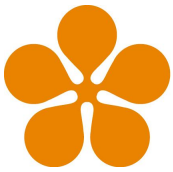


Pedagogická fakulta
Faculty of Education

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice


Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra informatiky


# E–bezpečnostní znalosti a chování osob pracujících ve státní správě

Bakalářská práce


**Vypracovala:** Marie Pólová

**Vedoucí práce:** Mgr. Václav Šimandl



České Budějovice 2016

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
**Fakulta pedagogická**
Akademický rok: **2014/2015**

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Marie PÓLOVÁ** |
| Osobní číslo: | **P13812** |
| Studijní program: | **B7507 Specializace v pedagogice** |
| Studijní obor: | **Informační technologie a e-learning** |
| Název tématu: | **E-bezpečnostní znalosti a chování osob pracujících ve státní správě** |
| Zadávající katedra: | **Katedra informatiky** |

Zásady pro vypracování:

Studentka realizuje dotazníkové šetření, které se bude zaměřovat na e-bezpečnostní znalosti a návyky osob produktivního věku ve vztahu k předpokládaným faktorům, které by tyto znalosti a návyky mohly ovlivňovat. Dotazník se bude zabývat tématem ochrany dat, především ochranou proti malwaru, spamu, hoaxu, phishingu, ztrátou dat a jejich zneužití a ochranou hesel. Studentka sestaví dotazník zabývající se výše uvedenými jevy a následně realizuje dotazníkové šetření, jehož respondenty se stanou osoby pracující ve státní správě. Data vzniklá z dotazníku studentka zpracuje za použití statistických metod. V teoretické části práce studentka popíše ochranu dat, jednotlivé druhy malwaru, spamu, hoaxu, phishingu, jak se jim bránit, možné důsledky rizikového chování, způsoby zálohování dat, ochranu a správu hesel.

Rozsah grafických prací: **CD ROM**

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:


1. **Gavora, P. Úvod do pedagogického výzkumu. Brno: Paido, 2010. ISBN 978-80-7315-185-0.**
2. **Chrástka, M. Metody pedagogického výzkumu. Praha: Grada, 2007. ISBN 978-80-247-1369-4.**
3. **Král, M. Bezpečnost domácího počítače: prakticky a názorně. 1. vyd. Praha: Grada, 2006, 334 s. ISBN 80-247-1408-6.**
4. **Livingstone, S. a L. Haddon. Kids online: Opportunities and risks for children. Bristol: Policy Press, 2009. ISBN 978-1-84742-438-9.**
5. **Neubauer, J., M. Sedlačík a O. Kříž. Základy statistiky: aplikace v technických a ekonomických oborech. 1. vyd. Praha: Grada, 2012, 236 s. ISBN 978-80-247-4273-1.**
6. **Sechler, J. A Young Adult's Guide to Safety in the Digital Age. CreateSpace, 2010. ISBN 978-1-45361-841-4.**


Vedoucí bakalářské práce: **Mgr. Václav ŠIMANDL**
Katedra informatiky

Datum zadání bakalářské práce: **28. dubna 2015**

Termín odevzdání bakalářské práce: **29. dubna 2016**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 28. dubna 2015

# Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně, pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 11/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 28. 4. 2016

Marie Pólová

# Abstrakt

Cílem práce je zhodnotit problematiku e–bezpečnostních znalostí a návyků lidí pracujících ve státní správě. Zaměřila jsem se na ochranu před malwarem, phishingem a ztrátou dat. Dále jsem zjišťovala návyky při práci s bezpečnostními hesly a návyky při práci s elektronickou poštou. Zvolený problém jsem řešila pomocí dotazníkového průzkumu, kterým jsem zjišťovala, zda se pracovníci státní správy dokáží ochránit před počítačovými hrozbami. Výsledky byly zpracovány pomocí statistických metod Chí–kvadrát test, Studentů t–test a Jednoduchou analýzu rozptylu. Našla jsem faktory, které ovlivňují chování a návyky respondentů. Je to síla hesla, které používají k přístupu do aplikací s citlivými údaji a setkání s nákazou malwarem. Zde bylo zjištěno nejvíce potvrzených závislostí. Z osobnostních faktorů chování respondentů nejvíce ovlivňuje vzdělání a pak následuje pohlaví.



# Klíčová slova

Malware, data, hesla, bezpečnost, dotazník

# Abstract

The aim of the thesis is to evaluate the issue of e–safety related knowledge and habits of people working in civil service. I focused on protection against malware, phishing and data loss. Next, I examined the habits when working with security passwords and habits when working with electronic mail. I approached the issue at hand using a questionnaire aimed to find out whether civil servants are capable of protecting themselves against cyber threats. Selected problem I solved using a questionnaire, which I investigated whether civil servants are able to protect against computer threats. The results were processed using statistical methods chi-square statistic, Student t-test and Simple analysis of variance. I found the factors that influence the behavior and habits of the respondents. It is the strength of the password they use to access the applications with sensitive data and meeting with the malware infection. Here it was found the most addictions confirmed. Of the personality factors most influences the behavior of respondents education and then followed by sex.



# Keywords

Malware, data, passwords, security questionnaire

# Poděkování

Děkuji vedoucímu práce Mgr. Václavu Šimandlovi za jeho připomínky ke zpracování mé bakalářské práce, za jeho rady, vstřícnost, trpělivost a zodpovědnost. Mé poděkování patří i všem respondentům mého dotazníkového šetření. V neposlední řadě děkuji své rodině a blízkým za podporu během mého studia a zpracování této práce.

# Obsah

# 1 Úvod

Za posledních několik let se v mnohém zrychlil a změnil životní styl. Internet a elektronický způsob komunikace se stal běžnou součástí života. To vyplývá i ze šetření Českého statistického úřadu [1], které uvádí, že v roce 2014 vlastnilo 72 % domácností osobní počítač a 72 % jich bylo připojeno k internetu. Ještě k vyšším číslům se dostaneme, pokud nás budou zajímat pouze domácnosti s dětmi, tak 94 % má osobní počítač a 93 % připojení k internetu. Jednoznačně nejoblíbenější skupinou činností provozovanou na internetu pro soukromé účely je komunikace. Celých 93 % českých uživatelů internetu jej používá k zasílání a přijímání emailů, 87 % prostřednictvím internetu vyhledává informace a 57 % české populace využívá internetové bankovnictví. Výpočetní technika nás obklopuje na každém kroku, vše se elektronizuje. Čteme elektronické knihy, pořizujeme digitální fotky, místo pohlednic posíláme mms a sms zprávy, dopisy jsou nahrazeny e–maily. Zcela běžně používáme internetového bankovnictví. Firmy používají datové schránky.

Internet nám dává možnost získávat informace odborné i jiné, nehledě na hranice. Zprostředkovává nám aktuální informace z celého světa, přičemž dostupný je v civilizovaném světě prakticky každému (viz. chytré telefony). Jiné je to ovšem s ověřováním věrohodnosti zdroje poskytovaných informací.

Tím, jak stoupá dostupnost a využívání internetu, stoupá i riziko útoků na počítač a vše, co obsahuje. Motivem těchto útoků je finanční zisk, jak dokazuje i studie společnosti Trustware [2]. Podle studie se návratnost investice pohybuje až na hranici 1425 %, za investovaných 5900 $ je možné získat zpět 84 100 $.

Změna způsobu komunikace nám život ulehčuje, ale zároveň přináší i stinné stránky v podobě zvýšených rizik útoků na počítač a vše co obsahuje. Na vzestupu je využívání sociálního inženýrství k těmto útokům, kdy se zneužívá přirozené důvěřivosti uživatelů internetu.

# 2 Cíle práce

Cílem práce je zhodnotit problematiku e–bezpečnostních znalostí a návyků lidí pracujících ve státní správě. Práce shrnuje, zda pracovníci státní správy znají základní bezpečnostní pravidla práce s počítačem a jak se chrání proti malwaru. Zda používají antivirovou ochranu, firewall a automatické aktualizace. Jak chrání svá data před ztrátou. Pozornost zaměřím i na to, zda rozumí problematice sociálního inženýrství a dokáží rozpoznat phishingový útok. Dále zjišťuji návyky při práci s bezpečnostními hesly, používání silného vs. slabého hesla, používání stejných hesel ve více aplikacích, obměnu hesel a ochranu hesel. Prozkoumám návyky při práci s elektronickou poštou.

Cílem je analyzovat možné závislosti mezi zkoumanými jevy, zvláště pak věkem, pohlavím a vzděláním.

Cílem teoretické části práce je zmapovat počítačové a internetové hrozby, popsat možná rizika, která hrozí pracovníkům státní správy, navrhnout obranu proti těmto rizikům a vykreslit možné důsledky rizikového chování.

# 3 Metoda práce

Bakalářská práce je rozdělena na dvě části, teoretickou a praktickou.

Studiem odborné literatury jsem načerpala informace pro svou teoretickou část. Tato teorie je podpořena srovnávacími testy a průzkumy, které již byly v dané oblasti vykonány. Ty jsou většinou zveřejňovány hlavně na webových stránkách. Vyhledala jsem studie, které se zabývají využíváním počítačů, analýzou hesel a ochranou počítače. Antivirové firmy vydávají řadu odborných článků, které lze využít při analýze rizik ohledně malwaru a spamu. Je řada firem, které se specializují na bezpečnost a zveřejňují svoje analýzy. Čerpala jsem i z článků firmy Microsoft, jelikož je nejsilnější výrobce operačních systémů. Ve východiscích práce jsem zmínila, že internet je využíván k získávání informací. I při psaní mé bakalářská práce byl můj hlavní zdroj informací internet a vyhledávač Google. Všechny tyto studie mi pomohly si vytvořit obraz o aktuální situaci. Tyto informace byly použity k vytvoření praktické části.

V praktické části je proveden vlastní dotazníkový průzkum. Na základě teoretických poznatků jsem stanovila výzkumné problémy, vytvořila hypotézy a podle nich jsem sestavila dotazník. V dotazníku jsem použila jak znalostní, tak i situační otázky. Dotazník obsahuje otevřené i uzavřené otázky na dané téma. Po dokončení dotazníku byl proveden předvýzkum na ověření srozumitelnosti a jednoznačnosti otázek a také byl ověřen čas, který je potřeba pro jeho vyplnění. Zapracováním výsledků pretestu do dotazníku jsem získala konečnou podobu dotazníku pro elektronické dotazování, který jsem následně použila pro sběr dat.

Cílovým vzorkem jsou pracovníci státní správy. Abych zajistila přesnou cílovou skupinu respondentů, zveřejnila jsem elektronickou verzi dotazníku na intranetu, kde byla nastavena práva pouze pro danou skupinu. Využila jsem větvení Sharepointu a vytvořila jsem dotazník, kdy se na základě odpovědi respondenta zobrazují pouze ty otázky, které mu podle odpovědi přísluší. Díky nastavení povinných otázek jsem zajistila úplnost dat. Dotazník byl publikován na intranetu po dobu jednoho měsíce. Výsledky byly automaticky ukládány na server a po uplynutí doby sběru byly statisticky zpracovány. K zpracování dat jsem použila statistických metod Chí–kvadrát test, Studentův t–test a Jednoduchou analýzu rozptylu.

V závěru jsou porovnána výsledná data s obecně doporučovanými standardy. Výsledkem je zmapování situace v dané oblasti. Dále budou získané informace zveřejněny na intranetu, aby oslovení respondenti získali zpětnou vazbu na daný dotazníkový průzkum, na němž se podíleli.

# 4 Hrozby při práci s ICT

## 4.1 Malware

Malware vznikl složením z anglických slov malicius a software, česky škodlivé programy. Jedná se o škodlivé, zákeřné či nežádoucí programy, které se dostaly (většinou) bez vědomí uživatele do jeho zařízení, u kterých po spuštění dochází k úmyslné škodě na operačním systému.

Zpočátku šlo o experimentování s možností samovolně se šířících virů. V průběhu 80. let se začaly objevovat skutečné viry a vzhledem k počtu počítačů a počítačových sítí byly dominantní viry, konkrétně souborové a bootsektorové založené na platformě MS–DOS. Šířily se hlavně disketami. S příchodem operačního systému Windows 95 a programů MS Office se vše změnilo. Makrojazyk v produktech Microsoft posílil natolik, že v něm bylo možné vytvořit i replikující se program - makrovirus[3]. Díky svému rychlému rozvoji se v současnosti stal internet hlavním nositelem šíření malwaru.

Jednotlivé druhy malwaru se liší podle toho, za jakým účelem byly napsány, podle výše nebezpečnosti, mohou mít rozdílné spouštěcí vlastnosti, některé mohou být naprogramovány na spuštění v určitý čas, či aby reagovaly na určitou událost.

Velice často útočník pro dosažení lepších výsledků kombinuje různé druhy. Podle autorů knihy Hacking - manuál hackera [4] „*se malware vyvinul natolik, že se z něj stal jeden z nejrafinovanějších a navíc automatizovaných způsobů hackingu. Útočníkovi stačí investovat nějakou počáteční námahu do vytvoření aplikace, další škody už probíhají automaticky a nevyžadují z jeho strany žádné úsilí. Konkrétní postupy používané malwarem jsou většinou stejné jako ty, které řada útočníků provádí ručně.*"

### 4.1.1 Viry

Vir je škodlivý kód, který se vyskytuje uvnitř souborů. S biologickým virem má mnoho společného, potřebuje svého hostitele (program), kterého nakazí (zkopíruje svoje tělo) a dál se šíří. Umí se vložit do spustitelného souboru, po jehož spuštění se aktivuje a snaží se modifikovat kopií svého kódu do dalších souborů. Při ukončení infikovaného programu, pak vir zůstává v paměti zařízení. Úkolem viru je změna,

poškození či destrukce dat, proto je důležité data pravidelně zálohovat.

Viry můžeme rozlišovat podle cíle infekce: [5]

- Bootovací viry - vir se uloží v bootsektoru diskety či v Master Boot Record pevného disku a při každém spuštění počítače je zaveden do systému. Vir se tak rozšíří ještě předtím, než se spustí antivirový program. Dnes jsou bootviry velmi vzácné, neboť diskety, jako nositelky virů, se dnes používají velmi zřídka.
- Souborové viry - infikují spustitelné soubory a následně vykonávají svůj kód.
- Makroviry - jsou součástí textového souboru podporujícího makra. Tvůrci makrovirů využili možnosti, že lidé častěji sdílí textové dokumenty, než spustitelné programy. Jsou přenášeny infikovanými dokumenty.

První bootovací vir byl virus Brain. Basit a Amjads Farooq Alvi, bratři z Pákistánu, napsali vir s úmyslem infikovat diskety obsahující nelegální software. Brain byl boot virus, šířící se přes disketu, zapomenutou při startu PC v mechanice.[3]

```
Welcome to the Dungeon
© 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN
PHONE :430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination.............  $#@%$@!!
```

Obrázek 1: Zpráva viru Brain

Zároveň je to první a asi i poslední případ, kdy vir obsahuje pravá jména, telefonní čísla a adresu svých autorů a díky tomu nebyl problém autory kontaktovat.

### 4.1.2 Trojský kůň (trojan horses)

Trojský kůň je program vypadající jako legální software, ale zároveň obsahuje skrytou část, která provádí škodlivé operace a to vše bez vědomí uživatele. Maskují se jako užitečná aplikace (např. hry či servisní programy - utility).[6]

Trojský kůň nevytváří další kopie a nedokáže se sám šířit. Aktivuje se nainstalováním a pak začne provádět škodlivé operace.

Druhy trojský koní: [7]

- Backdooor - obchází standardní autentizační mechanismy, instaluje zadní vrátka a skrytě zpřístupňuje počítač útočníkovi a umožňuje mu plné ovládání infikovaného počítače.
- Sniffer - odposlouchává přístupová jména, hesla či čísla platebních karet.
- Keylloger – zaznamenává všechny stisky klávesnice
- Spam server – program je využit pro rozesílání spamu z napadaného zařízení
- Security software disabler – vypíná bezpečnostní programy (firewall, antivirovou ochranu apod.)
- Denial–of–service - slouží K DDoS útokům

Trojský kůň waterfalls.src vypadá jako volně šiřitelný spořič obrazovky a po instalaci otevírá porty počítače a poskytuje vzdálený přístup do infikovaného počítače, aniž by to uživatel tušil.

### 4.1.3 Červi (worm)

Z anglického slova worm. Je to nezávislý program, který sám sebe replikuje do dalších počítačových systémů, kde probíhá škodlivá činnost, pro kterou byl naprogramován. Vyhledávají se jím bezpečnostní skuliny v systémech nebo v poštovních programech. [6]

Nejčastěji se šíří elektronickou poštou, obsahující přílohu s infikovaným souborem. K šíření zneužívají bezpečnostních děr v počítači a rozesílají infikované přílohy uživatelům, kteří jsou evidováni v adresáři kontaktů. Tím je zajištěno, že korespondence je pokládána za věrohodnou. Další možností šíření je počítačová síť. Červ sleduje ostatní počítače v síti a pokud vyhledá zranitelné počítače, tak je napadne. Červi využívají i sdílených prostorů, typickým příkladem jsou weby

typu Ulož.to, odkud si je uživatelé sami stáhnou v domnění, že stahují pouze film. Poslední možností je instant messaging[1], kde červi díky rychlému chatu rozesílají odkaz na infikované stránky, či přímo infikovaný soubor. [8]

Zajímavým červem je I Love You. [9] V roce 2000 infikoval asi 10 % všech počítačů připojených na internet a způsobil škody přes 5 miliard amerických dolarů. Šířil se e–mailem s uvedením textu I LOVE YOU a přílohou LOVE-LETTER-FOR-YOU.TXT.vbs. Pomocí dvojité přípony, měl přimět uživatele k otevření přílohy (v domnění, že se jedná o dokument), poté došlo k infikování počítače a rozeslání kopií infikovaných příloh pomocí uživatelovy e–mailové adresy (tím se zajistilo, že příchozí zpráva pak působila důvěryhodně) na všechny adresy, co byly k dispozici, došlo k úpravě registrů a k provedení změn systémových souborů.

### 4.1.4 Špionážní programy (spyware)

Spyware [10] vznikl složením z anglických slov spy a software, česky vyzvídat, sledovat. Jsou to programy, které bez vědomí uživatele shromažďují a odesílají informace o počítači a chování uživatele. Data jsou obvykle odesílána autorovi za účelem možného zneužití či poskytnutí těchto dat dalším osobám. Programy jsou většinou instalovány nevědomě s jiným instalovaným programem jako doplňková aplikace. Programy pak sledují jména, hesla, e–mailové adresy, navštívené webové stránky, čísla bankovních účtů, čísla platebních karet, licenční čísla softwaru atd. Spyware není schopen sebereplikace.

