifikácia

Z13

Abstrakt

Informační bezpečnost a ochrana osobních údajů se v dnešní době řadí k hlavním tématům informační společnosti. Se zajištěním co nejméně rizikového chování jednotlivce v současné době je úzce spjat pojem sociální inženýrství a sociotechnika.

Cílem diplomové práce je vytvořit analýzu procesu rozhodování jednotlivce - podle čeho se rozhoduje a co ovlivňuje jeho rozhodování. V teoretické části je definován pojem sociální inženýrství, jeho metody, postupy, vlastnosti subjektů, které sociální inženýrství využívá. V praktické části je k analýze rozhodovacího procesu použito dotazníkové šetření, který se týká náchylnosti vůči sociálnímu inženýrství. Na otázky dotazníku odpovědělo platně 203 respondentů, kteří byli pro účely analýzy výsledků rozděleni podle různých kritérií do osmi různých dělení.

Výsledky dotazníkového průzkumu jsou prezentovány formou ověření správnosti pěti předem stanovených hypotéz, které předpokládají určité stereotypy dané chování skupin jedinců. Závěrem diplomové práce je určení míry rizikovosti chování jednotlivých skupin při různých sociotechnických útocích resp. míra účinnosti různých metod sociálního inženýrství na různé skupiny jedinců.

S metodami a postupy sociálního inženýrství by se mělo seznámit co nejvíce osob, kterým záleží na bezpečnosti a minimalizaci rizika úniku osobních informací v současné moderní informační společnosti.

Klíčová slova

Sociální inženýrství, sociotechnika, útok, informační bezpečnost, manipulace, ovlivňování.

JEL klasifikace

Z13

Abstract

Information security and personal data protection belong to one of the main topics of the information society nowadays. To ensure the least risk behavior of the individual today the concept of social engineering and sociotechnics is closely related.

The aim of the bachelor thesis is to create an analysis of the decision-making process of an individual - according to what he decides/is he deciding and what influences the process of his decision making. The theoretical part defines the concept of social engineering, its methods, tools, and properties of subjects that the social engineering uses. In the practical part, a questionnaire survey to analyze the decision-making process is used, which focuses on susceptibility to social engineering. The survey's questions were answered validly by 203 respondents who were then divided into eight different divisions according to various criteria for the purpose of analyzing the distribution of the results.

The results of the questionnaire survey are presented in the form of confirmation of the rightfulness of five pre-determined hypotheses, which assume certain stereotypically given behavior of groups of individuals. The conclusion of the bachelor thesis is to determine the level of risk behavior of individual groups in various sociotechnical attacks and/or of effectiveness of different social engineering methods for different groups of individuals respectively.

Social engineering methods and procedures should be introduced to the maximum number of people who care about the safety and minimalization of the risk of leakage of personal information in today's modern information society.

Keywords

Social engineering, sociotechnics, attack, information security, manipulation, influencing.

JEL classification

Z13

Obsah

Úvod	8
1 Sociálne inžinierstvo	9
2 Metódy útokov používané v sociálnom inžinierstve	11
2.1 Ako útočník získava informácie	11
2.2 Nástroje podporujúce úspech útoku prostredníctvom osobného kontaktu	11
2.3 Sociotechnické metódy pomocou internetu alebo telefónneho rozhovoru	13
3 Rozhodovanie jedinca	15
3.1 Dvojprocesné modely rozhodovania	15
3.2 Teória sociálnej zmeny	16
3.3 Atribučná teória	16
4 Vlastnosti ľudí, ktoré využíva útočník	18
4.1 Spoločné vlastnosti populácie	18
4.2 Vlastnosti skupín	18
4.3 Postoje jednotlivca	18
5 Faktory ovplyvňujúce rozhodnutie jedinca	20
5.1 Heuristiky	20
5.2 Emócie	25
6 Skupiny respondentov	27
7 Dotazník	28
8 Hypotézy	35
9 Vyhodnotenie dotazníka	36
Záver	43
Použitá literatúra	45
Príloha	Error! Bookmark not defined.
Dotazník – úplné znenie	Error! Bookmark not defined.

Úvod

Informačná bezpečnosť a ochrana osobných údajov sa v dnešnej dobe radia k hlavným témam informačnej spoločnosti. So zabezpečením čo najmenej rizikového správania jednotlivca v súčasnej dobe je úzko spätý pojem sociálne inžinierstvo a sociotechnika. Je dôležité uvedomiť si, že nejde len o bezpečné využívanie informačno-komunikačných technológií, ale aj o bezpečné správanie sa v každodenných životných situáciách, pri ktorých číha na obeť nebezpečenstvo úniku osobných informácií, prípadne manipulácie správania jednotlivca zo strany útočníka.

Cieľom mojej bakalárskej práce je vytvoriť analýzu rozhodovacieho procesu jednotlivca – podľa čoho sa rozhoduje a čo ovplyvňuje jeho rozhodovanie. V úvodnej – teoretickej časti definujem pojem sociálne inžinierstvo, jeho metódy, postupy, vlastnosti subjektov, ktoré sociálne inžinierstvo využíva. Teoretická časť je členená do piatich kapitol – Sociálne inžinierstvo, Metódy útokov používané v sociálnom inžinierstve, Rozhodovanie jedinca, Vlastnosti ľudí, ktoré využíva útočník a Čo ovplyvňuje rozhodnutie jedinca.

V praktickej časti, rozdelenej do štyroch kapitol, na analyzovanie rozhodovacieho procesu využívam dotazníkový prieskum, ktorý sa týka náchylnosti voči sociálnemu inžinierstvu.

Otázky dotazníka určeného pre prieskum uvádzajú respondenta do rôznych situácií v ktorých je vystavený pôsobeniu rôznych metód sociálneho inžinierstva. Dotazník zadávam vzorke minimálne 200 ľudí, pričom sa zameriavam na rôzne vekové a sociálne skupiny. Dotazník zadávam prostredníctvom formulára Google Docs a v printovej forme (pre seniorské vekové kategórie). Respondentov som rozdelil do skupín z hľadiska rozličných kritérií, aby som mohol vyhodnotiť rizikovosť jednotlivých metód sociálneho inžinierstva v rôznych kategóriách respondentov. Stanovil som si 5 hypotéz, ktorých pravdivosť som overil analýzou odpovedí na dotazníkový prieskum. Odpovede na príslušné otázky som spracoval aj v grafickej forme kvôli lepšej prehľadnosti.

Podľa môjho názoru je analýza účinnosti metód sociálneho inžinierstva dôležitá pre osoby vystavené pôsobeniu útoku sociálneho inžinierstva. Výsledky prieskumu, ktorý je súčasťou mojej bakalárskej práce čiastočne moje hypotézy potvrdili a čiastočne vyvrátili ich pravdivosť. Výsledky podobného prieskumu by mohli byť užitočné tak pre útočníka – overí si, aká metóda najviac pôsobí na akú kategóriu jednotlivcov, ako aj pre potenciálnu obeť – uvedomí si, v akých situáciách si má dávať lepšiu pozor a aké jeho správanie je z hľadiska sociotechnického útoku rizikové.

1 Sociálne inžinierstvo

Sociálne inžinierstvo nazývané aj human hacking sa v kontexte informačnej bezpečnosti, týka psychologickéj manipulácie ľudí s vykonávaním činností alebo sprístupňovaním dôverných informácií. Typ dôveryhodného triku na účely zhromažďovania informácií, podvodov alebo prístupu k systému, je často jedným z mnohých krokov v komplexnejšom systéme podvodov (Anderson, 2008).

Taktiež môže byť sociálne inžinierstvo definované „ako akýkoľvek čin, ktorý ovplyvňuje osobu, aby prijala akciu, ktorá môže alebo nemusí byť v ich najlepšom záujme“.

Metóda, ktorá je využívaná v sociálnom inžinierstve sa nazýva sociotechnika.

Sociotechnika sa zameriava na človeka, pretože človek predstavuje nedeliteľnú časť väčšiny systémov spoločností. Sociotechnik od neho získava citlivé údaje prostredníctvom technológií, ale taktiež pomocou osobného kontaktu. A teda aj napriek tomu, že firmy investujú nemalé peniaze do bezpečnosti systému, sociotechnika využíva ľudskú myseľ, ktorá sa dá v mnoho prípadoch oklamať tak, že obeť ani nemusí vedieť, že sa stal cieľom útoku.

Sociotechnikovi ide väčšinou o získanie mena a hesla k bankovému účtu, marketingové plány firiem, výpisy z účtovníctva, ale aj o citlivé osobné údaje.

Najväčšiu skupinu tvoria hackeri, ktorí získavajú informácie prostredníctvom technológií a to predovšetkým nelegálnou cestou. Po získaní chcú tieto informácie zneužiť vo svoj prospech.

Ďalšou skupinou sú penetrační tester. Na rozdiel od hackerov, všetky informácie získavajú legálne a nesnažia sa ich zneužiť. Sú najatí firmami na skontrolovanie ich softvérového zabezpečenia a prípadne jeho zlepšenia alebo opravy, proti reálnym útokom tretej strany. Okrem toho sa snažia odhaliť nelegálnych zamestnancov, alebo zamestnancov, ktorí nedodržiavajú firemnú stratégiu.

Neposlednou skupinou sú napríklad marketingový pracovník, ktorí sa snažia pomocou reklám presvedčiť ľudí, aby si kúpili práve ich výrobok napriek tomu, že ho ľudia vôbec nepotrebujú, ba dokonca im v niektorých prípadoch môže škodiť (napríklad fast food), ale aj politické strany, ktoré vplývajú na ľudí aby volili práve ich.

V minulých rokoch sa stávali útoky viac bežné a bolo potrebné si na nich dať väčší pozor. V roku 2017 sa priemerné náklady veľkých firiem na kyber ochranu vyšplhali na 11.7 miliónov \$, čo je o 22.7% viac ako v roku 2016. Zároveň sa zvýšilo aj priemerné číslo prelomenia bezpečnosti na 130, čo je nárast o 27.4%.

Pre potrebu identifikácie sociálneho útoku, je potrebné, si definovať jednotlivé typy útokov. Útoky sa dajú rozdeliť na dve skupiny (Vyskoč, 2004):

1) Autonómne – útoky realizované kompletne v rámci výpočetnej a komunikačnej štruktúry. Nevyžadujú žiadny zásah zo strany užívateľa (pr. SQL injection).

Kognitívne- vyžaduje určitú zmenu chovania užívateľa, vyvolanú manipuláciou jeho vnímania. Užívateľova činnosť alebo nečinnosť je v útoku kľúčová (pr. Zaslanie infikovaného emailu, ktorý musí užívateľ otvoriť).

2) Fyzické – klasický útok na fyzické komponenty (pr. Krádež harddiskov).

Syntaktické – snaha o vyradenie syntaktickej logiky siete alebo systému a jej následné zneschopnenie (pr. DDOS).

Sémantické – produkovanie či podsúvanie nepravdivých alebo zavádzajúcich informácií užívateľovi tak, aby podľa nich jednal určitým spôsobom.

Sociotechnikovi k získaniu údajov netreba žiadne zložité informačné technológie. Od obete môže získať informácie napríklad pomocou sociálnych sietí, telefónneho hovoru alebo pomocou osobného kontaktu. Preto by mal byť sociotechnik autoritatívny, presvedčivý a mal by dobre vedieť komunikovať s ľuďmi. Okrem spomínaných schopností by mal dokonale ovládať psychológiu človeka a mal by byť schopný nájsť rôzne informácie, ktoré cieľová osoba často nevedome vypustila na internet, ale aj informácie, ktoré sú chránené.

2 Metódy útokov používané v sociálnom inžinierstve

2.1 Ako útočník získava informácie

Sociálne siete

Mnoho ľudí si neuvedomuje, čo všetko má vo svojom profile na sociálnej sieti verejne dostupné. Sociotechnik si tak ľahko môže zistiť telefónne číslo, e-mailovú adresu, ale aj to kde obeť študuje alebo pracuje, a kde sa práve nachádza. Okrem toho si vie zistiť aj jej záujmy a koníčky a to využiť pri nadväzovaní kontaktu.

Dumpster diving

Dumpster diving je hľadanie informácií v odpade rôznych firiem. Nemusí sa jednať iba o hľadanie prístupového mena a hesla do firemnej siete. Mnoho firiem vyhadzuje lekárske záznamy, fotky, e-maily, výpisy z účtovníctva a ďalšie dôležité veci, ktoré sociotechnik môže využiť vo svoj prospech. Veľa firiem má z toho dôvodu zamknuté kontajnery vo vnútri areálu, alebo všetky tieto záznamy skartuje.

