Univerzita Palackého v Olomouci

Fakulta tělesné kultury

Fakulta
tělesné kultury

KYBERNETICKÁ BEZPEČNOST U ŽÁKŮ ZÁKLADNÍCH ŠKOL

Diplomová práce

Autor: Bc. Jiří Odvářka

Studijní program: Ochrana Obyvatelstva

Vedoucí práce: Mgr. František Chmelík, Ph.D.

Olomouc 2022

Bibliografická identifikace

Jméno autora: Bc. Jiří Odvářka
Název práce: Kybernetická bezpečnost u žáků základních škol

Vedoucí práce: Mgr. František Chmelík, Ph.D.
Pracoviště: Institut aktivního životního stylu
Rok obhajoby: 2022

Abstrakt:

Diplomová práce pojednává o aktuálních celosvětových kybernetických hrozbách a způsobech napadení v kybernetickém prostoru. Výstupem je pochopení úzce profilované problematiky, která se týká získávání dat uživatele prostřednictvím nejnovějších metod. Práce v teoretické části si klade za cíl přehledně charakterizovat formy sociálního inženýrství a vsadit jej do aktuální doby. V praktické části se diplomová práce zaměřuje na dvě skupiny studentů, přičemž jedna skupina se účastnila školení kybernetické bezpečnosti a druhá nikoli. Výsledkem jsou informace týkající se potřeby zvyšování povědomí v kyberprostoru.

Klíčová slova: phishing, baiting, pretexting, kybernetická bezpečnost, anonymita, malware, sociální inženýrství

Bibliographical identification

Author: Bc. Jiří Odvářka

Title: Cyber security and primary school pupils

Supervisor: Mgr. František Chmelík, Ph.D.
Department: Institute of Active Lifestyle

Year: 2022

Abstract:

The diploma thesis deals with current global cyber threats and methods of attack in cyberspace. The output is an understanding of a narrowly profiled issue that concerns the acquisition of user data through the latest methods. The work in the theoretical part aims to clearly characterize the forms of social engineering and place it in the present time. In the practical part, the thesis focused on groups of students, with one group participating in two parts of the cyber security course and the other not. The output is information on the need to raise awareness in cyberspace.

Keywords: phishing, baiting, pretexting, cyber security, anonymity, malware, social engineering

Prohlašuji, že jsem tuto práci zpracoval samostatně pod vedením Mgr. Františka Chmelíka, Ph.D., uvedl všechny použité literární a odborné zdroje a dodržoval zásady vědecké etiky.

V Olomouc dne 25. května 2022

.....

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce Mgr. Františkovi Chmelíkovi, PhD. za odborné vedení, poskytnutí cenných rad a připomínek, které jsem využil při její tvorbě.

OBSAH

1 ÚVOD

Informační a komunikační technologie a s němi často spojovaná bezpečnost není pouze trend aktuální doby, ale také téměř nutnost každého jedince porozumět principům kybernetického prostředí.

Rychle rostoucí technologická doba do určité míry usnadňuje a zrychluje práci v každodenním životě, ale s ní se pojí i vysoké kybernetické trestné činnosti a následné riziko úniku dat, které mohou být pro většinu uživatelů klíčové. Vznikají nové typy zařízení a celosvětová síť internet se neustále zrychluje.

Není tomu tak dávno, kdy připojení k internetu bylo doménou pouze dospělých lidí a v domácnosti se vyskytoval pouze jeden tzv. „rodinný počítač“. Skokem se dostáváme do doby, kdy si prakticky nikdo nedokáže představit běžný den bez zařízení, které je permanentně připojeno k internetu.

Nejvíce ohroženou skupinou, která se může stát terčem počítačové kriminality nebo jakékoli kybernetické formy napadení v kyberprostoru jsou děti. Ty už prakticky považují připojený mobilní telefon jako úplnou samozřejmost.

Ve své bakalářské práci jsem dospěl k závěru, že běžná populace není ve využívání informačních a komunikačních technologií na úrovni, které vyžadují základní znalosti z oblasti kybernetické bezpečnosti. V tomto okamžiku chci navázat svou diplomovou prací v okamžiku, kdy mým výzkumným problémem bude srovnání dvou skupin uživatelů ve věku 14-15 let, kdy jedna ze skupin projde školením pro kybernetickou bezpečnost a úkolem je tedy zjistit, zda má školení v tomto bezpečnostním směru určitý smysl či nikoli.

Svět v éře Covid-19 se neúprosně přibližuje celkové digitalizaci různých aspektů života. Stále více jsme nuceni se spoléhat na počítačové systémy, díky kterým jsme schopni komunikovat, nakupovat nebo sdílet informace a mírnit tak dopad absence sociálního kontaktu.

2 PŘEHLED POZNATKŮ

2.1 Kybernetické prostředí

Pojmem kyberprostor (převzato z anglického *cyberspace*) se rozumí virtuální počítačový svět, který tvoří světovou počítačovou síť a je základním kamenem digitální komunikace. Je to „mainstreamové“ prostředí, prostřednictvím kterého nejčastěji komunikujeme, sdílíme a různými způsoby vyměňujeme informace všeho druhu, jako jsou i obchodní transakce nebo osobní data.

Termín kyberprostor poprvé použil v roce 1984 William Gibson ve své knize Neuromancer (1984):

„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita.“

2.1.1 Rozdělení kyberprostoru

V dokumentu Cyberspace Operations: Concept Capability Plan se kyberprostor rozděluje do třech vrstev:

1) Fyzická vrstva zahrnuje geografickou složku a fyzickou síť komponent. Geografickou složkou je myšleno konkrétní umístění síťových prvků ve fyzickém prostředí. Fyzickou síť komponent je pak myšlena infrastruktura, tedy kabely, síťové prvky a ostatní zařízení. Zatímco v kyberprostoru lze geopolitickou hranici překročit rychlostí blížící se rychlostí světla, tak v reálném světě existuje spousta omezení, která vyplývají z podstaty fyzického světa.
2) Logická vrstva sestává z komponent logické sítě, kterými jsou myšlena spojení síťových uzlů. Síťovými uzly se rozumí jakákoli zařízení připojená k počítačové síti.
3) Sociální vrstva je rozdělena na kyberosobnost a osobnost. Základním pravidlem je fakt, že jedna osobnost může mít více kybernetických osobností.

Jednodušší formou lze kyberprostor definovat jako celek, který se skládá ze služeb, dat, uživatelů a PC systémů, které se vyskytují ve virtuální prostoru. Hranice nejsou omezeny jako ve fyzickém světě, z čehož vyplývá, že nejúčinnější metodou je souhra státní

správy a bezpečnostních složek na mezinárodní úrovni, které jsou podporovány vývojáři informačních a komunikačních technologií.

2.2 Kybernetická bezpečnost

Dle *Itgoverance (2021)* je kybernetická bezpečnost aplikování technologií, procesů a kontrol k ochraně systémů, sítí, programů, zařízení a dat před kybernetickými útoky. Základní složkou kybernetické bezpečnosti je identifikace, vyhodnocování a realizace reakcí na bezpečnostní události a incidenty.

Dle serveru *vláda.cz* lze kybernetickou bezpečnost charakterizovat jako *celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována* ***bezpečnost informací.***

Pojem kybernetická bezpečnost se často zaměňuje s pojmem informační bezpečnost. Dle dokumentu *From information security to cyber security* se kybernetická bezpečnost a informační bezpečnost výrazně překrývá a tyto dva koncepty nejsou zcela analogické. Z dokumentu vyplývá, že kybernetická bezpečnost překračuje hranice tradiční informační bezpečnosti a zahrnuje nejen ochranu informačních zdrojů, ale i dalších aktiv, včetně člověka samotného. V kybernetické bezpečnosti má tento faktor další rozměr a tím je člověk jako potenciální cíl kybernetického útoku, a to včetně nevědomé účasti na kybernetickém útoku. Tento faktor má etické důsledky pro společnost, protože ochranu určitých zranitelných skupin, např. dětí, lze považovat za společenskou odpovědnost.

Vzhledem k celosvětovému rozvoji informačních a komunikačních technologií se dostávají tyto technologie do popředí a jsou terčem zpravodajských služeb po celém světě. Bohatý rozvoj technologií s sebou nese plnou řadu výhod, ale i sním spjatá rizika a stále nové hrozby, které jsou monitorovány právě bezpečnostními institucemi.

2.3 Kybernetická kriminalita (IT crime, cybercrime)

V posledních letech se kyberkriminalita stala jednou z nejrychleji rostoucích oblastí kriminality. Nové technologie přináší nové příležitosti právě v oblasti kyberkriminality a stávají se stále sofistikovanějšími. V důsledku toho se jednotlivci, korporace i vlády ocitají tváří v tvář mnoha hrozbám kybernetické kriminality, které začínají na nejjednodušším způsobu narušení soukromí a sahají až po různé typy hackingu či ransomwaru.

Někteří z kybernetických útočníků páchající tyto trestné činy používají tzv. DeepWeb, ke kterému běžný uživatel nemá přístup a často nemá zdání o jeho existenci. O samotné téma DeepWeb jsem se zajímal ve své bakalářské práci, kde jsem na základě dotazníkového šetření dospěl k závěru, že téměř 87 % respondentů DeepWeb nenavštívilo a z toho 74 % nemá tušení o významu DeepWebu.

Důvodem je separace tzv. SurfaceWebu („všem známé WWW – World Wide Web“) a DeepWeb, kde právě druhý jmenovaný není přístupný z mainstreamových vyhledávačů jako je Google, Seznam, Bing a další.

Pro přístup do DarkWebu (místní část DeepWebu, kde se vyskytuje ohnisko nelegálních činností) je zapotřebí specializovaný nástroj se sofistikovanými technikami směrování a šifrování, kde nejznámější z nich je prohlížeč tzv. Tor. Na tomto místě kyberzločinci provádějí nelegální elektronické obchody (e-commerce), tvz. „praní“ špinavých peněz, prodávají kompromitované bankovní informace nebo tvorba různých programů (malware) využívající metody sociálního inženýrství.

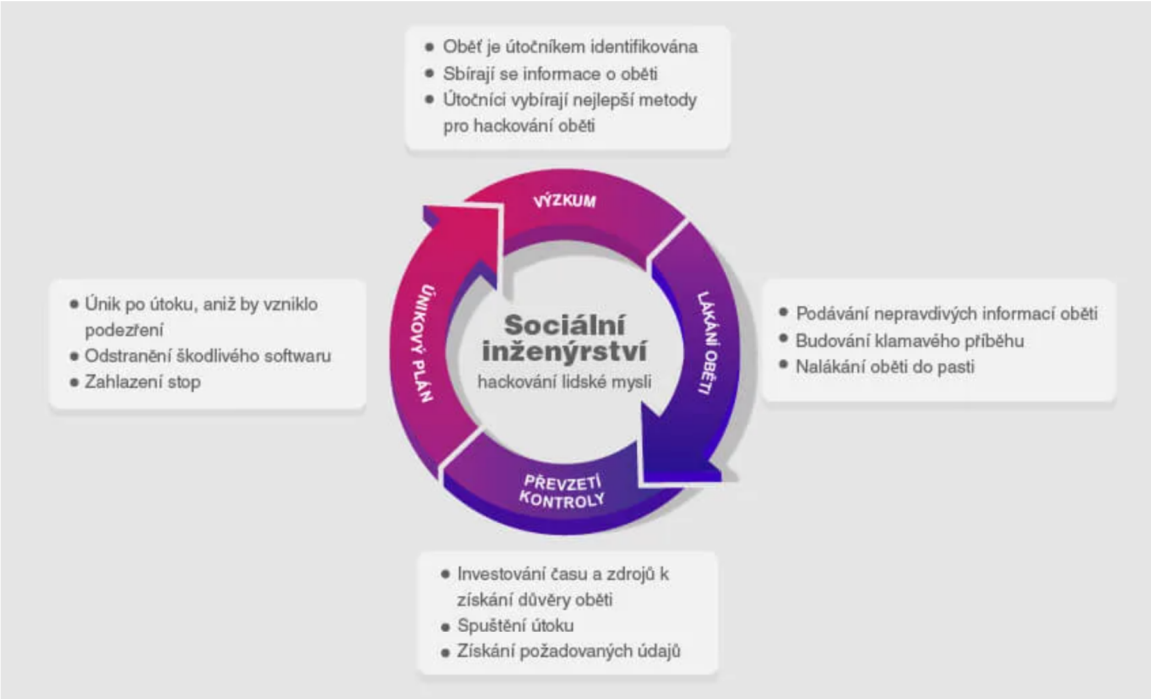
2.4 Sociální inženýrství

Sociální inženýrství je termín, který je nejčastěji užíván pro manipulační techniku, která využívá lidské chyby a tím získání určitých informací. Nejedná se tedy o překonávání technických prostředků, ale o samotného uživatele. Neinformovaní a nezkušení uživatelé jsou cílem těchto bezpečnostních incidentů, avšak úspěšné útoky postihují i odborníky v oblasti IT. Dle serveru *safetydetectives.com* bylo v roce 2018 toto číslo na hodnotě 83 procent.

Útočníci využívají vysoce sofistikované metody, které se vyvíjí ruku v ruce s nejnovějšími technologiemi. Ani kryptoměny hýbající světem se těmto typům útoků nevyhnuly. Nebezpečná a zároveň nejrozšířenější forma, která vešla do povědomí má název phishing, která vychází ze způsobu lidského rozhodování. V psychologii též známá jako kognitivní chyba úsudku a této metodě se budu více věnovat v pozdějších kapitolách. Útočník využívající techniky sociálního inženýrství se nazývá sociotechnik. Útočníci používají jak online, tak offline nástroje k tomu, aby přiměli nic netušící uživatele ke kroku, který ohrožuje jejich bezpečnost.

Podle zprávy The Human Factor od společnosti *Proofpoint* z roku 2019 využívá celých 99 % kybernetických útoků techniky sociálního inženýrství, aby uživatele donutilo k instalaci malwaru.

Obrázek 1. Sociální inženýrství



Zdroj: safetydetectives.com

2.5 Typy útočníků a lokace

Kybernetičtí útočníci jsou útočníci útočící na počítačový systém. Je důležité vědět, kterému typu útočníka uživatel čelí a podle toho také jednat a připravit se na něj. Důležitým parametrem je také taxonomie útočníků dle motivace. Tím se dá minimálně teoreticky odhadnout, čeho může být útočník schopen a někdy i doba trvání útoku. Také lokace útočníka hraje významnou roli, která je pro útočníka z pohledu logické lokace daleko přijatelnější a otvírá více možností k útoku.

Existují také různé programy, které dané kroky automatizují a není zapotřebí přítomnost fyzického útočníka. Často se jedná o uživatelsky přívětivé programy, které jsou jednoduché k nastavení a lze díky nim napáchat velké množství škody. Jedná se o nástroje útočné, které nejsou v kybernetickém prostoru novinkou, ale slouží „testerům“ pro kontrolu bezpečnosti a náchylnost k napadení konkrétních systémů. Nyní si své místo našly i v nelegálních činnostech. Prostřednictvím různých serverů lze daný program stáhnout volně bez jakéhokoli ověření či platby a útočníkem se tedy může stát prakticky kdokoliv.

2.5.1 Typy útočníků

V kybernetickém prostoru existují různé typy útočníků, ale já se zaměřím na první tři nejrozšířenější typy, kteří mají různé schopnosti, pomocí kterých útoky realizují. Jsou jimi boti, amatéři, hackeři a profesionálové. S každým typem útočníků se může běžný uživatel dostat relativně snadno do kontaktu.

2.5.1.1 Boti

Jedná se o sofistikovaný počítačový program, který má za úkol nejčastěji sběr dat. Častokrát běží na předem uzpůsobených serverech s nepřetržitým provozem a má jasně definovanou automatizaci.

2.5.1.2 Amatéři

Jedná se o fyzické osoby tvořící především „technologické nadšence“, kteří jeví zájem o danou problematiku. Je to nejpočetnější skupina útočníků a považuje se za nejméně nebezpečnou. Prostřednictvím webových stránek na internetu je pro většinu uživatelů jednoduché se s daným útočným programem seznámit a základní funkce aktivovat. Přispívají tomu také čím dál více rozšířená „tutoriálová“ videa a textové návody, které jsou k dispozici v různých jazycích častokrát včetně češtiny. Mnohdy pouze zkouší, zda jejich nabyté informace lze reálně využít u vhodné příležitosti. Je znám případ, kdy student střední školy využil tuto metodu pro získání informací o připraveném testu od učitele. Dostáváme se tedy na hranici nelegálního jednání, které si student často nemusí uvědomovat.
Předcházet tomuto způsobu napadení lze relativně snadno. Základní princip spočívá v dodržování kyberbezpečnostních zásad, kterým se budu dále věnovat v následujících kapitolách.