### 4.1.5 Přesměrovače (hijacker)

Hijacker [11], česky únosce, mění nastavení webového prohlížeče a jeho domovskou stránku. Uživatel je přesunut na úplně jiné webové stránky, než kam chtěl. Tyto stránky pak obsahují řadu hrozeb (často jsou infikované, či s nevhodným a nevyžádaným obsahem).

[1] internetová služba sloužící pro chatování v reálném čase

### 4.1.6 Rootkit

Rootkit sám o sobě není malware, ale spíše nástroj jak utajit malware. Sám o sobě neškodí, ale mění chování operačního systému a zabrání tak jeho odhalení. Nyní se používá rootkit hlavně ke skrývání trojských koní.

První rootkit byl vytvořen firmou SONY a měl bránit nelegálnímu kopírování hudby. Byl přidán přímo na originálním CD s hudbou a tento rootkit sledoval chování uživatele a v případě, že uživatel chtěl získat nelegálně hudbu, zabránil mu v tom. Zároveň odesílal firmě SONY informace o uživateli a to bez jeho vědomí. [12]

### 4.1.7 Botnet, Zombie

Jedná se o malware, který po spuštění zpřístupní infikované zařízení útočníkovi. Útočník tímto způsobem získá více počítačů a tím si vytváří svoji botnetovou síť. Tuto síť pak následně využívá k rozesílání spamu, malwaru či k DDoS útokům [2]. Uživatel napadaného počítače obvykle nic netuší, může zaznamenat zpomalení počítače. Botnety jsou většinou tvořeny řádově desítkami až stovkami tisíc nakažených počítačů, ale mohou dosáhnout i několik desítek milionů. Největší známá botnetová síť BredoLab byla z Arménie. V letech 2009–2010 nakazila 30 milionů počítačů. [13]

### 4.1.8 Logická bomba

Logická bomba je aplikace, skript nebo kód, který je přidán do existujícího programu a je spuštěn po splnění zadaných podmínek (v určitý den, po určitém úkonu - smazání uživatele, provedení zálohy apod.). Aby se logická bomba dostala do zařízení, musí mít útočník k zařízení přístup a patřičná práva. Tento malware může využít administrátor při svém odchodu z práce. [14]

[2]Distributed Denial of Service - (česky odmítnutí služby) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele

### 4.1.9 Adware

Z anglického slova advertising a software, česky reklamní software. Je to aplikace, která zobrazuje reklamu, většinou pomocí vyskakujících oken s reklamou. Je instalován s vědomím a souhlasem uživatele a uživatel je informován o zobrazování reklamy. [15]

## 4.2 Ochrana před malware

Útočníci budou vždy aktivnější, kombinují různé druhy malwaru, tak aby dosáhli větší účinnosti. Proto nestačí chránit se před jedním druhem, ale musíme zavést ochranu před všemi. V následujících kapitolách je popsána ochrana před malware, kterou bychom měli používat jako celek.

Společnost McAffe v roce 2012 pomocí Windows Security Scan plus skenovala 17 mil. počítačů a zjistila, že pouze 83 % zkoumaných počítačů využívá základní ochranu zahrnující antivirový a antispywarový software a firewall. Zbývá tedy 17 % počítačů, které nemají v podstatě žádnou ochranu před malware a dalšími hrozbami. [16]

### 4.2.1 Antivirová ochrana

Antivirový program je základní a nejběžnější ochranou před malwarem. Neposkytuje pouze ochranu před malwarem, ale funguje i jako nástroj pro odstranění malwaru. Měl by být instalován jako první program, teprve později vše ostatní. Po instalaci bychom měli nastavit pravidelnou aktualizaci virové databáze, neboť právě to zajišťuje ochranu proti aktuálním hrozbám.

Většina antivirových programů umožňuje zapnutí rezidentních štítů (real time protection, active shield apod.), která v reálném čase automaticky kontroluje bez zásahu uživatele činnost PC a uživatele. Jakmile začneme pracovat s libovolným souborem, antivir ho ihned zkontroluje. [17]

Tím, že dochází ke kontrole souboru ještě předtím, než dojde k jeho otevření či spuštění, dokážeme kontrolovat i přílohy v e–mailových zprávách [3].

Antivirový program zná pouze známý malware, tudíž poskytuje ochranu před

již rozpoznanými hrozbami. Vždy vznikne mezera mezi objevením nové infekce a vydáním definic a jejich aktualizací.[3] V tento moment je zařízení proti nové infekci nechráněno. Proto je vhodné nastavit u antiviru pravidelnou kontrolu celého disku, abychom našli i malware, který se mohl dostat v této době do zařízení.

Antivirový program může být volně dostupný, nebo komerční. Liší se od sebe dalšími funkcemi a službami, které komerční programy nabízejí navíc, avšak základní antivirovou ochranu nabízejí všechny.

Nemělo by se kombinovat více antivirových systémů.[17] Může docházet ke vzájemným kolizím a nesprávnému detekování malware.

### 4.2.2 Antispywarová ochrana

Antispywarová ochrana, jak už z názvu vyplývá, je určena na ochranu proti spyware, stará se o detekci a odstranění spywarových hrozeb. V současné době řada komerčních antivirových programů poskytuje v rámci svého balíku i antispywarovou ochranu a většinu spywarových hrozeb spolehlivě zachytí. Pokud antivirový program neobsahuje antispywarovou ochranu, pak můžeme použít Windows Defender [18], který je přímo v operačním systému integrován od verze Windows Vista (lze ho doinstalovat i do Windows XP a 2000). Pro důkladnou kontrolu je výhodné použít specializované programy - antispyware, samostatné programy na detekci spyware. Jako u antivirové ochrany, tak i u antispywarové ochrany je důležité nastavit aktualizace databáze.

### 4.2.3 Firewall

Firewall, česky něco jako bezpečnostní brána, má za úkol oddělovat provoz mezi dvěma sítěmi (naší domácí a internetem). Chrání tak před průniky zvenčí a odesílání dat ze sítě bez vědomí a souhlasu uživatele. Firewall je buď zařízení či software sledující a blokující síťový provoz počítače ve směru z internetu do počítače a opačně. [19] Nastavení brány firewall je důležitým krokem při ochraně počítače, který by měl být proveden ještě před připojením k internetu. Firewall je běžnou součástí Windows a ve výchozím nastavení je zapnutý.

### 4.2.4 Aktualizace nejen operačního systému

V každém operačním systému, nebo programu se vyskytují bezpečnostní chyby. Jejich tvůrci se snaží tyto chyby odstraňovat a poskytují opravy těchto chyb. Firma Microsoft vydává pravidelně aktualizace svých produktů, nejen operačního systému, ale i kancelářské balíčky, internetové prohlížeče, Visual Studio, NET.Framework apod. K aktualizaci využijeme zabudované funkce Windows Update, které jen zapneme a nastavíme. Pokud se množství aktualizací nahromadí, jsou vydány Service Packy. [20] Je to aktualizace systému Windows, která často kombinuje dříve vydané aktualizace a pomáhá zajistit vyšší spolehlivost systému Windows.

Měli bychom pravidelně aktualizovat i další programy jiných výrobců. V případě, že daný program nabízí automatické aktualizace, je vhodné je zapnout, abychom měli stále aktuální verzi programu. Existují i programy, které kontrolují dostupné nové verze a informují o nich uživatele např. Secunia Personal Software Inspector.

Dokud uživatelé nebudou udržovat svá zařízení aktuální, budou útočníci této skutečnosti využívat k šíření malwaru. [21]

### 4.2.5 Uživatelská práva

„*Standardní účet pomáhá chránit počítač tím, že zabraňuje uživatelům provádět změny, které mají vliv na všechny uživatele počítače, například odstranění souborů, které jsou nezbytné pro provoz počítače. Doporučuje se pro každého uživatele vytvořit standardní uživatelský účet.*" [22]

Bezpečnostní zpráva firmy Avecto [23] za rok 2015 zkoumala zranitelnosti, které ovlivňují Windows, Office, Windows Server, Internet Explorer a další.

Výsledky toho, kolik zranitelností mohlo být zmírněno, pokud by uživatel neměl administrátorská práva:

- 85 % všech kritických zranitelností zdokumentovaných ve zprávě.
- 99.5 % všech zranitelností hlášených v aplikaci Internet Explorer.

- 82 % všech zranitelností, které ovlivňují Microsoft Office.

## 4.3 Spam

Spam je nevyžádaná elektronická pošta, rozeslaná na velké množství e–mailových adres, často s podvrženou adresou odesílatele. Dnes se spam vyskytuje i v diskuzích, blogách, fórech, návštěvních knihách atd. Hlavním důvodem rozesílání spamu je zisk. Internet je prohledáván roboty za účelem vytvoření databází e–mailových adres, které se dále poskytují za úplatu dalším osobám, většinou za účelem rozesílání dalšího spamu.

Král [19] uvádí, že spam představoval v roce 2006 60–70 % příchozích poštovních zpráv. Ve studii společnosti Trustware[2] se uvádí, že v roce 2014 je 60 % emailových zpráv spam, z toho 6 % je infekčních.

Antispywarové řešení pracuje pomocí seznamu důvěryhodných (whitelist) a spamových (blacklist) adres. Pokud je odesílatel na jednom ze seznamů, je e–mail doručen či označen za spam. Ostatní e–maily jsou kontrolovány (vzorky zpráv, statistická heuristika, rozpoznávací algoritmy a další jedinečné metody) a označeny, zda se jedná o spam, nebo ne [24].

### 4.3.1 Ochrana před spamem

- Na svém e–mailovém účtu aktivujeme antispamovou kontrolu, pokud již není aktivovaná.
- Nezveřejňujeme nadbytečně na internetu svou e–mailovou adresu.
- Jsme opatrní a neotvíráme e–maily od neznámého odesílatele.
- Není vhodné klikat na všechny odkazy a spouštět přílohy.
- Na nevyžádané zprávy nereagujeme.
- Aktualizujeme operační systém a používáme aktualizovaný antivir a firewall, abychom se vyhnuli nákaze a sami nerozesílali spam z našeho zařízení.

## 4.4 Hoax

Anglické slovo hoax v překladu znamená: falešná zpráva, mystifikace, novinářská kachna, podvod, poplašná zpráva, výmysl, žert, čí kanadský žertík. V počítačovém světě slovem hoax nejčastěji označujeme zprávu, která uživatele varuje před určitým nebezpečí, či prosby o pomoc, často s výzvou o rozeslání na další adresy. Mohou to být i již neaktuální prosby o pomoc, které jsou stále posílány. [25]

Hoax obtěžuje příjemce, zatěžuje linky a poštovní servery, v horším případě je přetíží a může sloužit ke sběru e–mailových adres.

### 4.4.1 Ochrana před hoaxem

- Hlavní ochranou před hoaxem je vnímavý uživatel, který dokáže nad obsahem sdělení e–mailu přemýšlet. Pokud e–mail obsahuje popis nebezpečí, či prosbu o pomoc a zároveň výzvu k přeposílání, bude se s velkou pravděpodobností jednat o hoax.
- Při pochybnostech nad obsahem, mohu provést kontrolu, zda se nejedná o hoax v databázi www.hoax.cz.
- Pokud je to vhodné poskytneme osvětu – slušně napíšeme odesilateli, zda ví o tom, že posílá hoax.

## 4.5 Hesla

K autentizaci uživatele můžeme použít mnoho nástrojů jak ověřit identitu osoby, která přistupuje k systému.

Základní metody autentizace:

- Znalost tajné informace – např. znalost kombinace jména a hesla, nebo PIN
- Vlastnictví autentizačního předmětu – např. hardwarový klíč, čipová karta, token
- Biometrické údaje – např. otisk prstu, snímek oční duhovky, obraz krevního řečiště apod.

Můžeme se setkat i s vícefaktorovou autentizací uživatele, kdy dochází ke kombinaci předešlých metod. Nejčastější použití je v elektronickém bankovnictví při použití certifikátu na čipové kartě (vlastnictví autentizačního předmětu) a znalosti PINU (znalost tajné informace). V budoucnu se s dvoufaktorovou autentizací seznámí každý občan ČR. Ministerstvo vnitra v projektu eIDAS [26] připravuje občanský průkaz s čipem jako datový nosič státem garantované identity.

Nejčastěji užívanou autentizační metodou je autentizace důkazem znalostí, tedy například znalostí hesla. [27]

### 4.5.1 Síla hesla

Síla hesla může ovlivňovat dobu, po kterou zůstane heslo tajné, měli bychom dodržovat několik doporučení firmy Microsoft.

Silné heslo splňuje tyto podmínky:

- Je alespoň osm znaků dlouhé.
- Neobsahuje uživatelské jméno, skutečné jméno nebo jméno společnosti.
- Neobsahuje úplné slovo.
- Je výrazně odlišné od předchozích hesel.
- Obsahuje znaky ze všech čtyř následujících kategorií:
  - Velká písmena
  - Malá písmena
  - Číslice
  - Symboly na klávesnici (všechny znaky na klávesnici, které nespadají do kategorie písmen či číslic) a mezery např. ‘ ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; ” ’ < > , . ? / [28]

Selecký[29] ještě uvádí jako ideální počet znaků v některých případech až 14 znaků a heslo by nemělo obsahovat stejné znaky ze stejné skupiny.

### 4.5.2 Útoky proti heslům

Podle způsobu provedení a podle technických prostředků můžeme útoky na prolomení hesel rozdělit na [30]:

- Útok hrubou silou (brute–force) - útočník systematicky zkouší všechny možné kombinace znaků (variace s opakováním). Je časově náročný, vhodný pouze pro slabá hesla. Jediná obrana je komplexnost hesla a jeho délka.
- Slovníkový útok - útočník zkouší fráze, které jsou obsaženy ve slovníku, tím dochází k zúžení variant. Slovník obsahuje jména, časté loginy, běžná slova a fráze, sekvence kláves (asdfg, q1w2e3) apod.
- Recyklace hesla - útočník využívá, že uživatelé mnohdy používají stejné heslo k více účtům. Pokud útočník získá toto heslo, získá tím přístup i do ostatních aplikací, které byly chráněny stejným heslem.
- Sociální inženýrství - útočník odhalí heslo na základě znalostí o uživateli.

### 4.5.3 Passphrase

Roboti, kteří jsou použiti k útokům na heslo, o nich nic nevědí, neznají strukturu hesla a musí ho uhádnout jako celek. Z toho vychází Thomas Baedal [31] který tvrdí, že heslo, které se skládá z několika slov a je podstatně delší než běžné heslo, je bezpečnější než komplexní heslo. To popírá všechny doporučované postupy, pointou celého článku je předpoklad, že trojsloví „this is fun" je jako heslo bezpečnější než zdánlivě nesrozumitelný a nerozpoznatelný text „ j4fS<2".

### 4.5.4 Ochrana hesel

Při ochraně hesel hodně záleží na tom, jak s nimi zacházíme a jak je používáme.

- Hesla nesdělujeme dalším osobám, společná hesla jsou časem prozrazena.
- Hesla zadáváme tak, aby nemohla být odpozorována.
- Neposíláme heslo v e–mailu.

- V prohlížeči nepoužíváme zapamatování hesel, při ovládnutí systému získá útočník i uložená hesla.
- Při prolomení hesla zkusí útočník heslo i do dalších aplikací, proto nepoužíváme stejná hesla do více aplikací. [30]
- Pravidelnou obměnou hesla můžeme zajistit, že platnost hesla bude kratší, než doba potřebná k jeho prolomení a ztížíme práci útočníkům. Obecně platí čím slabší heslo, tím častější obměna hesla. Král [19] doporučuje pravidelnou obměnu hesla 90 dní.
- Pokud nemáme zařízení pod kontrolou (veřejně přístupné počítače - počítače v internetových kavárnách, na letištích, v informačních kioscích), nepoužíváme v těchto zařízeních svá hesla.

Pokud si musíme svá hesla poznamenat, uložíme je na bezpečném místě, případně použijeme vhodný program pro správu hesel např. KeePass, 1Password, LastPass, Sticky Password a další. Jde o softwarový trezor, do kterého si uložíte Vaše hesla, často jdou uložit do programu i jiné cenné informace. Některé z nich jsou bezplatné.

Některé systémy umožňují získat zapomenuté heslo pomocí kontrolních otázek, kterým bychom měli věnovat naší pozornost. Útočník může předstírat, že zapomněl heslo a využít těchto kontrolních otázek, zvláště pokud může tyto informace získat z jiných zdrojů. Doporučuje se na tyto otázky neodpovídat pravdivě, najít si souvislost s otázkou a odpovědí tak, abychom si jí zapamatovali, případně si jí zapsat do programů pro správu hesel.

### 4.5.5 Historie úniků hesel a jejich analýza

Podle průzkumu roku 12/2009, kdy bylo společností Imperva[32] analyzováno 32. mil. hesel, vyplývá:

- Zhruba 50 % uživatelů používá krátké heslo (7 znaků a méně).
- Téměř 60 % uživatelů má hesla, která obsahují pouze písmena a číslice.

- Asi 50 % lidí používá stejné (nebo velmi podobné) heslo pro všechny weby.
- Téměř 50 % uživatelů používá snadno odhadnutelná hesla.
- Nejběžnějším heslem je „123456“.

Souvisí to i s další studií [33] analýzy hesel, kdy ze společnosti Adobe uniklo cca 150. mil hesel. Výsledkem analýzy bylo zjištění, že 1,9 mil. uživatelů mělo nejběžnější heslo „123456“.

V 11/2010 byl nezávislou agenturou Javelin Research & Strategy proveden průzkum[34] mezi 1003 uživateli internetu starších 18 let pro firmu Symnatec. Zde jsou výsledky:

- Téměř polovina (46 %) dotázaných přiznala, že nikdy nezměnila své heslo e–mailového účtu.
- Přibližně třetina (31 %) nikdy nezměnila své heslo bankovního a finančního účtu.
- 42 % respondentů nikdy nezměnila své heslo na stránkách sociálních sítí.
- 72 % respondentů, kteří mají jedno heslo na různých účtech / webových stránkách, tvrdí, že to tak mají, protože je snadnější si to pamatovat.

Na přelomu roku 2015/6 byl napaden twitterový účet premiéra Sobotky [35] a jeho soukromý e–mail hackery i přestože měl dostatečně silné heslo.

V roce 2014 unikly z cloudového úložiště Applu fotky řady celebrit. Některé z nich byly značně choulostivé. Podle prohlášení Applu [36] nedošlo k průniku do některého systému Applu, včetně iCloudu nebo funkce Find my iPhone. Účty byly napadeny útokem cíleným na uživatelská jména, hesla a kontrolní otázky.

Studie společnosti Google[37] potvrzuje, že kontrolní otázky mohou být velkou bezpečnostní dírou, která umožní útočníkům prolomit bezpečnostní údaje. Ve studii si 40 % uživatelů vůbec nedokázalo vzpomenout na správnou odpověď na kontrolní otázku a u otázky „Vaše oblíbené jídlo?“ odpovědělo 20 % anglicky mluvících uživatelů pizza.