Piggybacking

Piggybacking je efektívny spôsob ako sa sociotechnik môže dostať do stráženej budovy tým, že využíva dobrosrdečnosť a nepozornosť ľudí. Môže sa jednať napríklad o využitie situácie keď útočník predstiera, že hľadá svoju identifikačnú kartu a zamestnanec mu preto ochotne otvorí dvere.

Shoulder surfing

Shoulder surfing alebo pozeranie cez rameno je jednoduchý spôsob, pri ktorom útočník využíva nepozornosť obete na získanie informácií. Môže sa jednať o užívateľské meno a heslo, heslo prístupu do mobilu alebo PIN kód platobnej karty. Shoulder surfing nemusí znamenať zásah do firmy alebo domu obete. Môže to byť vykonané všade kde človek otvorí počítač, napríklad v kaviarni, autobuse alebo v bare.

2.2 Nástroje podporujúce úspech útoku prostredníctvom osobného kontaktu

Pretexting

Pretexting je vytváranie a využívanie vymysleného scenára s cieľom presvedčiť obeť k vykonaniu potrebnej akcie alebo k získaniu potrebnej informácie. Jedná sa o skĺbenie

klamstva s kúskom pravdivej informácie získanej skôr. Pretexter môže využiť napríklad emócie a empatiu, autoritu a strach aby od obete získal napríklad dátum narodenia, rodné meno matky, meno nadriadeného, číslo účtu a podobne.

Tieto údaje ho zaujímajú hlavne preto, lebo veľké množstvo firiem stále overuje totožnosť klienta práve podľa rodného čísla, rodného mena matky či iných, relatívne ľahko dostupných informácií.

Taktiež si pretexter musí naštudovať obor v ktorom bude vystupovať (pr. Keď chce vystupovať ako právnik obchodnej firmy, musí si naštudovať obchodné právo), ale tak isto sa musí pripraviť na všetky možné scenáre reakcie obete, ktorá ho nesmie odhaliť.

Quid pro quo

Quid pro quo, alebo inak nazývané “niečo za niečo” je jedna z najčastejšie používaných metód v sociálnom inžinierstve. V obeti chce sociotechnik vyvolať pocit dôvery, napríklad podržaním dverí a následným “nevinným” rozhovorom v ktorom prezradí nejakú dôvernú informáciu, ktorú si pripravil vo fázy pretextingu a teda nemusí byť vôbec pravdivá a očakáva, že obeť mu na oplátku prezradí podobnú dôvernú informáciu.

Na úrovni telefónneho kontaktu s obeťou môže byť quid pro quo využité napríklad tak, že sociálny inžinier volá na všetky čísla danej spoločnosti, ktoré našiel a predstavuje sa ako IT technik. Skúša nahovoriť zamestnancom, že majú problém s PC a sľubuje im rýchlu opravu za výmenu vypnutia svojho antivírusového systému a následného nainštalovania škodlivého malwaru.

Reč tela

Zahrňa všetky neverbálne prejavy komunikácie. Ide o mimiku a gestá. Na rozdiel od reči prebieha na inej báze. Podáva informácie o emóciách, pocitoch a vyjadruje čo si osoba myslí. Napodobenie reči tela inej osoby, môže tieto osoby zbližovať. Sociotechnik využíva reč tela na doplnenie pretextu, aby sa v danej situácii zatajil klamstvo, pôsobil uveriteľne a získal sympatie obetí.

Súčasťou reči tela sú aj mikrovýrazy v tvári, ktoré sa nevedome objavujú na 1/25 sekundy. Pre sociálneho inžiniera je dôležité sa naučiť tieto výrazy postrehnúť a čítať. Sú to hnev, pohrdavosť, znechutenie, strach, šťastie, smútok, prekvapenie.

Sympatie

Väčšina ľudí viac verí človeku čo je mu sympatický ako človeku, ktorý mu je nesympatický. Sociotechnik sa preto snaží o dokonalé zosynchronizovanie svojej reči tela, chovania, prejavu a vzhľadu, aby si získal čo najväčšie sympatie svojej obete.

2.3 Sociotechnické metódy pomocou internetu alebo telefónneho rozhovoru

Phishing

Phishing považuje za najnebezpečnejšiu metódu, ktorá sa v sociálnom inžinierstve používa. Je to podvodná technika používaná na internete k získavaniu citlivých údajov v elektronickej komunikácii. K nalákaniu dôverčivej verejnosti komunikácia predstiera, že z populárnych sociálnych sietí, online platobných portálov, úradov štátnej správy alebo od IT administrátorov.

Princípom phishingu je typické rozosielanie e-mailových správ, ktoré často vyzývajú adresáta k zadaniu osobných údajov na falošnú stránku, ktorej podoba je skoro identická s tou oficiálnou. Útočníkovi stačí skopírovať html kód a vložiť ho na vlastnú stránku, ktorej názov sa od originálu líši iba jedným písmenom napríklad steamcommunity.com a steamcomunity.com

Phishing sa stal hlavným prenosným médiom pre ransomware, ktorý zašifruje disky a neumožní prístup k dátam, kým užívateľ nezaplatí určitú čiastku.

Spear phishing

Namiesto posielania tisícov e-mailov náhodným ľuďom dúfajúc, že sa nájde pár ľudí, ktorí sa nechajú nachytať sa spear phishing sústreďuje na skupinu ľudí, ktorí majú niečo, čo útočník chce. Tieto rozosielané maily sa môžu týkať práce alebo záľub, ktoré obeť uviedla napríklad na sociálnej sieti. Správa môže vyzeráť, že bola odoslaná od známeho alebo kamaráta, a dokonca aj so správnou adresou odosielať.

Clone phishing

Útočník zistí, aký mail bol obeť doručený a odošle jej mail s rovnakým obsahom z rovnako vyzerajúcej adresy, ale so3 zmenením odkazom. Navyiac sa v ňom môže tvrdiť, že sa jedná o re-send alebo o aktualizovanú verziu originálu.

Whaling

Podobne ako spear phishing, sa whaling sústreďuje na skupinu ľudí s tým rozdielom, že ide o skupinu vyššie postavených ľudí. Napríklad na výkonných riaditeľov, finančných riaditeľov, úspešných podnikateľov, alebo tých ktorí majú prístup ku tajným vládnym informáciám. Keďže sú ciele vysoko postavené, je dôležité aby útočník urobil podrobnejší výskum a lepšie sa pripravil. Útočníci zvyknú odosielať maily s veľmi citlivou témou dúfajúc, že obeť na odkaz klikne.

Telefónny phishing

Táto technika využíva falošný hlasový automat s podobnou štruktúrou ako má originálny bankový automat (pr. "Pre zmenu hesla stlačte 1"...). Obeť je väčšinou e-mailom k zavolaniu

do banky za účelom overenia informácie. Tu je následne požadované prihlásenie pomocou PINu alebo hesla. Automat následne prenesú obeť do kontaktu s útočníkom vystupujúcim v roli bankového poradcu, čo mu umožňuje kladeniu ďalších otázok.

Vishing

Jedná sa o zistenie citlivých dát pomocou telefónneho hovoru. Útočník si musí zistiť meno, telefónne číslo a banku obete a následne je pre útočníka ľahšie presvedčiť obeť o tom, že v banke pracuje. Falošný bankový pracovník obeti oznámi, že má problém s účtom a tak mu obeť po stresom dobrovoľne vydá všetky osobné údaje.

SMiShing

SMiShing funguje podobne ako phishing s tým rozdielom, že je obeti miesto e-mailu poslaná sms ktorej obsah navádza obeť kliknúť na priložený odkaz.

Baiting

Baiting môže byť považovaný za trójskeho koňa v reálnom svete. Pri tomto spôsobe útoku útočník nechá infikované USB na mieste, kde ho obeť s veľkou pravdepodobnosťou nájde, napríklad v kaviarni, vo výťahu, na parkovisku. Potom nechá zapracovať zvedavosť, s ktorou obeť vloží toto USB do svojho počítača. Tým dôjde k inštalácii vírusu, za pomoci ktorého získa útočník prístup k počítaču alebo celej počítačovej sieti.

Pharming

Jedná sa o napadnutie DNS serveru k prepísaniu IP adresy, vďaka čomu bude obeť pri vyhľadávaní určitej stránky navedená na stránku vytvorenú útočníkom, za účelom poškodenia obeti. Pharming vyžaduje nechránený prístup k zacieleniu na počítač, ako napríklad počítač domáceho používateľa.

3 Rozhodovanie jedinca

Predmetom tejto kapitoly mojej práce bude popis procesu ovplyvnenia obete z pohľadu sociálnej psychológie. V sociotechnickom útoku sa útočník snaží predovšetkým ovplyvniť a presvedčiť obeť o určitej skutočnosti a získať tak pre seba potrebné informácie. Presvedčenie je tu definované ako „utváranie alebo zmena postojov, často v reakcii na argumenty alebo ďalšie informácie (Hewstone & Stroebe, 2006).

3.1 Dvojprocesné modely rozhodovania

V sociálnej psychológii je ovplyvňovanie skúmané predovšetkým cez tzv. dvojprocesné modely rozhodovania (DMR) (Hewstone & Stroebe, 2006). Ide sa o dva veľmi podobné modely - model pravdepodobnosti rozpracovania a heuristicko-systematický model – ktoré skúmajú proces presvedčovania podľa úrovne rozpracovania, ktoré predstavuje mieru spracovania argumentov obsiahnutých vo vyjadrení.

Prvý spôsob spracovania informácií, ktorý označujeme ako primárny (systematický/centrálny podľa DMR) predstavuje pozorné a vyčerpávajúce preskúmanie argumentov oznamu a analytický spôsob získavania všetkých informácií, ktoré sú využité pri rozhodovaní (Hewstone & Stroebe, 2006). V tomto prípade poslucháč pozorne vníma a analyzuje obsah oznamov. Ide sa o zložitejší spôsob presvedčovania, ktorý nutne vyžaduje kvalitné argumenty a fakty na presvedčenie. Pre jeho použitie však poslucháč potrebuje množstvo energie. Podľa rozdelenia D. Kahnemana sa dá systematický spôsob spracovania informácií zahrnúť pod Systém 2, ktorý zaisťuje vedomú, duševnú činnosť (Kahneman, 2011).

Druhý, sekundárny (heuristický/periférny) spôsob spracovania zahŕňa vyhodnotenie podľa nie príliš namáhavých a zjednodušujúcich mechanizmov ako je podmieňovanie a heuristik (Hewstone & Stroebe, 2006). Spracovanie informácií pomocou heuristik predstavuje využitie jednoduchých pravidiel rozhodovania. Tento spôsob podľa Kahnemana zasa predstavuje Systém 1, automatické rozhodovanie, ktoré si nevyžaduje väčšie úsilie alebo vedomú kontrolu.

Aby človek použil pri spracovaní informácií primárny spôsob – a teda podstatne presnejšiu metódu, potrebuje mať nasledujúce (Hewstone & Stroebe, 2006):

Motiváciu – záujem o pochopenie a vyhodnotenie správy

Energiu – potrebnú na vyhodnotenie informácií

Schopnosť pochopenia – byť schopný interpretovať a porozumieť informáciám

Osobnú angažovanosť a zodpovednosť – ako veľmi sa rozhodovanie týka danej osoby

Ak by tieto podmienky neboli splnené (napr. v prípade, že je poslucháč rozrušený, téme nerozumie alebo sa o výsledok správy nebude zaujímať) zvýši sa riziko, že pri rozhodovaní dôjde k použitiu sekundárneho spracovania.

Väčšinou je cieľom útočníka dosiahnuť u obete sekundárne spracovanie. V podmienkach sekundárneho spracovania sa obeť nebude veľmi zaoberať detailmi a faktickými informáciami o situácii, ale skôr okamžitými pocitmi a heuristikami, ktoré môže útočník lepšie ovplyvniť. Heuristiky predstavujú jednoduché mentálne skratky a pravidlá (napr. väčšina alebo odborník majú vždy pravdu), podľa ktorých sa ľudia rozhodujú. Heuristiky vedú k predvídateľným chybám (Tversky & Kahneman, 1974). Práve vďaka ich systematickosti a predvídateľnosti sú sociotechnici schopní využiť heuristiky na dosiahnutie svojich cieľov.

Jedným z príkladov ovplyvnenia rozpracovania obete je zámerné rušenie správy – nejasné vyjadrovanie alebo striedanie komunikačných kanálov. Dôležitú rolu v nielen zrozumiteľnosti správy, ale taktiež v emóciách aké vyvoláva hrá spôsob výberu slov (viz. farming). Útočník môže docieľiť sekundárne rozpracovanie aj ovplyvnením ďalších faktorov, ktoré hrajú rolu v úrovni rozpracovania, napríklad pomocou emócií.