2.5.1.3 Hackeři

Jedná se o nejnebezpečnější skupinu, která má vysoce odborné znalosti v oblasti výpočetní techniky a její efektivní využití. Většinou se jedná o studenty informačních technologií nebo programátory, kteří přesně rozumí dané problematice a funkcionalitě každého kroku. Dokážou principiálně nastavit tzv. „ohýbání“ útočných metod pro své potřeby.

2.5.1.4 Profesionálové

Poslední skupinou, kterou zde uvedu jsou počítačoví profesionálové. Charakterizují je bohaté zkušenosti z praxe. Cílený záměr vykonávají jak samostatně, tak v organizovaných skupinách. Motivace k provedení činnosti se různí. Nejčastěji sem patří různé vládní organizace, které mají jasně definovaný cíl a různé světové tajné služby. Jejich technologická vybavenost je na nejvyšší úrovni, možnosti bývají často neomezené.

Pro běžného uživatele je ovšem velice malá pravděpodobnost, že na útočníka/y tohoto typu narazí, protože se jedná o nezajímavý cíl a zaměřují se na hodnotné cíle. Valné většiny uživatelů se tato skupina prakticky netýká, ale zmíněna je zde především z toho důvodu, aby jedinci věnující se kybernetické bezpečnosti nezískali pocit absolutního bezpečí.

2.5.2 Lokace útočníků

Podstatnou roli v přístupu ke sdíleným prostředkům hraje také odlišná fyzická a logická lokace. Základním principem je informace, která nese, kdo má kde, jaký přístup k počítačovým sítím. V tom spočívá variabilita a komplikace útoků.

2.6 Kybernetická bezpečnost za éry Covid-19

Je evidentní, že dnešní svět je naprosto odlišný od toho, ve kterém jsme žili před pár lety. Pandemie Covid-19 přinesla doslova „vlnu“ změn, která ovlivňuje všemožné aspekty našeho života. Ani kybernetická bezpečnost těmto změnám neunikla a vznikly nové „příležitosti“, které jsou útočníky často napadány. Například postupný přechod na tzv. „home office“ otevřel nové příležitosti různým typům útočníků. Je to nejistota a strach populace, která přináší nové příležitosti pro kybernetické zločince, kteří využívají formy jako phishing nebo různé druhy malwaru (ransomware a další).

Dle serveru *Comparitech* jsou kybernetické útoky řazeny do vzorců, které po určitou dobu zachovávají svůj trend. Ale vzhledem k neustále se vyvíjejícímu technologickému vývoji, ani studie z roku 2019 nevykreslují přesný obraz hrozeb, kterým čelíme nyní. Existuje naštěstí několik serverů, které zhodnocují současnou situaci, aby se populace mohla do jisté míry připravit na postpandemické kybernetické prostředí.

Podle Emanuela Cleavera hovořící na *House meeting on illegal digital activities* byl zaznamenán v online kriminalitě do června 2020 až 75% nárůst denních kybernetických útoků od začátků pandemie. Nejedná se ale o nejvyšší nárůst v průběhu roku. Na úplném začátku pandemie se kybernetická kriminalita zvýšila čtyřnásobně.

V srpnu 2022 byla publikována zpráva společnosti Malwarebytes (2022) o reportu, kde pětina dotázaných společností na otázky o kybernetické bezpečnosti přiznala, že došlo k narušení bezpečnosti, které bylo důsledkem akcí zaměstnance pracujícího z domova.

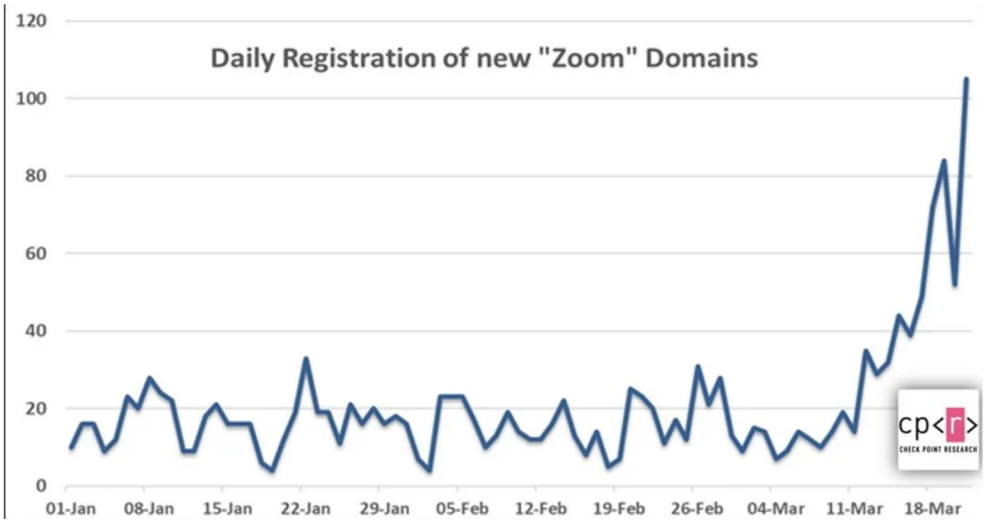
Tento výsledek není natolik překvapivý, protože 18 % dotázaných organizací uvedlo, že jejich zaměstnanci nepovažují kybernetickou bezpečnost za prioritu. Následných 5 % organizací považuje své zaměstnance za bezpečnostní riziko z důvodu ignorování kyberbezpečnostních praktik.

The UK's Action Fraud National Fraud & Cyber Crime Reporting Centre sleduje počet podvodů souvisejících s Covid-19. Do února 2021 zjistila, že bylo hlášeno více než 6000 případů podvodů kybernetické kriminality související s pandemií, přičemž oběti přišly o 34,5 milionu liber. Do července 2020 byla přitom tato částka na třikrát menší hodnotě.

Platforma Zoom pro videokonference se v době koronavirové stala bezesporu jedna z nejpopulárnějších. Snaha společnosti *Zoom Video Communications* o co největší flexibilitu využití při videokonferencích za doby pandemie nesla s sebou i četná rizika.

Kladení menšího důrazu na bezpečnostní záplaty a méně kvalitní zálohy. Přesně to byl důvod, proč se do poloviny dubna roku 2020 objevily k prodeji na DarkWebu podrobnosti o 530 000 účtech platformy Zoom. Dalším krokem útočníků na platformě Zoom byl mimořádně velký počet registrací s falešnými údaji s vidinou škodlivých útoků přes tuto platformu.

Obrázek 2. Počet registrací Zoom



Zdroj: Bleepingcomputer

Dle společnosti Microsoft se každou 1 vteřinu na celém světě odehraje 921 hackerských útoků, přitom až 98 % z nich jde předejít pomoci několika relativně jednoduchých kroků, kterým se budu dále věnovat.

Společnost ESET uvádí, že rok 2020 se nesl ve znamení „krádeže identity“. Tento rok vznikla řada podvodných inzerátů, které se týkaly „výhodné“ nabídky půjčky a v České republice probíhá následovně:

Člověk požadující půjčku, odepíše na inzerát s žádostí o půjčku. Podvodník si následně vyžádá osobní údaje, které uživatel pošle a vzápětí následuje požadavek o vyfocení občanského průkazu s obhájením, že se jedná o kontrolu, zda dotyčný není v exekuci. Pak už dochází ke kroku, kdy po uživateli podvodník vyžaduje odeslání 1 Kč na „ověřovací účet jeho společnosti“ s konkrétním variabilním symbolem, aby bylo zřejmé, že platbu odeslal konkrétní uživatel. Ve skutečnosti se ale „rozběhl za oponou“ neuvěřitelný sled událostí. Podvodník využil dokladů, zaslal je bance a založil si účet na dané jméno. Aby banka mohla účet aktivovat, tak požaduje právě aktivační platbu 1 Kč se specifickým variabilním symbolem, pomocí které potvrdí, že si účet zakládá tento skutečný člověk. Podvedený uživatel si myslí, že zasílá platbu někomu, kdo mu bude posílat na účet půjčku. Ve skutečnosti ale posílá platbu bance, která právě založila účet na jméno daného uživatele a podvodník k němu má kompletní přístup. Podvedený nemá zdání, že na něj nějaký účet vznikl a půjčku žádnou nedostane, protože žádná neexistuje.

Jde tedy čistě o zneužití osobních údajů, protože tento „digitální otisk“ má skutečně obrovskou cenu a mnoho lidí nemá ponětí, jak důležité může být své osobní údaje držet v soukromí.

Zdroj: Finex

2.7 Sociální inženýrství je jeho metody

2.7.1 Phishing

Phishing je typ útoků sociálního inženýrství, který se nejčastěji užívá k odcizení uživatelských dat (přihlašovací údaje, čísla kreditních karet aj.). Může k němu dojít např. když útočník, který se vydává za důvěryhodnou entitu, naláká oběť k provedení žádoucích kroků (otevření přílohy e-mailu, www odkazu nebo různých aplikací, nejčastěji s příponou „.exe“). Následující interakce aplikuje škodlivý kód, který provede předpřipravenou automatizovanou činnost, která může vést k instalaci malwaru, zamrznutí systému nebo např. úniku uživatelských dat.

Útok může mít kritické následky, které mohou vést k neoprávněným nákupům, krádežím finančních prostředků nebo krádeži identity.

Mimo jiné se phishing často používá v podnikových či vládních sítích jako součást většího útoku, tzv. APT (Advanced Persistent Threat, pokročilá perzistentní hrozba). Reálně se jedná o typ síťového útoku, při kterém je vytýčen konkrétní cíl a použití pokročilých technologií se analyzuje a monitoruje po dobu týdnů, měsíců nebo i několik let. Tento útok často končí až v momentě, kdy se dosáhne požadovaného výsledku nebo k neúspěšnému výsledku. Málo kdy tento útok končí předčasně.

Dle serveru *mobilizujeme.cz* přišla společnost ESET, která se zabývá kybernetickou bezpečností s aktuální statistikou pro květen roku 2022. Ta obsahuje data, která udávají, že od začátku roku 2022 byl v porovnání s rokem minulým, nárůst phishingových útoků až o neuvěřitelných 440 %. Útoky se nevyhýbají žádným sférám, kde dle serveru *it-market.cz*

tvoří největší část útoky proti finančnímu sektoru (23,6 %). Hned v závěsu jsou útoky proti webmailu a poskytovatelům softwarových služeb. Oproti roku předešlému se také zvýšil útok na kryptoměnové burzy.

2.7.1.1 Phishing a kryptoměny

Společnost Avast software s.r.o provedla roku 2021 analýzu, která byla zaměřena na kryptoměnové podvody. Z analýzy vyplývá, že nejčastějšími cíli „krypto-podvodů" jsou jednoznačně USA, Brazílie a Nigérie. Ve velké míře se však vyskytují podvody také ve Velké Británii, Rusku, Francii a také v Česku.

Dle *Finex* (2022) jsou kryptoměny elektronicky tvořené digitální měny, které mají reálnou hodnotu danou nabídkou a poptávkou, která dlouhodobě lineárně roste. K roku 2021 se udává 100 milionů uživatelů kryptoměn na celém světě. Tím se kryptoměny stávají ve světě velice zajímavým terčem kybernetické kriminality. Kryptoměny se dají jednoduše charakterizovat jako číslo v databázi, ale záleží pouze na každém uživateli, jak svoje kryptoměny zabezpečí.

Na začátek je důležité říct, že existuje několik způsobů, jak ukládat kryptoměny. Jedná se o správcovské peněženky, softwarové peněženky, papírové peněženky a hardwarové peněženky.

2.7.1.1.1 Správcovské peněženky

Tento typ peněženky je spravován další entitou. Tou může být například kryptoměnová burza. Princip fungování správcovské burzy by se dal přirovnat tradičnímu bankovnímu učtu, kam má uživatel po autorizaci přístup a může své prostředky spravovat. Výhodou této peněženky je částečné zabezpečení, které náleží poskytovateli služby a uživateli dává určitou záruku a pojištění. Jedná-li se o podvodnou nebo služba zkrachuje, tak o své finanční prostředky uživatel může přijít.

Důležité je brát v úvahu, že se jedná o účet, jako každý jiný a jeho autentifikace je chráněna jen do takové míry, v jaké ji uživatel sám chrání. Právě zmíněný phishing je nejčastějším způsobem napadající správcovské peněženky. Pro příklad uvedu kryproměnovou burzu Binance, sídlící na Maltě a dle serveru *entuzio.cz* se jedná o největší a zároveň nejrychleji rostoucí burzu na světě. Útočníci vytvoří falešný web, připomínající onu zmíněnou kryptoburzu Binance, která se liší od originálu na první pohled pouze malými detaily.

Může se často jednat pouze o podobné typy fontů písma, mírně odlišné odstíny barev, ale základním rozdílem je jiná URL adresa, která je pro rozpoznání phishingových podvodů klíčová.

2.7.1.1.2 Softwarové peněženky

Jedná se o typ aplikace spravující soukromé klíče majitelů kryptoměn. Výhodou softwarových peněženek je jejich uživatelská přívětivost a přehled nad svými kryptoměnami. Slabou stránkou této metody uchování prostředků je riziko napadení zařízení, z kterého peněženku uživatel spravuje. Častým typem útoků u této metody je ransomware, který inicializuje peněženku formou zašifrování a pro jeho dešifrování vyžaduje výkupné. Dalším riziko představuje také škodlivý kód (Trojský kůň), který si do systému zavede tvz. backdoor (zadní vrátka), pomocí kterého se do systému mohou proniknout další útočníci.

2.7.1.1.3 Papírové peněženky

Nejjednodušší řešení představuje forma fyzické papírové peněženky, která nemá svou digitální podobu a uživatel si svůj unikátní klíč musí zapsat fyzicky. Velkou výhodou je jeho finanční nenáročnost a žádné riziko kybernetického napadení. Riziko představuje zapomenutí, ztráta nebo krádež papíru.

2.7.1.1.4 Hardwarové peněženky

Za zcela nejbezpečnější metodu se považují hardwarové peněženky. Jedná se o samostatný fyzická zařízení, nejčastěji USB klíčenky, které v sobě nesou zašifrovaný unikátní kód ke kryptoměnám. Často se k hw peněženkám dodává tvrzená ocelová tabulka, pro případnou obnovu, která odolá žáru. Jedinečný klíč je třeba do tabulky vyřezat. Výhodou hw peněženky je vysoká bezpečnost a „prolomení“ takového zabezpečení jsou schopni pouze profesionální hackeři za předpokladu dlouhodobého fyzického přístupu. Lze tedy předpokládat, že i po ukradení USB klíčenky zbývá dostatek času k tomu, aby kryptoměny pomocí unikátního kódu zaznamenaného na tvrzené ocelové tabulce byly přesměrovány a unikátní kód znehodnocen. Je zde vysoká pravděpodobnost že i po ztrátě hw peněženky zůstanou kryptoměny netknuté, protože se jedná o poměrně bezpečnou variantu. Nevýhodou je vyšší pořizovací cena.