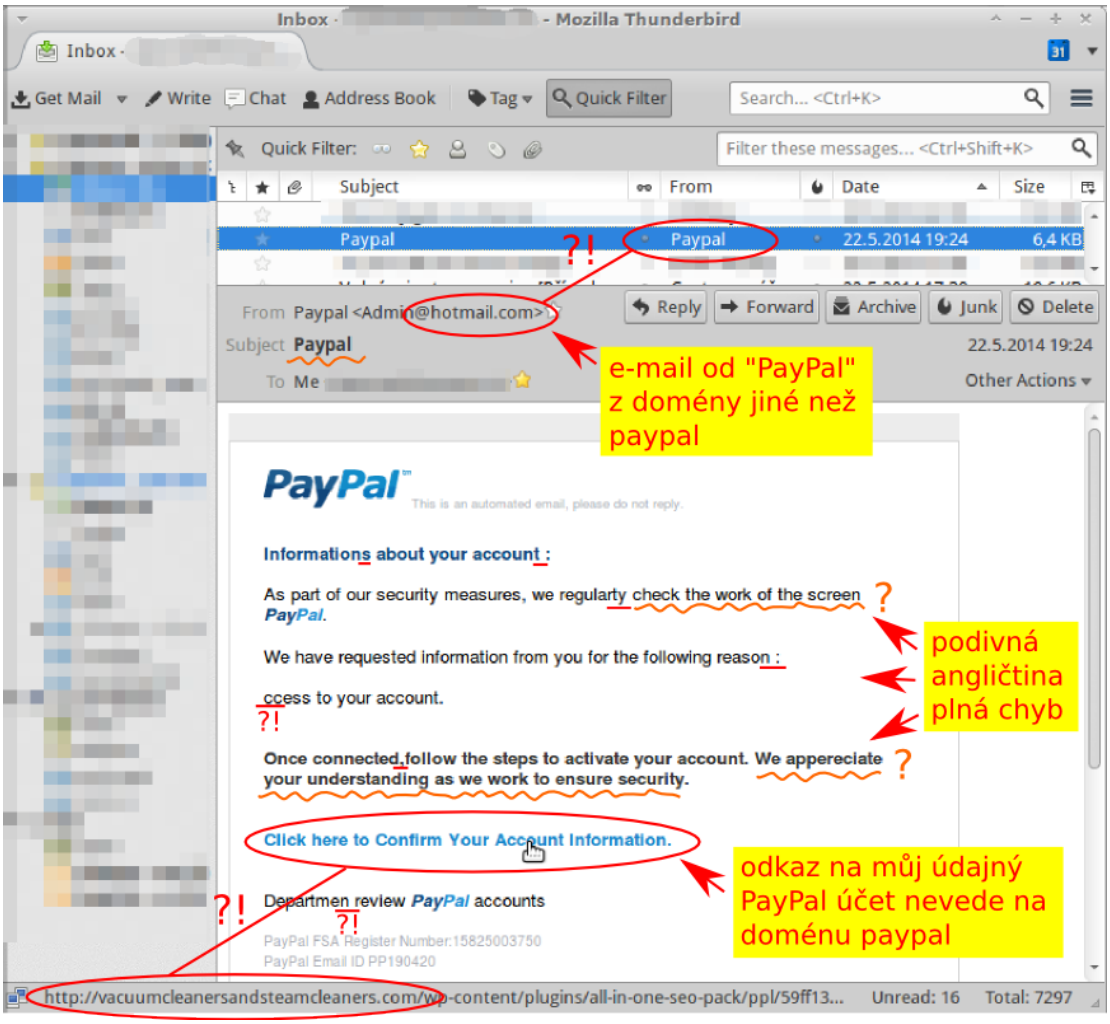
## 4.6 Phishing

Phishing vzniklo spojením dvou anglických výrazů fishing a phreaking. Můžeme se také setkat s označením rhybaření. [38]

Phishing využívá metodu sociálního inženýrství, rozesláním falešného e–mailu příjemci, který napodobuje legální instituci s cílem vyzvědět od příjemce důvěrné informace. Takový e–mail většinou vyzývá adresáta, aby navštívil falešné webové stránky, které jsou na první pohled totožné jako oficiální stránky instituce, vypadají věrohodně a jsou těžko rozeznatelné. Na těchto stránkách má uživatel zadat důvěrné informace (číslo platební karty, heslo k bankovnímu účtu) a tím prozradit útočníkům údaje, které jsou následně zneužity. [10]

Podle NBÚ se útoky za rok 2013 a 2014 příliš neliší. Nejvíce útoků je založeno na bázi sociálního inženýrství (phishing, spear–phishing). Ačkoli útočníci používají stále nové a sofistikovanější metody, cílem útoků je získání přístupových hesel, případně zajištění přísunu užitečných informací. [39]

Phishingové útoky už několik let sleduje společnost APWD [40] a z posledního reportu za 4. čtvrtletí roku 2014 vyplývá, že phishingových útoků za dané období bylo 197 252. Je to nárůst oproti předchozímu čtvrtletí o 18 %. Zajímavé je, v jakých odvětvích jsou phishingové útoky prováděny. Cílem útoků byl maloobchod 30 %, platební služby 25 %, finanční služby 21 %, e–mail 12 % a sociální sítě 6 %.




Obrázek 2: Ukázka phishingového e–mailu s vysvětlením Autor: crysman – Vlastní dílo, CC0, https://commons.wikimedia.org/w/index.php?curid=33067716

### 4.6.1 Pharming

Pharming[41] je pokročilejší variantou phishingu, jde o útok, kdy je správná IP adresa změněna na IP adresu webu škůdce, napadený potom komunikuje s útočníkem v domnění, že se jedná o správnou instituci (například banku).

### 4.6.2 Ochrana před phishingem a pharmingem

- Používáme základní bezpečnostní software - aktualizovaný operační systém, antivirový program, antispywarový program a firewall.
- Potřebujeme–li vstoupit na stránky internetového bankovnictví nebo na stránky příslušné organizace, raději napíšeme internetovou adresu do prohlížeče sami, nepoužíváme poslané odkazy z e–maliové zprávy.
- Pokud se elektronické bankovnictví chová nestandardně nebo jsou požadovány jiné údaje než obvykle, nezadáváme je a aplikaci ukončíme.
- Nespouštíme neznámé programy, které přijdou e–mailem, ani na které e–mail odkazuje.
- Zařízení, které nemáme pod kontrolou, nepoužíváme k přístupu do aplikací, kde zadáváme citlivé informace.
- Dávejme pozor na překlepy v adresách webů. [42]
- Banky po svých klientech nepožadují zasílání citlivých údajů po internetu.

## 4.7 Zálohování

Za nejcennější v počítači považujeme svá data, a proto bychom je měli chránit před jejich ztrátou. K té může dojít poškozením pevného disku, ztrátou zařízení, smazáním souborů, nebo při napadení zařízení malwarem, ale i nezkušeností či nepozorností uživatele . Pravidelné zálohování je prevence před ztrátou dat.

Zálohovat můžeme zkopírováním dat na externí úložiště dat, např. druhý disk, externí disk nebo jiné datové úložiště, můžeme také využít specializovaný zálohovací program, nebo možností operačního systému vytvářet zálohy, tím si vytvoříme bezpečnostní kopie důležitých souborů. [43]

Zálohování slouží také k zachycení aktuálního obrazu celého systému. Nejvhodnější doba pro vytvoření obrazu je po instalaci operačního systému a přidání

nezbytných programů. S takovou zálohou můžeme kdykoliv obnovit svoje zařízení do stavu, ve kterém byl při vytváření obrazu. [44]

Pokud považujeme svá data za citlivá, můžeme použít na ochranu těchto dat šifrování. Šifrování je kryptografický algoritmus, který převádí čitelná data na její nečitelnou podobu neboli šifrový text. Šifrování dat nás chrání především v případě ztráty, nebo krádeže našeho notebooku, či přenosného média. [45]

Podle průzkumu [46] v roce 2011 35 % uživatelů nikdy nezálohovalo svůj počítač. 51 % uživatelů zálohuje méně než jednou za rok nebo vůbec. Pouze 7 % uživatelů zálohovalo denně, 14 % provádělo zálohy alespoň jednou týdně. Jednou za měsíc svá data zálohovalo 27 % uživatelů.

Zajímavá zjištění přináší i analýza výrobce počítačů HAL3000. Ukazují, že 75 % domácností nechrání svá data proti ztrátě. Nejčastější příčinou ztráty dat je podle výrobce počítačů HAL3000 selhání hardwaru, které je na vině ve 35,7 % případů. Následuje selhání lidského faktoru s podílem 30,3 %, fyzická krádež hardwaru s podílem 19,3 % a paradoxně i selhání samotného zálohování s podílem 14,9 % případů ztráty dat. [47]

# 5 Výzkumný záměr

## 5.1 Formulace výzkumného problému, a definování hypotéz

Stanovila jsem hlavní výzkumný problém.

- Jaké faktory hrají roli při bezpečném chování při používání ICT?

Určila jsem výzkumné otázky:

- Existuje vztah mezi ztrátou dat a zálohováním?
- Jak lidé zálohují svá data?
- Existuje vztah mezi ochranou před malwarem a nákazou malwarem?
- Používají lidé základní softwarovou ochranu před útoky?
- Jsou obezřetní při e–mailové komunikaci?
- Má pohlaví, věk, nebo vzdělání lidí vliv na nákazu malwarem?
- Má pohlaví, věk, nebo vzdělání lidí vliv na zabezpečení PC?
- Má pohlaví, věk, nebo vzdělání lidí vliv na zálohování?
- Má pohlaví, věk, nebo vzdělání lidí vliv na ztrátu dat?
- Má pohlaví, věk, nebo vzdělání lidí vliv na phishingový útok?
- Dokáží lidé odhalit phishingový útok?
- Jak lidé pracují s hesly?
- Má pohlaví, věk, nebo vzdělání lidí vliv na používání hesel?
- Existuje vztah mezi sílou hesla, počtem hesel, počtem obměn hesel k různým aplikacím?

- Dokáží lidé stanovit míru bezpečnosti svých hesel?
- Existuje vztah mezi používáním internetového bankovnictví a sílou hesla?

Na základě těchto výzkumných otázek byly stanoveny hypotézy:

- H01: Mezi zálohováním a ztrátou dat neexistuje závislost.
- HA1: Mezi zálohováním a ztrátou dat existuje závislost.
- H02: Mezi používáním antivirového programu a nákazou malwarem neexistuje závislost.
- HA2: Mezi používáním antivirového programu a nákazou malwarem existuje závislost.
- H03: Mezi používáním základní softwarové ochrany a nákazou malwarem neexistuje závislost.
- HA3: Mezi používáním základní softwarové ochrany a nákazou malwarem existuje závislost.
- H04: Mezi používáním firewallu a nákazou malwarem neexistuje závislost.
- HA4: Mezi používáním firewallu a nákazou malwarem existuje závislost.
- H05: Mezi aktualizací operačního systému a nákazou malwarem neexistuje závislost.
- HA5: Mezi aktualizací operačního systému a nákazou malwarem existuje závislost.
- H06: Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele neexistuje závislost.
- HA6: Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele existuje závislost.

- H07: Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu neexistuje závislost..
- HA7: Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu existuje závislost.
- H08: Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech neexistuje závislost.
- HA8: Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech existuje závislost.
- H09: Mezi ztrátou dat a nákazou malwarem neexistuje závislost.
- HA9: Mezi ztrátou dat a nákazou malwarem existuje závislost.
- H010: Mezi zálohováním a nákazou malwarem neexistuje závislost.
- HA10: Mezi zálohováním a nákazou malwarem existuje závislost.
- H011: Mezi nákazou malwarem a pohlavím neexistuje závislost.
- HA11: Mezi nákazou malwarem a pohlavím existuje závislost.
- H012: Mezi nákazou malwarem a vzděláním neexistuje závislost.
- HA12: Mezi nákazou malwarem a vzděláním existuje závislost.
- H013: Mezi nákazou malwarem a věkem neexistuje závislost.
- HA13: Mezi nákazou malwarem a věkem existuje závislost.
- H014: Mezi používáním základní softwarové ochrany a pohlavím neexistuje závislost.
- HA14: Mezi používáním základní softwarové ochrany a pohlavím existuje závislost.

- H015: Mezi používáním základní softwarové ochrany a vzděláním neexistuje závislost.
- HA15: Mezi používáním základní softwarové ochrany a vzděláním existuje závislost.
- H016: Mezi používáním základní softwarové ochrany a věkem neexistuje závislost.
- HA16: Mezi používáním základní softwarové ochrany a věkem existuje závislost.
- H017: Mezi zálohováním a pohlavím neexistuje závislost.
- HA17: Mezi zálohováním a pohlavím existuje závislost.
- H018: Mezi zálohováním a vzděláním neexistuje závislost.
- HA18: Mezi zálohováním a vzděláním existuje závislost.
- H019: Mezi zálohováním a věkem neexistuje závislost.
- HA19: Mezi zálohováním a věkem existuje závislost.
- H020: Mezi ztrátou dat a pohlavím neexistuje závislost.
- HA20: Mezi ztrátou dat a pohlavím existuje závislost.
- H021: Mezi ztrátou dat a vzděláním neexistuje závislost.
- HA21: Mezi ztrátou dat a vzděláním existuje závislost.
- H022: Mezi ztrátou dat a věkem neexistuje závislost.
- HA22: Mezi ztrátou dat a věkem existuje závislost.
- H023: Mezi setkáním s phishingovým útokem a pohlavím neexistuje závislost.
- HA23: Mezi setkáním s phishingovým útokem a pohlavím existuje závislost.

- H024: Mezi setkáním s phishingovým útokem a vzděláním neexistuje závislost.
- HA24: Mezi setkáním s phishingovým útokem a vzděláním existuje závislost.
- H025: Mezi setkáním s phishingovým útokem a věkem neexistuje závislost.
- HA25: Mezi setkáním s phishingovým útokem a věkem existuje závislost.
- H026: Mezi setkáním s phishingovým útokem a otázkou na potvrzení hesla neexistuje závislost.
- HA26: Mezi setkáním s phishingovým útokem a otázkou na potvrzení hesla existuje závislost.
- H027: Muži a ženy se neliší v síle hesla.
- HA27: Muži a ženy se liší v síle hesla.
- H028: Mezi sílou hesla a vzděláním neexistuje závislost.
- HA28: Mezi sílou hesla a vzděláním existuje závislost.
- H029: Mezi sílou hesla a věkem neexistuje závislost.
- HA29: Mezi sílou hesla a věkem existuje závislost.
- H030: Mezi sílou hesla a používáním internetového bankovnictví neexistuje závislost.
- HA30: Mezi sílou hesla a používáním internetového bankovnictví existuje závislost.
- H031: Mezi sílou hesla a představou o bezpečnosti hesla neexistuje závislost.
- HA31: Mezi sílou hesla a představou o bezpečnosti hesla neexistuje závislost.
- H032: Mezi sílou hesla a obměnou hesla neexistuje závislost.

- HA32: Mezi sílou hesla a obměnou hesla existuje závislost.
- H033: Mezi sílou hesla a počtem používaných hesel neexistuje závislost.
- HA33: Mezi sílou hesla a počtem používaných hesel existuje závislost.
- H034: Mezi sílou hesla a používáním antivirové ochrany neexistuje závislost.
- HA34: Mezi sílou hesla a používáním antivirové ochrany existuje závislost.
- H035: Mezi sílou hesla a používáním firewallu neexistuje závislost.
- HA35: Mezi sílou hesla a používáním firewallu existuje závislost.
- H036: Mezi sílou hesla a aktualizací operačního systému neexistuje závislost.
- HA36: Mezi sílou hesla a aktualizací operačního systému existuje závislost.
- H037: Mezi sílou hesla a používáním základní softwarové ochrany neexistuje závislost.
- HA37: Mezi sílou hesla a používáním základní softwarové ochrany existuje závislost.
- H038: Mezi sílou hesla a nákazou malwarem neexistuje závislost.
- HA38: Mezi sílou hesla a nákazou malwarem existuje závislost.
- H039: Mezi sílou hesla a ztrátou dat neexistuje závislost.
- HA39: Mezi sílou hesla a ztrátou dat existuje závislost.
- H040: Mezi sílou hesla a zálohováním neexistuje závislost.
- HA40: Mezi sílou hesla a zálohováním existuje závislost.

## 5.2 Cílová skupina

Cílovým vzorkem jsou osoby pracující ve státní správě. Za účastníky výzkumu byli vybráni pracovníci Finančního úřadu pro Jihočeský kraj, jeho podřízené Územní pracoviště a Centrum služeb v Českých Budějovicích. Celkově bylo osloveno 951 lidí. Návratnost dotazníku je 387 zodpovězených dotazníků, což činí 41 % z celkového počtu. Dotazník byl zveřejněn v období 21. 1.–23. 2. 2016.

## 5.3 Způsob sběru dat

Jako nejvhodnější metoda sběru dat byla vybrána metoda elektronického dotazování pro své výhodné zaměření na cílovou skupinu. Dotazník byl zveřejněn na intranetu Finančního úřadu pro Jihočeský kraj, kde byla ošetřena práva na web tak, aby všichni respondenti odpovídali pouze vybrané cílové skupině. Díky zvolené metodě jsou všechny zodpovězené dotazníky ukládány v elektronické podobě a tím odpadá i chybovost při přepisu získaných dat z dotazníku do počítače. Díky nastavení povinných otázek jsem zajistila úplnost všech odpovědí. V případě, že respondent nevyplnil dotazník až do konce, nedošlo k jeho uložení. Využila jsem i větvení v Sharepointu, kdy se respondentovi v souvislosti s odpovědí na předchozí otázky zobrazí jen  otázky, na které má odpovídat. Ostatní otázky jsou pro něj skryty.

## 5.4 Návrh výzkumného nástroje, dotazníku

Pro předvýzkum a samotný výzkum byla zvolena výzkumná metoda dotazník. V dotazníku byly použity jak otázky otevřené, tak i uzavřené.[48]

Otevřené otázky nenabízí žádnou variantu odpovědi, respondent na ně odpovídá vlastními slovy. Výhodou je, že získáváme širší pohled respondenta na otázku, často se objevují i nečekané odpovědi. Nevýhodou je náročnější analýza a také záleží na vyjadřovacích schopnostech respondenta.

Ukázka otázky:

`Napište do jakých aplikací sdílíte hesla`

. . . . . .

Uzavřené otázky předem nabízí několik možných variant odpovědi a respondent je tak rychle a snadno zodpoví. Další výhodou je rychlá analýza dat. Nevýhodou je nutnost volit jen z daných variant odpovědí a pokud nejsou odpovědi dobře formulovány, může se stát, že respondent nenajde tu správnou odpověď, která odpovídá jeho představám. [49]

Ukázka otázky:

```
Došlo u Vás někdy ke ztrátě dat?
o Ano, data byla zálohovaná, ke ztrátě nakonec nedošlo
o Ano, data nebyla zálohovaná a nemrzelo mě to
o Ano, data nebyla zálohovaná a mrzelo mě to
o Ne
```

Dále byly v dotazníku použity otázky dichotomické, trichotomické, vícehodnotové, filtrační a kontaktní.