Ak ale bude samotná správa útočníka obsahovo nezmyselná alebo v rozpore s faktami (nepresvedčivá), ani tieto vplyvy nutne nemusia viesť k úspechu útočníka.

K presvedčeniu obete môže samozrejme dôjsť aj prostredníctvom primárneho spracovania – v takom prípade musí mať útočník dostatok informácií k presvedčeniu (napr. musí sa preukázať takými informáciami, akými by sa preukázal skutočný pracovník).

3.2 Teória sociálnej zmeny

Ďalšia teória, pomocou ktorej môžeme interakciu útočníka s obeťou skúmať, je teória sociálnej zmeny (Hayesová, 1993). Tá považuje sociálnu interakciu za výsledok sociálnej zmeny, kde sa obeť snaží maximalizovať „zisk“ (sociálne prijatie, pochvalu, dar atď.) a minimalizovať „straty“ (odmietnutie, trest atď.)

Existuje mnoho situácií, ktoré človeka ovplyvňujú negatívne (kognitívna disonancia, odpor voči skupine atď.) alebo pozitívne („dobrý pocit“ z poskytnutia sociálnej pomoci atď.). Táto teória poskytuje dodatočné vysvetlenie ľudskej motivácie u takých druhov presvedčovacích metód. Teória sociálnej zmeny nevysvetľuje všetky aspekty sociálnej interakcie, ale v tomto kontexte poskytuje dodatočné vysvetlenie vplyvu techník, ktoré sociotechnik používa.

3.3 Atribučná teória

Ide o teóriu, podľa ktorej človek laickým spôsobom skúma a vysvetľuje svoje vlastné správanie (Hewstone & Stroebe, 2006). Človek vníma svet okolo seba zo svojho vlastného pohľadu na základe svojich skúseností, kedy podnetom prisudzuje význam na základe

svojho rozumu a skúseností. Ľudské rozhodovanie sa tak vo veľkej miere odvíja od vlastných názorov a vnímania sveta.

Podľa tejto teórie je možné vnímať svet z hľadiska príčiny a následku, čo je označované ako normatívny model, ktorý predstavuje rozumné uvažovanie. Na druhej strane nie je možné určiť ako často a za akých okolností k tomuto spôsobu premýšľania dochádza. Ellen Langerová vo svojej kritike uviedla, že veľká časť zdanlivo premysleného správania je vlastne bezmyšlienkovitá. Z tohto základu vychádza teória spontánnej kauzálnej atribúcie. Tá predstavuje automatický proces, keď pri očakávanom výsledku alebo známej činnosti sa ľudia správajú podľa naučených scenárov, bez hlbšej úvahy o kontexte situácie (napr. úvaha „prečo dávam spolupracovníkovi informácie, ktoré v jeho pozícii nepotrebuje“). Tieto rozhodnutia šetria pri známych situáciách mentálnu energiu, ale rovnako ako heuristiky môžu viesť k omylom.

4 Vlastnosti ľudí, ktoré využíva útočník

Napriek tomu, že ľudia sú presvedčení, že ich rozhodovanie je racionálne. Toto rozhodovanie zvykne byť obmedzené možnosťami dosahovania racionality. Ľudské rozhodovanie je často nekonzistentné, neefektívne a založené na irelevantných informáciách (Malhotra & Bazerman, 2008).

V tejto časti svojej práce sa budem venovať jednotlivým vlastnostiam, ktoré ľudia využívajú pri rozhodovaní a ktoré môže útočník zneužiť.

4.1 Spoločné vlastnosti populácie

Spoločné ľudské vlastnosti – dané evolučne alebo spoločensky - zahŕňajú vlastnosti, ktoré má väčšina populácie naučené alebo vrodene (napr. vlastnosti heuristiky, vplyv emócií).

Ďalšími spoločenskými vlastnosťami, ktoré je útočník schopný zneužiť je súcit, empatia a ochota pomôcť. Všetky tieto vlastnosti smerujú k prosociálnemu správaniu. Ide o prirodzené vlastnosti, užitočné pri vytváraní bližších vzťahov, ktoré u človeka hrajú veľmi významnú rolu (McLeod, 2014). Výsledkom je, že ľudia majú prirodzenú tendenciu pomôcť, keď ich o to niekto požiada (Hajnagy, 2011; Mitnick, 2002). Podobne platí, že ľudia majú túžbu byť obľúbení (Hewstone & Stroebe, 2006).

4.2 Vlastnosti skupín

Vlastnosti spoločné pre skupiny sú vlastnosti charakteristické pre určitú spoločenskú skupinu. Môže sa jednať menšiu skupinu (napr. pracovná skupina, spoločenská skupina) alebo o väčšiu skupinu (napr. kultúra, národnosť).

Sociotechnici sa vo väčšine prípadov sústreďujú na pracovnú skupinu, z ktorej môžu získať informácie napríklad o tom, aké má firma kvality a nedostatky alebo čo firma plánuje do budúcnosti. Veľkú rolu v súvislosti so skupinou bude predstavovať taktiež sociálna identita obete, vízia v rámci organizácie, a podobne.

4.3 Postoje jednotlivca

Do tejto skupiny vlastností patria jedinečné vlastnosti každého jedinca a úroveň vplyvu týchto vlastností na správanie človeka. Ide predovšetkým o osobnosť a postoje jednotlivca a od nich sa odvíjajúce emócie a reakcie. Informácie o vlastnostiach jedinca musí útočník získavať osobitne od jednotlivých osôb. Budú teda použité hlavne u cieleného útoku, pričom predchádzajúce dve skupiny vlastností sa väčšinou používajú v rámci širšieho útoku.

Osobnosť jednotlivca môže zahŕňať rôzne úrovne napríklad prosociálneho správania (nakolko je obeť vedená k pomoci), submisivity (keď je obeť ľahko ovládaná autoritou), potreby poznania (motivácia k poznaniu a premýšľaniu o rôznych situáciách) (Hewstone & Stroebe, 2006). Ich odhalenie môže útočníkovi výrazne pomôcť pri vedení útoku a dosiahnutí svojho cieľa.

5 Faktory ovplyvňujúce rozhodnutie jedinca

5.1 Heuristiky

Nakoľko nie je možné, aby bol jedinec dlhodobo naplno sústredený a mal dostatočné množstvo energie na rozhodovanie primárnym spôsobom, rozhodovanie ľudí sa vo veľkej miere odvíja od heuristik – zaužívaných pravidiel, podľa ktorých sa ľudia rozhodujú (napr. odborník vo svojom odbore má väčšinou pravdu, väčšina sa zväčša nemýli). Heuristika predstavuje kompromis medzi racionalitou a úspornosťou. Rozhodovanie sa tak stáva rýchlejšim, automatickejšim, menej vyčerpávajúcim, ale taktiež menej presným a vedie k predvídateľným chybám (Tversky & Kahneman, 1974).

Vplyv

R. Cialdini rozdelil ľudské heuristiky do šiestich princípov (Cialdini R. B., 2012):

1. Reciprocita
2. Konzistencia
3. Sociálny vplyv
4. Sympatie
5. Autorita
6. Nedostatok

Reciprocita

Reciprocita je princíp, kedy sa jeden človek druhému snaží oplatiť záväzok (Trivers, 1971). Toto správanie je u väčšiny ľudí tak samovoľné, že si ho vôbec nemusia uvedomovať. V tomto stave sa jeden človek cíti byť druhému zaviazaný, či už pozitívne (keď sa snaží vrátiť mu láskavosť) alebo negatívne (chce mu oplatiť nepravosť).

Reciprocita sa používa predovšetkým v neziskovom sektore a v predaji – obeť získa darček alebo láskavosť a prirodzene ju to vedie ku kúpe alebo dotácii. Je využiteľná aj v sociotechnickom útoku, kedy si útočník poskytnutím láskavosti môže získať dôveru obeť, ktorá následne vyhovie jeho požiadavkám.

Pravidlo reciprocity riadi aj budovanie kompromisov. Bolo odsledované, že určitá požiadavka má oveľa väčšiu šancu úspechu, ak nasleduje po extrémnej, až neprijateľnej požiadavke (Cialdini, Vincent, Lewis, & Catalan, 1975). Obeť potom vníma túto druhú - menej extrémnu požiadavku ako ústupok útočníka a pristúpi na ňu.

V rámci budovania kompromisov hrá rolu naviac tzv. princíp kontrastného vnímania. Podľa tohto princípu, porovnávaním medzi dvoma stimulmi môže obeť vnímať rozdiely medzi nimi ako väčšie, ako keby posudzovala stimuly zvlášť (Cialdini R. B., 2012). V súlade s tým sa potom druhá – menej extrémna požiadavka javí ako prijateľná a obeť na ňu ľahšie pristúpi.

Konzistencia

Podstatou tohto princípu je snaha človeka, aby sa jeho správanie javilo ako konzistentné s jeho presvedčením. Nestálosť správania sa u ľudí vníma ako negatívny atribút (Allgeier, Byrne, Brooks, & Revnes, 1979). Poväčšine sa spája s nedôveryhodnosťou a nepredvídateľnosťou. Naopak konzistentnosť a stálosť je vysoko cenená. To spôsobuje, že človek sa tohto pravidla drží doslova podvedome.

Ľudia sa identifikujú svojím správaním a tým, ako sa javia svojmu okoliu. Vnútorne presvedčenie a osobné názory sú veľmi silným impulzom pre ďalšie správanie jednotlivca. Ukázalo sa, že najviac ovplyvnení touto heuristikou sú starší ľudia (nad 50 rokov) a osoby individualistických kultúr, ktoré kladú väčší dôraz na vlastné ja a teda je pre nich dobrý dojem veľmi dôležitý (Cialdini R. B., 2012).

Kognitívna disonancia je stav, keď sa kvôli nekonzistentnosti človek cíti nepríjemne a má snahu napätie medzi nekonzistentnými vplyvmi odstrániť – zmeniť názor, presvedčenie. Následne nastáva jav selektívnej expozície, keď človek aktívne zameriava svoju pozornosť na informácie konzistentné s jeho postojmi a vyhýba sa rušivým informáciám (Hewstone & Stroebe, 2006).

Postup eskalácie záväzkov (tzv. technika foot-in-the-door) je tiež vlastne využitím heuristiky konzistencie. Táto technika využíva postupnosť drobných žiadostí útočníka (pre neho bezvýznamných), na ktoré obeť začne odpovedať a konzistenciou správania potom útočník má možnosť získať dôležitejšie a cennejšie informácie.

Spomeňme ešte tzv. „what the hell efekt“, ktorý sa vyznačuje tým, že po prelomení určitej zásady má jedinec väčší predpoklad, že danú zásadu následne poruší opakovane (Selig, 2011). Práve týmto efektom je následne možné vysvetliť názor sociotechnikov, že niektoré kontakty mohli používať opakovane ako zdroj informácií. Ak už obeť raz útočníkovi informácie odhalila, bude náchylná k tomu, aby mu pomáhala aj opakovane.

Sociálny vplyv

Princípom tejto heuristiky je to, že ľudské správanie je silne ovplyvnené okolím. Podľa pravidla sociálneho vplyvu človek rozlišuje, čo je správne na základe toho, čo za správne považujú ostatní ľudia (Lun, Sinclair, Whitchurch, & Glenn, 2007).

Myšlienku, na ktorej je táto heuristika založená by sme mohli sformulovať tak, že „ak súhlasí väčšina, asi to bude pravda“. V tom prípade nedochádza u obete k hlbšej analýze, ale skôr automaticky a bez väčšieho rozmýšľania nasleduje správanie skupiny.

Vplyv skupiny skúmal Solomon Ash pod názvom konformita (Ash, 1955). Jemu sa dokonca podarilo u účastníka prostredníctvom skupiny ovplyvniť vnímanie dĺžky čiar. Okrem toho, že sa účastník podvolil názoru skupiny, bola u neho dokonca pozorovaná „úzkosť“ vyplývajúca z odporu voči skupine. Už samotný uvedený pocit úzkosti ovplyvňuje rozhodovanie. Uvedený experiment výborne ilustruje vplyv skupiny na proces rozhodovania jednotlivca.

Pre sociotechnika nie je nutné, aby pre ovplyvnenie použil skutočnú skupinu (Cialdini R. B., 2012). Jednotlivca ovplyvní už len predstava, že viac účastníkov sa správalo istým spôsobom. Je teda postačujúce, keď útočník obeť stimuluje náznakom toho, že „veľa ľudí mu vyhovel“. Môže spomenúť napríklad nadriadených alebo kolegov obete. V uvedenej situácii nastáva jav, že už len zmienka a následná predstava toho, že ostatní sa správajú určitým spôsobom ovplyvní obeť pri jej rozhodovaní.