Obrázek 3. HW peněženka Ledger

Zdroj: The Crypto Pavilion

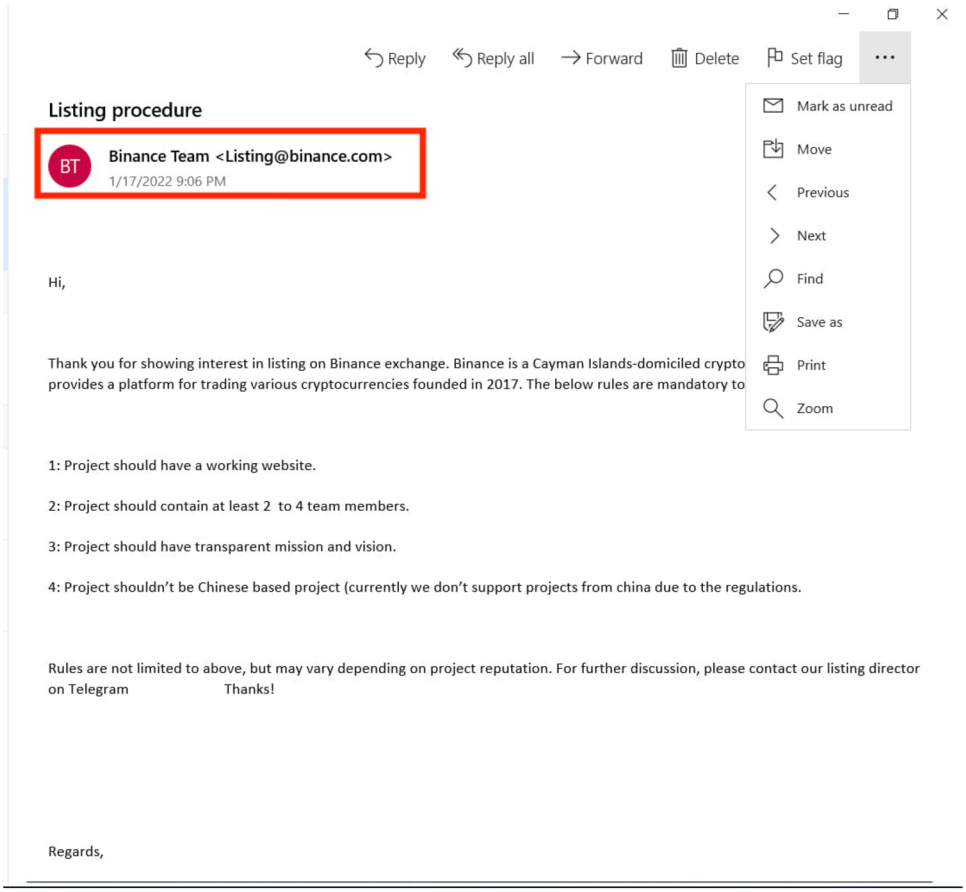
2.7.1.1.5 Phishing kryptoburzy

Příklady pochází přímo ze serveru *Binance.cz* a nachází se v sekci „support“, jedná se tedy o bezpečnostní tipy pro klienty této platformy.

2.7.1.1.5.1 Příklad č.1

Tento phishingový e-mail má za úkol vzbudit dojem, že se jedná o oficiální upozornění od služby Binance. Ačkoli je doména legitimní, nejedná se o e-mail, který by této burze patřil a byl odeslán z oficiálního e-mailového serveru.

Obrázek 4. Phishing příklad 1



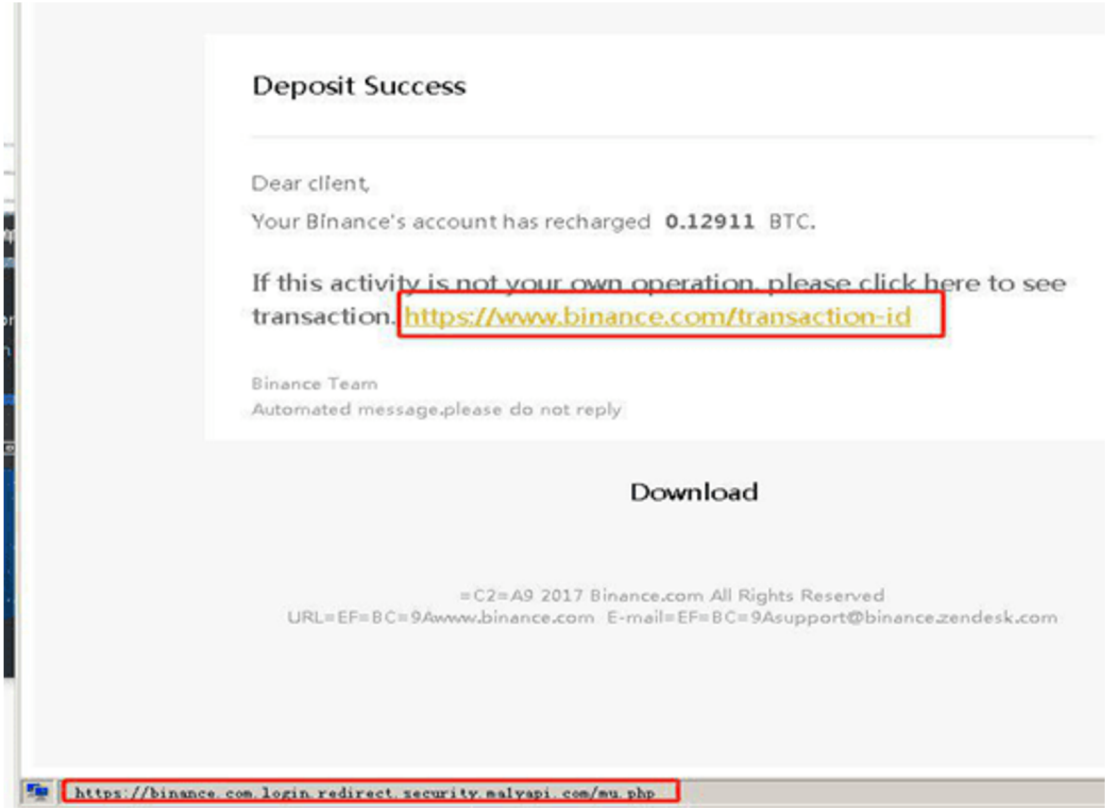
Zdroj: Binance

Phishingový e-mail přesvědčuje uživatele, aby na platformě Telegram kontaktoval falešné pracovníky platformy Binance. Následuje žádost o vložení kryptoměny na jeho blockchain (repozitář kryptoměň). U těchto typů e-mailů zpravidla bývá obsažený velký počet příliš pozitivních zpráv (může se jednat o levné nabídky tokenů nebo i rozdávání kryptoměn).

2.7.1.1.5.2 Příklad č.2

Tento phishingový e-mail nabádá uživatele, aby kliknul na škodlivý odkaz, po kterém má dojít k získání 0,129 BTC. Dá se očekávat, že po rozkliknutí se aktivuje škodlivá webová aplikace, která bude schopna při nejmenším monitorovat kroky uživatele nebo bude následovat žádost o přihlášení do falešného webového portálu Binance.

Obrázek 5. Phishing příklad 2

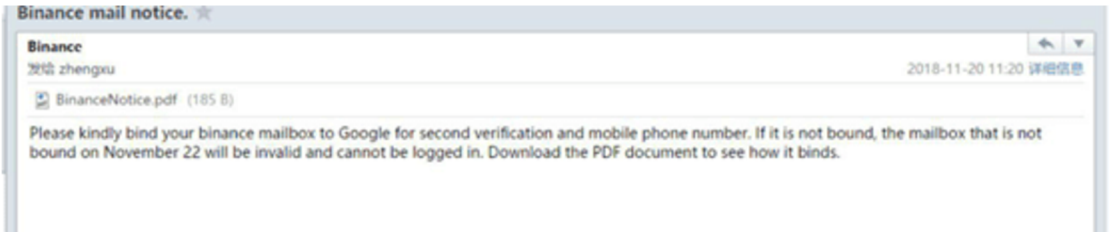


Zdroj: Binance

2.7.1.1.5.3 Příklad č.3

Tento typ e-mailu nabádá uživatele ke stažení škodlivého souboru ve formátu PDF, který obsahuje malware. Často lze e-mail rozeznat i na základě struktury, rozvržení textu, nespisovného jazyka nebo gramatických chyb.

Obrázek 6. Phishing příklad 3



Zdroj: Binance

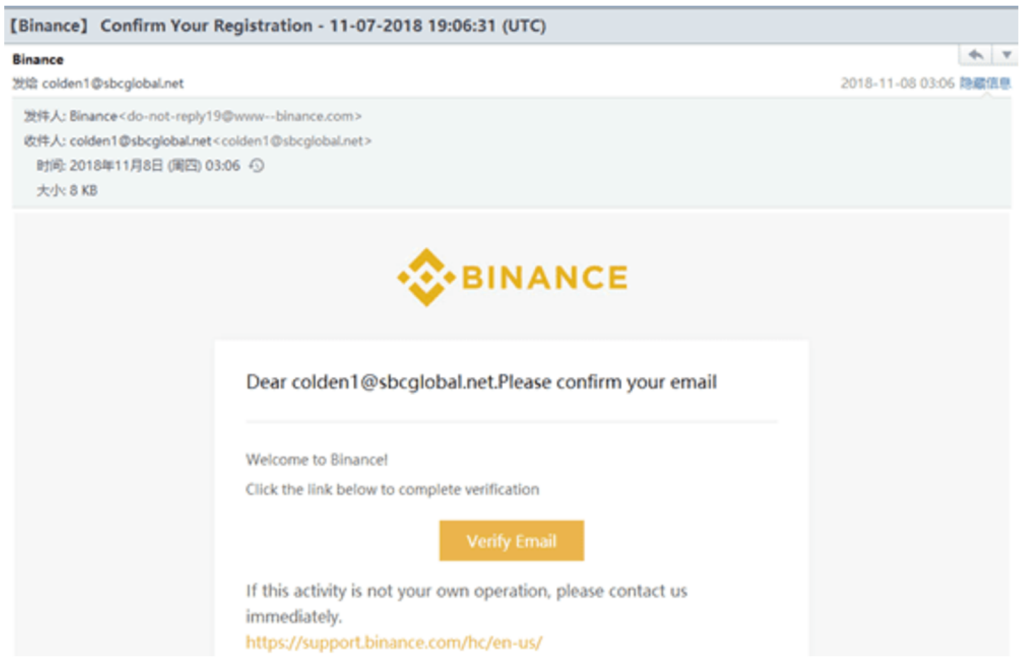
2.7.1.1.5.4 Příklad č.4

Poslední varianta, kterou zde uvedu, je považována za nejpočetnější. Jedná se o typ e-mailu, který útočník vytvořil se záměrem získat přístup ke skutečnému e-mailovému účtu, heslu a záložnímu klíči pro dvoufaktorové ověření.

Pod logem Binance se nachází e-mail cíleného uživatele, který má nabýt dojmu, že se jedná o ověření jeho vlastního Binance účtu. Ve vyobrazeném políčku odesílatele se nachází sice Binance doména, ale nepřesná.

Tento phishingový útok byl odeslán z do-not-reply19@www--binance.com, která používá podobnou doménu. Jedná se o nejčastější způsob, kterými se snaží útočníci vydávat za danou platformu.

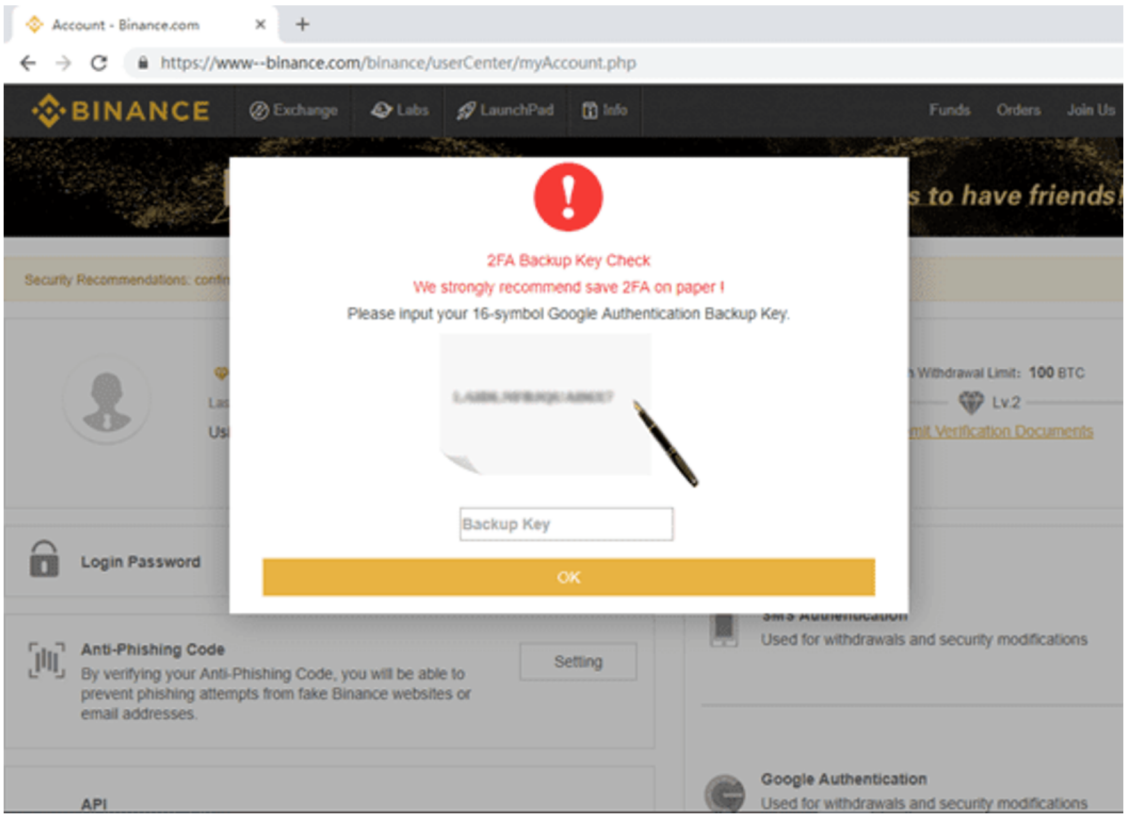
Obrázek 7. Phishing příklad 4



Zdroj: Binance

Po následné interakci na tlačítko „Ověřit e-mail“ si lze všimnout podvodné URL adresy, která je https://www--binance.com/binance/login.php. Nepozorný či nezkušený uživatel vyplní své přihlašovací údaje pro oficiální Binance účet a útočníkovi se do databáze uloží potřebná data, s kterými může dále interagovat.

Obrázek 8. Phishing příklad 4



Zdroj: Binance

Pokud uživatel využívá dvoufaktorové ověření, web jej požádá o záložní klíč a tím se provedl poslední nezbytný krok, pro přihlášení. Z podstaty věci se web přesměruje do „hluchého místa“, odkud dále nelze pokračovat. Útočník získal všechny potřebné informace.

2.7.1.1.6 Jak rozpoznat phishing?

- Phishingový e-mail často postrádá specifické oslovení a obsahuje pouze obecný pozdrav. Organizace při komunikaci se svými klienty totiž často nastaví e-mail tak, aby obsahoval oslovení jména.
- Osahuje zvláštní nebo chybný pravopis
- Nutná kontrola URL adresy (link by měl směřovat na oficiální stránky organizace)

2.7.2 Pharming

Pharming je technologicky pokročilejší forma phishingu. Zadáním webové adresy přesměruje uživatele na falešnou webovou adresu, která je vzhledově podobná (mnohdy nerozpoznatelná) od originální. V důsledku tohoto mohou být jakékoli informace poskytnuté na falešném webu, jako jsou např. čísla účtů nebo hesla, odcizeny. Princip spočívá v napadení DNS serveru a nahrazení IP adresy alternativní adresou. Dle Kaspersky, 2021 je 83 % případů napadení formou pharmingu zaměřeno na finanční sféru.

Dle portálu Lupa má pharming dvě podoby. První podoba je značně efektivní, avšak pro útočníka velice obtížná, což omezuje její užití. Druhá podoba je pro útočníka jednodušší, nicméně také s nižší spolehlivostí. Pharming je způsob napadení DNS serveru (seznam internetových domén a daných IP adres). Podaří-li se útočníkovi jednu z cílených adres změnit (typicky internetové bankovnictví), po zadání potřebné adresy do prohlížeče dostane uživatel alternativní webovou stránku, která je často vypracovaná natolik detailně, že ji téměř nelze rozeznat. „Zlatým pravidlem“ je kontrola URL adres, ovšem nyní se potýkáme s metodou, která svou adresu zachovává. Jsou tedy velmi malé šance, že uživatel na daný podvod příjde. Jedinou přijatelnou metodou uživatele je kontrola certifikátu pro šifrování dat. Ten není útočník schopen padělat, ale lze navodit pocit z pohledu uživatele, že bez podrobného průzkumu se zdá být vše v pořádku.

Druhou podobu lze nazvat jako „lokální pharming“. V tomto případě útok neprobíhá přes DNS server, ale je cíleno na konkrétní PC s operačním systémem Windows. Ten obsahuje soubor „hosts“, který má stejný princip fungování, jako právě zmíněný server DNS, který obsahuje seznam IP adres a adekvátní domény. Podaří-li se útočníkovi v souboru provést změny a připsat adresu své falešné stránky (např. internetové bankovnictví), pak se jedná o stejný výsledek jako v případě předešlém. V praxi to znamená, že i po zadání korektní adresy URL se zobrazí alternativní stránka útočníka.

První metoda není závislá na cílových zařízeních, ale je zapotřebí „prolomit“ ochranu DNS serveru. Zároveň DNS servery tvoří páteřní sítě internetu, a tak jsou velice často vysoce chráněny. Jedná se tedy o způsob pro velice zdatné útočníky. Z toho důvodu se využívá především metoda druhá.