Dichotomické otázky - nabízejí jen dvě možnosti odpovědí, ano či ne. Jedná se o lehce zodpověditelné otázky, často jsou využívány také ke třídění.

Ukázka otázky:

```
Měníte si své heslo?
o Ano
o Ne
```

Trichotomické otázky - jedná se o rozšířenou dichotomickou otázku, ke které je přidána úniková otázka nevím, či neznám. Využívají se tam, kde respondent nemusí mít potřebné znalosti k zodpovězení otázky a nedochází tak ke zkreslení výsledků.

Ukázka otázky:

```
Používáte na svém zařízení firewall?
o Ano
o Ne
o Nevím, o zařízení se stará někdo jiný
```

Vícehodnotové otázky - respondenti mohou vybírat jednu nebo více odpovědí.

Ukázka otázky:

```
Víte jakou cestou se škodlivý software dostal do Vašeho zařízení?
```

☐ Nákazou z přílohy v e-mailu
☐ Nákazou z webových stránek
☐ Absence antiviru
☐ Neaktualizovaný antivir
☐ Nakažené médium (CD, USB disk)
☐ Nevím

Filtrační otázky - jsou určeny k třídění respondentů v souvislosti s odpověďmi na otázky. Další otázky závisí od toho, do jaké skupiny byl respondent zařazen.[50]

Ukázka otázky:

Zálohujete svá data?
o Ano, pravidelně
o Ano, nepravidelně vždy po nějaké události
o Ne
o Nevím co je zálohování dat

Pokud respondent vybere jakékoliv „Ano" bude odpovídat na otázky ohledně zálohování, ostatní respondenti bude pokračovat v dotazníku dalšími otázkami.

Kontaktní otázky - jsou jednoduché, srozumitelné otázky, které mají respondenta zaujmout.

Ukázka otázky:

Které z následujících zařízení používáte k přístupu na internet?
☐ Notebook/netbook
☐ Stolní počítač
☐ Chytrý mobilní telefon
☐ Tablet

Na začátku dotazníku byly použity kontaktní otázky. Následovaly otázky formulované na základě hypotéz a poznatků z teoretické části. V závěru dotazníku byly použity identifikační údaje. Dbala jsem na to, aby respondent přesně pochopil, nač je tázán, a aby výběr odpovědí byl co nejširší a nejvýstižnější. Toto jsem ověřovala v předvýzkumu.

## 5.5 Předvýzkum

Před samotným výzkumem byl proveden předvýzkum formou písemného dotazování. Cílem bylo ověřit reakce na jednotlivé otázky. Bylo osloveno celkem osm lidí, čtyři pracovníci IT a čtyři běžní pracovníci. Ověřovala jsem srozumitelnost a formulování otázek, zda respondent našel v nabídkách odpovědí svoji požadovanou a prověřovala jsem délku vyplňování. Pracovníci IT byli navíc požádáni o kontrolu, zda u otázek nemůže nastat ještě další možná varianta odpovědi a běžní pracovníci byli navíc požádáni o kontrolu srozumitelnosti textu, zda nejsou v dotazníku použity odborné výrazy, kterým by nerozuměli. Také mě zajímala doba, kterou respondent strávil při vyplňování dotazníku [48].

Na základě zjištěných informací jsem upravila dotazník pro elektronické dotazování tak, aby mohl být zveřejněn na Sharepointu. Došlo k vyřazení otázky č.23 Jak přistupujete do internetového bankovnictví?

## 5.6 Použitá statistická metoda

K analýze dat jsem použila statistické metody Chí–kvadrát test - test nezávislosti, Studentův t–test - dvouvýběrový a Jednoduchou analýzu rozptylu. Pro neúplnost odpovědí jsem vyřadila jeden vzorek.

### 5.6.1 Chí–kvadrát test - test nezávislosti

Jedná se o statistickou neparametrickou metodu, pro analýzu nominálních dat. Používá se k zjištění závislosti dvou kvalitativních veličin měřených na prvcích téhož výběru. Porovnáváme pozorované a očekávané četnosti. Při výpočtu vycházíme z předpokladu, že platí nulová hypotéza, která předpokládá, že mezi dvěma kvalitativními veličinami není žádná závislost. Velikost rozdílů posuzujeme pomocí testové statistiky $X^2$. Dále určíme počet stupňů volnosti tabulky a hladinu významnosti. Vypočítá se hladina významnosti testu $p$–hodnota. Pokud je menší než hladina významnosti, nulovou hypotézu zamítáme a přijímáme alternativní. Test nezávislosti nelze použít pokud více než 20 % očekávaných četností je menších než 5, nebo v případě, že v některé z očekávaných četností je menší než 1.

[51]

$$X^2 = \sum_{i,j} \frac{(ZjištěnáČetnost_{ij} - OčekávanáČetnost_{ij})^2}{OčekávanáČetnost_{ij}}$$

Obrázek 3: Chí-kvadrát - vzorec pro testovou statistiku

### 5.6.2 Studentův t–test - dvouvýběrový

Jedná se o statistický test významnosti pro analýzu metrických dat. Používá se k hodnocení rozdílů dvou výběrových průměrů nezávislých souborů. Rozhodujeme, zda dva soubory dat, získané měření ve dvou různých skupinách, mají stejný aritmetický průměr. Tento test předpokládá, že rozptyly jsou v obou skupinách stejné. Dále určíme hladinu významnosti a vypočítáme hladinu významnosti testu $p$–hodnota. Pokud je menší než hladina významnosti, nulovou hypotézu zamítáme a přijímáme alternativní. [49]

### 5.6.3 Jednoduchá analýzu rozptylu

Jedná se o statistický test významnosti pro analýzu metrických dat. Umožňuje provádět vícenásobné porovnávání středních hodnot. Je založena na hodnocení vztahů mezi rozptyly porovnávaných výběrových skupin. Tento test předpokládá, že rozptyly jsou v obou skupinách stejné. Dále určíme hladinu významnosti a vypočítáme hladinu významnosti testu $p$–hodnota. Pokud je menší než hladina významnosti, nulovou hypotézu zamítáme a přijímáme alternativní. [51]

### 5.6.4 Hesla a jejich ohodnocení

Požadavkům na sílu hesla od firmy Microsoft [28] odpovídá pouze 12 respondentů. Požadavky jsou: heslo má obsahovat malá písmena, velká písmena, číslice, speciální znak, v hesle se nepoužívá osobní údaj ani slovo nějakého významu a zároveň počet znaků v hesle je větší něž 7.

Proto jsem pro další hypotézy jsem každé heslo obodovala podle následující tabulky.

| | Důležitost | | Text hodnoty | Body | Ano | Ne |
|---|---|---|---|---|---|---|
| | $d_1$ | 0,75 | Heslo obsahuje malá písmena | $b_1$ | 1 | 0 |
| | $d_2$ | 0,75 | Heslo obsahuje velká písmena | $b_2$ | 1 | 0 |
| Struktura | $d_3$ | 0,75 | Heslo obsahuje číslice | $b_3$ | 1 | 0 |
| hesla | $d_4$ | 0,75 | Heslo obsahuje speciální znaky | $b_4$ | 1 | 0 |
| (60 %) | $d_5$ | 1,5 | V hesle používá osobní údaj | $b_5$ | 0 | 1 |
| | $d_6$ | 1,5 | V hesle používá slovo nějakého významu | $b_6$ | 0 | 1 |
| Délka | $d_7$ | 1 | Počet znaků v hesle 0-7 | $b_7$ | 0 | |
| hesla | $d_7$ | 1 | Počet znaků v hesle 8-14 | $b_7$ | 2 | |
| (40 %) | $d_7$ | 1 | Počet znaků v hesle 15 a více | $b_7$ | 4 | |

Tabulka 1: Výpočet ohodnocení hesla

Struktura hesla je 60 % hodnocení hesla. Body vždy získají, pokud dodrží dané pravidlo, jinak získají 0 bodů. Důležitost u malých, velkých písmen, číslic a speciálního znaku jsem stanovila u všech stejně na 0,75. U údaje, kdy respondent používá osobní údaj jsem zvýšila důležitost na 1,5, neboť zde hrozí riziko slovníkového útoku. U údaje, kdy respondent v hesle používá slovo nějakého významu, jsem zvýšila důležitost na 1,5, protože zde hrozí riziko odhalení hesla pomocí sociálního inženýrství.

Délka hesla je 40 % hodnocení hesla. Za nebezpečné heslo 0–7 znaků respondent nezíská žádný bod, za klasickou délku hesla 8–14 získá 2 body, pokud má heslo 15 a více znaků může získat další 2 body tedy celkem 4 body.

Pro stanovení hodnoty hesla jsem použila vzorec:

$$Hodnota = d_1b_1 + d_2b_2 + d_3b_3 + d_4b_4 + d_5b_5 + d_6b_6 + d_7b_7$$

Obrázek 4: Vzorec pro stanovení hodnoty hesla

Pro lepší představu jsem připravila tabulku s ukázkovými hesly a jejich ohodnocení.

| Příklady hesel | Ohodnocení |
|---|---|
| qwerty | 2,25 |
| master | 2,25 |
| 12345678 | 4,25 |
| jstz46 | 4,5 |
| Po457812 | 5,75 |
| Hfsd87GG45 | 7,25 |
| MojeDlouheHeslo1 | 7,75 |
| KunaNeseNanuk1* | 8,5 |
| 17jdhfd6_9AR7fz*147r | 10 |

Tabulka 2: Hesla a jejich síla

Při kontrole dat jsem našla kombinaci, kdy respondent odpověděl, že nepoužívá ani malá, ani velká písmena a přesto používá v hesle slovo nějakého významu. Došlo k nepochopení otázky, a proto bylo všem těmto případům připočteno 0,75 bodu za používání jakéhokoliv písmene. Tím jsem data zkorigovala.

# 6 Výsledky výzkumu

## 6.1 $H_1$: Mezi zálohováním a ztrátou dat neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{01}$ oproti alternativní hypotéze $H_{A1}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{01}$: Mezi zálohováním a ztrátou dat neexistuje závislost.

$H_{A1}$: Mezi zálohováním a ztrátou dat existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, kteří zálohují a kteří nezálohují. Dále na ty, u kterých došlo ke ztrátě dat a na ty, kde ke ztrátě dat nedošlo. Vyloučila jsem respondenty, kteří nevědí, co je zálohování. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0000395$. Tato hodnota je menší než hladina významnosti, a proto můžeme odmítnout nulovou hypotézu a přijmout alternativní hypotézu.

**Mezi zálohováním a ztrátou dat existuje závislost.**

## 6.2 $H_2$: Mezi používáním antivirového programu a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{02}$ oproti alternativní hypotéze $H_{A2}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{02}$: Mezi používáním antivirového programu a nákazou malwarem neexistuje závislost.

$H_{A2}$: Mezi používáním antivirového programu a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále na ty, kteří používají a nepoužívají antivirový program. Vyloučila jsem respondenty, kteří nevědí, zda používají antivirový program a nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Očekávané četnosti

mají tak nízkou hodnotu, že nemůžeme použít metodu chí–kvadrát. Fisherův exaktní test kombinatorický test jsem nepoužila, neboť pouze 5 lidí nepoužívá antivir a použití tohoto testu by nedávalo smysl.

**Hypotéza nebyla potvrzena.**

## 6.3 H3: Mezi používáním základní softwarové ochrany a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H03 oproti alternativní hypotéze HA3 na hladině významnosti $\alpha = 0{,}05$.

H03: Mezi používáním základní softwarové ochrany a nákazou malwarem neexistuje závislost.

HA3: Mezi používáním základní softwarové ochrany a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, kteří používají antivirovou ochranu a zároveň mají zapnutý firewall i automatické aktualizace a na ty, kteří tyto 3 programy nevyužívají. Dále na ty, kteří se nakazili malwarem a nenakazili se malwarem. Vyloučila jsem respondenty, kteří nevědí, zda se malwarem nakazili. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}000165$. Tato hodnota je menší než hladina významnosti, a proto můžeme odmítnout nulovou hypotézu a přijmout alternativní hypotézu.

**Mezi používáním základní softwarové ochrany a nákazou malwarem existuje závislost.**

## 6.4 H4: Mezi používáním firewallu a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H04 oproti alternativní hypotéze HA4 na hladině významnosti $\alpha = 0{,}05$.

H04: Mezi používáním firewallu a nákazou malwarem neexistuje závislost.

HA4: Mezi používáním firewallu a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále na ty, kteří používají a nepoužívají firewall. Vyloučila jsem respondenty, kteří nevědí, zda používají firewall, nebo nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,173. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi používáním firewallu a nákazou malwarem neexistuje závislost.**

## 6.5 $H_5$: Mezi aktualizací operačního systému a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{05}$ oproti alternativní hypotéze $H_{A5}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{05}$: Mezi aktualizací operačního systému a nákazou malwarem neexistuje závislost.

$H_{A5}$: Mezi aktualizací operačního systému a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále na ty, kteří pravidelně aktualizují a neaktualizují operační systém. Vyloučila jsem respondenty, kteří nevědí, zda aktualizují operační systém, nebo nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,678. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi aktualizací operačního systému a nákazou malwarem neexistuje závislost.**

## 6.6 H6: Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H06 oproti alternativní hypotéze HA6 na hladině významnosti α = 0,05.

H06: Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele neexistuje závislost.

HA6: Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále jsem je roztřídila podle způsobu nakládání s e–mailem od neznámého odesílatele. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru.Vytvořila jsem kontingenční tabulku se získanými četnostmi. Při výpočtu očekávaných hodnot, byla vypočtena u odpovědi „Otevřu a přečtu si ho" hodnota 0,72, což je nepřípustné a proto byla tato odpověď sloučena s odpovědí „Otevřu, jen pokud mě v náhledu něco zaujme". Vypočítala jsem pravděpodobnost chyby p = 0,200. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi nákazou malwarem a otevíráním e–mailu od neznámého odesílatele neexistuje závislost.**

## 6.7 H7: Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H07 oproti alternativní hypotéze HA7 na hladině významnosti α = 0,05.

H07: Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu neexistuje závislost..

HA7: Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále na ty, kteří ote-

vírají a neotevírají nevyžádané přílohy v e–mailech. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru.Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,284. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi nákazou malwarem a otevíráním nevyžádaných příloh v e–mailu neexistuje závislost.**

## 6.8 $H_8$: Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{08}$ oproti alternativní hypotéze $H_{A8}$ na hladině významnosti α = 0,05.

$H_{08}$: Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech neexistuje závislost.

$H_{A8}$: Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále jsem je roztřídila podle toho, zda klikají či neklikají na odkazy uvedené v e–mailu. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,880. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi nákazou malwarem a klikáním na odkazy uvedené v e–mailech neexistuje závislost.**

## 6.9 $H_9$: Mezi ztrátou dat a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{09}$ oproti alternativní hypotéze $H_{A9}$ na hladině významnosti α = 0,05.

H09: Mezi ztrátou dat a nákazou malwarem neexistuje závislost.

HA9: Mezi ztrátou dat a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru.. Dále na ty, kteří ztratili a neztratili svá data. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru.. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,000000000017. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi ztrátou dat a nákazou malwarem existuje závislost.**

## 6.10 H10: Mezi zálohováním a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H010 oproti alternativní hypotéze HA10 na hladině významnosti α = 0,05.

H010: Mezi zálohováním a nákazou malwarem neexistuje závislost.

HA10: Mezi zálohováním a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí malwaru a pak na ty, jež se obětí nákazy malwaru nestali. Dále na ty, kteří zálohují a nezálohují. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru, nebo nevědí co je zálohování. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,000559. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi zálohováním a nákazou malwarem existuje závislost.**

## 6.11 $H_{11}$: Mezi nákazou malwarem a pohlavím neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{011}$ oproti alternativní hypotéze $H_{A11}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{011}$: Mezi nákazou malwarem a pohlavím neexistuje závislost.

$H_{A11}$: Mezi nákazou malwarem a pohlavím existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále jsem respondenty rozdělila podle pohlaví. Vyloučila jsem respondenty, kteří nevědí zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0000423$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi nákazou malwarem a pohlavím existuje závislost.**

## 6.12 $H_{12}$: Mezi nákazou malwarem a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{012}$ oproti alternativní hypotéze $H_{A12}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{012}$: Mezi nákazou malwarem a vzděláním neexistuje závislost.

$H_{A12}$: Mezi nákazou malwarem a vzděláním existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále jsem respondenty rozdělila podle vzdělání. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0543$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi nákazou malwarem a vzděláním neexistuje závislost.**

## 6.13 H13: Mezi nákazou malwarem a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H013 oproti alternativní hypotéze HA13 na hladině významnosti $\alpha = 0{,}05$.

H013: Mezi nákazou malwarem a věkem neexistuje závislost.

HA13: Mezi nákazou malwarem a věkem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se stali a nestali obětí nákazy malwaru. Dále jsem respondenty rozdělila podle věku. Vyloučila jsem respondenty, kteří nevědí, zda se stali obětí škodlivého softwaru. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}350$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi nákazou malwarem a věkem neexistuje závislost.**

## 6.14 H14: Mezi používáním základní softwarové ochrany a pohlavím neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H014 oproti alternativní hypotéze HA14 na hladině významnosti $\alpha = 0{,}05$.

H014: Mezi používáním základní softwarové ochrany a pohlavím neexistuje závislost.

HA14: Mezi používáním základní softwarové ochrany a pohlavím existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, kteří používají antivirovou ochranu a zároveň mají zapnutý firewall i automatické aktualizace a na ty, kteří tyto 3 programy nevyužívají. Dále jsem respondenty jsem rozdělila podle pohlaví. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}000006$. Tato hodnota je menší než hladina významnosti, a proto můžeme odmítnout nulovou hypotézu a přijmout alternativní hypotézu.

**Mezi používáním základní softwarové ochrany a pohlavím existuje závislost.**

## 6.15 $H_{15}$: Mezi používáním základní softwarové ochrany a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H015 oproti alternativní hypotéze HA15 na hladině významnosti $\alpha = 0{,}05$.

H015: Mezi používáním základní softwarové ochrany a vzděláním neexistuje závislost.

HA15: Mezi používáním základní softwarové ochrany a vzděláním existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, kteří používají antivirovou ochranu a zároveň mají zapnutý firewall i automatické aktualizace a na ty, kteří tyto 3 programy nevyužívají. Dále jsem respondenty rozdělila podle vzdělání. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0497$. Tato hodnota je menší než hladina významnosti, a proto můžeme odmítnout nulovou hypotézu a přijmout alternativní hypotézu.