Sympatie

V tomto prípade ide o jednoduchú heuristiku – človek má tendenciu skôr vyhovieť tomu, kto je mu sympatický. Aj sociotechnici sú schopní vyvolať sympatie.

Cialdini uvádza nasledujúce faktory na vyvolanie sympatií:

- Vzhľad – do úvahy je potrebné zobrať atraktivnosť. Atraktívnym ľuďom sú zväčša pripisované pozitívne vlastnosti – iba na základe vzhľadu.
- Podobnosť – súčasťou vyvolávania sympatií je na druhom mieste podobnosť útočníka s obeťou, ktorá u obete vyvolá silnejší pocit spolunáležitosti k vzťažnej skupine a teda aj sympatie. Podobnosť môže byť v zmysle vzhľadu, správania, záujmov, názorov atď.
- Komplimenty – ak útočník obeti lichotí a obeť nerozozná, že lichôtkami ju chce útočník ovplyvniť, môže útočník získať jej sympatie a následne ich využiť na získanie informácií.
- Kontakt a spolupráca – v prípade, že obeť spolupracuje s útočníkom v istej situácii, získava pocit spolunáležitosti a tým aj sympatie. Ukázalo sa, že spolupráca na rovnakom ciele môže vyvolať okrem sympatií aj veľmi silný pocit spolunáležitosti, ktorý môže slúžiť ako heuristická pomôcka pri rozhodovaní (Sherif & kol, 1961).

V prípade, že sa človek opakovane stretáva s pozitívnymi stimulmi počas dlhodobejšej spolupráce, spojí si tieto pozitívne emócie s danou osobou – útočníkom. Je to v súlade s atribučnou teóriou. Ak teda dôjde k spojeniu osoby útočníka s pozitívnymi vplyvmi, môže si získať priazeň obete (asociácia).

Autorita

Táto heuristika pracuje s predstavou, že „autorita“ má vždy pravdu a človek sa jej musí držať. Množstvo experimentov potvrdilo, že autorita (napr. vedecká) dokázala prinútiť

bežných účastníkov experimentu k potenciálne smrtiacemu správaniu. Napriek tomu, že subjekty s rozhodnutím autority nesúhlasili, vykonali jej príkazy.

Veľkú váhu v tomto vplyve má neočakávanosť. Milgram prikladá dôvod vysokej úrovne vyhovenia autorite hlboko vžitej úcte a poslušnosti voči autoritám v spoločnosti (Cialdini R. B., 2012). Ľudia sú často autoritou ovplyvnení celoživotne (učitelia, rodičia atď.) a prirodzene sa naučili považovať ju za dôveryhodnú. Organizáciám ako je armáda alebo polícia je prisudzovaná ešte silnejšia autorita.

Ako ďalší faktor tejto heuristiky stanovil Milgram zmenu pôvodcu deja (Hewstone & Stroebe, 2006). Znamená to, že keď obeť prisúdi príkaz (pôvod deja) autorite, zbyví sa tým zodpovednosti na čin samotný.

Je dôležité dodať, že vo väčšine experimentov skúmajúcich tento vplyv sa autoritatívna osoba nemusela ani nijak preukázať – pôsobila len vzhľadom a správaním (Cialdini R. B., 2012). Stačí teda použiť len symboly autority, ako je oblačenie (oblek, plášť, uniforma), rekvizity (odznak, preukaz, vizitka) a typické správanie.

Útočník môže využiť viac druhov autority – organizačnú autoritu (v pracovnom prostredí napr. nadriadený), legálnu autoritu (sudca, policajt) alebo spoločenskú autoritu (neformálna osobnosť založená na čistej presvedčivosti správania).

Nedostatok

Podstatou tohto princípu je, že ľuďom sa predmety javia cennejšie a príťažlivejšie, ak sú pre nich vzácne (až nedostupné). K udalostiam je možné pristupovať skôr tak, že obeť niečo stráca skôr ako niečo získava. V rámci množstva experimentov bolo pozorované, že ak je rovnaká informácia formulovaná ako strata oproti zisku (napr. ušetriť peniaze oproti prísť o peniaze), človeka oveľa viac motivuje potenciálna strata ako zisk (Tversky & Kahneman, 1991).

Táto vlastnosť sa v súvislosti so sociotechnikou používa v oblasti phishingových emailov, ktoré sa venujú obmedzenej ponuke. V súvislosti s nedostatkom v podstatne širšom poňatí je možné hovoriť o obmedzení časom. Limitované časové možnosti obmedzujúce rozhodovanie spôsobujú podstatne silnejšiu emočnú odozvu – pozitívnu alebo negatívnu (Teuscher, 2005). Je teda veľmi pravdepodobné, že následkom časového nátlaku obeť pri vyhodnocovaní skĺzne k heuristickému spracovaniu.

Status Quo Bias

Základom tejto heuristiky je fakt, že ľudia sa boja zmeny a teda sú motivovaní k udržiavaniu systému a nemenných názorov, hoci zmena môže viesť k celkovému zlepšeniu. Tento efekt skúmal sa označuje ako status quo bias (Tversky & Kahneman, 1991).

Silne motivujúco môže pôsobiť udržanie statusu quo v kontraste s možnosťou negatívnej zmeny (napr. zablokovanie časti systému), ktorá nastane v prípade, že obeť útočníkovi nepomôže. To ju teda bude vlastne motivovať k pomoci útočníkovi.

Stereotypy

Kvôli jednoduchosti je pre človeka prirodzená snaha rozdeliť svet do kategórií. Tým sa napriek nepresnosti výrazne uľahčuje rozmýšľanie, pretože človek nemusí hodnotiť a uvažovať o každej entite osobitne, ale v kontexte kategórie, do ktorej patrí (Hayesová, 1993).

Stereotypizovanie ako myšlienková skratka predstavuje priradenie vlastností charakteristických pre skupinu (pohlavie, povolanie, národnosť atď) jednotlivcovi, namiesto charakterizovania vlastností individuálne (Hamilton & Rose, 1980). Tento spôsob rozmýšľania šetrí mentálnu energiu a útočník ho môže využiť. Môže využiť automatické reakcie obete pomocou predstierania určitého stereotypu.

Obdobne je možné stereotypizovať aj isté situácie, ktoré povedú jednotlivca k automatickému správaniu.

Mylná paralela

U mylnej paralely ide o skreslenie, ktoré úzko súvisí s atribučnou teóriou a dopĺňa teóriu o stereotypoch. Podľa nej človek „vyvodzuje závery o osobnostných rysoch aktéra na základe pozorovaného správania, aj keď je tento zámer neopodstatnený“ (Hewstone & Stroebe, 2006).

Túto vlastnosť výborne dokresľuje tzv. halo efekt (efekt svätožiary). Podľa neho je pre človeka prirodzené prisudzovať atraktívnym ľuďom pozitívne vlastnosti iba na základe vzhľadu (Lachman & Bass, 1985; Dion & Berscheid, 1972).

Ak sa útočník bude správať určitým spôsobom, obeť mu automaticky na základe svojho pocitu samovoľne priradí pozitívne vlastnosti – napr. môže posudzovať človeka ako spoľahlivého len na základe vzhľadu.

Sociálna identita

V interpersonálnej interakcii (bežné správanie) vychádza správanie jednotlivca z jeho vlastných jedinečných rysov.

Medziskupinové správanie na druhej strane predstavuje správanie jedinca ako člena skupiny s vlastnosťami a rysmi skupiny, s ktorou sa jednotliviec v danej chvíli identifikuje (Tajfel H. , 1982).

Ak bude útočník vedieť o pocite členstva obete v skupine, môže u nej predpokladať znaky správania špecifické pre skupinu. Obdobne ako v istej skupine nadobúda jednotlivec vlastnosti charakteristické pre danú skupinu, tak v istej roli získava vlastnosti špecifické pre danú rolu.

Na postoje úzko nadväzuje sociálna identita. Jedná sa o vedomie jedinca odvodené z jeho členstva v istej skupine. Vzťah človeka k ostatným je logicky ovplyvnený identifikáciou so skupinou. Vzťah je ovplyvnený tým, či sú ostatní zo vzťažnej skupiny jednotlivca alebo z nevzťažnej skupiny (Sherif & kol, 1961). V tom prípade jedinec zvýhodňuje svoju vzťažnú skupinu v porovnaní s nevzťažnou (Tajfel & Turner, 1986; Levine, 2005). Ak sa teda útočník bude vydávať za člena vzťažnej skupiny,, môže očakávať vyššiu možnosť vyhovenia jeho požiadavkám.

Obet sa bude pravdepodobne vnímať ako člen v danej situácii najvýznamnejšej skupiny. V kontexte útoku to bude najčastejšie pracovná skupina (ak sa hovorí o útoku v pracovnom prostredí).

Tým, že by sa útočník vydával za pracovníka firmy (alebo za iného člena vzťažnej skupiny obete) mohol by potom tento získať veľmi silnú heuristickú pomôcku na získanie dôvery a pomoci. Tomuto spôsobu útoku naviac môže napomáhať to, že dosiahnutie jednotnej, priateľskej a dôvernej podnikovej kultúry je jedným z najvýznamnejších cieľov manažerov (Brooks, 2003).

5.2 Emócie

Emócie sú ďalším dôležitým aspektom ovplyvňovania rozhodovania človeka. Spoločne so silnými emóciami dochádza v tele k nabudeniu centrálného autonómneho nervového systému (Hewstone & Stroebe, 2006). Tým je významne ovplyvnené rozhodovanie. Emócie pripravujú telo na akciu v závislosti na podnete. Vyvolaním silných emócií môže útočník istým spôsobom nastaviť správanie obete, ktoré sa bude riadiť v závislosti na prežívaní emócií (Frijda, 1986; Hewstone & Stroebe, 2006).

Pri dostatočne silnom emočnom podnete sa mozog monopolizuje pre konanie na základe emócií a preto sa ľudia následne rozhodujú skôr pomocou emócií ako na základe racionálnej úvahy. Emócie sú pri útoku zo strany obete veľmi problematické. Aj keď obeť vie o spôsobe útoku a pozná možnosti obrany, myslenie sa aktivovaním emócií oslabí až potlačí a racionálne premýšľanie sa stáva neúčinným.

Vyvolanie emočnej reakcie u obete môže viesť ako k reakcii špecifickej pre danú emóciu, tak aj všeobecne k väčšej prevahe rýchlych záverov nad racionálnymi argumentami (Kahneman, 2011).

Pozitívne sebaponímanie

Zameranie sa na seba je jednou zo základných emočných vlastností človeka. Dá sa to skúmať na egocentrizme a motivovanej ilúzii, za predpokladu, že človek uprednostňuje pozitívne sebaponaťie pred negatívnym (Tajfel & Turner, 1986).

To, že väčšina ľudí vidí samých seba pozitívnejšie ako je v skutočnosti, dáva útočníkovi možnosť využiť zdanlivé ľudské kvality, pretože správanie v rozpore sebaponímania by pre obeť znamenalo kognitívnu disonanciu. V rámci motivovanej ilúzie napr. vyvolanie pocitu múdrosti a nápomocnosti u obete vedie k vyhoveniu požiadavkám útočníka, ktoré sú v súlade s týmito vlastnosťami.

Za podobné skreslenie by sme mohli považovať egocentrizmus. V kontexte vyjednávania majú strany tendenciu dať väčšiu váhu pohľadom podporujúcim seba samého (Bazerman, Curhan, & Moore, 2000). Toto nie je len ponímanie egocentrizmu, ale aj selektívnej expozície. V súlade s kognitívnu disonanciou sú ľudia motivovanejší lepšie vnímať informácie, ktoré sú v súlade s ich názormi. Útočník teda môže upraviť štýl útoku podľa momentálneho stavu obete, aby ho vnímala v najväčšej možnej miere. Tieto princípy môžu útočníkovi napomáhať upraviť útok tak, aby sa obeť v ňom sústredila na to, čo útočníka je predmetom záujmu útočníka.

Po hlbšej analýze jednotlivých faktorov, ktoré ovplyvňujú proces rozhodovania jednotlivca je možné vysloviť isté predpoklady ohľadne správania sa ľudí v simulovaných situáciách sociotechnického útoku.