Druhá metoda vyžaduje přístup pro zápis dat do systému. Tedy e-mail nebo webová stránka touto funkcionalitou nedisponují. Přichází tak na řadu nejčastěji Trojský kůň, který často bývá maskován jako doplněk softwaru. Může být zaslán e-mailem v příloze, v odkaze

ke stažení nebo být přibalen u oficiální aplikace. Po úspěšné změně souboru „hosts“ následují výše zmíněné útoky.

Pokud tedy porovnáme obě výše zmíněné metody, kterými může útočník postupovat, tak v obou případech je zapotřebí uživatelská interakce a s patřičnou znalostí lze do jisté míry tomuto napadení předcházet. Z porovnání vychází, že pharming je nebezpečnější metoda než phishing a lze ní oklamat i zkušeného uživatele. Webové prohlížeče často obsahují nejrůznější formy ochran proti různým druhům kybernetických útoků, ale často není zaručena detekce, jelikož musí být web označen za škodlivý a tento proces často trvá příliš dlouho.

Ochrana proti pharmingu na úrovni DNS serverů není v moci uživatele, ale u lokálního napadení je důležitá prevence a sice antivirový program, který má pravidelně aktualizovanou databázi. Dochází ke kontrole jak elektronické pošty, tak stažených souborů z webu. Dojde-li k archivaci viru do souborů (rar, zip), antivirový program přichází na řadu v reálné době jeho extrahování.

2.7.3 Baiting

Jednou z jednodušších technik napadení zařízení je tzv. baiting. Spočívá v nastražení přenosného paměťového média (cd, flashdisk, paměťová karta), které najde oběť a z něj spustí škodlivý kód. Metoda spoléhá na zvědavost jedince.

Nebezpečí tkví už v pouhém připojení přenosného média a často není podmínkou přímé otevření souboru. Pro útočníka je výhodou finanční nenáročnost, kde platí pouze za přenosné médium a častokrát není zapotřebí ani to, jelikož spousta organizací jej rozdávají jako reklamní či propagační předměty.

Nejnáročnější částí této techniky je umístění média k oběti a následná motivace připojit jej k osobnímu zařízení. Lidská kreativita ovšem nezná mezí a útočníci přichází se stále novějšími a propracovanějšími způsoby, jak tíženého cíle dosáhnout. Originální médium může být prohozeno např. na pracovním stole, v restauraci, při skončení školení a chvíli nepozornosti nebo v pauze na oběd, záleží na dané situaci. Často má útočník možnost osobního kontaktu s cíleným zařízením a má možnost jej sám připojit.

Dle Passcamp (2021) je znám případ, kdy se útočník vydával za poctivého nálezce a následně jej ke svému osobnímu zařízení připojila část pracovníků firmy, po kterém byl malware schopen získat administrátorská oprávnění a odstartovat formátování všech dostupných disků.

Nejsilnější defenzívou odolávající baitingu je vzdělávání se a umění předvídat. Vzdělávání sebe i druhých je obecně nejsilnější obranou metodou proti sociálnímu inženýrství.

2.7.4 Quid Pro Quo

Nejvíce podobný tomuto způsobu je baiting. Pouze se zde využívá motivace oběti na finanční odměnu. Aktuální kryptoměnová éra tomuto způsobu podvodu jde čistě naproti, jelikož se na podvod s decentralizovanou měnou nelze odvolat na žádném úřadě.

Rozšířený je podvod v USA, který se týká správy sociálního zabezpečení (SSA) a její databáze čísel s kterými lze napáchat velké množství škody. Útočníci se vydávají za SSA zaměstnance, kteří fingují problém se svým pracovním PC a potřebují číslo jejich sociálního zabezpečení pro ověření identity, kde vzápětí dodají záminku, že je zapotřebí ověřit identita, jinak lze problém řešit pouze na pobočce. Obdoba tohoto podvodu zní podobně a sice „pomoc“ s požádáním o novou SSA kartu, ale jedná se čistě o krádež osobních údajů.

2.7.5 Tailgating

Jedná se o typ útoku, při kterém útočník sleduje autentifikovaný cíl, který má oprávněný vstup do systému. Při vstupu cíle do systému (např. autorizace zaměstnance do firemní sítě) sleduje útočník stejnou cestu a získá přístup do chráněné oblasti.

Zřejmě nejznámější případ se stal v roce 2020 o kterém informoval např. portál vas-hosting. Útok dostal název *Twitter Bitcoin Scam.* Útočníci získali přístup k interním nástrojům sociální sítě Twitter, čímž dostali možnost změnit jakýkoliv registrovaný e-mail a vyresetovat heslo k účtu. Napadeno bylo „pouze“ 130 účtů. Cíleně byly napadeny účty jako: Elon Musk, Kayne West, Joe Biden nebo Barack Obama. Dále byly účtu zneužity formou scamu, který obsahoval informace o slibu, kde každá částka přijatá v BTC bude zdvojnásobena a také tím daná osoba přispěje na charitu. Výsledkem bylo snížení akcií Twitteru o 4 % za den (snižování trvalo 8 dní) a pokuta pro útočníky ve výši 115 tisíc dolarů.

2.7.6 Pretexting

Jedná se podobnou metodu jako je phishing, ale více individualizovanou. Sociotechnik se více připravuje na konkrétní oběť formou jako jsou nejrůznější scénáře, které dopomohou z oběti dané informace vylákat. Po prvním kroku, kterým je vynucení interakce s obětí

přichází přesvědčení druhé strany, že k autorizace je zapotřebí více osobních informací (občanský průkaz, pas či jiný dokument). Jedná se tedy o krádež identity, která často bývá zneužita půjčkovými weby.

Od množství informací o dané osobě nebo organizaci se odvíjí možnosti zneužití. Typickým příkladem může být firma, která najímá externí síťovou bezpečnostní agenturu. Vydat se tedy za auditora a vstoupit fyzicky do soukromých prostor firmy není s potřebnými informacemi příliš potíž.

Phishingové útoky jsou využívány na základě strachu a určité naléhavosti, kterou útočník minimalizuje, protože zde působí sociální konformita, tedy přizpůsobení se při jednání pod tlakem.

Dle článku *Investice do prevence útoků a kontroly škod v kybernetické bezpečnosti* z roku 2016 vyplývá, že investice uživatelů a poskytovatelů softwaru jsou ve značeném nepoměru. Článek pojednává o vysokých investicích týkajících se kontroly škod, ale nedostatečnou prevenci útoků.

2.8 Anonymita

Návrh internetového prostředí se nenesl v duchu anonymity, ale funkcionality. K vzájemné komunikaci mezi zařízeními slouží IP adresy, které lze lokalizovat. Jako příklad může sloužit provider (poskytovatel internetového připojení), který všechny svoje zákazníky v databázi může snadno lokalizovat a analyzovat konkrétní IP adresy. Z mého pohledu je anonymita na internetu jednou ze základních důležitých znalostí moderního člověka. Myslím si, že každý uživatel by měl mít pojem o tom, jak se vyvarovat běžných chyb týkající se anonymity.

2.8.1 IP adresy a veřejná wi-fi

Komunikační uzly v domácnosti typu router mají schopnost sledovat tok dat v místní síti. Častokrát je využívána nejrychlejší a nejkratší cesta. Ke změně této cesty dochází pouze ve vynucených případech, a proto se stává tento uzel velice snadno odposlouchatelným. Je-li charakterizován datový tok a zdroj, lze odhadnout úmysl a zájem uživatele. Zvlášť nebezpečným místem pro internetové připojení jsou veřejná místa jako (restaurace, kavárny, škola aj.) a vybral jsem několik častých způsobů napadení na veřejné wifi síti.

2.8.2 Man-inThe-Middle Attack

Při přístupu k internetu přes wi-fi naváže zařízení spojení s routerem nebo serverem, který následně zařízení přiřadí IP adresu a připojí k internetu. K útoku Man-in-the-Middle dochází v moment, kdy se mezi uživatelské zařízení a nejčastěji směrovač (router) postaví útočník. Data prochází přes útočníka a „tečou“ dál. Reálně se dá charakterizovat útok jako monitoring toku dat s následným odfiltrováním potřebných informací, které jsou pro útočníka nějakým způsobem zajímavé. Kybernetičtí zločinci využívají specializovaný software pro „odposlech“ datového provozu.

Populární software nese název Wireshark a využívá se k analýze provozu v počítačových sítích (odstraňování problémů počítačových sítí, vývoj komunikačních protokolů nebo studium síťové komunikace). Své využití si našel i v kyberkriminálních činnostech, jako je právě zmíněný útok Man-in-the-Middle. Dostane-li se útočník na cílovou síť z které má zamýšlen odposlech, je schopný i méně zdatnější jedinec docílit tíženého výsledku s chvílemi samostudia. Silnou stránkou této metody je schopnost dešifrování autentifikačních serverů, ke kterým se uživatel přihlašuje za přítomnosti SSL certifikátu.

Zapotřebí jsou následující kroky:

1) Náhled do komunikace
   - Způsobů náhledu do komunikace existuje více, ale princip spočívá v nahrátí celé komunikace do souboru, kterému software dále rozumí.

2) Zachycení kryptografického materiálu
   - Součástí zisku dat jsou symetrické šifrovací klíče, které jsou u dané komunikace využívány.

3) Záznam provozu
   - Při záznamu provozu jsme schopni dešifrovat pouze ten obsah, ke kterému máme patřičné šifrovací klíče.

4) Dešifrování komunikace
   - Posledním krokem zbývá pouze kombinace kryptografických dat s dešifrovacími klíči.

- Při pokračování odposlouchávání provozu je veškerý obsah, ke kterému máme symetrické šifrovací klíče, v reálném čase dešifrován.

Princip analyzování datových paketů, tedy sledování provozu zařízení na síti se nazývá *sniffing*.

Jedná se tedy o velice účinnou metodu síťového napadení, prostřednictvím které je útočník schopen získat prakticky jakékoli informace jako jsou i citlivá data s přihlašovacími údaji nebo informace o kreditní kartě a následné finanční podvody.

2.8.3 Malware

Pokročilou technikou napadení je infikování wi-fi sítě malwarem. Po následném připojení uživatele k wi-fi síti malware infikuje zařízení. Někteří útočníci napadají samotný směrovač, který po připojení zasílá uživateli falešná vyskakovací okna s žádostí o aktualizaci softwaru, při kterém se malware po odsouhlasení nainstaluje.

Scénář dále pokračuje podle očekávání. Krádež citlivých informací, smazání souborů nebo i znefunkčnění zařízení. Zásadním problémem je pro uživatele anonymita malwaru, který je častokrát schopný se připojit k systémovému procesu, a tudíž se tváří jako legitimní pro operační systém.

2.8.4 Evil Twin Attacks

Do češtiny lze volně překládat jako „útok zlého dvojčete“. Obvzlášť nebezpečný typ útoku, při kterém kyberzločinec nastaví osobní nezabezpečený hotspot Wi-fi, který má jediný cíl, krádež uživatelských dat.

Základním pravidlem těchto útoků je získání věrohodného názvu a přimět uživatele se k síti připojit. Nejčastěji podle lokality vybírá kyberzločinec název, který se nese v blízkosti a s názvem známých podniků, jako jsou restaurace, kavárny nebo posilovny. Pro tuto techniku jsou charakteristické i útoky založené na serveru DNS, které jsem řešil v minulých kapitolách. Útočník nahradí adresu serveru adresou alternativní a uživatel nabyde dojmu, že se jedná o oficiální webovou stránku nebo je oběť donucena navštívit konkrétní napadenou nešifrovanou stránku.

2.8.5 Způsoby zabezpečení na veřejné síti

Zatímco pro bezpečnější veřejnou wi-fi nelze udělat mnoho, zabezpečit svá data lze hned několika způsoby. Nejlepší zabezpečení je být znalý a informován. S rychle rostoucím technologickým vývoj není snadné mít o všech nástrahách v kyberprostoru přesné povědomí, ale můžeme do určité míry dodržovat základní bezpečnostní pravidla jako:

2.8.5.1 Navštěvování pouze webových stránek s SSL certifikátem

Webové adresy jsou se zabezpečeným (https) nebo nezabezpečeným (http) připojením k webu. Ovšem webová stránka s SSL certifikátem (https) není zárukou bezpečného webu. Útočníci na svých webových stránkách také využívají SSL certifikáty, ale podle *Comparitech, 2022* jsou útoky značně redukovány, protože dešifrování informací na zabezpečených webových stránkách je i pro samotné administrátory náročnou činnosti a vyžaduje vyšší odbornou znalost v dané problematice. Oproti tomu web bez SSL certifikátu (http) má tu nevýhodu, že data jsou přenášena v prostém textu jako nám již známý útok Man-in-the-Middle při kterém by útočník dále nemusel vynakládat jakékoli další úsilí. Web *ITPro* provedl v první vlně Covid-19 průzkum, který poukázal na fakt, že dvě třetiny všechny napadených zařízení malwarem byly infikovány prostřednictvím šifrovaných připojení, načež z neznámých důvodů byla nejvíce zacílenou zemí Velká Británie.

Dle *ITPro* jsou nejbezpečnější veřejné sítě takové, které provádí v reálném čase kontrolu HTTPS pomocí tzv. strojového učení, prostřednictvím kterého dochází k pokročilé detekci hrozeb založené na chování uživatele.

2.8.5.2 Použití VPN

Stále větší popularitu nabývá tzv. VPN (Virtual Private Network – Virtuální privátní síť). Jedná se o software, který vytváří chráněné síťové připojení při využívání veřejných sítí. VPN dokáže šifrovat internetový provoz a také „maskovat“ online identitu. Šifrování probíhá v reálném čase a útočníkům značně komplikují monitoring online aktivity. VPN skrývá IP adresu uživatele tak, že dochází k přesměrování na speciálně konfigurovaný vzdálený server provozovaný VPN hostitelem. V praxi to znamená, že VPN se stává zdrojem dat a ISP (poskytovatel internetového připojení ani třetí strana nemá přístup, ke kterým internetovým stránkám uživatel přistupuje nebo která data odesílá a přijímá. Server *Entuzio* přichází

s testem nejlépe hodnocených VPN aplikací pro rok 2022, kde se na nejvyšších příčkách umístily produkty jako: NordVPN, PureVNP, CyberGhost VPN nebo ExpressVPN. Výběr hostingu klíčovou vlastností, kterou by měl uživatel poctivě zvážit, protože se na trhu vyskytují i takové VPN hostingy, které mají za cíl přesně opačnou funkci než s kterou ji uživatel pořizuje. Je proto dobré brát v potaz historii nebo recenze zákazníků při výběru hostingu.

Mimo anonymitu je velkým benefitem také způsob fungování, prostřednictvím kterého je možné si vybrat stát, z kterého chce uživatel přistupovat. Jedná se tedy o způsob, kterým lze zpřístupnit funkce daných služeb, které jsou v konkrétní zemi zakázány.

2.8.5.3 Využití mobilních dat

Připojení k internetu pomocí mobilních dat je obvykle šifrováno operátorem. Je tedy důležité zvážit, zda na cestách nevyužít mobilní data místo veřejné wi-fi sítě.

2.8.6 Chování na veřejné síti

Zde jsem popsal pár důležitých bodů, které sám považuji za důležité po připojení na veřejnou wi-fi síť:

- Nepřistupovat k osobním citlivým údajům (přihlášení na internetové bankovnictví nebo jiné účty týkající se financí a zároveň brát zřetel, které aplikace mají přístup k jakým datům)
- Navštěvovat na veřejné síti pouze takové stránky, které jsou v daný moment nezbytné a nejlépe osahují SSL certifikát
- Při využívání různých typů účtů myslet na odhlášení (spousta typů malwaru potřebuje pro napadení určitý čas, který se tímto minimalizuje)
- Velice důležitá věc je využívání stejných hesel na různých webech. Pokud útočník dostane přístup k jednomu konkrétnímu webu, je vysoká šance, že registrovaný e-mail využívá stejné heslo na jiném webu.
- Dbát na upozornění v prohlížečích. Mnoho moderních prohlížečů je schopno analyzovat web ještě před navštívením. Vyplatí se proto neignorovat tato varování.
- Nastavit své zařízení tak, aby se automaticky nepřipojovalo na danou wi-fi síť.

3 CÍLE

3.1 Hlavní cíl

Hlavním cílem mé diplomové práce je přehledně charakterizovat formy sociálního inženýrství a vsadit jej do aktuální doby se zaměřením na „denního“ uživatele (BFU). Cílem praktické části je porovnání dvou skupin studentů, přičemž jedna skupina se účastnila kurzu kybernetické bezpečnosti a druhá nikoli. Na základě těchto výsledků je dílčím cílem se zaměřit na nejvíce uživatelsky obtížnou část a vytvořit informační přehled.

3.2 Hypotézy

1) Studenti na internetu nejednají obezřetně.
2) I školení jedinci nejsou schopni při denním užívání schopni odhalit velkou řadu útoků.
3) Skupina, která neprošla intervencí nemá ve většině případů znalosti v problematice sociálního inženýrství

3.3 Výzkumné otázky

Pro správné pochopení dané problematiky se budu zabývat těmito otázkami:

- Má školení kybernetické bezpečnosti u dospívajících studentů vliv na obezřetnost v kyberprostoru?
- Která metoda napadení je v kyberprostoru nejčastější?

4 METODIKA

4.1 Výzkumný soubor

Výzkumný soubor je složen z 2 skupin. První skupina má 25 respondentů, druhá 26 respondentů.

Rozdíl mezi skupinami je takový, že jedna skupina prošla intervencí (školení o kybernetické bezpečnosti od Policie ČR) a druhá nikoli.

4.2 Metody sběru dat

Výzkum bude probíhat formou anketního šetření na ZŠ v Prostějově. Pro výzkum jsou vyhrazené hodiny informatiky. Všichni respondenti vyplní anketní šetření o 15 otázkách. Každá otázka má své identické opodstatnění, z kterého vyplývá přístup, kterým se respondent v kybernetickém prostoru pohybuje a jakým způsobem jedná v konkrétních situacích.

4.3 Statistické zpracování dat

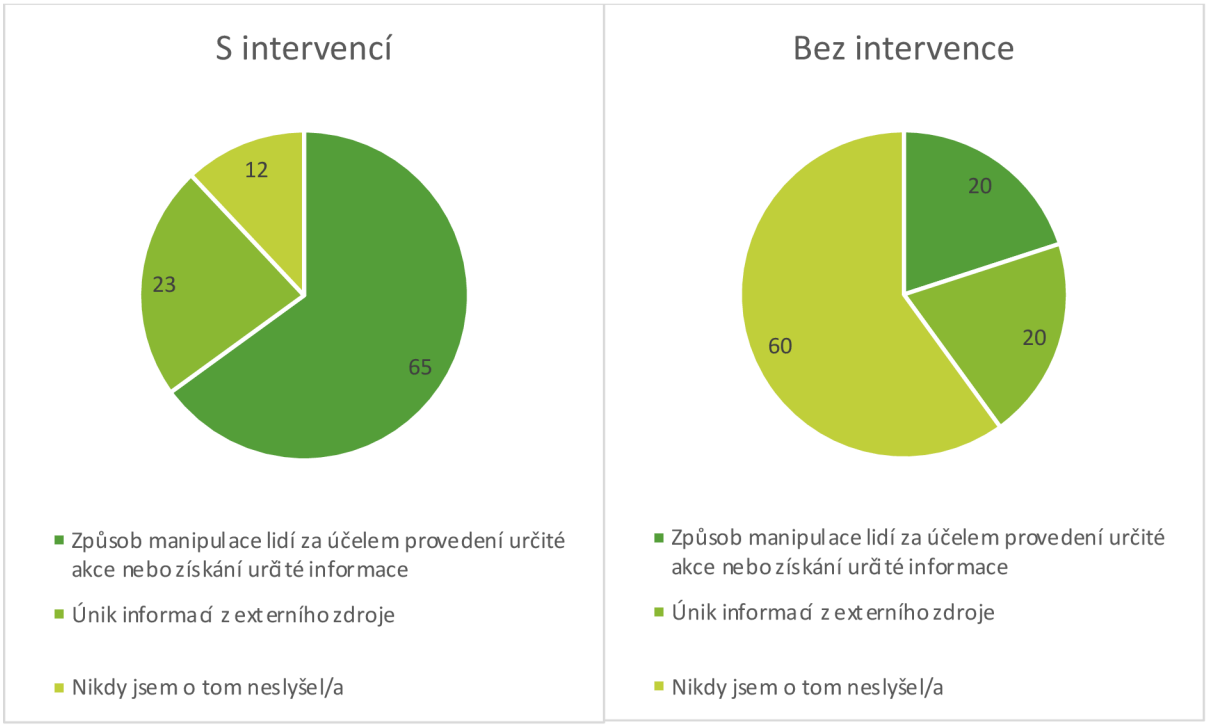
Nejdříve budou statistické údaje zaznamenány do MS Excel a následně budou vyhodnoceny ze zpracovaných údajů základní statistické veličiny a statistické korelace. Ty budou poté uspořádány do tabulek a grafů v programu SPSS vlastněná společností IBM.

5 VÝSLEDKY

U testovaných skupin byl kladen důraz, aby každý respondent odpovídal takovým způsobem, jakým se v konkrétních situacích v kybernetickém prostoru pohybuje. Každá otázka má své identické opodstatnění, z kterého vyplývá přístup uživatelů k prevenci v kybernetickém prostoru a jednání v konkrétních situacích.

5.1.1 Dotazníkové šetření - otázka č.1

Co podle vás znamená pojem sociální inženýrství?

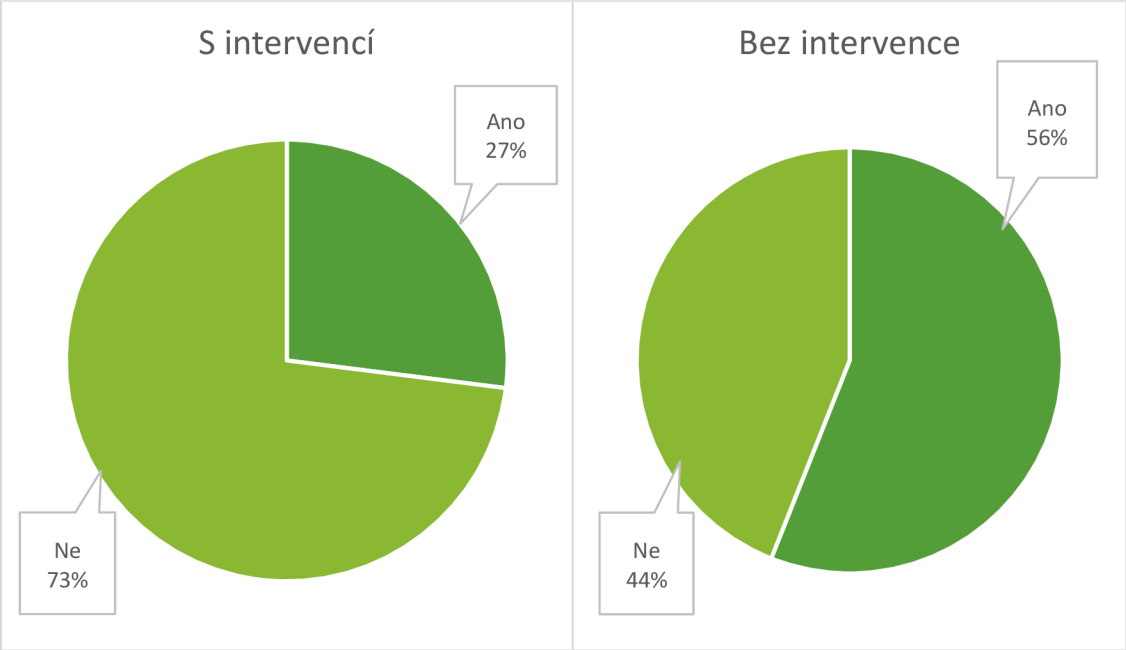


Graf 1. Odpovědi pro dotazníkové šetření otázky 1.

V odpovědích na otázku číslo 1 „Co podle vás znamená pojem sociální inženýrství?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 3,75$; $p = 0,04$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se prokázaly významné rozdíly mezi třídami v odpovědi „Způsob manipulace lidí...“ ($\chi^2 = 10,38$; $p < 0,01$) a „Nikdy jsem o tom neslyšel/a“ ($\chi^2 = 12,57$; $p < 0,01$), ale neprokázaly se u odpovědi „Únik informací...“ ($\chi^2 = 0,07$; $p = 0,80$).

5.1.2 Dotazníkové šetření - otázka č.2

Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech? (kavárny, restaurace, fitness)

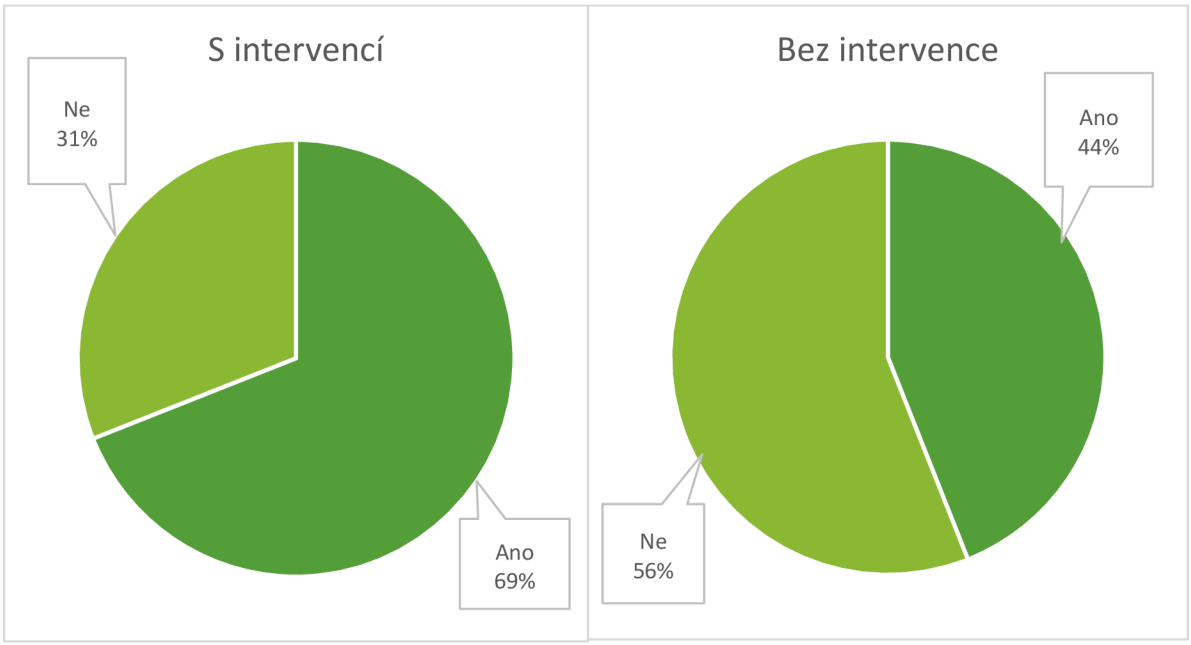


Graf 2. Odpovědi pro dotazníkové šetření otázky 2.

V odpovědích na otázku číslo 2 „Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 2{,}09$; $p = 0{,}04$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami prokázaly v odpovědi „Ano“ ($\chi^2 = 4{,}34$; $p = 0{,}04$) i „Ne“ ($\chi^2 = 4{,}38$; $p = 0{,}04$).

5.1.3 Dotazníkové šetření - otázka č.3

Kontrolujete si URL adresu navštívené webové stránky?

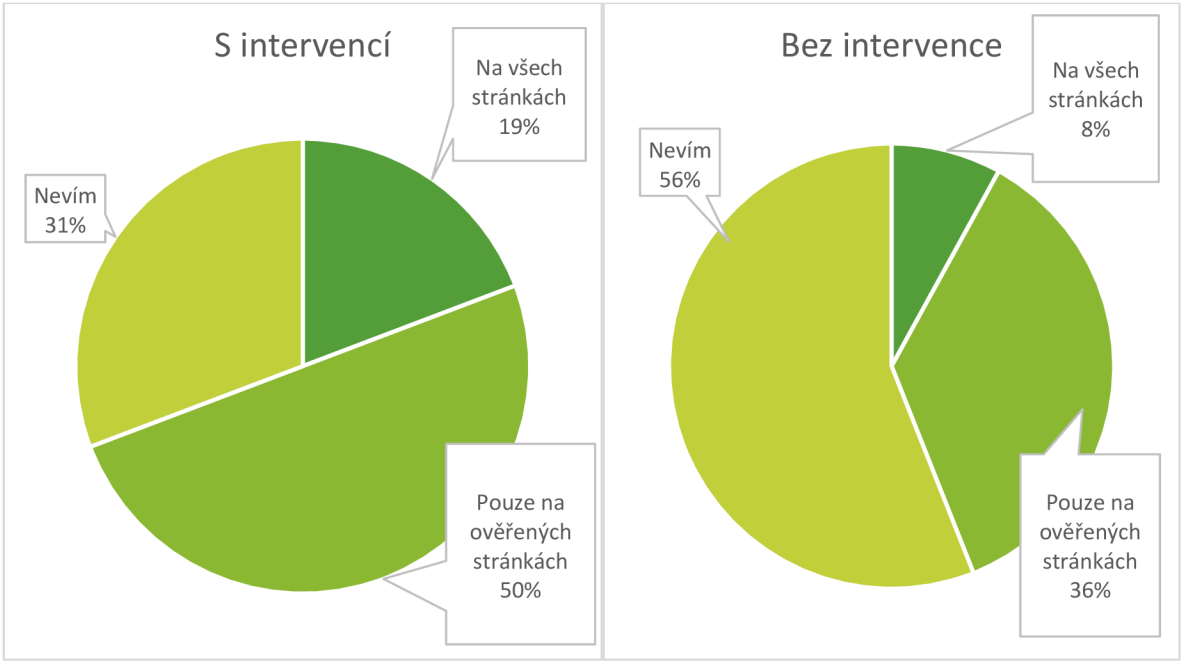


Graf 3. Odpovědi pro dotazníkové šetření otázky 3.

V odpovědích na otázku číslo 5: „Kontrolujete si URL adresu navštívené webové stránky?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}80$; $p = 0{,}07$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 3{,}18$; $p = 0{,}07$), „Ne“ ($\chi^2 = 3{,}18$; $p = 0{,}07$).

5.1.4 Dotazníkové šetření - otázka č.4

Registrujete se na stránkách bez ověřeného certifikátu?

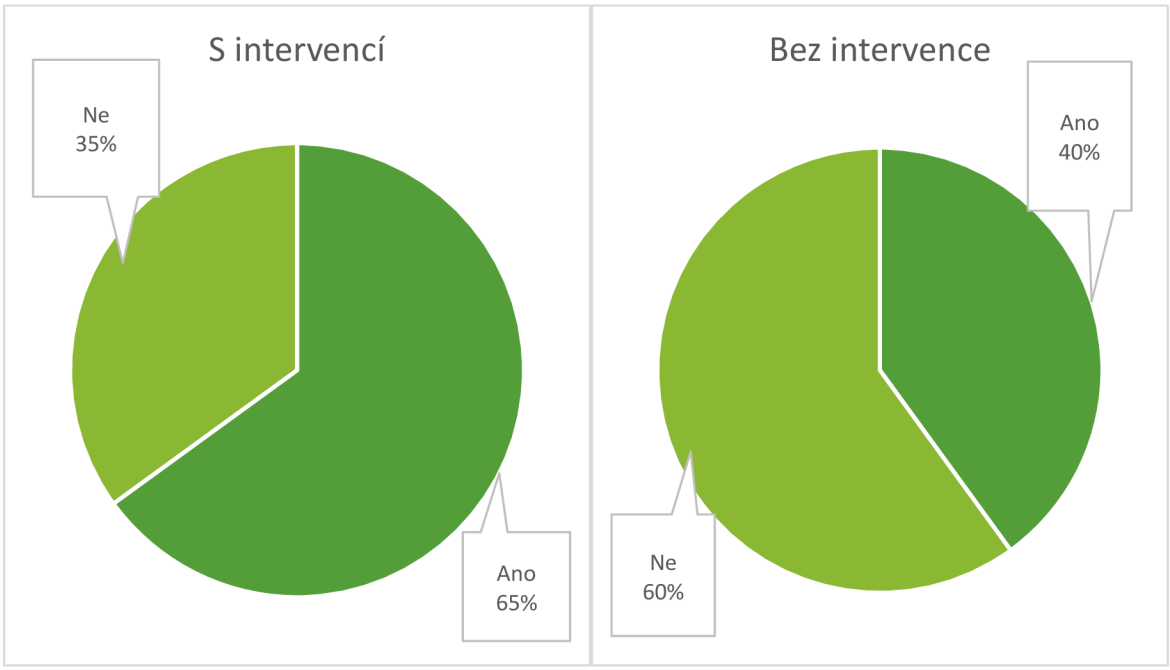


Graf 4. Odpovědi pro dotazníkové šetření otázky 4.

V odpovědích na otázku číslo 4: „Registrujete se na stránkách bez ověřeného certifikátu?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}88$; $p = 0{,}06$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Na všech stránkách“ ($\chi^2 = 1{,}29$; $p = 0{,}26$), „Pouze na ověřených stránkách“ ($\chi^2 = 1{,}00$; $p = 0{,}32$), ani „Nevím“ ($\chi^2 = 3{,}45$; $p = 0{,}06$).

5.1.5 *Dotazníkové šetření - otázka č.5*

Používáte na svém PC nelegální software?

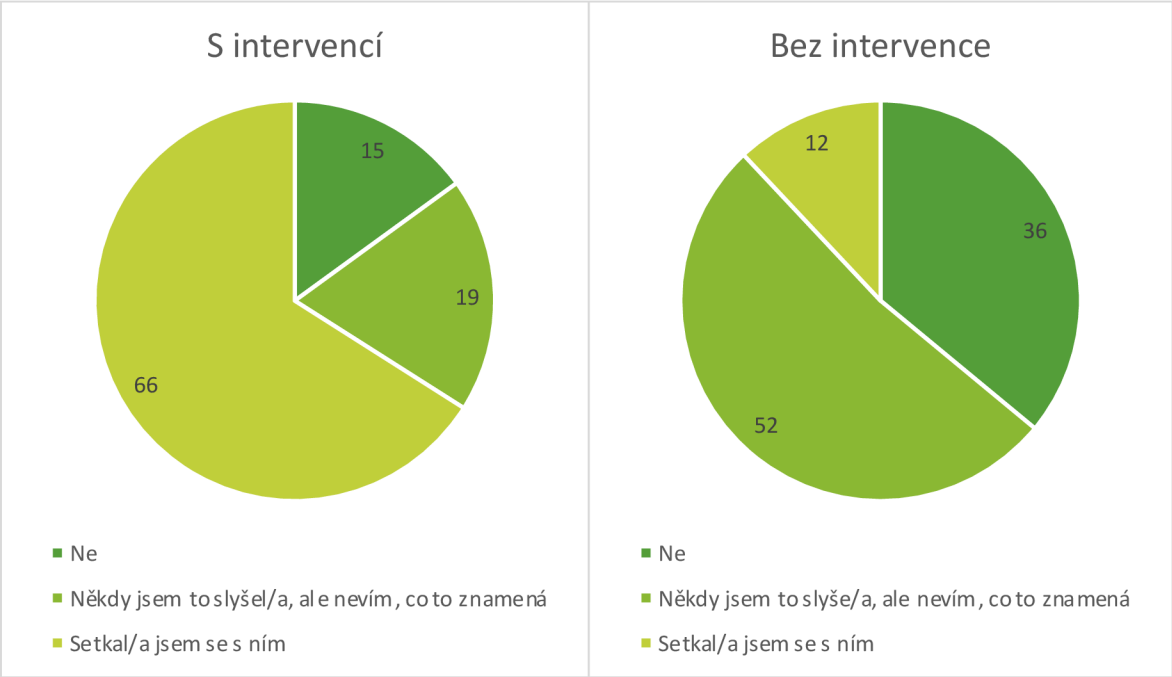


Graf 5. Odpovědi pro dotazníkové šetření otázky 5.

V odpovědích na otázku číslo 5: „Používáte na svém PC nelegální software?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}80$; $p = 0{,}07$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 3{,}13$; $p = 0{,}08$), „Ne“ ($\chi^2 = 3{,}13$; $p = 0{,}08$).

5.1.6 Dotazníkové šetření - otázka č.6

Říká vám něco pojem phishing?

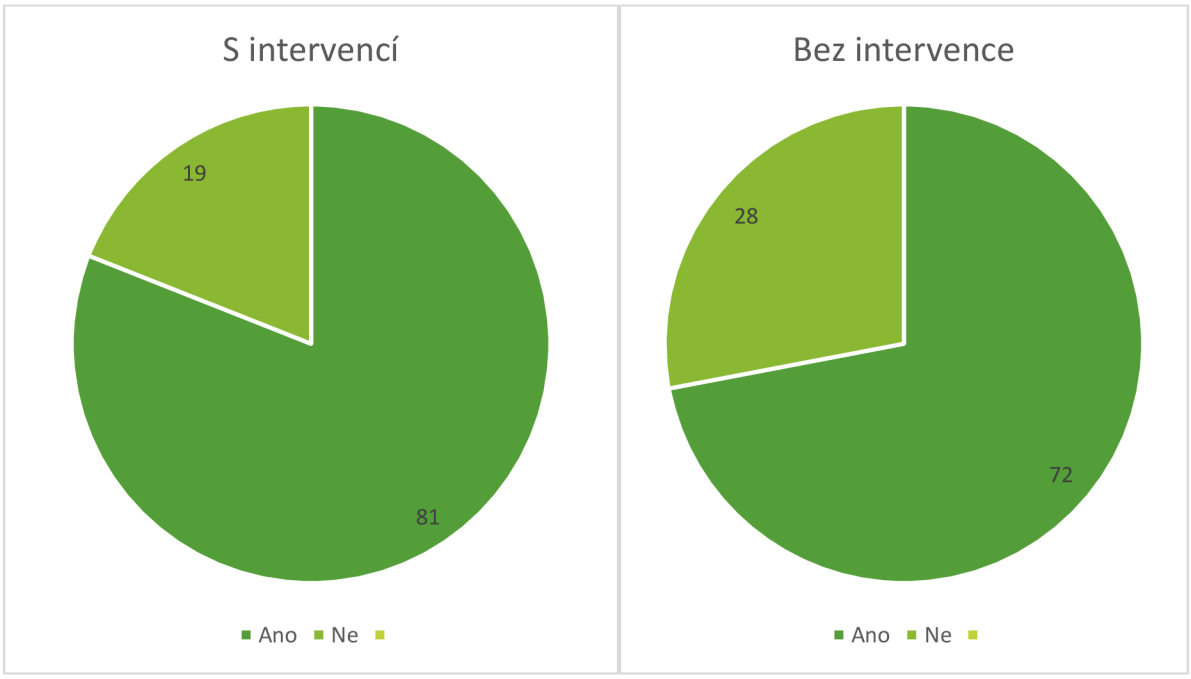


Graf 6. Odpovědi pro dotazníkové šetření otázky 6.

V odpovědích na otázku číslo 6: „Říká vám něco pojem phishing?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 3,42$; $p < 0,01$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ne“ ($\chi^2 = 2,92$; $p = 0,09$), „Někdy jsem to slyšel/a...“ ($\chi^2 = 5,97$; $p = 0,01$), ale prokázaly se v odpovědi „Setkal/a jsem se s ním“ ($\chi^2 = 14,75$; $p < 0,01$)

5.1.7 Dotazníkové šetření - otázka č.7

Používáte antivirový program?

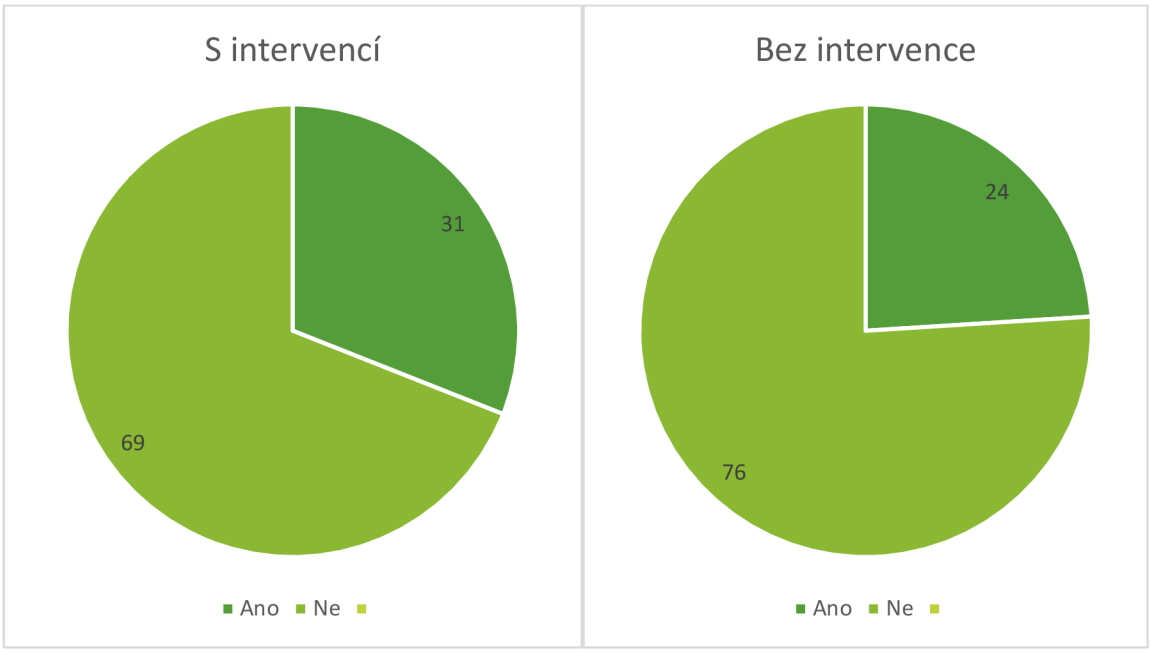


Graf 7. Odpovědi pro dotazníkové šetření otázky 7.

V odpovědích na otázku číslo 7: „Používáte antivirový program?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 0{,}73$; $p = 0{,}47$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 0{,}56$; $p < 0{,}45$), ani „Ne“ ($\chi^2 = 0{,}56$; $p = 0{,}45$).

5.1.8 Dotazníkové šetření - otázka č.8

Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN).

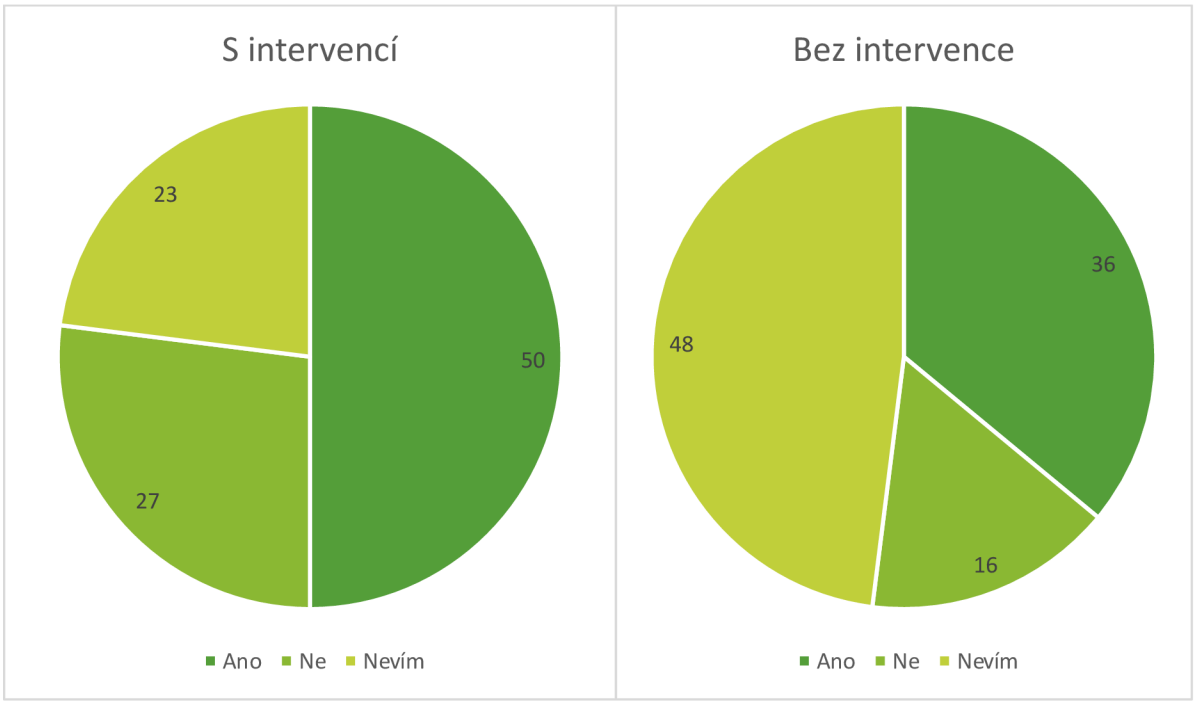


Graf 8. Odpovědi pro dotazníkové šetření otázky 8.

V odpovědích na otázku číslo 8: „Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN)“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 0,54$; $p = 0,59$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 0,31$; $p = 0,58$), ani „Ne“ ($\chi^2 = 0,31$; $p = 0,58$).

5.1.9 Dotazníkové šetření - otázka č.9

Máte nastavenou automatickou aktualizaci těchto programů?

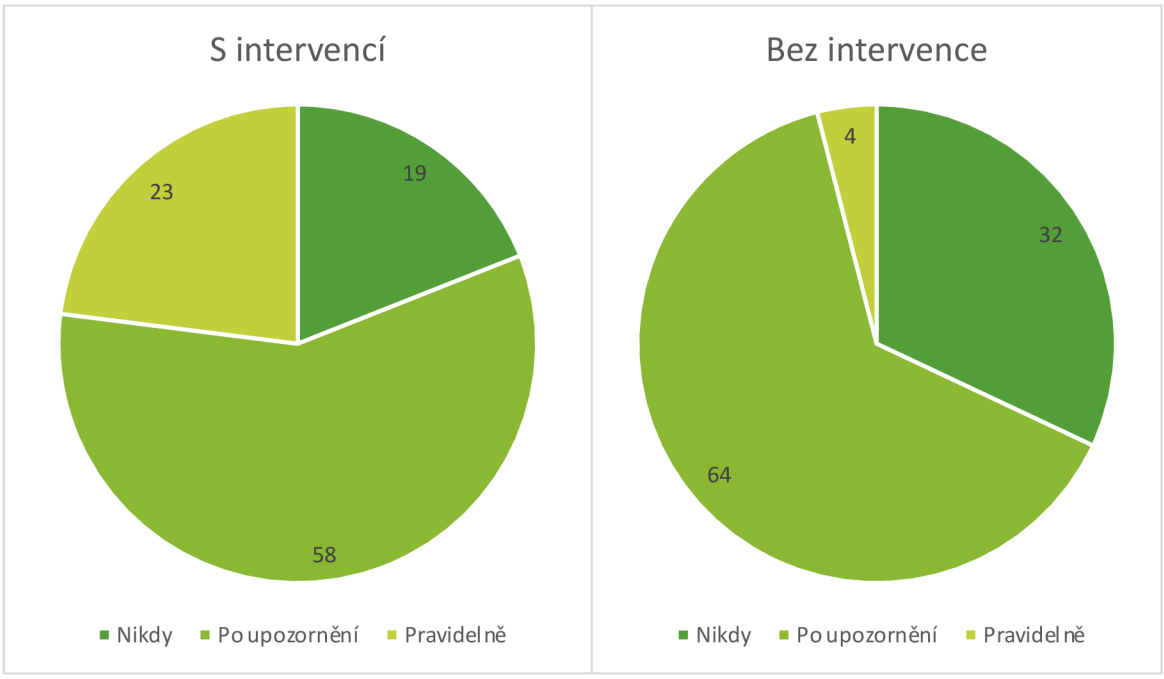


Graf 9. Odpovědi pro dotazníkové šetření otázky 9.

V odpovědích na otázku číslo 12: „Máte nastavenou automatickou aktualizaci těchto programů?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1,53$; $p = 0,13$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 0,99$; $p = 0,32$), „Ne“ ($\chi^2 = 0,89$; $p = 0,34$), ani „Nevím“
($\chi^2 = 3,42$; $p = 0,06$).

5.1.10 Dotazníkové šetření - otázka č.10

Jak často záměrně měníte svá hesla?

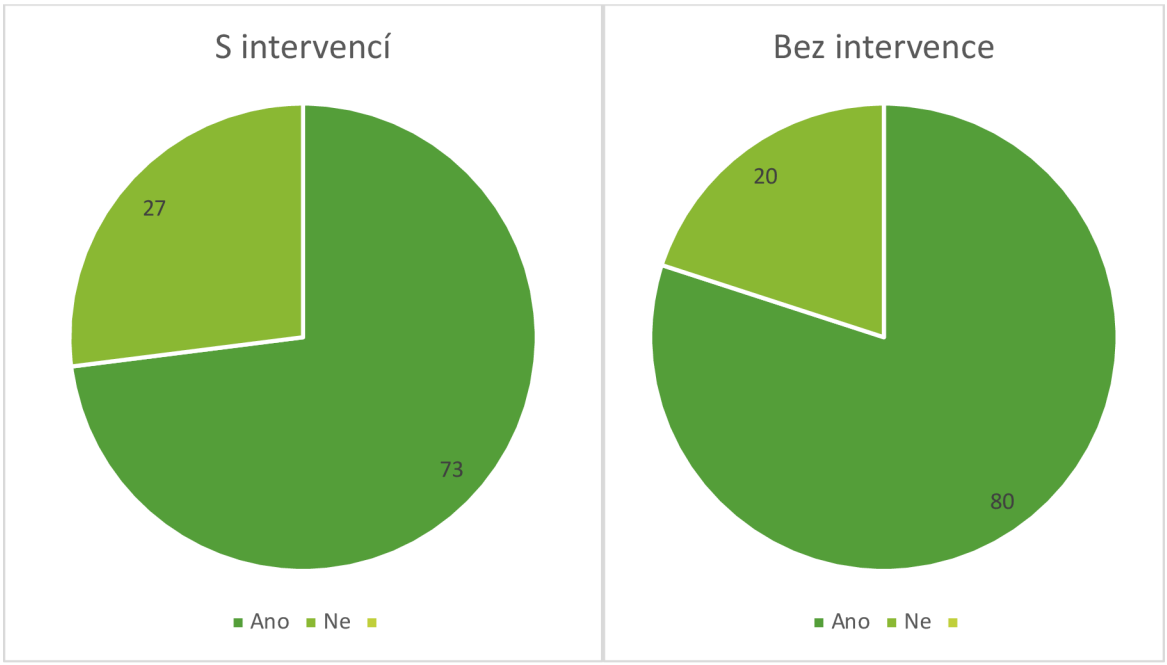


Graf 10. Odpovědi pro dotazníkové šetření otázky 10.

V odpovědích na otázku číslo 10: „Jak často záměrně měníte svá hesla?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}78$; $p = 0{,}08$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Nikdy“ ($\chi^2 = 1{,}12$; $p = 0{,}29$), „Po upozornění“ ($\chi^2 = 0{,}19$; $p = 0{,}66$), ani „Pravidelně“ ($\chi^2 = 3{,}82$; $p = 0{,}05$).

5.1.11 Dotazníkové šetření - otázka č.11

Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.

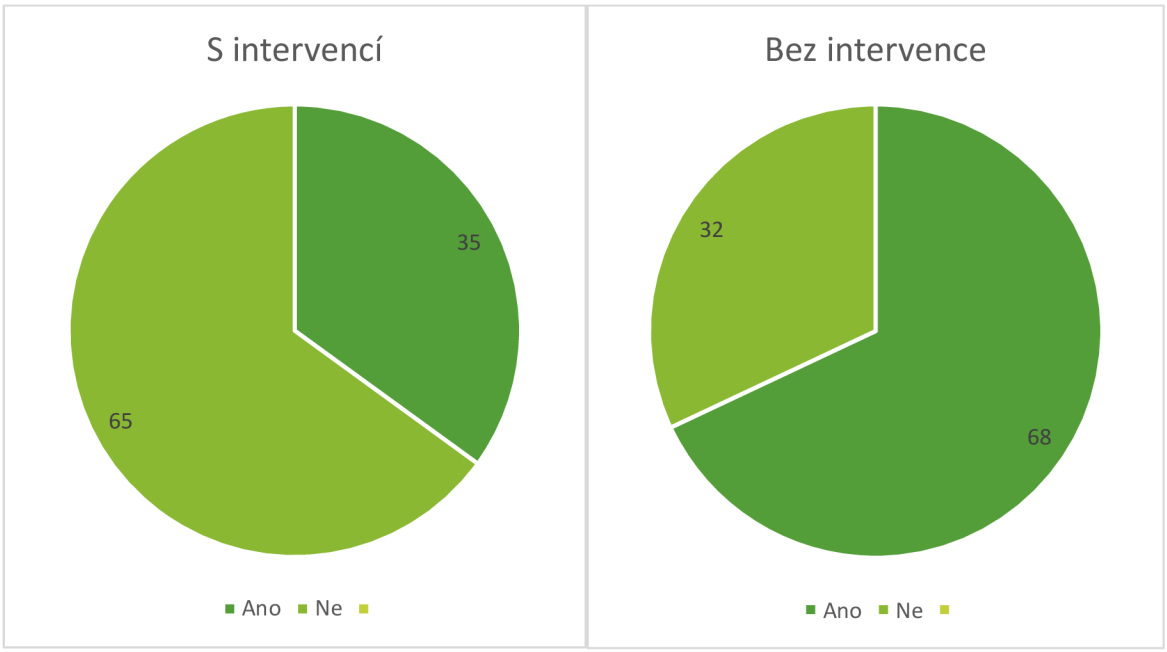


Graf 11. Odpovědi pro dotazníkové šetření otázky 11.

V odpovědích na otázku číslo 11: „Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 0,58$; $p = 0,56$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 0,34$; $p = 0,56$), ani „Ne“ ($\chi^2 = 0,34$; $p = 0,56$).

5.1.12 Dotazníkové šetření - otázka č.12

Používáte nebo upřednostňujete dvoufaktorové ověření?

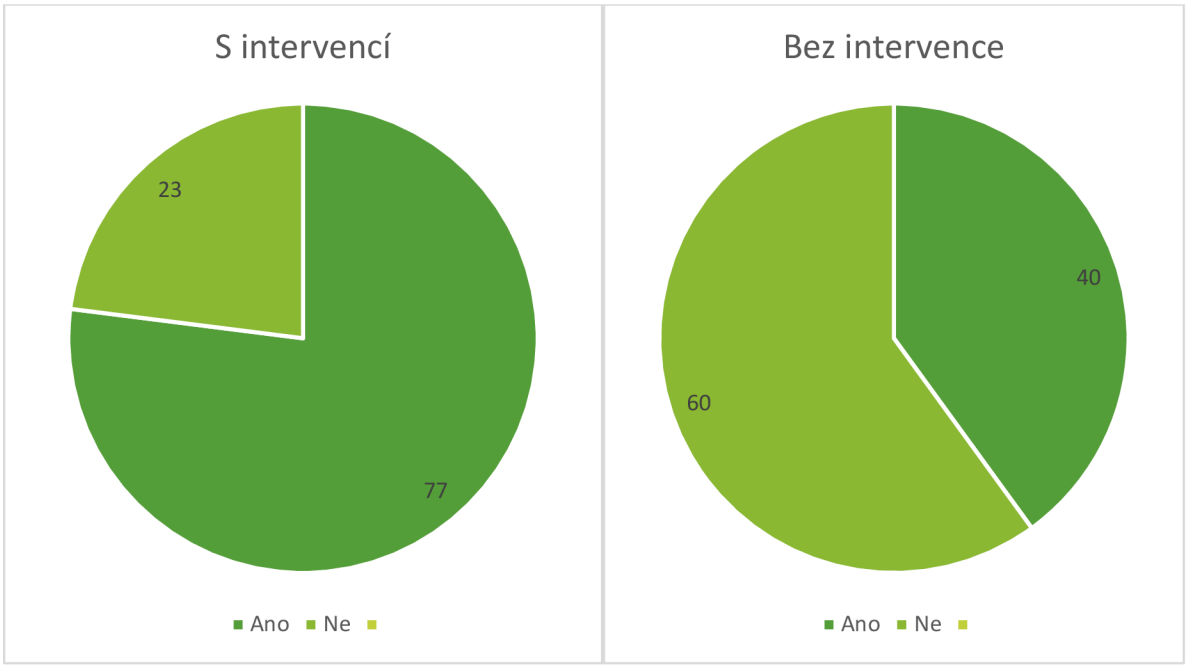


Graf 12. Odpovědi pro dotazníkové šetření otázky 12.

V odpovědích na otázku číslo 16: „Používáte nebo upřednostňujete dvoufaktorové ověření?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 2{,}36$; $p = 0{,}02$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami prokázaly v odpovědi „Ano“ ($\chi^2 = 5{,}45$; $p = 0{,}02$), i „Ne“ ($\chi^2 = 5{,}45$; $p = 0{,}02$).

5.1.13 Dotazníkové šetření - otázka č.13

Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?

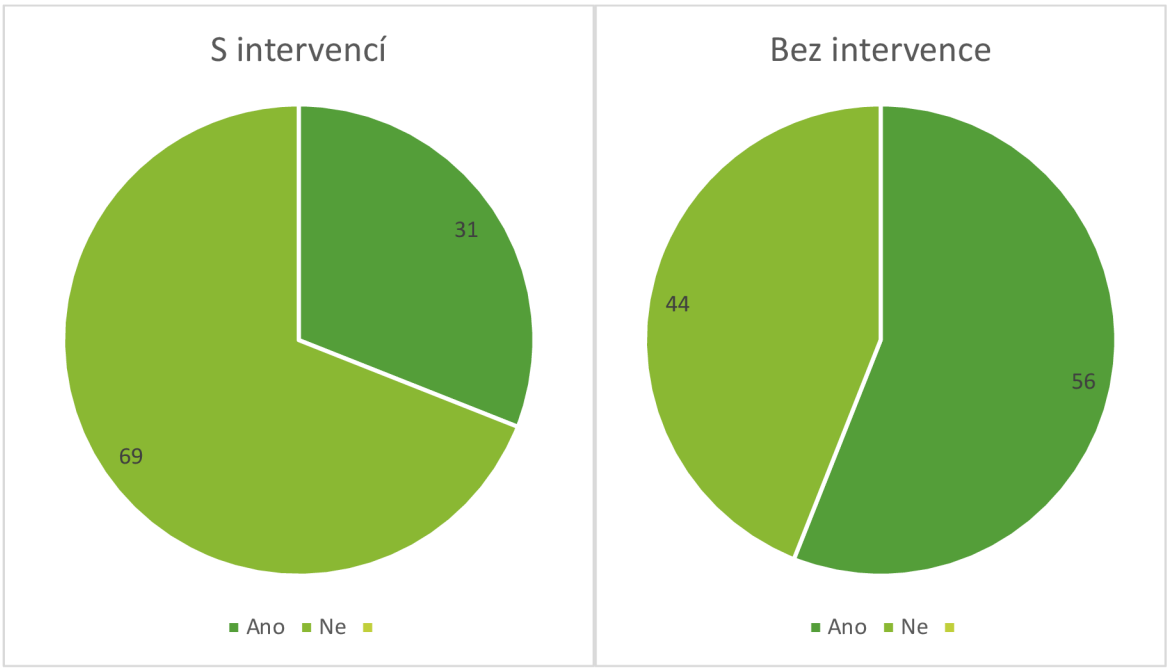


Graf 13. Odpovědi pro dotazníkové šetření otázky 13.

V odpovědích na otázku číslo 13: „Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 2{,}65$; $p = 0{,}01$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 7{,}06$; $p = 0{,}01$), i „Ne“ ($\chi^2 = 7{,}06$; $p = 0{,}01$).

5.1.14 Dotazníkové šetření - otázka č.14

Používáte pro přihlášení na různé stránky stejná hesla?

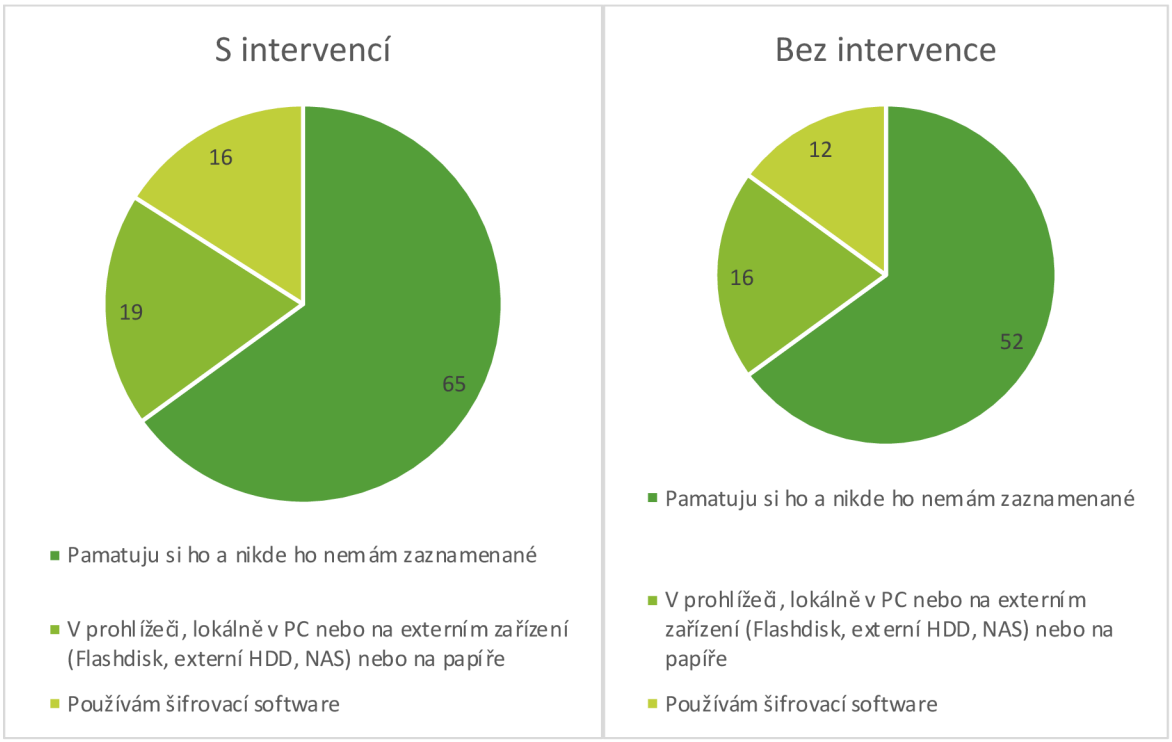


Graf 14. Odpovědi pro dotazníkové šetření otázky 14.

V odpovědích na otázku číslo 14: „Používáte pro přihlášení na různé stránky stejná hesla?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}80$; $p = 0{,}07$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi^2 = 3{,}45$; $p = 0{,}06$), ani „Ne“ ($\chi^2 = 3{,}18$; $p = 0{,}07$).

5.1.15 Dotazníkové šetření - otázka č.15

Jak pracujete s hesly?



Graf 15. Odpovědi pro dotazníkové šetření otázky 15.

V odpovědích na otázku číslo 15: „Jak pracujete s hesly?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 0{,}71$; $p = 0{,}48$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Pamatuju si ho a ...“ ($\chi^2 = 0{,}81$; $p = 0{,}35$), „V prohlížeči, lokálně ...“ ($\chi^2 = 1{,}82$; $p = 0{,}18$), ani „Používám šifrovací software“ ($\chi^2 = 0{,}09$; $p = 0{,}76$).

6 DISKUSE

Jedním z cílů práce bylo zhodnotit rozdíly dvou skupin (tříd ZŠ). První skupina prošla školením kybernetické bezpečnosti Policií ČR. Druhá skupina tuto možnost neměla. Otázky, které jsem pokládal v dotazníkovém šetření neměly vzájemnou návaznost. Studenti měli za úkol odpovídat dle svých vlastních preferencí, a to takovým způsobem, jak sami v internetovém prostředí jednají a ne tak, jak si myslí, že je psrávné jednat. Z důvodu relativně malého množství respondentů, u značného množství otázek, nevyplývají statistické signifikantní rozdíly mezi jednotlivými skupinami, jako významné, avšak odpovědi v zásadních otázkách, týkajících se bezpečnosti, se staly přínosné.

6.1.1 Shrnutí 1. otázky

První otázka: „Co podle vás znamená pojem sociální inženýrství?“ se ukázala ve skupině, která prošla intervencí, jako přínosná (následovala diskuse na téma sociální inženýrství). Správnou odpověď zaškrtlo 65 % respondentů, kdežto naproti tomu druhá skupina, která neprošla školením měla úspěšnost pouhých 20 %. Tento výsledek přikládám k faktu, že pojem Sociální inženýrství prozatím nenabylo patřičné popularity na internetu a studenti mají tedy minimální pravděpodobnost na tento pojem narazit.

6.1.2 Shrnutí 2. otázky

Druhá otázka: „Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech? (kavárny, restaurace, fitness). I v tomto případě proškolená skupina odpověděla ve vyšší míře, pro odpověď negativní (73 %) než skupina druhá (44 %). Po skončení testu u skupiny s intervencí jsem položil slovní otázku, zda se studenti připojují na veřejných místech výjimečně. Odpovědí mi byla ve většině případů „Pouze v nejnutnějších případech“ nebo „Z bezpečnostních důvodů využívám mobilní data“. Viz kapitola *Způsoby zabezpečení na veřejné síti.*

6.1.3 Shrnutí 3. otázky

Třetí otázka: „*Kontrolujete si URL adresu navštívené webové stránky?“*. Proškolená skupina v tomto případě kladně hlasovala v 69 % případů a druhá skupina v 44 %. Nejedná se tedy ani v jednom případě o nízké hodnoty. Antivirová společnost Norton (2022) uvádí ze svých zdrojů anonymní dotazník, ve kterém zazněla totožná otázka s pouhými 28 % kladných odpovědí. Domnívám se, že se jedná o klíčovou otázku týkající se kybernetické bezpečnosti. Viz. kapitola *Jak rozpoznat phishing.*

6.1.4 Shrnutí 4. otázky

Čtvrtá otázka: „*Registrujete se na stránkách bez ověřeného certifikátu?“*. U proškolené skupiny odpověděla rovná polovina respondentů tak, že se registrují pouze na ověřených stránkách a 19 % se registruje na všech webových stránkách a 31 % pro odpověď „Nevím. Jedná se tedy stále o vysoké hodnoty, které mohou bezpečnost narušit. U druhé skupiny hlasovalo 56 % respondentů pro odpověď „Nevím“ a je tedy podle očekávání daleko nižší znalost těchto „detailů“, kterých si uživatel musí při registraci všímat.

6.1.5 Shrnutí 5. otázky

Pátá otázka: „*Používáte na svém PC nelegální software?“*. Skupina s intervencí odpověděla kladně v 65 % případů, zatímco opačná skupina v „pouhých“ 40 % případů. Z těchto odpovědí vyplývá, že školení nemá vliv na využívání nelegálního softwaru, často nesoucí různou formu malwaru. Myslím si, že vliv na odpovědi na tuto otázku jsou vysoce individualizované a uživatel je přesvědčen, že platit za jakýkoliv software není jeho povinností, a to i na úkor bezpečnostních hrozeb. Zároveň se dá očekávat, že spoléhá na antivirové programy a další zabezpečovací software.

6.1.6 Shrnutí 6. otázky

Šestá otázka: „*Říká vám něco pojem phishing?“*. Z odpovědí na tuto otázku mám radost, jelikož se zde promítla znalost i první skupiny s intervencí. Odpověď „Setkal/a jsem se s ním“ odpovědělo 66 % respondentů, oproti 12 % skupiny druhé. Lze očekávat, že se s phishingem setkalo velké množství všech testovaných lidí, ale neprokázalo znalost v této problematice. Proto u otázky č.6 mohu konstatovat, že proces školení dospívajících studentů má v tomto oboru smysl.

6.1.7 Shrnutí 7. otázky

Sedmá otázka: „*Používáte antivirový program?“*. Skupina, která prošla bezpečnostním školením odpověděla „Ano“ v 81 % případů. U skupiny druhé, s výsledkem 72 % kladných odpovědí lze předpokládat, že o přítomnosti bezpečnostního software nemá povědomí. Výsledky u obou skupin jsou u této otázka téměř shodné a zde se tedy neprokázal vliv zvýšení o bezpečnostním povědomí.

6.1.8 Shrnutí 8.otázky

Osmá otázka: „*Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN)“*. Z výsledků obou skupin vyplynulo, že se téměř „zopakoval“ scénář otázky č.7 a lze tedy předpokládat, že na využívání bezpečnostního softwaru nemá absolvování školení důrazný vliv. Více se o tuto problematiku zajímám v kapitole *Anonymita.*

6.1.9 Shrnutí 9.otázky

Devátá otázka*: „Máte nastavenou automatickou aktualizaci těchto programů?“*. U první skupiny, která prošla intervencí zodpovědělo 50 % respondentů kladně a má tedy nastavenou automatickou aktualizaci bezpečnostního softwaru. Aktualizaci databází považuji za velice důležitou, především z důvodu vzniku nových bezpečnostních hrozeb. Druhá skupina odpověděla kladně v 36 % případů a dá se očekávat, že školení určitý vliv na studenty mělo právě v oblasti prevence.

6.1.10 Shrnutí 10.otázky

Desátá otázka: „*Jak často záměrně měníte svá hesla?*“. U skupiny, která prošla bezpečnostním školením podle odpovědí mění záměrně svá hesla 23 % respondentů pravidelně oproti 4 % z druhé skupiny. Je tedy zřejmé, že informace o kybernetické bezpečnosti se částečně pozitivně „zrcadlily“. Odpovědi, kdy respondenti odpověděli, že svá hesla aktualizují „Až po upozornění“, které jim web sám doporučí, byla v obou případech na hranici 60 %. Je tedy dle mého názoru obecná nezbytnost tuto funkcionalitu zavést na co možná největší množství serverů.

Důvodů, proč měnit svá hesla je hned několik, ovšem z mého pohledu je nejdůležitějším důvodem především častý únik databází z všemožných serverů, které obsahují přihlašovací údaje.

6.1.11 Shrnutí 11.otázky

Jedenáctá otázka: „*Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.*“. V případě kladných odpovědí na tuto otázku (73 % a 80 %) se domnívám, že mohou být důvodem častá „vynucení“ těchto kombinací samotnými weby. Jedná se tedy o poměrně velkou úspěšnost v odpovědích na tuto otázku. Je zapotřebí brát v potaz, že stále existují servery, které tuto kombinaci nevyžadují a představují potenciální riziko pro uživatele. Absence kombinací těchto znaků je častým terčem útoků tzv. „hrubou silou“. Jedná se o útok, který má snahu rozluštit šifru bez přítomnosti dešifrovacího klíče. V praxi to znamená, že útočník má k dispozici pouze výkonný hardware, na kterém probíhá automatizovaný útok, tedy zkoušení kombinací písmen, čísel a znaků v náhodném pořadí. Nebezpečnější alternativu představuje „slovníkový útok“ při kterém má útočník k dispozici hesla z uniklých databází.

6.1.12 Shrnutí 12.otázky

Dvanáctá otázka: „*Používáte nebo upřednostňujete dvoufaktorové ověření?*“. U odpovědí na tuto otázku se překvapivě vyšší úspěšnost prokázala u skupiny, která neprošla intervencí a sice 68 % a skupina s intervencí 35 %. Dle mého názoru si uživatel aktivuje dvoufaktorové ověření až v moment, kdy se stane sám obětí napadení. Mohu tedy konstatovat, že informace ohledně prevence zabezpečení a síly svého bezpečnostního hesla nejsou pro většinu studentů prioritní a přikládají důraz síle svého hesla. Možnosti, kterými by útočník překonal dvoufaktorové ověření (2FA) zde samozřejmě jsou, ale nelze popřít, že 2FA výrazně zabezpečuje účty prostřednictvím e-mailu nebo mobilního telefonu.

Dle společnosti Microsoft je dvoufaktorové ověření schopno zablokovat až 99,9 % automatizovaných útoků.

6.1.13 Shrnutí 13.otázky

Třináctá otázka: „*Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?“*. V odpovědích u skupiny s intervencí se prokázalo, že 77 % respondentů se s takovými e-maily setkalo a u druhé skupiny přišlo do kontaktu v tímto typem útoku „jen“ 40 %. Dle mého názoru se může jednat o důvod neznalosti daných uživatelů v problematice phishingových útoků. Více jsem se věnoval této problematice v kapitole *Sociální inženýrství a jeho metody.*

6.1.14 Shrnutí 14. otázky

Čtrnáctá otázka: „*Používáte pro přihlášení na různé webové stránky stejná hesla?“*. Školení kybernetické bezpečnosti se prokázalo u této otázky jako přínosné. Skupina, která prošla intervencí měla odpovědi na otázku, „zda uživatelé používají pro různé webové stránky stejná hesla“ na hodnotě 31 % oproti 56 % skupině druhé. Jedná se tedy o důležitou informaci týkající se osobní bezpečnosti. Důvodem tohoto bezpečnostního pravidla je především únik databází na veřejný internet a používá-li uživatel dané heslo i na jinch webech, je prokazatelně vyšší pravděpodobnost prolomení účtu právě na jiném serveru.

6.1.15 Shrnutí 15. otázky

Patnáctá otázka: „*Jak pracujete s hesly“* se prokázala jako nejméně významná, jelikož v obou případech se uživatelé „spoléhají“ především na své vlastní zapamatování hesel bez žádného záznamu. Nelze ovšem popřít, že znalost uživatelů není zcela dostačující z pohledu internetových prohlížečů, při kterých uživatelé svá hesla častokrát ukládá do nezabezpečených klíčenek internetových prohlížečů bez svého vědomí.

6.2 Výzkumná otázka č.1

Má školení kybernetické bezpečnosti u dospívajících studentů vliv na obezřetnost v kyberprostoru?

Pomocí dotazníkového šetření jsem vyhodnotil otázky týkající se z mého pohledu nejdůležitějších částí kybernetické bezpečnosti se zaměřením na „denního“ uživatele. Z dotazníkového šetření vyplývá, že silné uživatelské návyky mnohdy předchází pocitu bezpečí a prevence nebo následné řešení přichází až v okamžik, kdy je uživatel napaden. Otázkou tedy, zda školení nepostrádá smysl u těchto dospívajících studentů se prokázala jako negativní a dle mého názoru je zapotřebí více tuto problematiku vnést do školství.

6.3 Výzkumná otázka č.2

Která metoda napadení je v kyberprostoru nejčastější?

Kombinací názorů z dotazníkového šetření a některých výzkumů společnosti Microsoft se potvrdilo, že nejčastějším typem útoků v kyberprostoru je bezesporu phishing patřící mezi metody sociálního inženýrství.

7 ZÁVĚRY

- Definoval jsem nejčastější způsoby napadení uživatele v kybernetickém prostředí a do jisté míry charakterizoval řešení týkající se prevence.
- Velké množství útoků za pomocí sociálního inženýrství lze předejít jen prostřednictvím získání znalostí v tomto oboru.
- Z dotazníkového šetření vyplynulo, že moji hypotézu, která předpokládá, že studenti v kybernetickém prostředí nejednají obezřetně, lze potvrdit.
- V poslední řadě jsem provedl výzkum u dvou tříd studentů ZŠ, kde první třída prošla kurzem pro práci v kybernetickém prostředí a druhá nikoli, kde jsem dospěl k závěru, že tyto vzdělávací kurzy mají v klíčových situacích důležitý vliv na rozhodování každého jedince.
- Dále se potvrdila hypotéza, která předpokládala, že studenti bez školení o kybernetické bezpečnosti nemají znalosti v problematice sociálního inženýrství.

8 SOUHRN

Snahou autora této diplomové práce bylo poskytnout „denním“ uživatelům, pohybujících se v internetovém prostředí, potřebné informace týkající se kybernetické bezpečnosti se zaměřením na aktuální nejnovější trendy.

Úvodní kapitola jasně definovala základní cíle této práce týkající se teoretické části. Vymezily se metody, prostřednictvím kterých útočníci získávají data uživatele. Jednotlivé metody jsou podrobně charakterizovány a globálně nejpoužívanější metody jsou obohaceny o příklady z praxe.

Dále jsou sestaveny základní bezpečnostní doporučení, jak se na veřejné síti pohybovat s minimálním rizikem. Následně jsou v práci řešeny metody sociálního inženýrství a reálné příklady, často využívané útočníky v praxi.

V závěru mohu konstatovat, že je nezbytné zvýšit povědomí o kybernetických hrozbách jak v domácnostech, tak školských institucích z důvodu především velkého počtu zařízení, s kterými se člověk denně dostává do kontaktu.

9 SUMMARY

The effort of the author of this diploma thesis was to provide the "daily" users moving in the Internet environment with the necessary information regarding cyber security with a focus on the latest trends.

The introductory chapter clearly defined the basic objectives of this work concerning the theoretical part. Methods have been defined by which attackers obtain user data. The individual methods are characterized in detail and the globally most used methods are enriched with practical examples.

Furthermore, basic safety recommendations are compiled on how to move on the public network with minimal risk. Subsequently, the work deals with methods of social engineering and real examples, often used by attackers in practice.

In conclusion, I can state that it is necessary to raise awareness of cyber threats in both households and educational institutions, mainly due to the large number of facilities with which a person comes into contact on a daily basis.

10 SEZNAM POUŽITÝCH OBRÁZKŮ/GRAFŮ

10.1 Seznam obrázků

10.2 Seznam grafů

11 REFERENČNÍ SEZNAM

Achkoski, J., & Dojchinovski, M. (2000). Cyber terrorism and cybercrime. Retrieved 14. 4. 2022 from World Wide Web: https://core.ac.uk/download/pdf/35329569.pdf

Avast (2021). *Crypto based phishing scams.* Retrieved 12.5.2022 from the World Wide Web: https://blog.avast.com/cs/crypto-based-phishing-scams-avast

Bateman, R. (2020). 10 Best Anti-Spyware Software for 2020. Retrieved 25. 6. 2022 from the World Wide Web: https://www.safetydetectives.com/blog/the-best-anti-spywaresoftware/

Brenner, S. (2010). Cybercrime: Criminal Threats for Cyberspace. California: Greenwood Publishing Group.

Binance (2022). *Examples of Phishing E-mails.* Retrieved 19.6.2022 from the World Wide Web: https://www.binance.com/en/support/faq/360020817051

Entuzio (2022). *TOP 13 Burzy*. Retrieved 13.6.2022 from World Wide Web: https://entuzio.cz/krypto-burzy/

Forbes (2013). *Meet The Dread Pirate Roberts, The Man Behing Booming Black Market Drug Website Silk Road*. Retrieved 11. 5. 2022 from the World Wide Web: https://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirateroberts-the-man-behind-booming-black-market-drug-website-silkroad/#48caf9688b73

Igarapé institute (2018). *Brazil struggles with effective cyber-crime response*. Retrieved 5. 6. 2022 from the World Wide Web: https://igarape.org.br/en/brazil-struggles-witheffective-cyber-crime-response/

IntrustIT (2022*). Multi Factor Authentication.* Retrieved 17.6.2022 from the World Wide Web: https://www.intrust-it.com/multi-factor-authentication-what-the-microsoft-mfa-warning-really-means/

ITGovernance (2021). *Cyber security.* Retrieved 11.5.2022 from the World Wide Web: https://www.itgovernance.co.uk/cyber-health-check

IT Market (2022). *Phishing na nejvyšší úrovni*. Retrieved 17.6.2022 from the World Wide Web: https://www.it-market.cz/articles/phishing/phishing-na-nejvyssi-urovni-1-milion-utoku-v-1-ctvrtleti-2022

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial guide for handling cyber-terrorism and information warfare.* Retrieved 5. 5. 2022 from the World Wide Web: https://www.researchgate.net/publication/294563593_Managerial_guide_for_handling _cyber-terrorism_and_information_warfare

Kolouch, J. (2016). *CyberCrime*. Praha: CZ.NIC, z. s. p. o.

Lorents, P., & Ottis, R. (2011). Cyberspace: Definition and implications. Retrieved 15. 4. 2020 from the World Wide Web: https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_im plications

NATO Public Diplomacy Division (2007). Centre of Excellence Defence Against Terrorism, Ankara, Turkey. Retrieved 14. 6. 2022 from the World Wide Web: https://books.google.cz/books?id=Eg7vAgAAQBAJ&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Gibson, W (1984). *Neuromancer.* USA: Ace Books.

Passcamp (2021). *What is a baiting attack and how to prevent it?* Retrieved 20.6.2022 from the World Wide Web: https://www.passcamp.com/blog/what-is-a-baiting-attack-and-how-to-prevent-it/

Policie ČR (2020). *Kyberkriminalita*. Retrieved 5. 5. 2022 from the World Wide Web: https://www.policie.cz/clanek/kyberkriminalita.aspx

Sanders, A. (2022) Co je sociální inženýrství a proč je to hrozba v roce 2022? *Safetydetectives. Retrieved 14.5.2022 from the World Wide Web:*

https://cs.safetydetectives.com/blog/co-je-socialni-inzenyrstvi-a-proc-je-to-takova-hrozba/

Solms, R.V., Niekerk, J. V. (2013). *From information security to cyber security. Retrieved 19.5.2022 f*rom the World Wide Web: https://doi.org/10.1016/j.cose.2013.04.004

The Jargon File (2016). *Hacker slang and hacker culture.* Retrieved 9. 5. 2022 from the World Wide Web: http://catb.org/jargon/html/distinctions.html

US Army (2010) *Cyberspace Operations Concept Capability Plan 2016-2028.* Retrieved 11.5.2022 from the World Wide Web: https://irp.fas.org/doddir/army/pam525-7-8.pdf

Vláda České republiky (2021) *Kybernetická bezpečnost.* Retrieved 11.5.2022 from the World Wide Web: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/