**Mezi používáním základní softwarové ochrany a vzděláním existuje závislost.**

## 6.16 $H_{16}$: Mezi používáním základní softwarové ochrany a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H016 oproti alternativní hypotéze HA16 na hladině významnosti $\alpha = 0{,}05$.

H016: Mezi používáním základní softwarové ochrany a věkem neexistuje závislost.

HA16: Mezi používáním základní softwarové ochrany a věkem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, kteří používají antivirovou ochranu a zároveň mají zapnutý

firewall i automatické aktualizace a na ty, kteří tyto 3 programy nevyužívají. Dále jsem respondenty rozdělila podle věku. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,483. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi používáním základní softwarové ochrany a věkem neexistuje závislost.**

## 6.17 $H_{17}$: Mezi zálohováním a pohlavím neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{017}$ oproti alternativní hypotéze $H_{A17}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{017}$: Mezi zálohováním a pohlavím neexistuje závislost.

$H_{A17}$: Mezi zálohováním a pohlavím existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, co zálohují a na ty, co nezálohují. Dále jsem respondenty rozdělila podle pohlaví. Vyloučila jsem respondenty, kteří nevědí co je zálohování. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,0686. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi zálohováním a pohlavím neexistuje závislost.**

## 6.18 $H_{18}$: Mezi zálohováním a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{018}$ oproti alternativní hypotéze $H_{A18}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{018}$: Mezi zálohováním a vzděláním neexistuje závislost.

$H_{A18}$: Mezi zálohováním a vzděláním existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, co zálohují a na ty, co nezálohují.. Dále jsem respondenty

rozdělila podle vzdělání. Vyloučila jsem respondenty, kteří nevědí co je zálohování. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,0543. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi zálohováním a vzděláním neexistuje závislost.**

## 6.19 $H_{19}$: Mezi zálohováním a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{019}$ oproti alternativní hypotéze $H_{A19}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{019}$: Mezi zálohováním a věkem neexistuje závislost.

$H_{A19}$: Mezi zálohováním a věkem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, co zálohují a na ty, co nezálohují.. Dále jsem respondenty rozdělila podle věku. Vyloučila jsem respondenty, kteří nevědí co je zálohování. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,486. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi zálohováním a věkem existuje závislost.**

## 6.20 $H_{20}$: Mezi ztrátou dat a pohlavím neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{020}$ oproti alternativní hypotéze $H_{A20}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{020}$: Mezi ztrátou dat a pohlavím neexistuje závislost.

$H_{A20}$: Mezi ztrátou dat a pohlavím existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež ztratili a neztratili data. Dále jsem respondenty rozdělila podle pohlaví. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby p = 0,0915. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi ztrátou dat a pohlavím neexistuje závislost.**

## 6.21 $H_{21}$: Mezi ztrátou dat a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{021}$ oproti alternativní hypotéze $H_{A21}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{021}$: Mezi ztrátou dat a vzděláním neexistuje závislost.

$H_{A21}$: Mezi ztrátou dat a vzděláním existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež ztratili a neztratili data. Dále jsem respondenty rozdělila podle vzdělání. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0370$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi ztrátou dat a vzděláním existuje závislost.**

## 6.22 $H_{22}$: Mezi ztrátou dat a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{022}$ oproti alternativní hypotéze $H_{A22}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{022}$: Mezi ztrátou dat a věkem neexistuje závislost.

$H_{A22}$: Mezi ztrátou dat a věkem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež ztratili a neztratili data. Dále jsem respondenty rozdělila podle věku. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}486$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi ztrátou dat a věkem neexistuje závislost.**

## 6.23 $H_{23}$: Mezi setkáním s phishingovým útokem a pohlavím neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{023}$ oproti alternativní hypotéze $H_{A23}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{023}$: Mezi setkáním s phishingovým útokem a pohlavím neexistuje závislost.

$H_{A23}$: Mezi setkáním s phishingovým útokem a pohlavím existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se setkali a nesetkali s phishingovým útokem. Dále jsem respondenty rozdělila podle pohlaví. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0950$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi setkáním s phishingovým útokem a pohlavím neexistuje závislost.**

## 6.24 $H_{24}$: Mezi setkáním s phishingovým útokem a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{024}$ oproti alternativní hypotéze $H_{A24}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{024}$: Mezi setkáním s phishingovým útokem a vzděláním neexistuje závislost.

$H_{A24}$: Mezi setkáním s phishingovým útokem a vzděláním existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se setkali a nesetkali s phishingovým útokem. Dále jsem respondenty rozdělila podle vzdělání. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0198$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi setkáním s phishingovým útokem a vzděláním existuje závislost.**

## 6.25 $H_{25}$: Mezi setkáním s phishingovým útokem a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{025}$ oproti alternativní hypotéze $H_{A25}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{025}$: Mezi setkáním s phishingovým útokem a věkem neexistuje závislost.

$H_{A25}$: Mezi setkáním s phishingovým útokem a věkem existuje závislost.

Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se setkali a nesetkali s phishingovým útokem. Dále jsem respondenty rozdělila podle věku. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0086$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní hypotézu.

**Mezi setkáním s phishingovým útokem a věkem existuje závislost.**

## 6.26 $H_{26}$: Mezi setkáním s phishingovým útokem a otázkou na potvrzení přihlašovacích údajů neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{026}$ oproti alternativní hypotéze $H_{A26}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{026}$: Mezi setkáním s phishingovým útokem a otázkou na potvrzení hesla neexistuje závislost.

$H_{A26}$: Mezi setkáním s phishingovým útokem a otázkou na potvrzení hesla existuje závislost.

Tato hypotéza souvisí s otázkou „Co uděláte pokud Vám přijde e–mail s žádostí, aby jste pro zvýšení zabezpečení potvrdili své přihlašovací heslo?" Respondent měl na výběr odpovědi - „Na e–mail odpovím a zvýším si tak svou internetovou bezpečnost", „Na e–mail odpovím, ale heslo sdělím až poté, co mi odesílatel v dalším e–mailu potvrdí, k čemu přesně mé heslo potřebuje", nebo „Na e–mail v žádném případě neodpovídám". Použila jsem statistickou metodu Chí–kvadrát test. Respondenty jsem rozdělila do skupin na ty, jež se setkali a nesetkali s phishin-

govým útokem. Dále na ty, kteří by v otázce na potvrzení přihlašovacích údajů své údaje potvrdili či nepotvrdili. Vytvořila jsem kontingenční tabulku se získanými četnostmi. Očekávané četnosti mají tak nízkou hodnotu, že nemůžeme použít metodu Chí–kvadrát test. Fisherův exaktní test kombinatorický test jsem nepoužila, protože pouze 2 respondenti by své přihlašovací údaje potvrdili.

**Hypotéza nebyla potvrzena.**

## 6.27 $H_{27}$: Muži a ženy se neliší v síle hesla.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{027}$ oproti alternativní hypotéze $H_{A27}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{027}$: Muži a ženy se neliší v síle hesla.

$H_{A27}$: Muži a ženy se liší v síle hesla.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}001$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Muži a ženy se liší v síle hesla. Průměrná síla hesla mužů má 6,12 bodů a žen má 5,47 bodů. Muži používají bezpečnější hesla, než ženy.**

## 6.28 $H_{28}$: Mezi sílou hesla a vzděláním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{028}$ oproti alternativní hypotéze $H_{A28}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{028}$: Mezi sílou hesla a vzděláním neexistuje závislost.

$H_{A28}$: Mezi sílou hesla a vzděláním existuje závislost.

Použila jsem statistickou metodu Jednoduchá analýza rozptylu. Vypočítala jsem pravděpodobnost chyby $p = 0{,}014$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a vzděláním existuje závislost. Průměrná síla hesla u ZŠ+SŠ má 5,26 bodů, u VOŠ má 5,5 bodů a u VŠ má 5,9 bodů. Se vzděláním se zvyšuje bezpečnost hesla.**

## 6.29 $H_{29}$: Mezi sílou hesla a věkem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{029}$ oproti alternativní hypotéze $H_{A29}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{029}$: Mezi sílou hesla a věkem neexistuje závislost.

$H_{A29}$: Mezi sílou hesla a věkem existuje závislost.

Použila jsem statistickou metodu Jednoduchá analýza rozptylu. Vypočítala jsem pravděpodobnost chyby $p = 0{,}07$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi sílou hesla a věkem neexistuje závislost.**

## 6.30 $H_{30}$: Mezi sílou hesla a používáním internetového bankovnictví neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{030}$ oproti alternativní hypotéze $H_{A30}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{030}$: Mezi sílou hesla a používáním internetového bankovnictví neexistuje závislost.

$H_{A30}$: Mezi sílou hesla a používáním internetového bankovnictví existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0000006$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a používáním internetového bankovnictví existuje závislost. Průměrná síla hesla respondentů používající internetové bankovnictví má 5,90 bodů a respondenti nepoužívající internetové bankovnictví má 4,91 bodů. Respondenti využívající internetové bankovnictví používají bezpečnější hesla.**

## 6.31 H31: Mezi sílou hesla a představou o bezpečnosti hesla neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H031 oproti alternativní hypotéze HA31 na hladině významnosti α = 0,05.

H031: Mezi sílou hesla a představou o bezpečnosti hesla neexistuje závislost.

HA31: Mezi sílou hesla a představou o bezpečnosti hesla neexistuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby p = 0,00002 Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a představou o bezpečnosti hesla existuje závislost. Průměrná síla hesla respondentů domnívající se, že používají bezpečné heslo má 6,12 bodů a respondenti domnívající se, že používají nebezpečné heslo má 5,23 bodů. Respondenti mají představu o bezpečnosti svého hesla.**

## 6.32 H32: Mezi sílou hesla a obměnou hesla neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H032 oproti alternativní hypotéze HA32 na hladině významnosti α = 0,05.

H032: Mezi sílou hesla a obměnou hesla neexistuje závislost.

HA32: Mezi sílou hesla a obměnou hesla existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby p = 0,00002 Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a obměnou hesla existuje závislost. Průměrná síla hesla respondentů měnícího si hesla má 6,00 bodů a respondenti neměnící si hesla má 5,35 bodů. Respondenti měnící si heslo používají bezpečnější hesla.**

## 6.33 H33: Mezi sílou hesla a počtem používaných hesel neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H033 oproti alternativní hypotéze HA33 na hladině významnosti $\alpha = 0{,}05$.

H033: Mezi sílou hesla a počtem používaných hesel neexistuje závislost.

HA33: Mezi sílou hesla a počtem používaných hesel existuje závislost.

Použila jsem statistickou metodu Studentův t–test.Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}00006$ Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a počtem používaných hesel existuje závislost. Průměrná síla hesla respondentů používající všude stejné heslo má 5,92 bodů, respondenti používající několik hesel má 4,75 bodů a respondenti, kteří mají ke každé aplikaci jiné heslo má 5,54 bodů. Respondenti používající pouze jedno heslo mají silnější hesla, naopak ti, kteří používají několik hesel mají slabší hesla. Respondenti používající ke každé aplikaci jiné heslo jsou se sílou hesla mezi nimi.**

## 6.34 H34: Mezi sílou hesla a používáním antivirové ochrany neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H034 oproti alternativní hypotéze HA34 na hladině významnosti $\alpha = 0{,}05$.

H034: Mezi sílou hesla a používáním antivirové ochrany neexistuje závislost.

HA34: Mezi sílou hesla a používáním antivirové ochrany existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}09$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a používáním antivirové ochrany existuje závislost. Průměrná síla hesla respondentů používající antivirovou ochranu má**

**5,71 bodů a respondenti nepoužívající antivirovou ochranu má 7,03 bodů. Respondenti používající antivirovou ochranu mají méně bezpečná hesla, než respondenti používající softwarovou ochranu.**

## 6.35 $H_{35}$: Mezi sílou hesla a používáním firewallu neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{035}$ oproti alternativní hypotéze $H_{A35}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{035}$: Mezi sílou hesla a používáním firewallu neexistuje závislost.

$H_{A35}$: Mezi sílou hesla a používáním firewallu existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}30$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi sílou hesla a používáním firewallu neexistuje závislost.**

## 6.36 $H_{36}$: Mezi sílou hesla a aktualizací operačního systému neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy $H_{036}$ oproti alternativní hypotéze $H_{A36}$ na hladině významnosti $\alpha = 0{,}05$.

$H_{036}$: Mezi sílou hesla a aktualizací operačního systému neexistuje závislost.

$H_{A36}$: Mezi sílou hesla a aktualizací operačního systému existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}10$. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu.

**Mezi sílou hesla a aktualizací operačního systému neexistuje závislost.**

## 6.37 H37: Mezi sílou hesla a používáním základní softwarové ochrany neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H037 oproti alternativní hypotéze HA37 na hladině významnosti α = 0,05.

H037: Mezi sílou hesla a používáním základní softwarové ochrany neexistuje závislost.

HA37: Mezi sílou hesla a používáním základní softwarové ochrany existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby p = 0,00000008. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a používáním základní softwarové ochrany existuje závislost. Průměrná síla hesla respondentů používající základní softwarovou ochranu má 6,26 bodů a respondenti nepoužívající základní softwarovou ochranu má 5,28 bodů. Respondenti používající základní softwarovou ochranu používají bezpečnější hesla.**

## 6.38 H38: Mezi sílou hesla a nákazou malwarem neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H038 oproti alternativní hypotéze HA38 na hladině významnosti α = 0,05.

H038: Mezi sílou hesla a nákazou malwarem neexistuje závislost.

HA38: Mezi sílou hesla a nákazou malwarem existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby p = 0,00054. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a nákazou malwarem existuje závislost. Průměrná síla hesla respondentů, kteří se nakazili malwarem má 6,14 bodů a re-**

**spondenti, kteří se nenakazili malwarem má 5,45 bodů. Kdo prodělal nákazu malwarem používá bezpečnější heslo.**

## 6.39 H39: Mezi sílou hesla a ztrátou dat neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H039 oproti alternativní hypotéze HA39 na hladině významnosti $\alpha = 0{,}05$.

H039: Mezi sílou hesla a ztrátou dat neexistuje závislost.

HA39: Mezi sílou hesla a ztrátou dat existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}0005$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a ztrátou dat existuje závislost. Průměrná síla hesla respondentů, kteří ztratili data má 6,26 bodů a respondenti, kteří neztratili data má 5,28 bodů. Kdo prodělal ztrátu dat používá bezpečnější heslo.**

## 6.40 H40: Mezi sílou hesla a zálohováním neexistuje závislost.

Při dokazování hypotézy ověřujeme platnost nulové hypotézy H040 oproti alternativní hypotéze HA40 na hladině významnosti $\alpha = 0{,}05$.

H040: Mezi sílou hesla a zálohováním neexistuje závislost.

HA40: Mezi sílou hesla a zálohováním existuje závislost.

Použila jsem statistickou metodu Studentův t–test. Nejprve jsem ověřila, že dané skupiny mají stejný rozptyl. Dále jsem provedla Studentův t–test. Vypočítala jsem pravděpodobnost chyby $p = 0{,}03$. Tato hodnota je menší než hladina významnosti, a proto přijímáme alternativní hypotézu.

**Mezi sílou hesla a zálohováním existuje závislost. Průměrná síla hesla zálohujících respondentů má 5,75 bodů a nezálohujících respondentů má 5,25 bodů. Kdo zálohuje používá bezpečnější heslo.**

# 7 Shrnutí výsledků a diskuze

Pro lepší přehlednost jsem shrnula výsledky do tématických tabulek. Následující tabulka zobrazuje používání ochranných prvků respondentů.

| Používání v % | Ano | Ne | Neví |
|---|---|---|---|
| Antivirová ochrana | 85 | 1 | 14 |
| Firewall | 45 | 10 | 45 |
| Aktualizace OS | 55 | 10 | 35 |
| Zálohování | 79 | 18 | 3 |

Tabulka 3: Ochrana respondentů proti hrozbám

Respondenti používají antivirovou ochranu, pouze 1 % respondentů odpovědělo, že antivirovou ochranu nepoužívá. U odpovědí na používáni firewallu a aktualizací operačního systému se vyskytují dosti vysoká čísla u odpovědi nevím. Mohlo by to být dáno tím, že respondent neví, co to firewall a aktualizace operačního systému vlastně znamená, a proč by je měl používat. Domnívám se, že netušili, na co jsem se jich ptala. Není to ani příliš medializováno a v povědomí lidí to není. V předvýzkumu jsem to neodhalila, ale následné dotazování mých respondentů mi moje tušení potvrdilo. Vzhledem k tomu že, ve výchozím stavu jsou oba programy zapnuté, můžeme se domnívat, že počet používajících respondentů bude vyšší. U zálohování jsme se dostali k 79 % používání. Překvapilo mě, že z pravidelně zálohujících respondentů jich 37 % zálohuje denně (11 % všech respondentů). Ptala jsem se na zařízení, které používají k přístupu na internet a to může být i pracovní počítač či notebook. To mohlo ovlivnit odpověď na danou otázku. V práci si ukládají svá data na server právě proto, že vědí, že jejich data jsou tak pravidelně denně zálohována.

| Setkání v % | Ano | Ne | Neví |
|---|---|---|---|
| Nákaza malwarem | 30 | 53 | 17 |
| Ztráta dat | 40 | 60 | - |
| Phishingový útok | 25 | 75 | - |

Tabulka 4: Setkání respondentů s hrozbami

Tato tabulka popisuje setkání respondentů s hrozbami. 30 % respondentů zažilo nákazu malwarem, 40 % prodělalo ztrátu dat a 25 % respondentů se setkalo s phishingovým útokem. Dokazuje to, že min. 40 % respondentů se setkalo s alespoň jednou hrozbou. Je to poměrně vysoké číslo a velký důvod pro využívání prostředků pro ochranu zařízení. Phishingové útoky jsou oproti nákaze malwarem záležitostí několika posledních let a přesto se s phishingovým útokem setkalo už 25 % respondentů. To ukazuje na vzrůstající tendenci tak, jak je to uváděno i ve zprávě NBÚ [40] a společnosti APWD [41]. Můžeme se proto domnívat, že v budoucnu tato hrozba ještě poroste.

V otázce na vyzrazení údajů pouze 2 respondenti přiznali, že by potvrdili ihned své přihlašovací údaje. Myslím, že z této odpovědi můžeme jen těžko vyvodit nějaký závěr. Důvodem je samotná problematika phishingu, která je natolik rozsáhlá a zároveň velice aktuální, že by si zasloužila samostatný výzkum. Bylo by vhodné v rámci dotazování provést znalostní a situační testy na odhalení, zda lidé dokáží rozpoznat phishingový útok.

| Existence závislosti | Nákaza malwarem |
|---|---|
| Používání antivirové ochrany | - |
| Používání základní softwarové ochrany | Ano |
| Používání firewallu | Ne |
| Aktualizace operačního systému | Ne |
| Otevírání e–mailu od neznámého odesílatele | Ne |
| Otevírání nevyžádaných příloh v e–mailu | Ne |
| Klikání na odkazy uvedené v e–mailu | Ne |
| Ztráta dat | Ano |
| Zálohování | Ano |

Tabulka 5: Existence závislostí u nákazy malwarem

Zde je přehled zjištěných závislostí s nákazou malwarem. Hypotézami jsme prokázali závislost mezi nákazou malwarem a používáním základní softwarové ochrany, ztrátou dat a zálohováním.