Som presvedčený, že v dnešnej dobe sa s istými formami sociálneho inžinierstva stretáva v bežnom každodennom živote väčšina ľudí z môjho okolia. Existujú tradičné názory o správaní sa napr. ľudí s vyšším vekom alebo o odlišnom správaní mužov a žien v rovnakých situáciách. Z toho dôvodu som sa rozhodol realizovať dotazníkový prieskum, ktorý by tieto tradičné názory potvrdil alebo vyvrátil.

6 Skupiny respondentov

Zo stereotypov, ktoré vychádzajú z tradičného názoru na správanie som sformuloval niekoľko hypotéz, ktoré som vo svojej bakalárskej práci overoval. Overované hypotézy sa týkali napr. rizikovosti správania sa dôchodcov v prípade jednotlivých typov sociotechnického útoku, odlišnej resp. rovnakej miery rizikovosti správania sa ľudí českej a slovenskej národnosti, rozdielnej účinnosti konkrétnej metódy sociálneho inžinierstva u ľudí rozdelených podľa veľkosti obce, v ktorej bývajú a vplyvu znalostí sociálneho inžinierstva na rozhodovanie v prípade sociotechnického útoku.

Pre účely dosiahnutia cieľa mojej bakalárskej práce som sa rozhodol rozdeliť respondentov môjho prieskumu do skupín celkovo podľa 8 kritérií:

- Muži – Ženy
- Ľudia žijúci v meste – Ľudia žijúci mimo mesta
- Ľudia do 18 rokov – 18 až 35 rokov – 35 až 60 rokov – 60 a viac rokov
- Slováci – Česi
- Ľudia s ukončeným základným vzdelaním – S ukončeným stredoškolským vzdelaním – S ukončeným vysokoškolským vzdelaním
- Ľudia, ktorí vykonávajú manuálnu prácu – Ľudia, ktorí vykonávajú kancelársku prácu
- Zamestnaný resp. SZČO – Nezamestnaný – Študent – Dôchodca
- Ľudia, ktorí vedia čo je to sociálne inžinierstvo – Ľudia, ktorí nevedia čo je to sociálne inžinierstvo

Tieto skupiny som vyberal z dôvodu, aby som skúmal čo najširšie spektrum ľudí a nezameriaval sa len na jednu sféru (napríklad ľudia vyvíjajúci iOS software – ľudia vyvíjajúci Android software).

Dotazovaní boli z môjho širšieho okolia, najmä moji spolužiaci, bývalí spolužiaci, kamaráti a rodina. Ale aj moji kolegovia, kolegovia mojich rodičov, žiaci na strednej škole a pod. So skupinou ľudí, ktorí majú 60 a viac rokov mi pomohli moji starí rodičia. Jednalo sa najmä o ich známych a o ľudí v domove dôchodcov.

7 Dotazník

Dotazník, ktorý som vytvoril pre účely mojej bakalárskej práce obsahuje 23 otázok skúmajúcich správanie respondentov v rôznych situáciách, v ktorých môže dôjsť k sociotechnickému útoku. Dotazník som spracoval pomocou formuláru Google a tie isté otázky som použil aj v tlačenej podobe, z dôvodu zapojenia ľudí v dôchodcovskom veku, ktorí bežne nepoužívajú internet. Dotazník vypracovávaný cez internet bol zadávaný spôsobom, v ktorom sa nedá vrátiť a opraviť predošlú odpoveď. Je to tak z dôvodu, aby ľudia nemohli opravovať to, pre čo sa už raz rozhodli, keďže vo väčšine otázok si majú predstaviť, čo by robili v danej situácii. Priemerná dĺžka vyplnenia dotazníka bola tri a pol minúty. Dotazník vyplnený za 0 až 2 minúty neberiem vo vyhodnotení do úvahy. Jedná sa pravdepodobne o niekoho, kto otázky vôbec nečítal a len rýchlo navolil rôzne odpovede.

Jednotlivé otázky v dotazníku sa zameriavajú na rôzne metódy sociotechnického útoku. Podľa vopred zvolených hypotéz som vyhodnotil a priradil k jednotlivým skupinám metódy, ktoré sú pre danú skupinu najnebezpečnejšie.

Otázky č. 1 až č. 8 sú použité z dôvodu priradenia respondenta do jednotlivých skúmaných skupín.

01. Aké je vaše pohlavie:

- a) Muž
- b) Žena

02. Aká je vaša národnosť:

- a) Slovenská
- b) Česká
- c) Iná

03. Aký je váš vek:

- a) Pod 18
- b) 18 – 35
- c) 35 – 60
- d) Nad 60

04. V akej veľkej obci žijete:

- a) Pod 10 000 obyvateľov

- b) 10 000 – 100 000 obyvateľov
- c) 100 000 – 500 000 obyvateľov
- d) Nad 500 000 obyvateľov

05. Aké je vaše najvyššie dosiahnuté vzdelanie:

- a) Základné
- b) Stredoškolské bez maturity
- c) Stredoškolské s maturitou
- d) Vyššia odborná škola
- e) Vysokoškolské štúdium 1. stupňa (Bc.)
- f) Vysokoškolské štúdium 2. stupňa (Mgr., Ing.)
- g) Vysokoškolské štúdium 3. stupňa (PhD.)

06. Ste:

- a) Zamestnaný resp. SZČO
- b) Nezamestnaný
- c) Študent
- d) Študent aj zamestnaný
- e) Dôchodca

07. Aký typ práce vykonávate (zobrazí sa len vtedy ak v predošlej otázke zaklikol „zamestnaný“):

- a) Kancelárska
- b) Manuálna

08. Viete čo je sociálne inžinierstvo, čo skúma a aké praktiky využíva?

Stupnica 0 - 4 (0 - vôbec nepoznám, 4 – poznám veľmi dobre)

Otázky č. 9, 12, 20, 21 skúmajú, či by útočník mohol získať od dotazovaného potrebné informácie bez väčšej snahy. V uvedených otázkach popisuje dotazovaný svoj prístup k ochrane osobných údajov.

09. Využívate sociálne siete alebo mail?

- a) Využívam sociálne siete aj e-mail
- b) Využívam iba sociálne siete
- c) Využívam iba e-mail
- d) Nevyužívam ani jedno

12. Máte zverejnené svoje osobné údaje na sociálnej sieti? (napr. telefónne číslo, koníčky, školu, fotky, aktuálnu polohu atp.)

- a) Áno
- b) Nie
- c) Len časť (napíšte aké osobné údaje máte zverejnené)

20. Predstavte si, že ste pracovník v budove do ktorej je možné sa dostať iba pomocou identifikačnej karty. Pred vchodom narazíte na človeka, ktorý je zúfalý a svoju identifikačnú kartu všade hľadá. Čo urobíte?

- a) Nepustím ho dnu.
- b) Pustím ho dnu.
- c) Spýtam sa ho kto je a keď mi potvrdí, že je pracovník, pustím ho dnu.
- d) Iné (otvorená odpoveď)

21. Dávate si pozor na to, aby vám nikto nevidel vaše údaje na platobnej karte pri nakupovaní v obchode?

- a) Áno
- b) Nie
- c) Snažím sa, ale v niektorých prípadoch sa to nedá

Otázky č. 10, 15, 19 sa sústredia na metódu Quid pro Quo, ktorá je popísaná v teoretickej časti tejto práce. Vo svojich odpovediach dotazovaný popisuje svoje konanie v rôznych situáciách – sprístupnenie údajov v počítači alebo uvádzanie osobných údajov v telefonickom rozhovore.

10. Predstavte si, že vás telefonicky kontaktuje zástupca medicínskej firmy, ktorá sa zaoberá riešením kľbových problémov. Ponúka vám zadarmo vyskúšanie novej metódy a podrobne vysvetlí jej funkčnosť. Žiada si od vás kontaktné údaje a vek (meno, priezvisko, adresu, e-mail). Čo urobíte?

- a) Poskytnem mu len niektoré osobné údaje.

- b) Neposkytnem mu žiadne informácie.
- c) Poskytnem mu všetky informácie, ktoré požaduje.
- d) Iné (otvorená odpoveď)

15. Predstavte si, že vám cudzí človek podrží dvere do vášho paneláku, v ktorom bývate. Následne vám vo výťahu povie citlivú informáciu o sebe. Čo spravíte?

- a) Ignorujem ho a nerozprávam sa s ním.
- b) Vypočujem ho, ale nič mu o sebe nepoviem.
- c) Poďakujem mu za podržanie dverí a vyberiem si inú cestu ako sa dostanem domov (napr. pôjdem po schodoch).
- d) Taktiež mu poviem nejakú informáciu o mne.
- e) Iné (otvorená odpoveď)

19. Predstavte si, že ste pracovníkom vo firme v ktorej používate počítač. Zavolá vám človek, ktorý sa predstaví ako IT technik a povie vám, že máte problém s počítačom. Následne po vás chce vypnutie antivírusového programu aby mohol chybu opraviť. Čo urobíte?

- a) Poviem nech mi o pár minút zavolá späť a zatiaľ zavolám svojmu nadriadenému.
- b) Vypnem antivírusový program a urobím všetko čo vraví.
- c) Ignorujem ho a zložím telefón.
- d) Iné (otvorená odpoveď)

Otázka č. 11 skúma správanie dotazovaného k osobe, ktorá mu je sympatická.

11. Predstavte si, že za vami príde pre vás sympatický cudzí človek, ktorý sa s vami snaží nadviazať kontakt. Následne bude rozhovor smerovať k vašim rodinným záležitostiam. Čo urobíte?

- a) Nepoviem mu nič osobné
- b) Posnažím sa zmeniť tému.
- c) Pretože mi je sympatický a nechcem s ním prerušiť kontakt, poviem mu takmer všetko na čo sa spýta.
- d) Od začiatku ho ignorujem.
- e) Iné (otvorená odpoveď)

Otázky č. 13, 17, 22 sú zamerané na skúmanie phishingu, spear phishingu a clone phishingu pomocou internetu (konkrétne e-mailovej správy).

13. Predstavte si, že vám príde mail so žiadosťou o príspevok na zakúpenie prístroja na detskú onkológiu v ktorom sa nachádza link na zadanie údajov k platbe. Čo urobíte?

- a) Kliknem na link, prezriem si stránku, ale platbu nevykonám.
- b) Otvorím si stránku zdravotníckeho zariadenia (nejdem na ňu priamo cez link) a hľadám informácie o zbierke.
- c) Ignorujem mail a nič neurobím.
- d) Kliknem na link, vyplním údaje a odošlem platbu.
- e) Iné (otvorená odpoveď)

17. Predstavte si, že chcete schudnúť na leto do plaviek a začnete cvičiť. Na e-mail vám príde ponuka s odkazom ohľadom produktu, vďaka ktorému za mesiac schudnete 5kg úplne bez námahy. Čo spravíte?

- a) Otvorím odkaz a hneď si produkt kúpim.
- b) Otvorím odkaz a pozriem si čo je to za produkt.
- c) Pred tým ako otvorím odkaz, vyhľadám na internete informácie o akú spoločnosť a o aký produkt sa jedná.
- d) Ignorujem e-mail, pretože žiadny taký produkt nechcem.
- e) Iné (otvorená odpoveď)

22. Predstavte si, že vám dôjde e-mail od banky kde vás vyzývajú zmeniť si kvôli bezpečnosti heslo k vášmu účtu. O minútu na to vám príde identický mail z tej istej banky, ktorý tvrdí, že ide o aktualizovanú verziu. Čo spravíte?

- a) Otvorím odkaz v staršom maili, prihlásim sa a zmením si heslo.
- b) Otvorím odkaz v novšom maili, prihlásim sa a zmením si heslo.
- c) Otvorím si stránku mojej banky (nejdem na ňu priamo cez link v e-maili), prihlásim sa a zmením si heslo.
- d) Napíšem alebo zavolám na zákaznícku linku banky a spýtam sa, čo sa deje.
- e) Ignorujem obidva maily a nič nespravím.
- f) Iné (otvorená odpoveď)

Otázka č. 14 skúma phishing prostredníctvom telefónneho rozhovoru.

14. Predstavte si, že vám príde e-mail od vašej banky v ktorom sa píše, že máte zavolať na dané číslo, ktoré je napísané v maily, pretože sa na vašom účte dejú divné veci. Čo urobíte?

- a) Zavolám na zákaznícku podporu a spýtam sa čo to je za číslo.
- b) Nezavolám nikde a e-mail ignorujem.
- c) Zavolám na dané číslo.
- d) Zavolám na zákaznícku podporu a spýtam sa čo je za problém.
- e) Iné (otvorená odpoveď)

Otázka č. 16 skúma phishing prostredníctvom SMS.

16. Predstavte si, že vám banka pošle SMS a tvrdí, že si máte z bezpečnostných príčin zmeniť heslo k internet bankingu cez odkaz nižšie. Čo spravíte?

- a) Zavolám na zákaznícku podporu a spýtam sa aký je problém.
- b) Ignorujem SMS a nerobím nič.
- c) Prihlásim sa do internet bankingu pomocou internetu a zmením si heslo.
- d) Prihlásim sa do internet bankingu pomocou linku v SMS a zmením si heslo.
- e) Iné (otvorená odpoveď)

Otázka č. 18 skúma baiting.

18. Predstavte si, že v kaviarni na stole nájdete ležať USB kľúč. Čo spravíte?

- a) Zapojím ho do môjho počítača, aby som zistil čo sa na ňom nachádza a komu patrí.
- b) Zanesiem ho čašníčke a poviem kde som ho našiel.
- c) Neurobím nič a nechám ho na stole.
- d) Vyhodím ho.
- e) Iné (otvorená odpoveď)

Otázka č. 23 skúma, či sú respondenti chránení pred phishingom a pharmingom pomocou antivírusového softwaru.

23. Používate antivírusový systém?

- a) Áno
- b) Nie

- c) Používam viac ako 1 antivírusový systém
- d) Používam iba trial verzie
- e) Neviem

Všetky metódy, ktoré dotazník skúma sú popísané v teoretickej časti tejto práce.

Pri každej z otázok 9 až 23 je zámerne zaradená jediná odpoveď, ktorej výber vyjadruje najvyššiu mieru ohrozenia respondenta skúmanou metódou sociálneho inžinierstva.

Pri otázke číslo 8 za najvyššiu mieru ohrozenia považujem odpovede 0 a 1.

8 Hypotézy

Rozhodol som sa overovať pravdivosť piatich hypotéz. Volil som ich na základe rôznych predsudkov voči jednotlivým skupinám ľudí. V tejto časti nasleduje podrobnejší popis všetkých hypotéz.

H1: Ľudia v dôchodcovskom veku (60 a viac), ktorí používajú e-mail, by si mali dávať najväčší pozor na phishing zasielaný prostredníctvom mailu.

Rozšírený predsudok o starších ľuďoch je ten, že nemajú ani základné znalosti v oblasti IT a vedia si prinaľepšom napísať a skontrolovať e-mail. Podľa tohto predsudku som usúdil, že si starší ľudia nebudú vedomí toho, keď im príde e-mail, ktorý tvrdí, že sa na ich bankovom účte dejú divné veci a keď ich niekto bude vyzývať aby si zmenili heslo, tak mailu uveria, kliknú na odkaz a zmenia si heslo bez uvedomenia si toho, že niekto získal ich osobné údaje.

H2: Je pravdepodobnejšie, že ľudia, ktorí nevedia čo je sociálne inžinierstvo a aké metódy používa, sa stanú obeťou útočníka skôr, ako ľudia, ktorí sociálne inžinierstvo poznajú.

V tejto hypotéze predpokladám, že osoby známe problematiky sociálneho inžinierstva si viac uvedomujú nebezpečenstvo nástrah jeho metód a vedome sa im bránia a vyhýbajú. Na druhej strane osoby, ktoré o sociálnom inžinierstve vedomosť nemajú sa správajú živelné a podvedome konajú presne podľa predpokladu útočníka.

H3: Ľudia, ktorí žijú na vidieku alebo v menšom meste (do 10 000 obyvateľov), sú dôverčivejší k ľuďom, ktorých osobne stretnú.

Túto hypotézu som vytvoril na základe tradičnej predstavy o užších a úprimnejších medziľudských vzťahoch medzi obyvateľmi vidieka a menších miest. Obyvatelia väčších miest neudržiavajú užšie medziľudské vzťahy mimo najbližšej rodiny, žijú uzavretejším spôsobom života a so svojím okolím zdieľajú oveľa menej osobných informácií. Preto predpokladám, že sú menej dôverčiví a otvorení k svojmu okoliu.

H4: Medzi Slovákmi a Čechmi nie je žiadny výrazný rozdiel.

Táto moja hypotéza vyplýva zo spoločného pôvodu a veľmi podobnej mentality oboch národov.

H5: Najúspešnejšou metódou z pohľadu útočníka je phishing rozosielaný e-mailom.

Túto hypotézu som stanovil na základe impulzívneho správania sa ľudí vo vysoko stresových situáciách. Predpokladám, že človek v stave ohrozenia napríklad majetku koná unáhle a zabúda na pravidlá bezpečného správania.

9 Vyhodnotenie dotazníka

Na otázky dotazníka z mojej bakalárskej práce odpovedalo spolu 213 respondentov (v online forme alebo v printovej forme).

Desať odpovedí na dotazník bolo odoslaných v „podozrivo“ krátkom čase (stanovil som ho pod 2 minúty). Tieto odpovede som nebral vo svojom prieskume do úvahy a preto vo vyhodnotení vystupuje počet platných súborov odpovedí 203.

V ďalšej časti mojej bakalárskej práce vyhodnocujem pravdivosť jednotlivých hypotéz, ktoré som si stanovil.

H1: Ľudia v dôchodcovskom veku (60 a viac), ktorí používajú e-mail, by si mali dávať najväčší pozor na phishing zasielaný prostredníctvom mailu.

Ľudia v dôchodcovskom veku 60 a viac: 21

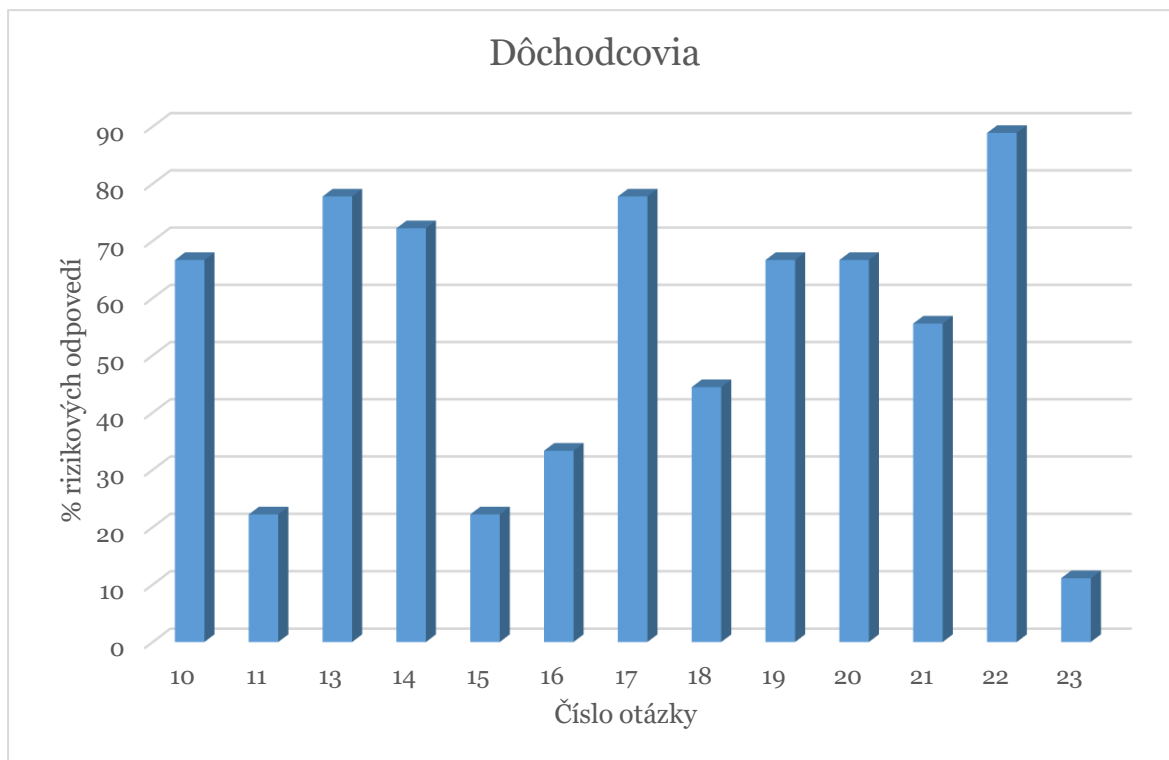
Traja respondenti odpovedali na otázku či používajú e-mailovú adresu negatívne, tým pádom neboli zarátaní do konečného skúmania prvej hypotézy, ktorá sa týka len starších ľudí, ktorí e-mailovú adresu používajú.

Percentuálnu hodnotu rizikových odpovedí, ktoré uviedli dôchodcovia pri jednotlivých situáciách popísaných v dotazníku uvádzam v Tabuľka 1 Miera rizikových odpovedí dôchodcov na jednotlivé otázky dotazníka. Výsledky overovania tejto hypotézy som následne spracoval v grafe Obr. 1 Miera rizikových odpovedí dôchodcov na jednotlivé otázky dotazníka.

Tabuľka 1 Miera rizikových odpovedí dôchodcov na jednotlivé otázky dotazníka

Číslo otázky	10	11	13	14	15	16	17
Rizikové odpovede dôchodcov [%]	66,7	22,22	77,78	72,22	22,22	33,33	77,78

Číslo otázky	18	19	20	21	22	23
Rizikové odpovede dôchodcov [%]	44,44	66,67	66,67	55,56	88,89	11,11



Obr. 1 Miera rizikových odpovedí dôchodcov na jednotlivé otázky dotazníka

Podľa výsledkov si môžeme všimnúť, že sa hypotéza potvrdila a teda, že najviac ľudí v dôchodcovskom veku sa nachytá práve prostredníctvom phishingu rozosielaného cez e-mail. Na druhom mieste z pohľadu nebezpečnosti úniku citlivých informácií u starších ľudí je phishing prostredníctvom telefonného rozhovoru kedy útočník taktiež z istej časti využije e-mail k tomu, aby sa s ním obeť sama skontaktovala cez telefón.

H2: Je pravdepodobnejšie, že ľudia, ktorí nevedia čo je sociálne inžinierstvo a aké metódy používa, sa stanú obeťou útočníka skôr, ako ľudia, ktorí sociálne inžinierstvo poznajú.

Vo svojich odpovediach sa 52 dotazovaných vyjadrilo, že pozná sociálne inžinierstvo, pričom všetci respondenti z uvedenej skupiny používajú aj sociálne siete. Na druhej strane 151 dotazovaných uviedlo, že nepoznajú metódy a postupy sociálneho inžinierstva, z nich 138 používa nejakú sociálnu sieť.

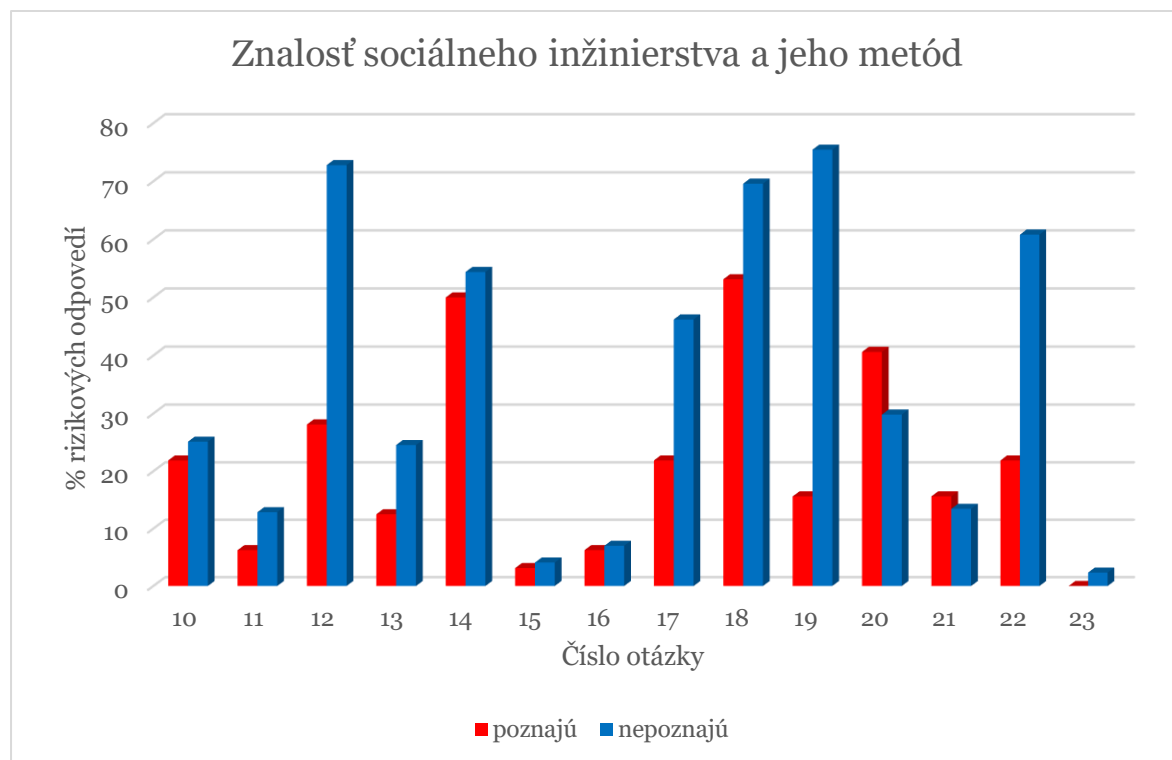
V Tabuľka 2 Miera rizikových odpovedí respondentov rozdelených podľa znalosti sociálneho inžinierstva sú uvedené percentuálne hodnoty rizikových odpovedí respondentov rozdelených do skupín podľa kritéria znalosti a neznalosti sociálneho inžinierstva a jeho metód.