Překvapivé bylo, že závislost se neprokázala mezi nákazou malwarem a otevíráním e–mailů od neznámého odesílatele, otevíráním nevyžádaných příloh v e–mailu a klikáním na odkazy uvedené v e–mailu. Přitom toto chování bychom mohli považovat za klíčový faktor nákazy malwarem. Jako důvod nákazy malwarem uvedli respondenti právě nákazu z příloh v e–mailu, hned po nákaze z webových stránek. Potěšující je, že většina odpovědí byla správných (bezpečných). Také se mohlo stát, že respondenti upravili svoji odpověď, aby vypadali lépe, než se ve skutečnosti chovají. Své odpovědi mohli přizpůsobit k bezpečnějším odpovědím a právě díky nízkým číslům (6–10 %) u odpovědí rizikového chování jsme existenci nezávislosti nemuseli potvrdit.

| Existence závislosti | Ztráta dat |
|---|---|
| Zálohování | Ano |

Tabulka 6: Existence závislostí u ztráty dat

Potvrdila se i očekávaná závislost mezi ztrátou dat a zálohováním.

| Existence závislosti | Pohlaví | Vzdělání | Věk |
|---|---|---|---|
| Nákaza malwarem | Ano | Ne | Ne |
| Používání zákl. soft. ochrany | Ano | Ano | Ne |
| Zálohování | Ne | Ne | Ne |
| Ztráta dat | Ne | Ano | Ne |
| Phishingový útok | Ne | Ano | Ano |
| Síla hesla | Ano | Ano | Ne |

Tabulka 7: Vliv pohlaví, vzdělání a věku

Analyzovala jsem vliv pohlaví, vzdělání a věku. Z tabulky vyplývá, že pohlaví a vzdělání by mohlo mít vliv na chování a návyky respondentů. Překvapivé bylo, že se neprokázal vliv věku. Očekávala jsem, že se zde projeví vliv výuky na škole u mladší generace, to se ale nestalo. Hypotézami bylo prokázáno, že muži používají silnější hesla než ženy. Vliv zde může hrát, že muži jsou více technicky zaměřeni než ženy a že se o techniku více zajímají.

Dále jsem analyzovala hesla respondentů. 19 % respondentů sdílí svá hesla s dalšími osobami. Nejčastěji sdílí svá hesla od e–mailové schránky a do internetového bankovnictví. Domnívám se, že sdílení těchto hesel nemusí být vždy bezpečnostní riziko. Pokud si člověk vybere správnou osobu, může to fungovat jako pojistka v případě, že se s dotyčným něco stane (např. pobyt v nemocnici).

Pouze 34 % respondentů má ke každé aplikaci jiné heslo a 13 % respondentů používá všude stejné heslo. Jenom 44 % lidí si mění své heslo. Program pro správu

hesel používá jen 4 % respondentů. Zároveň jen 3 % respondentů, se dostala do situace, že se někdo nepovolaný dostal k jejich datům. I to by mohlo hrát roli při rozhodování jak silné heslo zvolí, jak s ním bude pracovat a jak ho bude chránit. Roli může hrát i pohodlnost uživatele, pokud není síla hesla a jeho obměna vynucena restrikcemi.

| Existence závislosti | Síla hesla |
|---|---|
| Používání internetového bankovnictví | Ano |
| Představa o síle hesla | Ano |
| Obměna hesla | Ano |
| Počet hesel | Ano |
| Používání antivirové ochrany | Ano |
| Používání firewallu | Ne |
| Aktualizace operačního systému | Ne |
| Používání zákl. soft. ochrany | Ano |
| Nákaza malwarem | Ano |
| Ztráta dat | Ano |
| Zálohování | Ano |

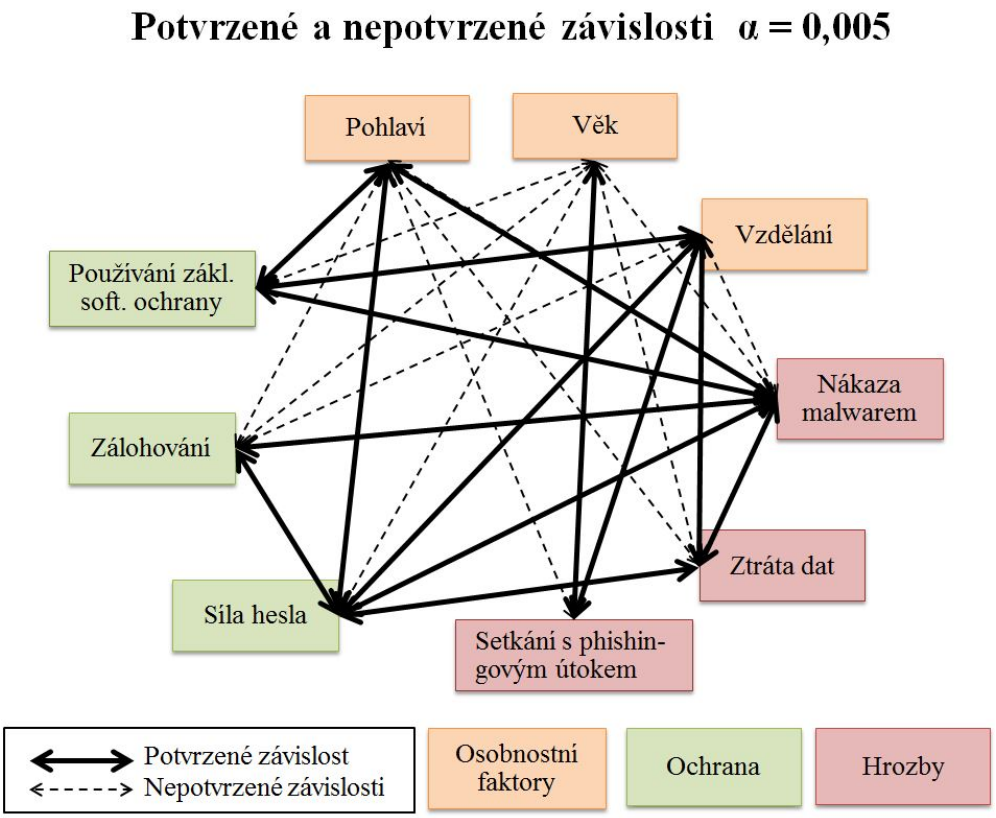
Tabulka 8: Existence závislostí u hesel

Zde se potvrdila skoro všechna očekávání s vyjímkou používání firewallu a aktualizací operačního systému. Jak jsem psala výše, mohlo to být ovlivněno tím, že hodně respondentů zvolilo únikovou otázku „nevím". Bylo potvrzeno, že v závislosti na využívání ochranných prostředků roste i síla hesla.

Shrnutí získaných údajů z hypotéz:

- Muži používají bezpečnější hesla, než ženy.
- Se vzděláním se zvyšuje bezpečnost hesla.

- Mezi sílou hesla a věkem neexistuje závislost.
- Respondenti využívající internetové bankovnictví používají bezpečnější hesla.
- Respondenti mají představu o bezpečnosti svého hesla.
- Respondenti měnící si heslo používají bezpečnější hesla.
- Respondenti používající pouze jedno heslo mají silnější hesla, naopak ti, kteří používají několik hesel mají slabší hesla. Respondenti používající ke každé aplikaci jiné heslo jsou se sílou hesla mezi nimi.
- Respondenti používající antivirovou ochranu mají méně bezpečná hesla, než respondenti používající softwarovou ochranu.
- Mezi sílou hesla a používáním firewallu neexistuje závislost.
- Mezi sílou hesla a aktualizací operačního systému neexistuje závislost.
- Respondenti používající základní softwarovou ochranu používají bezpečnější hesla.
- Kdo prodělal nákazu malwarem používá bezpečnější heslo.
- Kdo prodělal ztrátu dat používá bezpečnější heslo.
- Kdo zálohuje používá bezpečnější heslo.




Obrázek 5: Potvrzené a nepotvrzené závislosti

Pro lepší přehlednost jsem dala závislosti do obrázku, který znázorňuje potvrzené a nepotvrzené závislosti. Faktory, které ovlivňují chování a návyky respondentů jsou síla hesla a setkání s nákazou malwarem. Zde bylo zjištěno nejvíce potvrzených závislostí. Z osobnostních faktorů chování respondentů nejvíce ovlivňuje vzdělání a následuje pohlaví.

# 8 Závěr

Dotazníkovým šetřením bylo zjištěno, jak lidé ve vybraných státních organizacích používají výpočetní techniku, s jakými hrozbami se setkali a jaké mají bezpečnostní znalosti a návyky.

Statistickými metodami jsem našla faktory, které ovlivňují chování a návyky respondentů. Z osobnostních faktorů nejvíce ovlivňuje chování respondentů vzdělání a následuje pohlaví. Mezi rozhodující faktory patří setkání s nákazou malwarem. S dalšími projevy chování silně koreluje síla hesla potřebného pro přístup do aplikací s citlivými údaji. Zde bylo zjištěno nejvíce potvrzených závislostí.

Rozborem hesel jsem zjistila, že ten kdo dbá na bezpečnost hesla, dbá i na jeho obměnu. Respondenti používající pouze jedno heslo mají silnější hesla, naopak ti, kteří používají několik hesel mají slabší hesla. Respondenti používající ke každé aplikaci jiné heslo jsou se sílou hesla mezi nimi.

Překvapivé bylo, že závislost se neprokázala mezi nákazou malwarem a otevíráním e–mailů od neznámého odesílatele, otevíráním nevyžádaných příloh v e–mailu a klikáním na odkazy uvedené v e–mailu.

Přínosem této práce je samotné dotazníkové šetření, které jde v čase opakovat na stejném vzorku a zjistit tak změny. Bylo by zajímavé vybrat úplně jiný výzkumný vzorek a porovnat výsledky. Do dotazníku bych nezařazovala otázky ohledně phishingu. Tato problematika je natolik rozsáhlá a zároveň velice aktuální, že by si zasloužila samostatný výzkum. Bylo by vhodné v rámci dotazování provést znalostní a situační testy na odhalení rozpoznání phishingového útoku.

# Použitá literatura a zdroje

[1] Informační a komunikační technologie v českých domácnostech. *Czso.cz* [online]. 2015 [cit. 2015-08-26]. Dostupné z: https://www.czso.cz/documents/10180/20568875/06200414a.pdf/785cc0b3-818e-4307-81c3-8773dce61c0b?version=1.0

[2] New Trustwave Report Reveals Criminals Receive 1,425 Percent Return on Investment from Malware Attacks. *Trustwave.com* [online]. 2015 [cit. 2015-08-26]. Dostupné z: https://www.trustwave.com/Company/Newsroom/News/New-Trustwave-Report-Reveals-Criminals-Receive-1,425-Percent-Return-on-Investment-from-Malware-Attacks

[3] HÁK, Igor. *Moderní počítačové viry.* Hradec Králové, 2005. Bakalářská práce. Univerzita Hradec králové, Fakulta informatiky a managementu. Vedoucí práce Doc. RNDr. Josef Zelenka, CSc.

[4] HARRIS, Shon. *Manuál hackera.* 1. vyd. Praha: Grada, 2008, 399 s. Hacking (Grada). ISBN 978-80-247-1346-5.

[5] AYCOCK, John Daniel. *Computer viruses and malware.* New York: Springer, 2006, xvi, 227 p. ISBN 978-0-387-30236-2.

[6] Základní definice, vztahující se k tématu kybernetické bezpecnosti *Mvcr.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

[7] Explaining the Types of Trojan Horses. *Brighthub.com* [online]. 2012 [cit. 2016-02-29]. Dostupné z: http://www.brighthub.com/computing/smb-security/articles/97580.aspx

[8] Viry a červi. *Kaspersky.com* [online]. 2015 [cit. 2016-04-18]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/threats/viruses-worms

[9] Příchod hackerů: I Love You, Melissa. *Root.cz* [online]. 2016 [cit. 2016-04-18]. Dostupné z: http://www.root.cz/clanky/prichod-hackeru-i-love-you-melissa/

[10] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[11] Spyware a hijackery *Pcworld.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://pcworld.cz/software/spyware-a-hijackery-14732

[12] More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home *Microsoft.com* [online]. 2016 [cit. 2016-01-10]. Dostupné z: https://blogs.technet.microsoft.com/markrussinovich/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home

[13] Příchod hackerů: zlatá éra botnetů. *Root.cz* [online]. 2016 [cit. 2016-04-18]. Dostupné z: http://www.root.cz/clanky/prichod-hackeru-zlata-era-botnetu/

[14] Logická bomba *Cleverandsmart.cz* [online]. 2008-2016 [cit. 2016-01-10]. Dostupné z: http://www.cleverandsmart.cz/logicka-bomba

[15] Adware *Itslovnik.cz* [online]. 2008-2016 [cit. 2016-01-10]. Dostupné z: http://it-slovnik.cz/pojem/adware/?utm_source=cp&utm_medium=link-&utm_campaign=cp

[16] 17 Percent of PCs are exposed. *Blogs.mcaffe.com* [online]. 2015 [cit. 2015-08-26]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/17-of-pcs-are-exposed

[17] Dva antiviry - dva kohouti na jednom smetišti *Tipypropc.cz* [online]. 2016 [cit. 2016-02-29]. Dostupné z: http://www.tipypropc.cz/dva-antiviry-%E2%80%93-dva-kohouti-na-jednom-smetisti/

[18] BITTO, Ondřej. *Microsoft Windows 7: podrobná uživatelská příručka.* Vyd. 1. Brno: Computer Press, 2009. ISBN 978-80-251-2647-9.

[19] KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně.* 1. vyd. Praha: Grada, 2006, 334 s. ISBN 80-247-1408-6.

[20] Centrum aktualizací Service Pack a běžných aktualizací *Microsoft.com* [online]. 2016 [cit. 2016-02-29]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/service-packs-download#sptabs=win7

[21] Jaké kybernetické hrozby můžeme očekávat v roce 2016 *Cleverandsmart.cz* [online]. 2008-2016 [cit. 2016-02-29]. Dostupné z: http://www.cleverandsmart.cz/jake-kyberneticke-hrozby-muzeme-ocekavat-v-roce-2016

[22] Proč používat standardní uživatelský účet místo účtu správce? *Microsoft.com* [online]. 2016 [cit. 2016-04-18]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/why-standard-user-account#1TC=windows-7

[23] 9 Out Of 10 Windows Security Flaws Could Be Avoided By Just Removing Admin Rights. *Fossbytes.com* [online]. [cit. 2016-04-18]. Dostupné z: http://fossbytes.com/9-out-of-10-windows-security-flaws-can-be-solved-by-just-one-simple-step/

[24] Antispamová ochrana *Eset.com* [online]. 1992-2015 [cit. 2016-02-29]. Dostupné z: http://help.eset.com/ess/9/cs-CZ/index.html?idh_config_smon_main.htm

[25] Co je to hoax *Hoax.cz* [online]. 2000-2016 [cit. 2016-02-29]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

[26] Nařízení eIDAS bylo dne 28. srpna 2014 zveřejněno v Úředním věstníku EU *Mvcr.cz* [online]. 2015 [cit. 2015-01-03]. Dostupné z: http://www.mvcr.cz/clanek/elektronicky-podpis-dokumenty-narizeni-eidas-bylo-dne-28-srpna-2014-zverejneno-v-urednim-vestniku-eu.aspx

[27] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[28] Tipy pro vytvoření silného hesla *Microsoft.com* [online]. 2016 [cit. 2015-01-25]. Dostupné z: http://windows.microsoft.com/cs-cz/windows-vista/tips-for-creating-a-strong-password

[29] SELECKÝ, Matúš. *Penetrační testy a exploitace.* 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

[30] Jak je na tom Vaše heslo? *Muni.cz* [online]. 1996-2016 [cit. 2016-02-29]. Dostupné z: https://security.ics.muni.cz/18-Jak-je-na-tom-vase-heslo

[31] The Usability of Passwords *Baekdal.com* [online]. 2011 [cit. 2015-01-25]. Dostupné z: http://www.baekdal.com/insights/password-security-usability

[32] Consumer Password Worst Practices. *Imperva.com* [online]. 2014 [cit. 2015-08-26]. Dostupné z: https://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[33] 123456: Millions of Adobe hack victims used horrible passwords. *Pcworld.com* [online]. 2015 [cit. 2015-08-26]. Dostupné z: http://www.pcworld.com/article/2060825/123456-millions-of-adobe-hack-victims-used-horrible-passwords.html

[34] Studie Norton odhaluje, že nadměrné sdílení informací během svátků ohrožuje uživatele *Symantec.com* [online]. 1995-2016 [cit. 2016-01-26]. Dostupné z: http://www.symantec.com/cs/cz/about/news/release/article.jsp?-prid=20101229_01

[35] Prohlášení předsedy vlády Bohuslava Sobotky k útoku hackerů *Vlada.cz* [online]. 2009-2016 [cit. 2016-02-26]. Dostupné z: http://www.vlada.cz/cz/clenove-vlady/premier/projevy/prohlaseni-predsedy-vlady-bohuslava-sobotky-k-utoku-hackeru-138947

[36] Update to Celebrity Photo Investigation. *Aplle.com* [online]. 2016 [cit. 2016-02-15]. Dostupné z: http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html

[37] Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google *Dl.acm.org* [online]. 2016 [cit. 2015-01-25]. Dostupné z: http://dl.acm.org/citation.cfm?id=2741691

[38] JAMES, Lance. *Phishing bez záhad.* 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[39] Zpráva o stavu kybernetické bezpečnosti České republiky 2014. *Govcert* [online]. 2015 [cit. 2015-07-31]. Dostupné z: http://www.govcert.cz/cs/informacni-servis/bulletiny/zprava-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2014

[40] Phishing Activity Trends Report *Apwg.org* [online]. 2016 [cit. 2016-02-15]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

[41] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač.* První vydání. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[42] Co je to phishing. *Hoax.cz* [online]. 2016 [cit. 2016-04-18]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[43] Zálohování dat. *Bezpecnyinternet.cz* [online]. [cit. 2016-04-18]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-dat/zalohovani-dat.aspx

[44] 5 tipů pro bezpečné zálohování dat. *Jnp.zive.cz* [online]. 2016 [cit. 2016-04-18]. Dostupné z: http://jnp.zive.cz/5-tipu-pro-bezpecne-zalohovani-dat

[45] Šifrování. *Jaknainternet.cz* [online]. 2014 [cit. 2016-04-18]. Dostupné z: http://www.jaknainternet.cz/page/1251/sifrovani/

[46] 94% of computer users still risk data loss. *Backblaze.com* [online]. [cit. 2016-04-18]. Dostupné z: https://www.backblaze.com/blog/94-of-computer-users-still-risk-data-loss/

[47] 75 procent českých domácností může přijít o vzpomínky. *Mediakom.cz* [online]. 2015 [cit. 2015-08-26]. Dostupné z: http://www.mediakom.cz/cs-web/index.php?option=com_k2&view=item&id=905:75-procent-ceskych-domacnosti-muze-prijit-o-vzpominky.

[48] GAVORA, Peter. *Úvod do pedagogického výzkumu.* Brno: Paido, 2000. Edice pedagogické literatury. ISBN 80-859-3179-6.

[49] CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu.* Vyd. 1. Praha: Grada, 2007. Pedagogika (Grada). ISBN 978-80-247-1369-4.

[50] KREISLOVÁ, Gabriela. *Dotazníkové šetření.* Plzeň, 2008. Bakalářská práce. Fakulta aplikovaných věd, Katedra matematiky.

[51] NEUBAUER, Jiří, Marek SEDLAČÍK a Oldřich KŘÍŽ. Základy statistiky: aplikace v technických a ekonomických oborech. 1. vyd. Praha: Grada, 2012. ISBN 978-80-247-4273-1.

# Seznam obrázků

# Seznam tabulek

# Přílohy

## Dotazník - předvýzkum

1. Které z následujících zařízení používáte k přístupu na internet? (můžete označit i více odpovědí)

- Notebook/netbook
- Stolní počítač
- Chytrý mobilní telefon
- Tablet

2. K jakým účelům používáte Vaše zařízení? (můžete označit i více odpovědí)

- Komunikace a sociální sítě (např. facebook, email. . . )
- Internetové bankovnictví
- Online nakupování
- Práce
- Vyhledávání informací
- Stahování dat (filmy, hudba..)
- Online hry
- Jiné, uveďte účely

3. Jak často používáte své zařízení? (vyberte jednu z odpovědí)

- Každodenně
- Několikrát za týden

- Zřídka napište jak často za měsíc

4. Používáte na svém zařízení antivir? (vyberte jednu z odpovědí)

- Ano napište jaký
- Ne
- Nevím, o zařízení se stará někdo jiný

5. Používáte na svém zařízení firewall? (vyberte jednu z odpovědí)

- Ano
- Ne
- Nevím, o zařízení se stará někdo jiný

6. Aktualizujete pravidelně operační systém svého zařízení? (vyberte jednu z odpovědí)

- Ano
- Ne
- Nevím, o zařízení se stará někdo jiný

7. Zálohujete svá data? (vyberte jednu z odpovědí)

- Ne
- Ano pravidelně 1x za ... den/týden/měsíc/rok
- Ano, nepravidelně vždy po nějaké události (např. po dovolené fotky) napište událost....
- Nevím co je zálohování dat

8. Došlo u Vás někdy ke ztrátě dat?

- Ne

- Ano, data byla zálohovaná, ke ztrátě nakonec nedošlo
- Ano, data nebyla zálohovaná a nemrzelo mě to
- Ano, data nebyla zálohovaná a mrzelo mě to

9. Stali jste se někdy obětí škodlivého softwaru? (vyberte jednu z odpovědí)

- Ano, ale nestihl vykonat žádnou škodlivou činnost, nebo o ní nevím
- Ano, stihl vykonat škodlivou činnost
- Ne
- Nevím

Pokud zatrhl jakékoliv ano následuje otázka 10 a 11

10. Víte jakou cestou se škodlivý software dostal do Vašeho zařízení?

- Nákazou z přílohy v e–mailu
- Nákazou z webových stránek
- Absence antiviru
- Neaktualizovaný antivir
- Nakažené médium (CD, USB disk)
- Nevím

11. Jakou škodlivou činnost stihl škodlivý software vykonat? (můžete označit i více odpovědí)

- Ztráta dat smazáním nebo znepřístupnění dat
- Únik citlivých informací
- Ovládnutí zařízení hackerem

- Znemožnění přístupu do zařízení
- Ovládnutí internetového bankovnictví
- Jiné napište....

12. Považujete svá hesla za bezpečná? (vyberte jednu z odpovědí)

- Ano
- Ne
- Nevím, nedokážu to posoudit

13. Zná Vaše heslo ještě někdo jiný?

- Ne
- Ano, některá hesla sdílím s dalšími osobami , napište jaké aplikací to jsou např. (pošta, soc. sítě, bankovnictví, internetové obchody).....

14. Používáte stejná hesla do více aplikací? (vyberte jednu z odpovědí)

- Ano, používám všude stejné heslo
- Ano, používám několik hesel
- Ne, ke každé aplikaci mám jiné heslo

15. Jak často si měníte své heslo? (vyberte jednu z odpovědí)

- Nikdy si heslo neměním, mám stále stejné
- Měním pravidelně 1x za .....měsíce
- Jiné, napište....

16. Jakou podobu má Vaše heslo, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)? (můžete označit i více odpovědí)

- Napište počet znaků v hesle.....

- Heslo obsahuje malá písmena
- Heslo obsahuje velká písmena
- Heslo obsahuje číslice
- Heslo obsahuje speciální znaky (např. @,$,§,! apod.)
- V hesle používám osobní údaj (např. jméno dětí, město, datum narození)
- V hesle požívám slovo nějakého významu

17. Používáte nějaký program pro správu hesel? (vyberte jednu z odpovědí)
    - Nevím, že něco podobného existuje
    - Ne
    - Ano, uveďte jaký....
18. Dostal jste se do situace, že někdo nepovolaný se dostal K Vašim datům?
    - Ne
    - Ano, prozradil jsem heslo „nesprávné“ osobě, která ho zneužila
    - Ano, někdo z mého okolí mi heslo odkoukal
    - Ano, někdo z mého okolí mé heslo odhadl nebo získal jinak
    - Ano, můj účet napadli neznámí pachatelé (nikdo z mého okolí)
19. Co děláte s e–maily od neznámého odesilatele? (vyberte jednu z odpovědí)
    - Smažu ho
    - Označím jako spam
    - Otevřu jen, pokud mě v náhledu něco zaujme
    - Otevřu a přečtu si ho

- Jiné, napište. . . ..

20. Otevíráte nevyžádané přílohy v e–mailech? (vyberte jednu z odpovědí)

- Ano
- Ne

21. Klikáte na odkazy uvedené v emailech? (vyberte jednu z odpovědí)

- Ano na všechny
- Ano, pokud mě daný odkaz zaujme
- Ano , pokud jsou od známého zdroje
- Ne, klikám jen na odkazy, kterým důvěřuji a jejichž příchod jsem očekával
- Neklikám na žádný
- Jiné, napište. . . .

22. Co uděláte pokud Vám přijde e–mail s žádostí , aby jste pro zvýšení zabezpečení potvrdil jakékoli své přihlašovací heslo (vyberte jednu z odpovědí)

- na e–mail odpovím a zvýším si tak svou internetovou bezpečnost
- na e–mail odpovím, ale heslo sdělím až poté, co mi odesílatel v dalším e–mailu potvrdí, k čemu přesně mé heslo potřebuje
- na e–mail v žádném případě neodpovídám

Pokud respondent uvedl, že využívá internetové bankovnictví

23. Jak přistupujete do internetového bankovnictví?

- Pouze přes vlastní odkaz, záložky či oblíbené položky
- Ručně vypíšu adresu do webového prohlížeče
- Vyhledám přes vyhledávač typu Seznam, Google

24. Setkal jste se někdy s útokem phishing osobně? Phishing je nejčastěji druh podvodného emailu, vypadající jako odeslaný ze známé organizace (často banka) obsahující odkaz na falešné stránky ve stejném stylu jako originální stránky, s cílem získat přístupové údaje.

- Ano
- Ne

Pokud respondent uvedl ano

25. Jak jste reagovali na phishingový útok? (vyberte jednu z odpovědí)

- Nereagoval
- Reagoval, ale pak akci přerušil (tj. svá data nevyzradil)
- Reagoval a zadal požadované údaje, ale nic se nestalo
- Reagoval a zadal požadované údaje, a něco se stalo

26. Jaký je Váš věk?

- Napište Váš věk....

27. Jaké je Vaše pohlaví?

- Žena
- Muž

28. Jaké je Vaše dosažené vzdělání?

- vysokoškolské
- vyšší odborné
- středoškolské
- vyučen
- základní

# Dotazník - E-bezpečnostní znalosti a chování osob pracujících ve státní správě

Které z následujících zařízení používáte k přístupu na internet? (můžete označit i více odpovědí)

☐ Notebook/netbook

☐ Stolní počítač

☐ Chytrý mobilní telefon

☐ Tablet

K jakým účelům používáte Vaše zařízení? (můžete označit i více odpovědí)

☐ Komunikace a sociální sítě (např. facebook, e–mail. . . )

☐ Internetové bankovnictví

☐ Online nakupování

☐ Práce

☐ Vyhledávání informací

☐ Stahování dat (filmy, hudba..)

☐ Online hry

Jak často používáte své zařízení?

◯ Každodenně –> následující otázka Používáte na svém zařízení antivir?

◯ Několikrát za týden –> následující otázka Používáte na svém zařízení antivir?

◯ Zřídka –> následující otázka Napište jak často za měsíc používáte své zařízení.

Napište jak často za měsíc používáte své zařízení.

—

Používáte na svém zařízení antivir?

◯ Ano –> následující otázka Vyberte značku Vašeho antiviru

◯ Ne –> následující otázka Používáte na svém zařízení firewall?

◯ Nevím, o zařízení se stará někdo jiný –> následující otázka Používáte na svém zařízení firewall?

Vyberte značku Vašeho antiviru

☐ Avast!

☐ AEC TrustPort

☐ AntiVir Personal Edition

☐ AVG BitDefender

☐ CA Antivirus

☐ ClamAV

☐ Dr.Web

☐ eScan

☐ ESET NOD32 Antivirus

☐ eTrust Antivirus

☐ F–Secure Antivirus

☐ Kaspersky Antivirus

☐ McAffe Antivirus

☐ Microsoft Security Essentials

☐ Norman antivirus

☐ Norton Antivirus

☐ PC Tools AntiVirus

☐ Symantec EndPoint Security

☐ Sophos Antivirus

☐ Zoner Antivirus

☐ Jiný

Používáte na svém zařízení firewall?

◯ Ano

◯ Ne

◯ Nevím, o zařízení se stará někdo jiný

Aktualizujete pravidelně operační systém svého zařízení?

◯ Ano

◯ Ne

◯ Nevím, o zařízení se stará někdo jiný

Zálohujete svá data?

◯ Ano, pravidelně –> následující otázka S jakou pravidelností zálohujete svá data?

◯ Ano, nepravidelně vždy po nějaké události (např. po dovolené fotky) –> následující otázka Napište událost, po které zálohujete data

◯ Ne –> následující otázka Došlo u Vás někdy ke ztrátě dat?

◯ Nevím co je zálohování dat –> následující otázka Došlo u Vás někdy ke ztrátě dat?

Napište událost, po které zálohujete data

— –> následující otázka Došlo u Vás někdy ke ztrátě dat?

S jakou pravidelností zálohujete svá data?

◯ každý den

◯ každý týden

◯ každých 14 dní

◯ každý měsíc

◯ každé čtvrtletí

◯ každý půlrok

◯ každý rok

Došlo u Vás někdy ke ztrátě dat?

◯ Ano, data byla zálohovaná, ke ztrátě nakonec nedošlo

◯ Ano, data nebyla zálohovaná a nemrzelo mě to

◯ Ano, data nebyla zálohovaná a mrzelo mě to

◯ Ne

Stali jste se někdy obětí škodlivého softwaru?

◯ Ano, ale nestihl vykonat žádnou škodlivou činnost, nebo o ní nevím –> následující otázka Víte jakou cestou se škodlivý software dostal do Vašeho zařízení?

◯ Ano, stihl vykonat škodlivou činnost –> následující otázka Jakou škodlivou činnost stihl škodlivý software vykonat? (můžete označit i více odpovědí)

◯ Ne –> následující otázka Považujete svá hesla za bezpečná?

◯ Nevím –> následující otázka Považujete svá hesla za bezpečná?

Jakou škodlivou činnost stihl škodlivý software vykonat? (můžete označit i více odpovědí)

☐ Ztráta dat smazáním nebo znepřístupnění dat

☐ Únik citlivých informací

☐ Ovládnutí zařízení hackerem

☐ Znemožnění přístupu do zařízení

☐ Ovládnutí internetového bankovnictví

☐ Jiné

Víte jakou cestou se škodlivý software dostal do Vašeho zařízení?

☐ Nákazou z přílohy v e–mailu

☐ Nákazou z webových stránek

☐ Absence antiviru

☐ Neaktualizovaný antivir

☐ Nakažené médium (CD, USB disk)

☐ Nevím

Považujete svá hesla za bezpečná?

◯ Ano

◯ Ne

◯ Nevím, nedokážu to posoudit

Zná Vaše heslo ještě někdo jiný?

◯ Ano, některá hesla sdílím s dalšími osobami –> následující otázka Napište do jakých aplikací sdílíte hesla

◯ Ne –> následující otázka Používáte stejná hesla do více aplikací?

Napište do jakých aplikací sdílíte hesla

—

Používáte stejná hesla do více aplikací?

◯ Ano, používám všude stejné heslo

◯ Ano, používám několik hesel

◯ Ne, ke každé aplikaci mám jiné heslo

Měníte si své heslo?

◯ Ano –> následující otázka S jakou pravidelností měníte svá hesla?

◯ Ne –> následující otázka Jakou podobu má Vaše heslo, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)? (můžete označit i více odpovědí)

S jakou pravidelností měníte svá hesla?

◯ každý týden

◯ každých 14 dní

◯ každý měsíc

◯ každé čtvrtletí

◯ každý půlrok

◯ každý rok

Jakou podobu má Vaše heslo, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)? (můžete označit i více odpovědí)

☐ Heslo obsahuje malá písmena

☐ Heslo obsahuje velká písmena

☐ Heslo obsahuje číslice

☐ Heslo obsahuje speciální znaky (např. @,$,§,! apod.)

☐ V hesle používám osobní údaj (např. jméno dětí, město, datum narození)

☐ V hesle používám slovo nějakého významu

Napište počet znaků v hesle, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)?

—

Používáte nějaký program pro správu hesel?

◯ Ano –> následující otázka Uveďte jaký program pro správu hesel používáte

◯ Ne –> následující otázka Dostal jste se do situace, že někdo nepovolaný se dostal k Vašim datům?

◯ Nevím, že něco podobného existuje –> následující otázka Dostal jste se do situace, že někdo nepovolaný se dostal k Vašim datům?

Uveďte jaký program pro správu hesel používáte

◯ 1Password

◯ Dashlane

◯ KeePass

◯ LastPass

◯ LockCrypt

◯ Moje ID

◯ SafeInCloud

◯ StickyPassword

◯ PasswordBox

◯ Password Safe

◯ RoboForm

◯ Jiný

Dostal jste se do situace, že někdo nepovolaný se dostal k Vašim datům?

◯ Ano, prozradil jsem heslo „nesprávné“ osobě, která ho zneužila

◯ Ano, někdo z mého okolí mi heslo odkoukal

◯ Ano, někdo z mého okolí mé heslo odhadl nebo získal jinak

◯ Ano, můj účet napadli neznámí pachatelé (nikdo z mého okolí)

◯ Ne

Co děláte s e–maily od neznámého odesilatele?

◯ Smažu ho

◯ Označím jako spam

◯ Otevřu jen, pokud mě v náhledu něco zaujme

◯ Otevřu a přečtu si ho

Otevíráte nevyžádané přílohy v e–mailech?

◯ Ano

◯ Ne

Klikáte na odkazy uvedené v e–mailech?

◯ Ano na všechny

◯ Ano, pokud mě daný odkaz zaujme

◯ Ano, pokud jsou od známého zdroje

◯ Ne, klikám jen na odkazy, kterým důvěřuji a jejichž příchod jsem očekával

◯ Neklikám na žádný

Co uděláte pokud Vám přijde e–mail s žádostí, aby jste pro zvýšení zabezpečení potvrdili své přihlašovací heslo

◯ Na e–mail odpovím a zvýším si tak svou internetovou bezpečnost

◯ Na e–mail odpovím, ale heslo sdělím až poté, co mi odesílatel v dalším e–mailu potvrdí, k čemu přesně mé heslo potřebuje

◯ Na e–mail v žádném případě neodpovídám

Setkal jste se někdy s útokem phishing osobně? Phishing je nejčastěji druh podvodného emailu, vypadající jako odeslaný ze známé organizace (často banka) obsahující odkaz na falešné stránky ve stejném stylu jako originální stránky, s cílem získat přístupové údaje.

◯ Ano –> následující otázka Jak jste reagovali na phishingový útok?

◯ Ne –> následující otázka Jaký je Váš věk?

Jak jste reagovali na phishingový útok?

◯ Nereagoval

◯ Reagoval, ale pak akci přerušil (tj. svá data nevyzradil)

◯ Reagoval a zadal požadované údaje, ale nic se nestalo

◯ Reagoval a zadal požadované údaje, a něco se stalo

Jaký je Váš věk?

—

Jaké je Vaše pohlaví?

◯ Žena

◯ Muž

Jaké je Vaše dosažené vzdělání?

◯ Vysokoškolské

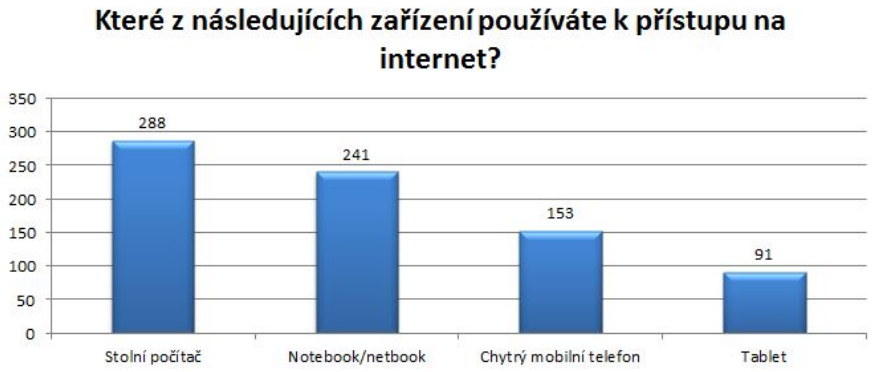
◯ Vyšší odborné

◯ Středoškolské

◯ Vyučen

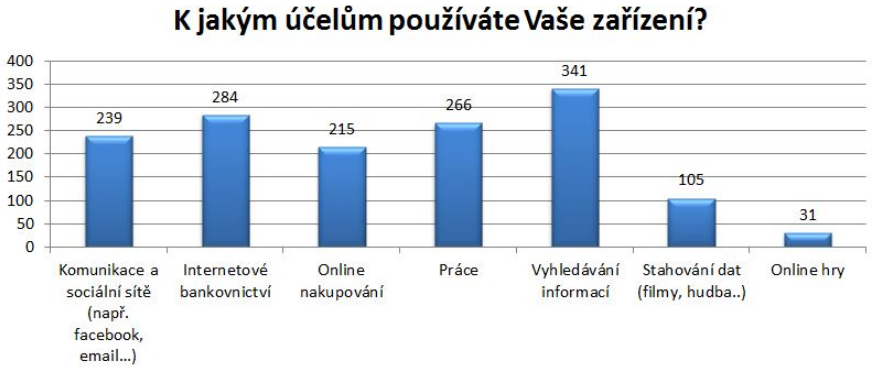
◯ Základní

# Analýza jednotlivých otázek



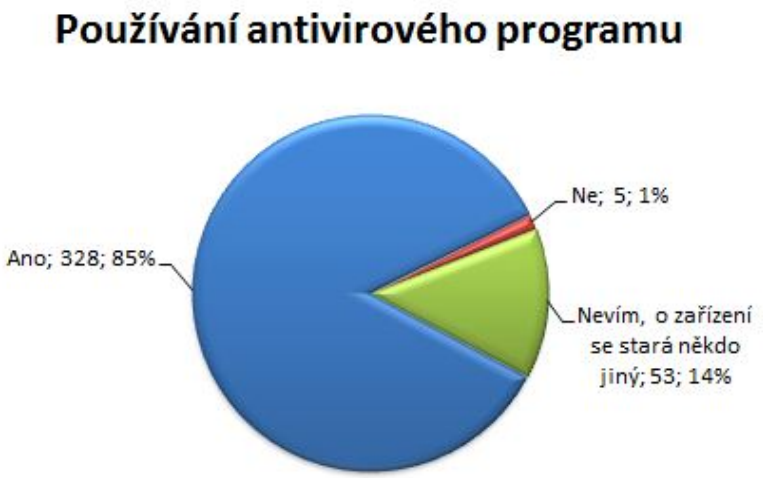

Obrázek 6: Otázka - Které z následujících zařízení používáte k přístupu na internet?

**Analýza otázky: Které z následujících zařízení používáte k přístupu na internet?**




Obrázek 7: Otázka - K jakým účelům používáte Vaše zařízení?

**Analýza otázky: K jakým účelům používáte Vaše zařízení?**



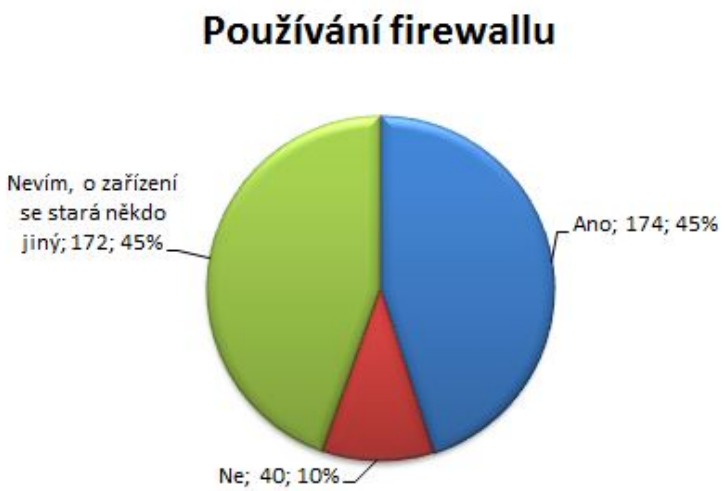

Obrázek 8: Otázka - Používáte na svém zařízení antivir?

**Analýza otázky: Používáte na svém zařízení antivir?**

| Antivirový program | Počet | % |
|---|---|---|
| Avast! | 203 | 48 |
| AVG | 66 | 15 |
| ESET NOD32 Antivirus | 49 | 12 |
| Symantec EndPoint Security | 33 | 8 |
| Microsoft Security Essentials | 14 | 3 |
| Norton Antivirus | 11 | 3 |

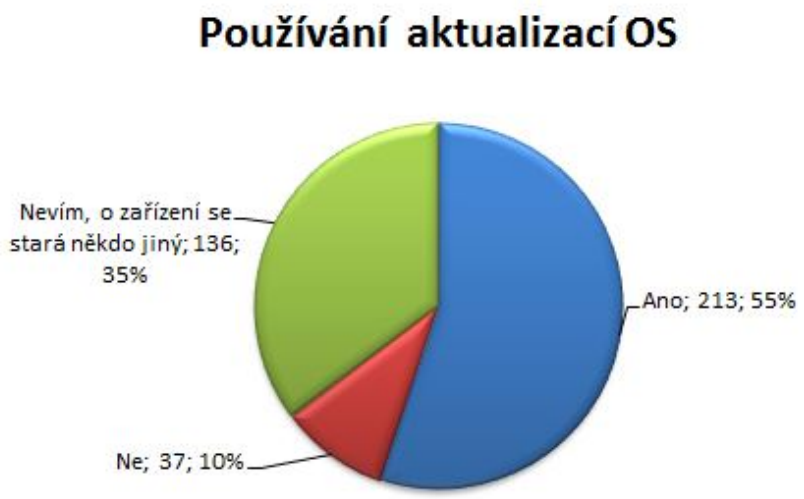
Tabulka 9: TOP 6 používaných antivirových programů

**Analýza otázky: Vyberte značku Vašeho antiviru.**




Obrázek 9: Otázka - Používáte na svém zařízení firewall?

**Analýza otázky: Používáte na svém zařízení firewall?**

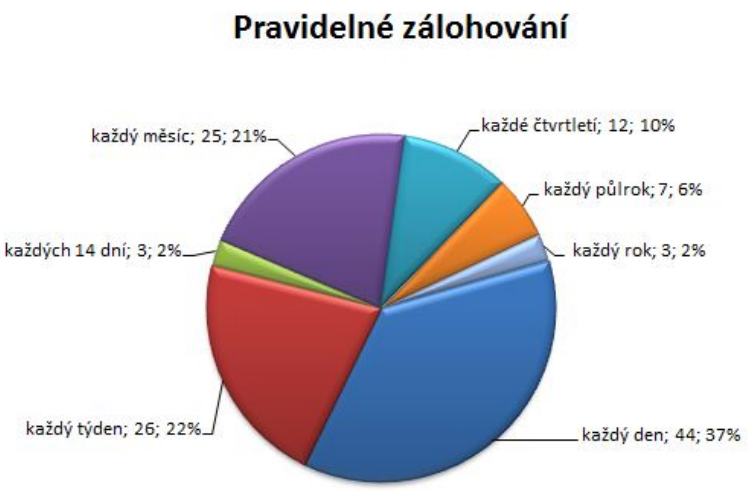



Obrázek 10: Otázka - Aktualizujete pravidelně operační systém svého zařízení?

**Analýza otázky: Aktualizujete pravidelně operační systém svého zařízení?**


Obrázek 11: Otázka - Zálohujete svá data?

**Analýza otázky: Zálohujete svá data?**




Obrázek 12: Otázka - S jakou pravidelností zálohujete svá data?

**Analýza otázky: S jakou pravidelností zálohujete svá data?**


Obrázek 13: Otázka - Došlo u Vás někdy ke ztrátě dat?

**Analýza otázky: Došlo u Vás někdy ke ztrátě dat?**


Stali jste se někdy obětí škodlivého softwaru?

**Analýza otázky: Stali jste se někdy obětí škodlivého softwaru?**


Obrázek 14: Otázka - Jakou škodlivou činnost stihl škodlivý software vykonat?

**Analýza otázky: Jakou škodlivou činnost stihl škodlivý software vykonat?**


Obrázek 15: Otázka - Jakou cestou se škodlivý software dostal do zařízení?

**Analýza otázky: Jakou cestou se škodlivý software dostal do zařízení?**


Obrázek 16: Otázka - Považujete svá hesla za bezpečná?

**Analýza otázky: Považujete svá hesla za bezpečná?**


Obrázek 17: Otázka - Zná Vaše heslo někdo jiný?

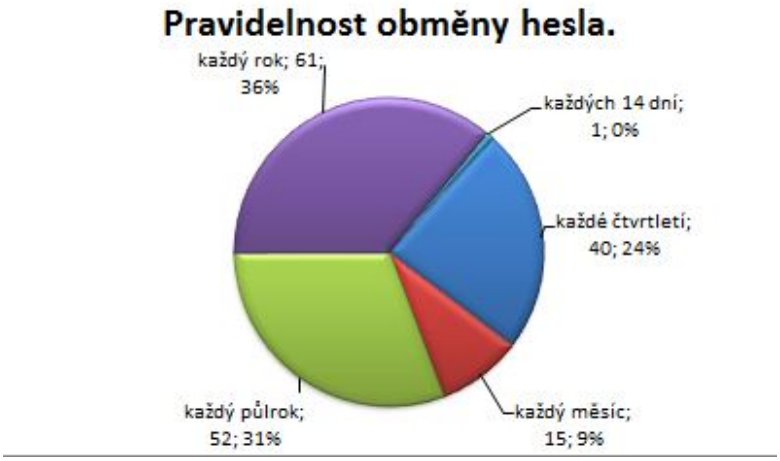
**Analýza otázky: Zná Vaše heslo někdo jiný?**


Obrázek 18: Otázka - Používáte stejná hesla do více aplikací?

**Analýza otázky: Používáte stejná hesla do více aplikací?**

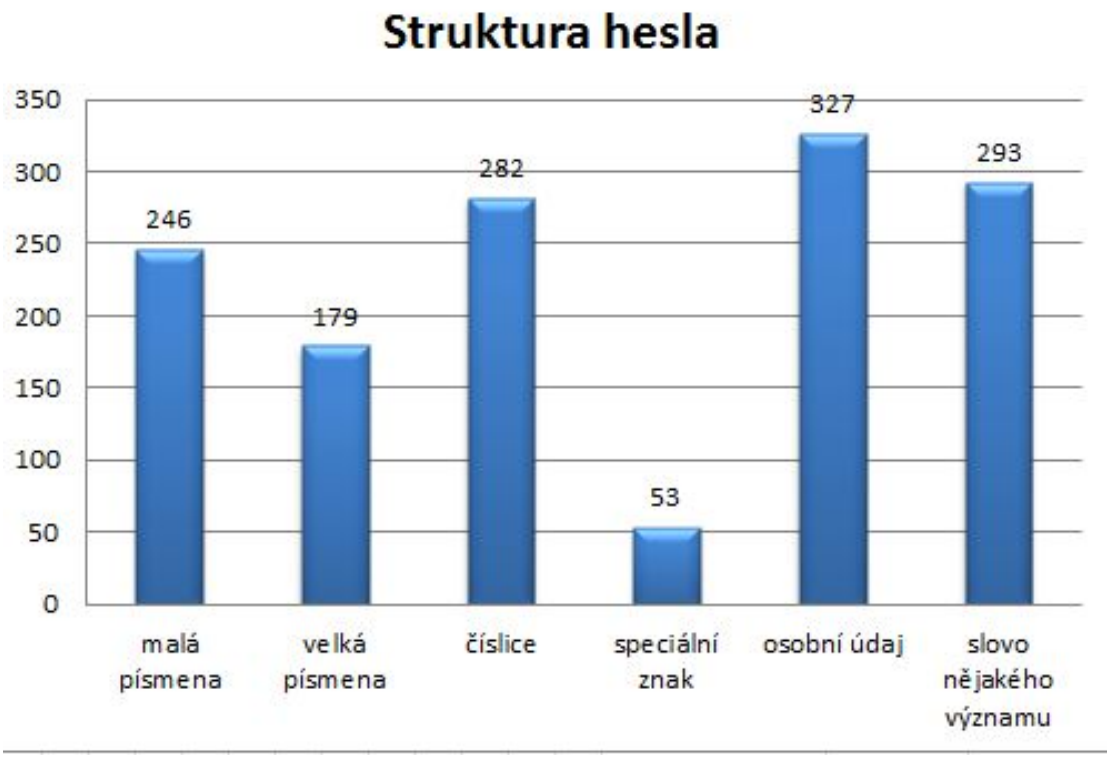

Obrázek 19: Otázka - Měníte si své heslo?

**Analýza otázky: Měníte si své heslo?**




Obrázek 20: Otázka - S jakou pravidelností měníte svá hesla?.

**Analýza otázky: S jakou pravidelností měníte svá hesla?**




Obrázek 21: Otázka - Jakou podobu má Vaše heslo, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)

**Analýza otázky: Jakou podobu má Vaše heslo, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)**


Obrázek 22: Otázka - Napište počet znaků v hesle, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)

**Analýza otázky: Napište počet znaků v hesle, které používáte k přístupu do aplikace s citlivými údaji? (např. bankovnictví, soc. sítě, e–mail)**


Obrázek 23: Otázka - Používáte nějaký program pro správu hesel?

**Analýza otázky: Používáte nějaký program pro správu hesel?**

| Program pro správu hesel | Počet |
|---|---|
| KeePass | 6 |
| 1Password | 2 |
| LastPass | 2 |
| Moje ID | 2 |
| Password Safe | 1 |
| Jiný | 1 |
| Celkem | 14 |

Tabulka 10: Používané programy pro správu hesel

**Analýza otázky: Aktualizujete pravidelně operační systém svého zařízení?**


Obrázek 24: Otázka - Dostal jste se do situace, že někdo nepovolaný se dostal k Vaším datům?

**Analýza otázky: Dostal jste se do situace, že někdo nepovolaný se dostal k Vaším datům?**


Obrázek 25: Otázka - Co děláte s e–maily od neznámého odesilatele?

**Analýza otázky: Co děláte s e–maily od neznámého odesilatele?**


Obrázek 26: Otázka - Otevíráte nevyžádané přílohy v e–mailech?

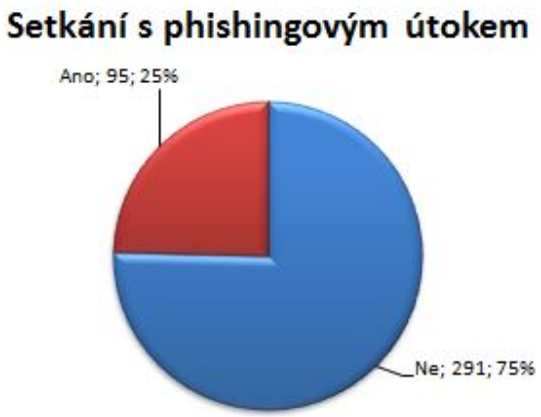
**Analýza otázky: Otevíráte nevyžádané přílohy v e–mailech?**


Obrázek 27: Otázka - Klikáte na odkazy uvedené v e–mailech?

**Analýza otázky: Klikáte na odkazy uvedené v e–mailech?**

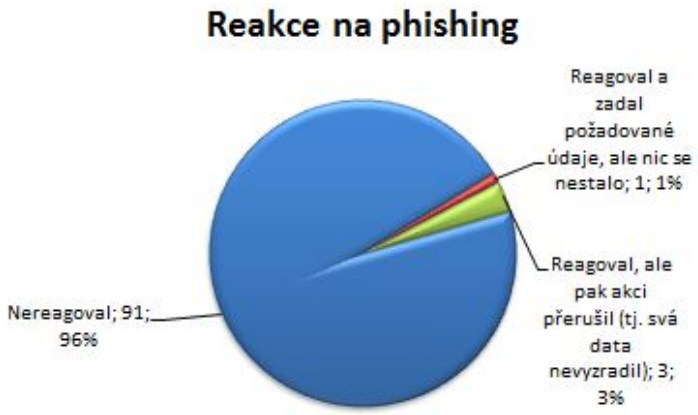

Obrázek 28: Otázka - Co uděláte pokud Vám přijde e–mail s žádostí, aby jste pro zvýšení zabezpečení potvrdili své přihlašovací heslo?

**Analýza otázky: Co uděláte pokud Vám přijde e–mail s žádostí, aby jste pro zvýšení zabezpečení potvrdili své přihlašovací heslo?**



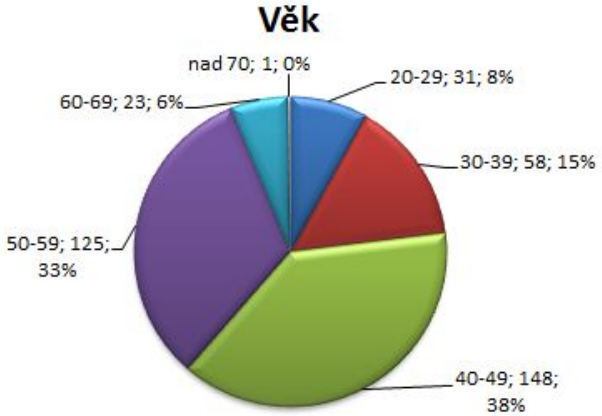

Obrázek 29: Otázka - Setkal jste se někdy s útokem phishing osobně?

**Analýza otázky: Setkal jste se někdy s útokem phishing osobně?**



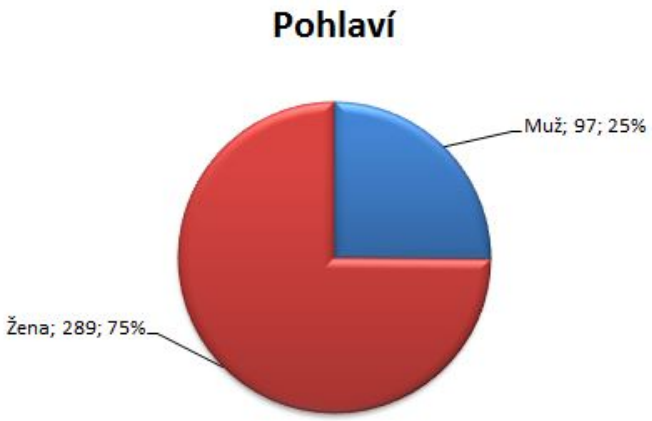

Obrázek 30: Otázka - Jak jste reagoval na phishingový útok?

**Analýza otázky: Jak jste reagoval na phishingový útok?**




Obrázek 31: Otázka - Jaký je Váš věk?

**Analýza otázky: Jaký je Váš věk?**




Obrázek 32: Otázka - Jaké je Vaše pohlaví?

**Analýza otázky: Jaké je Vaše pohlaví?**


Obrázek 33: Otázka - Jaké je Vaše dosažené vzdělání?

**Analýza otázky: Jaké je Vaše dosažené vzdělání?**