Grafické spracovanie overovania hypotézy č. 2 uvádzam v grafe na Obr. 2 Miera rizikových odpovedí respondentov rozdelených podľa znalosti sociálneho inžinierstva.

Tabuľka 2 Miera rizikových odpovedí respondentov rozdelených podľa znalosti sociálneho inžinierstva

Číslo otázky	10	11	12	13	14	15	16
Poznajú sociálne inžinierstvo [%]	21,88	6,25	28,13	12,50	50,00	3,13	6,25
Nepoznajú sociálne inžinierstvo [%]	25,15	12,87	72,78	24,56	54,39	4,09	7,02

Číslo otázky	17	18	19	20	21	22	23
Poznajú sociálne inžinierstvo [%]	21,88	53,13	15,63	40,63	15,63	21,88	0,00
Nepoznajú sociálne inžinierstvo [%]	46,20	69,59	75,44	29,82	13,45	60,82	2,34



Obr. 2 Miera rizikových odpovedí respondentov rozdelených podľa znalosti sociálneho inžinierstva

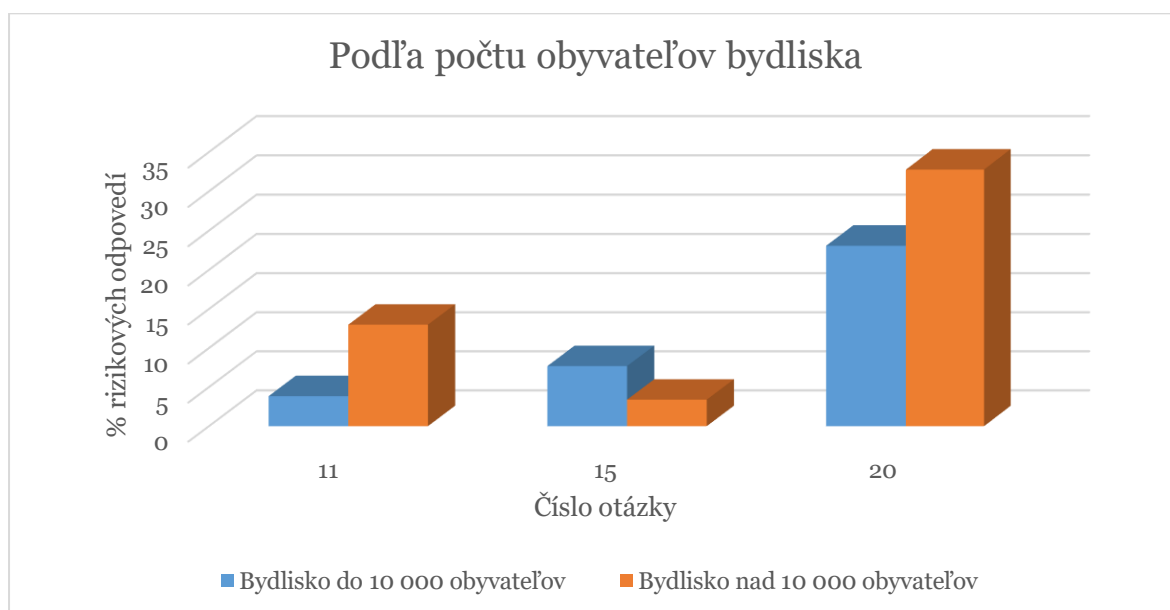
Z grafu na Obr. 2 Miera rizikových odpovedí respondentov rozdelených podľa znalosti sociálneho inžinierstva je zjavné, že platnosť hypotézy číslo 2 sa potvrdila nakoľko v odpovediach na väčšinu otázok vychádza vyššie riziko u skupiny, ktorá nepozná metódy sociálneho inžinierstva.

H3: Ľudia, ktorí žijú na vidieku alebo v menšom meste (do 10 000 obyvateľov), sú dôverčivejší k ľuďom, ktorých osobne stretnú.

26 respondentov, ktorí platne odpovedali na dotazník uviedlo, že žijú v obci menšej ako 10 000 obyvateľov. Na druhej strane zvyšných 177 dotazovaných žije v obci s počtom obyvateľov väčším ako 10 000. V Tabuľka 3 Miera rizikových odpovedí respondentov rozdelených podľa veľkosti bydliska sú uvedené percentuálne hodnoty rizikových odpovedí dotazovaných rozdelené podľa kritéria počtu obyvateľov obce, v ktorej žijú. V overovaní hypotézy č. 3 som bral do úvahy výlučne odpovede na otázky, ktoré sa týkajú sociotechnického útoku spojeného s osobným kontaktom obete a útočníka (otázky č. 11, č. 15 a č. 20). Odpovede a mieru ohrozenia som následne vyhodnotil graficky na Obr. 3 Miera rizikových odpovedí respondentov rozdelených podľa veľkosti bydliska.

Tabuľka 3 Miera rizikových odpovedí respondentov rozdelených podľa veľkosti bydliska

Číslo otázky	11	15	20
Bydlisko do 10 000 obyvateľov [%]	3,85	7,69	23,08
Bydlisko nad 10 000 obyvateľov [%]	12,99	3,39	32,77



Obr. 3 Miera rizikových odpovedí respondentov rozdelených podľa veľkosti bydliska

Z grafu je viditeľné, že hypotéza H3 sa nepotvrdila – účinnosť osobného kontaktu je v niektorých situáciách vyššia u ľudí z vidieka a v iných situáciách u ľudí z väčších miest. Nedá sa teda zovšeobecniť, že osobný kontakt je rizikovejší u ľudí, ktorí žijú v obciach s počtom obyvateľov do 10 000.

H4: Medzi Slováckmi a Čechmi nie je žiadny výrazný rozdiel.

Podľa kritéria národnosti sa respondenti môjho prieskumu rozdelili do 3 skupín – 118 uviedlo, že sú slovenskej národnosti, 83 uviedlo českú národnosť a 2 odpovedali na otázku číslo 2 v zmysle, že ich národnosť je iná ako Slovenská alebo Česká.

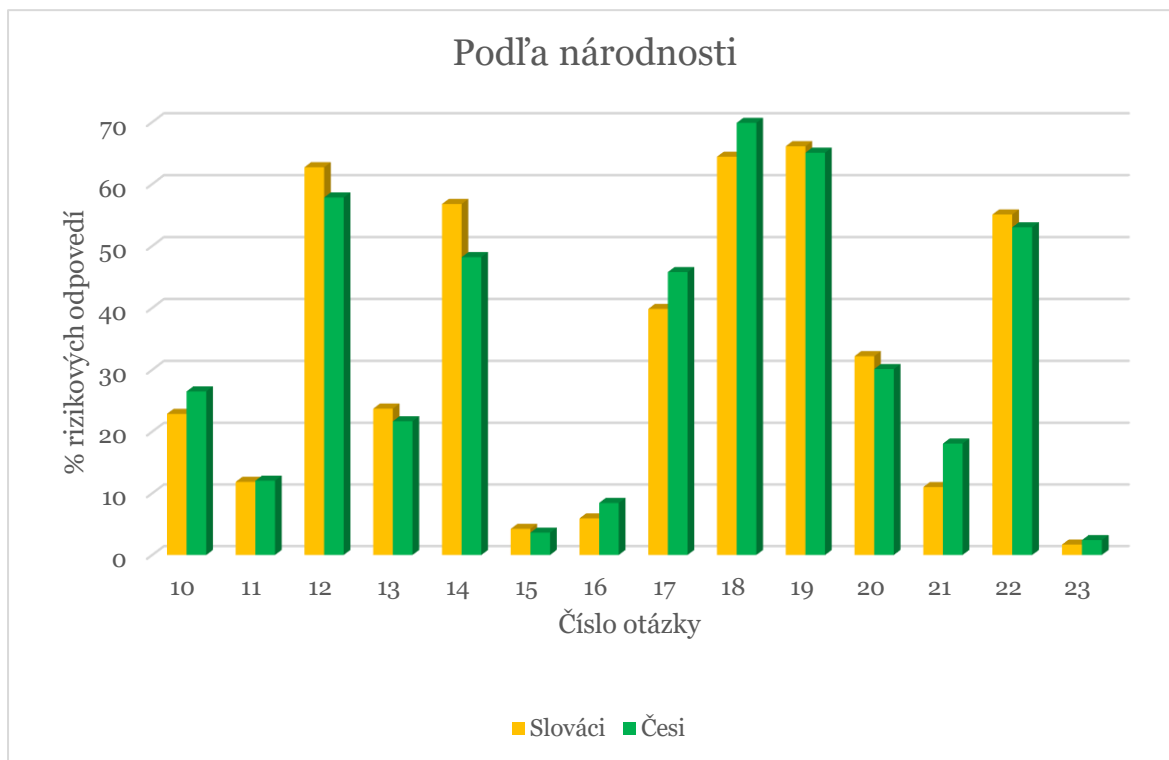
Percentuálne hodnoty ich ovplyvniteľnosti jednotlivými metódami sociotechnického útoku som spracoval v Tabuľka 4 Miera rizikových odpovedí respondentov rozdelených podľa národnosti.

Tabuľka 4 Miera rizikových odpovedí respondentov rozdelených podľa národnosti

Číslo otázky	10	11	12	13	14	15	16
Slováci [%]	22,88	11,86	62,71	23,73	56,78	4,24	5,93
Česi [%]	26,51	12,05	57,83	21,69	48,19	3,61	8,43

Číslo otázky	17	18	19	20	21	22	23
Slováci [%]	39,83	64,41	66,10	32,20	11,02	55,08	1,69
Česi [%]	45,78	69,88	65,06	30,12	18,07	53,01	2,41

Následne som výsledky overovania platnosti hypotézy číslo 4 spracoval v grafe na Obr. 4 Miera rizikových odpovedí respondentov rozdelených podľa národnosti.



Obr. 4 Miera rizikových odpovedí respondentov rozdelených podľa národnosti

Hypotéza sa potvrdila – rozdiely rizikovosti skupín podľa národností sú zanedbateľné (do 10%). Z výsledkov dotazníku nevyplývalo, či sa rizikovejšie správajú Česi alebo Slováci nakoľko v niektorých situáciách vyšla vyššia miera rizikovosti v jednej národnosti a v iných u druhej.

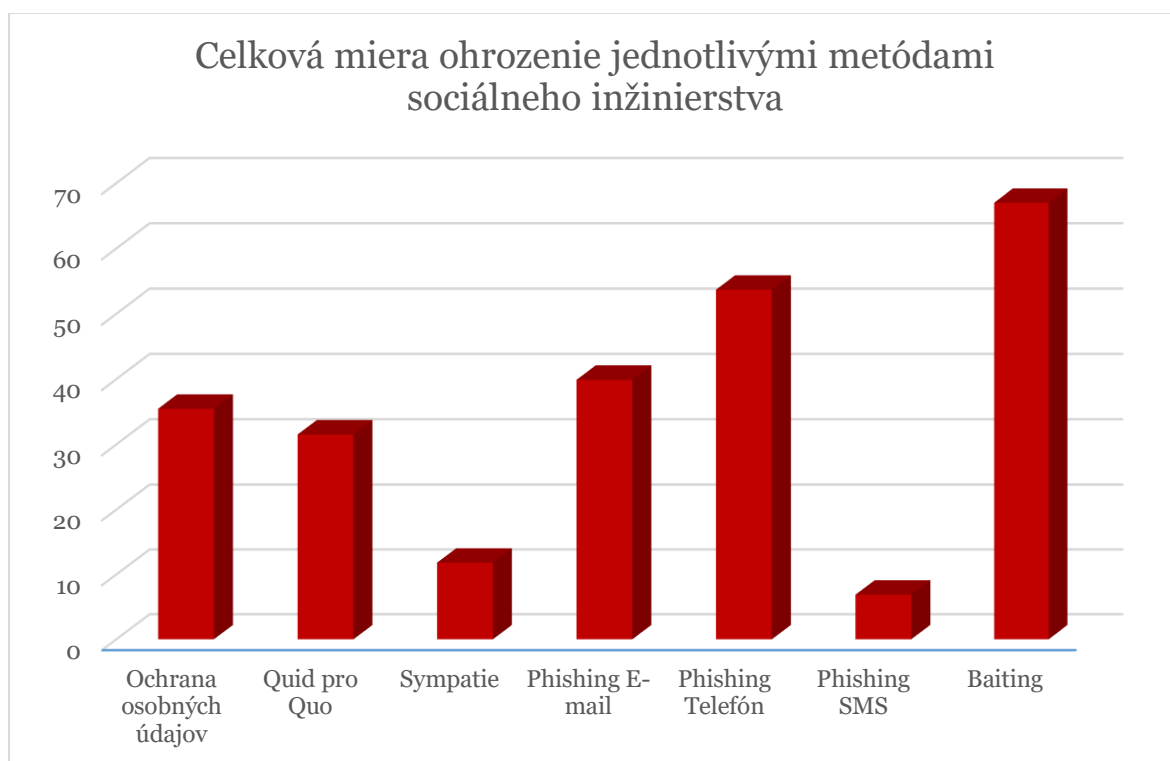
H5: Najúspešnejšou metódou z pohľadu útočníka je phishing rozosielaný e-mailom.

Z celkového vyhodnotenia všetkých odpovedí respondentov všetkých kategórií som spracoval Tabuľka 5 Celková miera ohrozenia jednotlivými metódami sociálneho inžinierstva. Sú v nej uvedené percentuálne hodnoty rizikových odpovedí na jednotlivé otázky. V prípade, že k niektorej metóde sociotechnického útoku sa viaže viac otázok, pracoval som s priemerom počtu rizikových odpovedí určenom pri započítaní všetkých odpovedí z týchto otázok.

Kvôli prehľadnosti vyhodnotenia prieskumu rizikovosti jednotlivých metód uvádzam aj pri tejto hypotéze graf na Obr. 5 Celková miera ohrozenia jednotlivými metódami sociálneho inžinierstva.

Tabuľka 5 Celková miera ohrozenia jednotlivými metódami sociálneho inžinierstva

Metóda	Ochrana osobných údajov	Quid pro Quo	Sympatie	Phishing E-mail	Phishing Telefón	Phishing SMS	Baiting
Priemer počtu rizikových odpovedí	72	64	24	81	109	14	136
% rizikových odpovedí	35,47	31,53	11,82	39,90	53,69	6,90	67,00



Obr. 5 Celková miera ohrozenia jednotlivými metódami sociálneho inžinierstva

Z výsledkov dotazníku je viditeľné, že moja hypotéza o najvyššom ohrození metódou phishingu odosielaného e-mailom nie je pravdivá. Ako najúspešnejšia metóda z pohľadu útočníka v celom rozsahu respondentov sa ukázala metóda baiting.

Záver

Vo svojej bakalárskej práci som spracoval tému sociálneho inžinierstva a sociotechnického útoku na jednotlivca. Po dôkladnej analýze rozhodovacieho procesu jedinca – podľa čoho sa rozhoduje a ako je možné jeho rozhodovanie ovplyvniť - som v súlade s teoretickými poznatkami vytvoril dotazník, ktorý som predložil dvesto trinástim respondentom. Následne som svoj dotazníkový prieskum vyhodnotil pomocou overenia správnosti piatich hypotéz, ktoré som si stanovil.

Moje predpoklady sa čiastočne potvrdili, ale čiastočne sa ich pravdivosť vyvrátila. Z výsledkov vyplynulo, že predpoklad o vysokej rizikivosti phishingu zasielaného prostredníctvom e-mailu u ľudí vo veku viac ako 60 rokov bol pravdivý. Táto metóda sociotechnického útoku je pre túto vekovú kategóriu najnebezpečnejšia.

Rovnako sa potvrdila platnosť hypotézy o tom, že správanie ľudí, ktorí nepoznajú princípy sociálneho inžinierstva je vo veľkej miere rizikovejšie ako správanie ľudí znalých metód sociotechnických útokov. Respondenti, ktorí sa už, aspoň v teoretickej rovine, stretli so situáciami z otázok si informácie a pokyny overovali, snažili sa chrániť svoje osobné údaje a bolo oveľa zložitejšie dostať ich do stresujúcej situácie, v ktorej by ich ostražitosť bola znížená

Naopak tretia hypotéza, ktorá predpokladá, že ľudia z menších sídiel sú dôverčivejší k ľuďom, ktorých osobne stretnú, sa nepotvrdila. Aj z grafického znázornenia zjavne vidno, že rizikovosť útoku osobným kontaktom nie je závislá od veľkosti bydliska obete vystavenej útoku. Je tomu oravdepodobne tak preto, že už ani ľudia žijúci na vidieku nemajú so svojimi susedmi a spoluobyvateľmi také blízke vzťahy. Aj na vidiek už prenikla vo veľkej miere tendencia chrániť si svoje súkromie a nezdieľať osobné informácie so svojím okolím.

Predpoklad, že medzi Slováckmi a Čechmi nie je žiadny výrazný rozdiel, sa potvrdil. Skutočne sa z odpovedí javí, že miera rizikivosti správania jednotlivcov nezávisí od národnosti – Česi aj Slováci odpovedali v podstate takmer rovnako.

Pri overovaní poslednej z mojich piatich hypotéz sa vyvrátil predpoklad, že najúspešnejšou metódou z pohľadu útočníka je phishing rozosielaný e-mailom. Z celkového súhrnu odpovedí všetkých kategórií respondentov na otázky ohľadne rôznych metód útoku vyplynulo, že najúspešnejšou metódou je Baiting.

Respondentov som rozdelil podľa rôznych kritérií do ôsmich rozličných členení. Toto rozanalizovanie odpovedí mi umožnilo vysloviť ďalšie zaujímavé závery:

- najnebezpečnejšia metóda pre ženy do 35 rokov žijúce vo väčších mestách je metóda Quid pro Quo
- pre mužov do 18 rokov s ukončeným základným vzdelaním je najnebezpečnejšia metóda phishing rozosielaný mailom

- Ľudia s minimálne vysokoškolským vzdelaním prvého stupňa, ktorí vykonávajú kancelársku prácu, sú celkovo najmenej náchylní podľahnúť sociotechnickému útoku.

Som si vedomý, že vzorka 203 platných odpovedí na dotazníkový prieskum nie je dostačujúca pre celkové zovšeobecnenie. Rovnako musíme brať do úvahy, že respondenti svoje odpovede často „prikrášľujú“ a keby sa reálne dostali do popisovanej situácie, správali by sa značne odlišne. Napriek tomu sú výsledky prieskumu uvedené v mojej bakalárskej práci podľa môjho názoru zaujímavé a užitočné – pre útočníka aj pre obeť sociotechnického útoku.

Informačná bezpečnosť a ochrana osobných údajov sú dnes veľmi aktuálnymi témami. S metódami a postupmi sociálneho inžinierstva by sa malo oboznámiť čo najviac osôb, ktorým záleží na bezpečnosti a minimalizácii rizika úniku osobných informácií v súčasnej modernej informačnej spoločnosti.

Výskum mojej bakalárskej práce som realizoval len na obmedzenej vzorke jednotlivcov, ale už aj podľa jeho výsledkov sa dá predpokladať, že tejto téme by bolo vhodné venovať viac času. Pokiaľ by sa podrobnejší a rozsiahlejší výskum realizoval v budúcnosti, jeho výsledky by stálo za to zapracovať napr. aj do učebných osnov na základných a stredných školách. Situácie spojené s ohrozením sociotechnickým útokom budú pre dnešných mladých ľudí bežnou súčasťou každodennej reality a preto by mali byť čo najlepšie pripravení. Ochrana osobných údajov už súčasťou učebných osnov je – ale zatiaľ sa nespája s pojmom sociálneho inžinierstva. V tejto oblasti vidím pre budúcnosť veľký priestor na pokračovanie v realizácii preventívnych programov zameraných na najrizikovejšie situácie sociotechnických útokov.

Použitá literatura

Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems. Indianapolis: IN: Wiley.

Allgeier, A., Byrne, D., Brooks, B., & Revnes, D. (1979). The Waffle Phenomenon: Negative Evaluations of Those Who Sift Attitudinally. *Journal of Applied Social Psychology*, stránky 170-182.

Bazerman, M., Curhan, J., & Moore, D. (2000). Negotiation. *Annual Reviews Psychology*, 279–314.

Brooks, I. (2003). Firemní kultura. Brno: Computer Press.

Cialdini, R. B. (2012). Vliv: Síla přesvědčování a manipulace. Brno: BizBooks.

Cialdini, R., Vincent, J., Lewis, S., & Catalan, J. (1975). Reciprocal Concession Procedure for Inducing Compliance. *Journal of Personality and Social Psychology*, 206-215.

Hadnagy, C. (2011). Social Engineerign: The Art of Human Hacking. Indianapolis, IN: Wiley publishing.

Hamilton, D., & Rose, T. (1980). Illusory correlation and the maintenance of stereotypic beliefs. *Journal of Personality and Social Psychology*, stránky 832-845.

Hayesová, N. (1993). Základy sociální psychologie. Praha: Portál s. r. o.

Hewstone, M., & Stroebe, W. (2006). Sociální psychologie. Praha: Portál s. r. o.

Hofling, C., Brotzman, E., Dalrymple, S., Graves, N., & Pierce, C. (1966). An Experimental Study in Nurse-Physician Relationships. *The Journal of Nervous and Mental Disease*, stránky 171-180.

Kahneman, D. (2011). Myšlení rychlé a pomalé. Příbram: Jan Melvin Publishing s. r. o.

Lachman, S., & Bass, A. (1985). A Direct Study of Halo Effect. *The Journal of Psychology*, 535 - 540.

Levine, M. (2005). Identity and Emergency intervention: How Social Group Membership and Inclusiveness of Group. *Personality and Social Psychology Bulletin*, 443-453.

Lun, J., Sinclair, S., Whitchurch, E., & Glenn, C. (2007). (Why) Do I think What You Think? *Journal of Personality and Social Psychology*, 957-972.

Malhotra, D., & Bazerman, M. H. (2008). Psychological Influence in Negotiation: An Introduction Long Overdue. *Journal of Management*, Vol. 34, stránky 509-531.

- McLeod, S. (2014). Maslow's hierarchy of needs. [online]. [cit. 28. marec 2019]. Dostupné na: <http://www.simplypsychology.org/maslow.html>
- Milgram, S. (1963). Behavioral study of obedience. *Journal of Abnormal and Social Psychology*, stránky 371-378.
- Mitnick, K. (2002). *Umění Klamu*. Helion.
- Sherif, M., & kol. (1961). *Intergroup conflict and cooperation: The Robbers Cave experiment*. University Book Exchange.
- Tajfel, H. (1982). *Social Psychology of Intergroup Relations*. *Annual Reviews Psychology*, stránky 1-39.
- Tajfel, H., & Turner, J. (1986). *The Social Identity Theory of Intergroup Behavior*. *Psychology of Intergroup Relations*.
- Teuscher, U. (2005). The effects of time limits and approaching endings on emotional intensity. *meetings of the American Psychological Society*.
- Tormala, Z., & Petty, R. (2007). Contextual contrast and perceived knowledge. *Journal of Experimental Social Psychology*, 17-30.
- Trivers, R. (1971). The Evolution of Reciprocal Altruism. *The Quarterly Review of Biology*, 35-57.
- Tversky, A., & Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference dependent model. *Quarterly Journal of Economics*.
- Vyskoč, J. (2004). *Není hacking jako hacking*. DSM – Data Security Management.
- The Social Engineering Framework* [online]. [cit. 28. marec 2019]. Dostupné na: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/?fbclid=IwAR22oaCMAcJfmc5RTSFzGKkMUPniKat3aEAu5AaGQ0x0T3SG_t2vKWGJQCY
- Social Engineering (Security)* [online]. [cit. 28. marec 2019]. Dostupné na: [https://en.wikipedia.org/wiki/Social_engineering_\(security\)#cite_note-1](https://en.wikipedia.org/wiki/Social_engineering_(security)#cite_note-1)
- Cost of Cyber Crime Study* [online]. [cit. 28. marec 2019]. Dostupné na: https://www.accenture.com/t20170926T072837Z_w_us-en/acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf