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

Bakalářská práce

Faktory ovlivňující chování studentů učitelství v oblasti technické e-bezpečnosti

Vypracoval: Vít Synek
Vedoucí práce: Mgr. Václav Šimandl Ph.D.

České Budějovice 2017

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

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 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 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 14. 07. 2017

Vít Synek

Abstrakt

Cílem bakalářské práce bude prozkoumat faktory, které ovlivňují chování studentů vysokých škol v určitých rizikových situacích týkajících se e-bezpečnosti. Faktorů, které studenty mohou ovlivňovat je v podstatě nekonečné množství, proto musí být vybrány jen ty nejvíce relevantní. K rizikovým situacím zde můžeme řadit jakoukoliv ztrátu dat od hackerského útoku až po neúmyslné smazání svého vlastního flash disku.

Za tímto účelem bude sestaven vhodný dotazník, ve kterém každý student zaznamená základní charakteristiky, například pohlaví, obor studia, absolvované středoškolské studium nebo demografický původ respondenta. Dále následují otázky na e-bezpečnost, u kterých jsou studenti dotazováni i na jejich pocity, jak nebezpečný a nepříjemný může konkrétní únik nebo ztráta dat být.

Celý dotazník je zpracován základními statistickými metodami, z nichž je zjišťováno, jestli dané faktory mají vliv na určité chování respondentů a jak velký vliv to popřípadě je.

Klíčová slova

E-bezpečnost, faktory, chování, studenti

Abstract

The aim of this thesis is to examine the factors that influence the behavior of university students in certain high-risk situations related to e-safety. Factors that may affect students are basically infinite and therefore only the most relevant factors were selected. Different risk situations ranging from hacker attack to accidental deleting their own flash drive were considered.

The study consisted of appropriate questionnaire in which each student will record basic characteristics, such as gender, field of study, completed secondary education or demographic origin of the respondent. Basic characteristics were followed by questions on e-safety in which, students were asked to give their perception of data leakage and loss.

The entire questionnaire was processed using basic statistical methods to evaluate how and to what extent the basic characteristics of the respondents affect their behavior.

Keywords

E-safety, factors, behavior, students

Poděkování

Děkuji vedoucímu své práce Mgr. Václavu Šimandlovi Ph.D. za jeho rady při vypracovávání práce a za pevné nervy.

Dále děkuji všem respondentům za jejich čas při vyplňování mého dotazníku.

Poslední dík patří mé rodině, která mě po celou dobu mého studia silně podporovala.

Obsah

1 Úvod

E-bezpečnost je v současné době ve světě velmi probíraným tématem, vzhledem k prudkému nárůstu technologií a následně tedy i dat, která by mohla být zneužita. Hrozeb je nyní již ve světě internetu i mimo něj nespočitatelné množství, proto se práce se bude opírat o hrozby, které se ve světě e-bezpečnosti nacházejí nejvíce frekventovaně. K úniku dat však nemusí dojít pouze působením třetí osoby, ale člověk svá data může ztratit i sám, což je v případě běžných fyzických osob, nikoliv tedy firem, častější možností ztráty. Nejnebezpečnějším místem z hlediska bezpečnosti je samozřejmě internet, proto i většina otázek v sestaveném dotazníku bude směřovaná právě na hrozby z něj. Dotazník bude směřovaný pro studenty vysokých škol, protože studenti nižších věkových kategorií si dobře neuvědomují rizika hrozeb a jejich následky, které mohou v oblasti bezpečnosti vyvstat. Roku 2014 byly globálně způsobeny škody za 445 miliard dolarů, což převyšuje předpokládané globální zisky z prodeje drog.[1]

2 Cíle práce

V této práci budou vysvětleny jednotlivé možnosti úniku dat, které budou i použity v dotazníku pro studenty. Prvním cílem je tudíž dostatečně vysvětlit různé hrozby, které způsobují úniky dat a podložit svá vysvětlení důležitými citacemi z odborné literatury. Dalším cílem práce je sestavit vhodný dotazník, který by měl být stručný a srozumitelný pro každého studenta libovolného zaměření, a vhodně v něm zakomponovat všechny rizikové faktory. Následně vyhledám vhodné skupiny respondentů, mezi které dotazník rozešlu a po vyplnění požadovaného počtu dotazníků začnu s analýzou výsledků. Podle analýzy výsledků dotazníkové akce bude zřejmé, které faktory mají největší vliv na chování respondentů. Práce by měla vysvětlit rozdílné chování respondentů vzhledem k jejich znalostem e-bezpečnosti a s tím související PC gramotnosti. Podle těchto výsledků by se mohla konkrétně směřovat proškolení studentů v e-bezpečnosti v přímé závislosti na jejich oboru. Hlavním cílem tudíž je, otestovat stanovené hypotézy a vyvození preventivních opatření proti běžným i méně častým ztrátám dat. Pokud by se podařilo prokázat, že některé z vybraných faktorů mají velký vliv na chování studentů, mohla by na shromážděné výsledky navázat další práce, která by už samotné studenty včas cíleně informovala o nebezpečí úniku dat.

3 Metoda práce

Prostuduji odbornou literaturu zabývající se tématem e-bezpečnosti a z ní následně zpracuji stručný rozbor možností úniků dat. v tomto rozboru bude dostatečně vysvětleno, jak která hrozba uživatele ohrožuje, jak se dá hrozbě předcházet a jak se zachovat pokud k napadení hrozbou již došlo. Dále si stanovím několik nejvíce relevantních faktorů, podle kterých vyberu skupiny respondentů. Sestavím dotazník, který bude pro všechny skupiny respondentů shodný. Dotazník bude korespondovat s vybranými statistickými metodami a u každé otázky popřípadě u skupiny otázek na daný faktor bude stanovena hypotéza, kterou se budu snažit výsledky potvrdit. Dotazník bude anonymní, studenti v něm o sobě budou zaznamenávat svůj věk, pohlaví, obor, který studují a typ studia. Tento dotazník rozešlu mezi studenty vysoké školy, fakulty?, kteří mají různé aprobace a jsou v různých věkových kategoriích. Očekáváný počet respondentů by se měl pohybovat v rozmezí 150 - 200 osob, z tohoto počtu by totiž již mělo být zřetelné, zda je některý z faktorů relevantní či není. Doba potřebná na vyplnění dotazníku by se měla pohybovat v rozmezí 8 - 12 minut. Prvním faktorem, podle kterého budu výsledky posuzovat je směr respondentova předchozího a současného vzdělání, to znamená, jestli jeho obor studia je technický, humanitní nebo například přírodovědecký. Dalšími důležitými faktory jsou samozřejmě demografický původ a pohlaví respondenta včetně jeho věku. Jako další faktory jsem zvolil, nakolik se konkrétní respondent zajímá o oblast informačních technologií nebo jak samotným bezpečnostním technologiím důvěřuje. Vysokoškolští studenti budou do tohoto dotazníku zaznamenávat, jestli se s jednotlivými úniky dat již setkali a jakou zkušenost v nich popřípadě zanechaly. Výsledky dotazníku pak budu porovnávat s faktory, které jsem si stanovil, a podle nich budu dále určovat, zda má jednotlivý faktor vliv na konkrétní chování respondentů. k vyhodnocení výsledků budu používat základní statistické metody jako je například jednoduchá analýza rozptylu, včetně grafického znázornění.

4 Rizika v oblasti e-bezpečnosti

4.1 Malware

Do pojmu malware se zahrnují všechny škodlivé programy, které se nám snaží do našeho počítače proniknout nebo se snaží uškodit operačnímu systému a datům, která v počítači jsou. Jakýkoliv software, který způsobuje uživateli nějakou škodu je považován za malware, což zahrnuje viry, trojské koně, červy, rootkits, scareware, spyware.[2] Zvláštní skupinou malware je pak adware. Slovo malware vzniklo spojením dvou anglických slov malicious a software. Z historického hlediska se vznik malware datuje kolem roku 1985, v této době většina škodlivých programů vznikala na univerzitách, kde se pak následně i šířila, protože v té době ještě většina lidí neměla své vlastní domácí počítače. Rozmach malwaru byl obrovský, protože během roku 1988 bylo společností pro obchod se software ADAPSO zaznamenáno, že v prvních dvou měsících roku 1988 existovalo přibližně 3000 druhů malware, ale v posledních dvou měsících roku už bylo zaznamenáno 30000 druhů, což je desetinásobný nárůst malware během jednoho roku.[3] Během věků se objevily již stovky tisíc různých malware, které se stejně jako veškeré další software zdokonalují a jsou tudíž čím dál více nebezpečné. Důvod, proč samotný malware vzniká, je za účelem obohacení, kdy útočník může proniknout do firemní sítě a ukrást citlivá data nebo dočasně odstavit například konkurenční firmu. Je spousta možných způsobů jak se k uživateli může malware dostat. McAfee uvádí, že stačí otevřít přílohu emailu od někoho, koho případně i znáte, ale kdo už byl napaden nebo stačí kliknout na link či banner v emailu nebo na nebezpečné stránce a prohlížeč už si virus sám stáhne.[4] Samotní útočníci většinou zůstanou utajeni, protože mohou využít maskovací prostředky. Jedním z nejvyužívanějších jsou Tor servery (The onion router). Tor je síť serverů, které jsou rozprostřeny po celém světě a útočníkův požadavek je posílán od počátečního až po koncový uzel šifrovanou komunikací, což zdroj požadavku učiní téměř nedohledatelný.[5]

4.1.1 Virus

Viry jsou nejspíše veřejně nejznámější skupinou malware. Tvůrci virů musí mít dobré znalosti slabých míst operačních systémů (tzv. exploit), aby se byl virus schopen i přes ochranu počítačů dostat. Viry jsou podle většiny počítačových expertů definovány jako škodlivé příkazy, které nejsou sestaveny pouze pro napadení cizích

programů, ale i pro jejich následnou úpravu a navíc mají vlastnost replikovat samy sebe.[3] Podle webroot jsou nejčastější cesty šíření virů stahování her, pluginů a dalších utilit, dále pak navštěvování infikovaných webových stránek. Možností, co viry v počítačích mohou provést, je mnoho. Některé viry jsou uzpůsobeny k tomu, aby napadaly nainstalovaný software a poškodily ho, dále viry mohou z počítačů odstraňovat data nebo dokonce zformátovat celý harddisk, což patří k těm nejhorším variantám symptomů. Mnohdy však uživatel pouze může pozorovat, že se jeho PC bezdůvodně zpomalil nebo dochází k častému restartu operačního systému.

Rozdělení virů není jednoduché, protože v dnešní době je virů nepřeberné množství a jejich vlastnosti se mohou různě prolínat. Viry lze rozdělit do těchto skupin [6]:

- Residentní viry - Jsou jedny z nejvíce nebezpečných, protože obývají RAM paměť počítače. Mohou upravovat spuštěné i vypnuté aplikace a libovolně ovlivňovat probíhající operace.
- Přepisovací viry - Kompletně nebo částečně přepisují nakažená data.
- Bootovací viry - Jsou nahrány v bootovací sekvenci harddisku a způsobují, že operační systém nemůže nabootovat.
- File infectors – Napadají executable soubory a po jejich spuštění působí škody.
- Directory viry – Tyto viry jsou schopné měnit své umístění. Program většinou běží na pozadí a uživatel o něm neví, změna umístění navíc způsobí, že virus není téměř možné v počítači najít.
- Macro viry – Postihují programy, které jsou schopné vytvářet nebo používat makra. Asi nejznámějším případem jsou napadení Microsoft Word a Excel.

4.1.2 Trojský kůň

Trojské koně byly příhodně pojmenovány podle bájného koně, který pronikl do města Trója. Hlavní rozdíl trojského koně oproti virům je, že se nijak v počítači

nereplikují, ale naopak se snaží zůstat utajeni mezi daty, která žádné škody nepůsobí. Trojské koně mohou vypadat v podstatě jako cokoliv, může to být stažená hra nebo písnička v Mp3 formátu[7]. Důležité však je, že tyto aplikace mají skrytou část, která obsahuje trojského koně, o kterém se však uživatel mnohdy po stažení ani nedozví.

Je mnoho možností jak se budou trojské koně v počítači chovat, většinou však zůstávají utajené a sbírají různá data. Existují i trojské koně, které uživateli znepříjemňují použití počítače tím, že například mění pozadí plochy, přidávají nesmyslné ikony nebo dokonce mažou některá data.[8] Zvláštním typem jsou pak backdoor trojské koně, které útočníkovi umožňují přístup k počítači bez vědomí uživatele.

Jedním z nejvíce známých trojských koňů je Zbot/Zeus, který napáchal v minulosti obrovské škody. Zbot byl vytvořen, aby útočníkovi poskytoval citlivá data, jako jsou například hesla k bankovnictví, emailům nebo přímo osobní detaily uživatele (jméno, datum narození). Některé verze dokázaly na oficiálních webových stránkách přidávat do formulářů extra textová pole, kde uživatel vyplnil data, která by normálně nezadával.[9]

4.1.3 Worm (červ)

Počítačoví červi jsou mnohdy považováni za viry, protože jsou si obecně tyto dvě skupiny velmi podobné. Stejně jako viry se i červi umí na počítači replikovat, čímž se šíří. Hlavním rozdílem ale je, že červi se umí šířit po síti a to bez jakéhokoliv přičinění uživatele. Červa tedy není nutno nijak spouštět nebo instalovat. Dalším rozdílem je, že červ nenapadá žádná další data v systému, ale pouze se šíří k dalším uživatelům. Červi typicky působí problémy sítím, které je hostují, tím že konzumují šířku pásma a přetěžují webservery.[10]

Jedním z nejvíce známých a nebezpečných červů je Code Red, který na internet pronikl v roce 2001. Tento červ byl naprogramován pro napadání Microsoft IIS na webových serverech. Využil exploitu, pomocí kterého zneužíval buffer a přetěžoval ho. Navíc byl schopen se rozšiřovat do dalších IIS a na webových serverech pak zobrazoval hlášku, kterou si jeho tvůrci vybrali.

Obrázek 1: Ukázka červa

4.1.4 Rootkit

Slovo rootkit je složenina dvou anglických slov root, které symbolizuje vlastníka nejvyšších oprávnění a kit, což může být vysvětleno jako soubor nástrojů. Rootkit je set technických kódů, které útočníkovi umožňují dostat kontrolu nad systémem a hardwarem počítače s právy roota a díky tomu umožňuje dalším škůdcům asi tu nejdůležitější věc pro jejich přežití a to schování se v počítači.[11]

Rootkit operuje v kernelu samotného systému. Vzhledem k tomu, že většina kernelů byla sestavena tak, aby je bylo v budoucnu možné nadále upravovat, je možné této cesty zneužít a kernel napadnout. Jedním z modulů kernelu je správce zařízení, který po napadení rootkitem může útočníkovi poskytnout správu jednotlivých komponent počítače.

4.1.5 Botnet

Botnet jako takový nijak uživateli neškodí, jedná se pouze o webovou infrastrukturu robotů. Slouží však jako transportní prostředek škodlivých prvků, ať už se jedná o spam nebo skripty, které přetěžují webové servery. Útočník, který má nad boty kontrolu je označován jako botmaster.[11] Jako botnet se označuje nejen síť napadených osobních počítačů, ale i napadené servery nebo pouze webhostingy.

Právě u webhostingů je v dnešní době dost časté napadení jejich CMS a následné šíření škodlivého obsahu pomocí skriptů.

4.1.6 Ransomware

Ransomware je v dnešní době jedním z nejvíce populárních druhů malware. Ransomware zamezuje uživateli přístup k jeho datům a operačnímu systému. Občas se také může jednat o krypto-ransomware/cryptoware, který celý počítač zašifruje a dokud uživatel nezaplatí „výpalné“ tak mu neposkytne přístup k PC. Tento druh malware je většinou připojen jako příloha nějakého emailu.

Obrázek 2: Ukázka ransomware

Velké škody za poslední dobu napáchal ransomware WannaCry, který požaduje po své oběti zaplacení 300 dolarů v bitcoinech a k datu 14. 05. 2017 bylo takto napadeno již přes 200 000 uživatelů.[12] Navíc pokud uživatel nezaplatí poplatek včas, zvyšuje se cena až na 1200 dolarů.

4.1.7 Adware

Adware je software který uživateli nabízí různé druhy reklamy. Do počítače se často dostává po instalaci nějakého pluginu do prohlížeče nebo po návštěvě nějakých pochybných stránek. Odstranitvirus.cz uvádí [13] „*Po instalaci do systému začne zobrazovat propagační obsah včetně vyskakovacích oken, bannerové reklamy, odkazů v textu a podobných reklam, které mají zvýšit popularitu webových stránek přidružených stran.“*

Adware nemusí nutně vždy pouze zobrazovat reklamu, ale může i o uživateli sbírat data o tom, které stránky uživatel navštěvuje, popřípadě co si koupil. Tato data přeposílá tvůrci adware, který pak data může prodat společnosti, která na základě nich sestaví pro uživatele cílenou reklamu.

4.2 Spam

Spam čili nevyžádaná zpráva je nejspíš každodenní součástí života všech, kteří používají emailovou schránku. Pojem Spam je ve skutečnosti však mnohem širší a jedná se o jakoukoliv formu nevyžádané zprávy, např. komentáře na sociálních sítích nebo SMS. Spam je definován třemi znaky a to tím, že je anonymní, nevyžádaný a masově se šíří. Na světě jsou v současné době 3,7 miliardy emailových schránek a denní počet odchozích spamů by se měl pohybovat kolem 269 miliard emailů denně.[14] Je tedy zřejmé, že počet odchozích spamů více než sedmdesátinásobně převyšuje počet emailových schránek. Za email spam považujeme všechno od nevyžádané reklamy až po phishingové útoky. Časté je také využití emailových příloh, ve kterých se dá odeslat malware či cryptoware, které pak uživatel může otevřít, pokud se jeví jako legitimní. Spameři se často také pokoušejí příjemce zmást tím, že přílohu pojmenují například faktura.pdf.exe, kdy se tedy nejedná o pdf, ale nějaký executable soubor.

V současné době je snaha o omezení množství odchozího spamu a proto byly doposud vyvinuty mechanismy jako je například DKIM (DomainKeys Identified Mail). DKIM do hlavičky emailů přidává DKIM –Signature, ve kterém je například hash obsahu emailu a pomocí DNS, ve kterých je uložen veřejný klíč. Server příjemce pak porovnává, zda nedošlo k nějaké změně nebo SPF (Sender Policy Framework), jenž na serveru příjemce kontroluje, zda je odchozí IP adresa oprávněna odesílat emaily z uvedené domény odesílatele emailu. i přes tuto obranu je však pro spamery stále relativně jednoduché spam rozesílat a to například založením email hostingu nebo crackem starších redakčních systémů webů, kam následně nahrají škodlivé skripty.

Z hlediska uživatele je asi nejdůležitější nastavení filtrů a blacklistu. Filtry nám umožňují zastavit příchod emailů z celých domén nebo dokonce blokovat emaily na základě jejich předmětu nebo obsahu. Do blacklistu můžeme umísťovat emailové adresy, které nám již v minulosti odeslaly Spam. Nadále by nám tedy od nich neměly už žádné další emaily přicházet. Pokud uživatel používá na svém PC emailového klienta, je také dobré používat Anti-Spam software. Uživatel by neměl nikdy otevírat přílohy z neznámých emailů a měl by kontrolovat v jakém formátu příloha je. Také je důležité mít svůj OS, email klient a případné Anti-Spam systém aktuální.

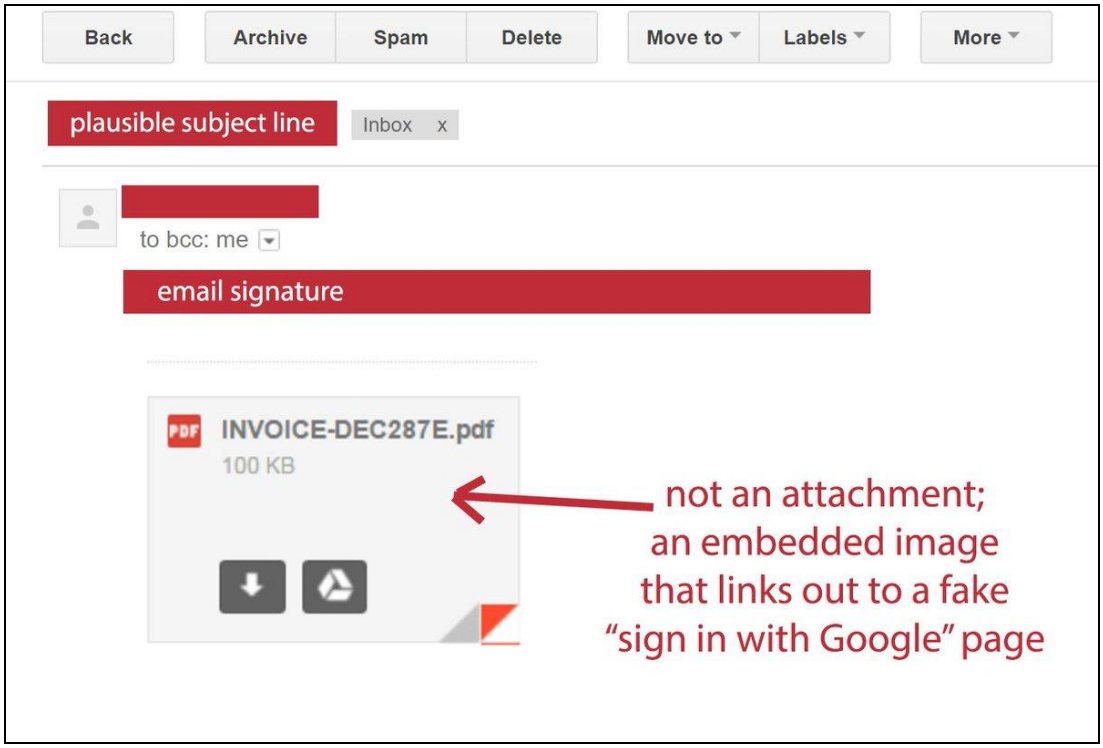
4.3 Phishing

Jednou z nejvíce rizikových hrozeb současnosti je phishing. Jedná se o velmi rafinovanou metodu, díky které útočník může získat přístup k účtům nebo osobní informace o své oběti. Nejčastějším cílem jsou tedy přístupy k účtům na sociálních sítích nebo k bankovním účtům. Za phishing se dá považovat i samotné sociální inženýrství, když se útočníci snaží od své oběti získat její osobní data, která nemusí nutně představovat velké riziko, ale mohou posloužit například pro crowdsourcing.

Nejčastějším prostředkem pro šíření phishingu jsou emaily. Tyto útočné emaily mohou mít hned několik podob. k nejpoužívanějším lstem však patří hypertextový odkaz, který svou oběť dovede na stránky, které se mohou jevit stejně legitimně jako například nějaký e-shop nebo login stránka sociální sítě. v případě e-shopu může útočník například lákat nízkou cenou jinak běžně drahého produktu a tak oběť donutit ke koupi a následné transakci peněz, za které však žádný produkt nedostane. U sociálních sítí může oběť odkaz zavést na stránku, která se zdánlivě jeví jako přihlašovací formulář dané sociální sítě, a získat tak přihlašovací údaje. Pokud je útočník dost zručný může hned po získání údajů svou oběť přesměrovat na opravdové stránky a tak je velká šance, že celý útok zůstane utajen. Dříve bylo po bližším prozkoumání odkazu zřejmé, že se jedná o podvrh, v odkazu byl například nepatrný překlep, ale v tu chvíli se už jednalo o jinou doménu. Nyní však mají útočníci ještě nebezpečnější zbraň, kterou jsou punycode domény. Punycode je systém, který umožnuje konvertovat znaky z unicode, které ASCII neobsahuje (například stará Řečtina) a reprezentovat je pomocí ASCII [15]. Veškeré DNS servery nebo mail servery používají totiž primárně ASCII kódování a není tedy možné si zaregistrovat doménu například starořeckými znaky. Díky punycode si může útočník nechat zaregistrovat doménu, jejíž URL odkaz se jeví jako legitimní, ale ve skutečnosti odkazuje úplně jinam. Například pokud by chtěl útočník mít doménu apple.com mohla by registrovaná doména vypadat takto xn--80ak6aa92e.com, ale URL odkaz by vypadal úplně stejně jako na normální doménu apple.com, protože by ho prezentoval v unicodu. Útočník totiž využívá toho, že některé znaky azbuky vypadají stejně jako latinská abeceda, ale kódované jsou jinak. Díky tomu je pak schopen naprosto svou oběť zmást.

Další možností, jak už bylo zmíněno, je využití přílohy emailu. Na začátku roku 2017 se například objevil nebezpečný případ phishingu u gmailu, se kterým měli

potíže samotní zaměstnanci firmy Google. Útočníci totiž vytvořili emailový účet, který byl příjemci znám jako například účet člena jeho rodiny a z něj odeslali email, který naoko obsahoval pdf přílohu. Přílohu však email neobsahoval, ale tlačítko s přílohou byl ve skutečnosti obrázek, který po kliknutí na stažení příjemce přesměroval na falešnou přihlašovací stránku.



Obrázek 3: Ukázka phishingu

4.4 Ochrana před hrozbami

4.4.1 Firewall

Je software nebo hardware, který dělí naši domácí síť od internetu a kontroluje mezi nimi datové toky podle předem nadefinovaných pravidel.[17] Hardwarové firewally se používají spíše ve firmách, základní funkce však plní i domácí routery, které mohou například blokovat různé porty. Z hlediska softwaru jsou Windows svým firewallem implicitně vybaveny. Uživatel si pak už sám definuje, zda chce některé své aplikaci povolit či nepovolit přístup do internetu. Firewall tedy uživatele může ochránit před útokem zvenku i zevnitř tím, že monitoruje paketový tok a zamezuje nepovoleným aplikacím přístup do počítače.

4.4.2 Antivirový systém

Naprostým standardem z hlediska bezpečnosti je používání antivirového systému. Funkce antivirového systému je skenovat počítač uživatele, nacházet možné hrozby a eliminovat je. Jsou dva základní typy skenování a to manuální nebo skeny „on access“[18]. Nejčastějším cílem hledáčku antivirů jsou viry, které se na počítač uživatele mohou dostat například při stahovaní z internetu. Dnešní antiviry se snaží zabránit útoku ještě dříve, než se dostanou škodlivá data do počítače. Navíc jsou schopné uživatele bránit i před dalšími hrozbami malware jako jsou červi, trojské koně nebo jen neškodný, ale obtěžující adware [19].

4.4.3 Hesla

Aby mohl uživatel chránit svá data, je nutné ke svým účtům nastavovat dobře postavená hesla. Nejlepší by bylo mít každé heslo jiné, aby se někdo, komu se podaří prolomit jedno, nedostal i ke zbytku účtů uživatele. To ale může být pro uživatele velice náročné na zapamatování a proto má možnost používat některý software pro správu hesel. To ale zatím není moc využívaná možnost, protože většina takových software není freeware a proto je nutné, aby si uživatel sestavil silné heslo. Pokud je to možné, heslo by mělo mít více než 12 znaků, obsahovat velké a malé znaky, číslice a speciální znaky, nemělo by se podobat žádnému slovníkovému slovu a nemělo by být zvoleno nápadně[20].

5 Výzkum

5.1 Určení faktorů a stanovení hypotéz

Nejprve jsem si stanovil faktory, které by nejspíše mohly ovlivňovat chování respondentů v e-bezpečnosti:

- Pohlaví
- Věk
- Aprobace studovaná na Pedagogické fakultě Jihočeské univerzity
- Velikost města odkud respondent pochází
- Typ vystudované střední školy
- Zájem o informační technologie
- Prodělání ztráty dat

Na základě těchto stanovených faktorů jsem vytvořil výzkumné otázky.

- Má pohlaví, věk nebo aprobace respondenta vliv na ztrátu dat?
- Má pohlaví, věk nebo aprobace respondenta vliv na setkání se s malwarem či phishingem?
- Má předchozí vzdělání vliv na nechtěné zformátování či na využití zálohování dat?
- Má pohlaví, věk, aprobace nebo velikost města odkud respondent pochází vliv na využití zálohování?
- Má pohlaví, věk, aprobace nebo velikost města původu respondenta vliv na nechtěné zformátování?
- Má předchozí vzdělání respondenta vliv na prodělání ztráty dat?
- Má předchozí vzdělání vliv na počet znaků v hesle používaném ke Stagu?
- Má předchozí vzdělání vliv na požité znaky v hesle od Stagu?
- Má předchozí vzdělání vliv na procentuální počet zálohovaných dat.
- Má zájem o informační technologie vliv na setkání se s malwarem či phishingem?
- Má zájem o informační technologie vliv na prodělání ztráty dat?
- Má pohlaví vliv na zájem o informační technologie?

Po stanovení těchto výzkumných otázek jsem si stanovil statistické hypotézy. Celkově jich bylo stanoveno 26. Za nulovou hypotézu, jsem považoval tvrzení, že mezi proměnnými není žádná závislost[21]. Alternativní hypotéza platí, pokud je mezi proměnnými závislost.

- $H1_0$: Neexistuje závislost mezi pohlavím a ztrátou dat.
- $H1_a$: Mezi pohlavím a ztrátou dat existuje závislost.
- $H2_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a ztrátou dat.
- $H2_a$: Mezi velikostí města, odkud student pochází, a ztrátou dat existuje závislost.
- $H3_0$ Neexistuje závislost mezi předchozím vzděláním a nechtěným formátováním.

- $H3_a$ Mezi předchozím vzděláním a nechtěným formátováním existuje závislost.
- $H4_0$: Neexistuje závislost mezi zaměřením předchozího studia a ztrátou dat.
- $H4_a$: Mezi zaměřením předchozího studia a ztrátou dat existuje závislost.
- $H5_0$: Neexistuje závislost mezi používáním antivirového systému a ztrátou dat.
- $H5_a$: Mezi používáním antivirového systému a ztrátou dat existuje závislost.
- $H6_0$: Neexistuje závislost mezi předchozím vzděláním a zálohovaním dat.
- $H6_a$: Mezi předchozím vzděláním a počtem zálohovaných dat existuje závislost.
- $H7_0$: Neexistuje závislost mezi ztrátou dat a zálohováním dat.
- $H7_a$: Mezi ztrátou dat a zálohováním dat existuje závislost.
- $H8_0$: Neexistuje závislost mezi pohlavím a zájmem o informační technologie.
- $H8_a$: Mezi pohlavím a zájmem o informační technologie existuje závislost.
- $H9_0$: Neexistuje závislost mezi pohlavím a setkáním se s phishingem.
- $H9_a$: Mezi pohlavím a setkáním se s phishingem existuje závislost.
- $H10_0$: Neexistuje závislost mezi pohlavím a setkáním se s malwarem.
- $H10_a$: Mezi pohlavím a setkáním se s malwarem existuje závislost.
- $H11_0$: Neexistuje závislost mezi pohlavím a zformátováním si vlastních dat.
- $H11_a$: Mezi pohlavím a zformátováním si vlastních dat existuje závislost.
- $H12_0$: Neexistuje závislost mezi pohlavím a délkou hesla.
- $H12_a$: Mezi pohlavím a délkou hesla existuje závislost.
- $H13_0$: Neexistuje závislost mezi pohlavím a složením hesla.
- $H13_a$: Mezi pohlavím a složením hesla existuje závislost.
- $H14_0$: Neexistuje závislost mezi složením hesla a velikostí města, odkud student pochází.
- $H14_a$: Mezi složením hesla a velikostí města, odkud student pochází, existuje závislost.
- $H15_0$: Neexistuje závislost mezi kategorií aprobace a ztrátou dat.
- $H15_a$: Mezi kategorií aprobace a ztrátou dat existuje závislost.
- $H16_0$: Neexistuje vztah mezi zájmem o informační technologie a ztrátou dat.
- $H16_a$: Mezi zájmem o informační technologie a ztrátou dat existuje závislost.
- $H17_0$: Neexistuje vztah mezi kategorií studia a použitím antivirového systému.
- $H17_a$: Mezi kategorií studia a použitím antivirového systému existuje závislost.
- $H18_0$: Neexistuje závislost mezi kategorií studia a počtem znaků hesla ve Stagu.
- $H18_a$: Mezi kategorií studia a počtem znaků hesla ve Stagu existuje závislost.
- $H19_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím antivirového systému.
- $H19_a$: Mezi velikostí města, odkud student pochází, a použitím antivirového systému existuje závislost.
- $H20_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím formátování.
- $H20_a$: Mezi velikostí města, odkud student pochází, a použitím formátování existuje závislost.
- $H21_0$: Neexistuje závislost mezi předchozím vzděláním a počtem znaků v hesle.
- $H21_a$: Mezi předchozím vzděláním a počtem znaků v hesle existuje závislost.
- $H22_0$: Neexistuje závislost mezi předchozím vzděláním a použitými znaky v hesle.

- $H22_a$: Mezi předchozím vzděláním a použitými znaky v hesle existuje závislost.
- $H23_0$: Neexistuje závislost mezi zájmem o informační technologie a setkáním se s malware.
- $H23_a$: Mezi zájmem o informační technologie a setkáním se s malware existuje závislost.
- $H24_0$: Neexistuje závislost mezi zájmem o informační technologie a setkáním se s phishingem.
- $H24_a$: Mezi zájmem o informační technologie a setkáním se s phishingem existuje závislost.
- $H25_0$: Neexistuje závislost mezi zájmem o IT a zálohováním dat.
- $H25_a$: Mezi zájmem o IT a zálohováním dat existuje závislost.
- $H26_0$: Neexistuje závislost mezi zájmem o IT a nechtěným smazáním dat.
- $H26_a$: Mezi zájmem o IT a nechtěným smazáním dat existuje závislost.

5.2 Sestavení dotazníku

Nejprve bylo třeba rozhodnout, zda bude distribuce dotazníku probíhat papírovou formou či elektronicky. Byla vybrána papírová forma, protože tento způsob byl, dle mého názoru, lépe kontrolovatelný a bylo možné lépe zajistit dosažení cílových skupin. Dotazník byl anonymní, obsahoval 14 otázek, z nichž některé měly i své podotázky. Dotazník obsahoval jak otevřené tak uzavřené otázky.

Otevřené otázky umožňují respondentům volnou tvorbu své odpovědi.[22] Se zpracováním je však více práce, protože se předpokládá, že většina odpovědí je originálních.

Ukázka otevřené otázky:

3. Napište zkratku aprobace, kterou na pedagogické fakultě studujete._____

Otázky uzavřené jsou nejpoužívanějším typem otázek vzhledem k dotazníkům. Jsou definované úplným výčtem odpovědí, ze kterých respondent může jednu, či více odpovědí (pokud to otázka dovoluje) zvolit. Respondent sice nemá volnost tvorby své vlastní odpovědi, ale podstatně se snižuje možnost chyby z nedorozumění, jelikož má na výběr pouze z několika předem vybraných odpovědí.

Ukázka uzavřené otázky:

4. Jak byste nejvýstižněji charakterizovali velikost města, odkud pocházíte?

a)Obec b) Městys c) Město (pod 30000 obyv.) d)Město (nad 30000 obyv.)

Uzavřené otázky se dále dělí na několik poddruhů, ze kterých byly v dotazníku použity otázky dichotomické, trichotomické a vícehodnotové otázky.

Dichotomické otázky umožňují respondentovi pouze dvě možnosti, jak odpovědět na danou otázku. Většinou se jedná o snadno zodpověditelné otázky s odpovědí typu (ano/ne) nebo (muž/žena).[21]

Ukázka dichotomické otázky:

1. Jaké je vaše pohlaví?

Muž Žena

Trichotomické otázky jsou rozšířením otázek dichotomických o odpověď typu (nevím/neznám). Tyto otázky se používají hlavně u otázek, kde můžeme u respondentů předpokládat neznalost dané problematiky.

Ukázka trichotomické otázky:

11. Setkali jste se s malwarem?

a) Ano, s malwarem jsem se setkal.b)Ne, nikdy jsem se s ním nesetkal.

c)Nevím, co je malware.

Vícehodnotové otázky umožňují respondentovi odpovědět více možnostmi. Odpovědi se většinou volí tak, aby byly co nejvíce výstižné a pomohly respondentům lépe pochopit a zodpovědět otázku. Je zde také možné označit za odpověď více než jednu z nabízených možností, pokud to zadání otázky umožňuje.

Ukázka vícehodnotové otázky:

5. Jaká byla vaše střední škola?

a) Gymnázium b) Střední odborná škola c) Speciální střední škola d) Odborné učiliště e) Jiná

Speciálním prvkem použitým v dotazníku je takzvané škálování, které slouží k vyjádření síly názorů či pocitů respondentů.

Ukázka škálové otázky:

6. Jak byste na stupnici od 1 do 10 (1 je nejméně) charakterizovali svůj zájem o informační technologie?

1 2 3 4 5 6 7 8 9 10

5.3 Respondenti

Skupinu mých respondentů tvořili pouze studenti pedagogické fakulty Jihočeské univerzity. Celkově bylo vybráno 203 použitelných dotazníků z celkově rozdaných 212 dotazníků. Vzhledem k pohlaví respondenty tvořilo 30 % mužů a 70 % žen. Aby bylo dosaženo co nejvyšší relevance sebraných dat, byli respondenti vybíráni podle svých studijních aprobací tak, aby byl zajištěn co nejširší sběr dat. Podle aprobace byli dále studenti rozděleni do tří skupin podle toho, jakého zaměření je jejich aprobace. Respondenti tedy mohli patřit do skupiny technické a enviromentální, humanitní, nebo smíšené.

5.4 Sběr dat a zpracování dat

Pro sběr dat byla zvolena metoda papírového dotazníku. Důvodem, proč byla zvolena tato metoda, je, aby bylo dosaženo jistoty, že respondent je opravdu

studentem pedagogické fakulty JU. Všechny dotazníky byly tedy rozdány ve škole před výukou nebo během výuky a ihned po vyplnění byly mnou nebo příslušným pedagogem sebrány.

Následně byla data z dotazníků přepsána do tabulkového procesoru, ze kterého byly jednoduše dostupné pro následné statistické zpracování. Každému dotazníku bylo přiděleno unikátní ID, aby bylo zaručeno, že nebude zpracován vícekrát a aby byl i přes to, že je dotazník anonymní, jednoduše dohledatelný.

5.5 Použité statistické metody

5.5.1 Test nezávislosti chí-kvadrát

Tento test se využívá k zjištění možné souvislosti mezi nominálně změřenými jevy. Pearsonův chí-kvadrát je nejpoužívanějším testem nezávislosti[23]. Aby bylo možné tuto metodu správně aplikovat, je nejprve nutné z dat získaných z dotazníků vytvořit kontingenční tabulku. Z kontingenční tabulky je zřejmé, jakou četnost má daná odpověď. Ověřujeme proti sobě nulovou a alternativní hypotézu. Používá se hladina významnosti 0,05. Stanovujeme také počet stupňů volnosti podle dané kontingenční tabulky. Porovnáváme výsledek testové statistiky X^2 s kritickou hodnotou, která je stanovena podle počtu stupňů volnosti a podle hladiny významnosti. Pokud je výsledek větší než kritická hodnota, přijímáme nulovou hypotézu.

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

Obrázek 4: Vzorec pro testovou statistiku

O_i = Zjištěné četnosti

E_i = Očekávané četnosti

5.5.2 Jednoduchá analýza rozptylu (ANOVA)

Anova umožňuje porovnat střední hodnoty nezávislých náhodných výběrů. Princip je takový, že se celý rozptyl dat rozloží na složky objasněné a složku neobjasněnou. Pomocí této metody analyzujeme metrická data. Důležitým předpokladem je, že každý z nezávislých výběrů má stejný rozptyl. Porovnáváme hladinu významnosti

stanovenou s hladinou významnosti vypočítanou. Pokud je vypočítaná hladina významnosti větší než stanovená, přijímáme nulovou hypotézu.

6 Zpracování a výsledky výzkumu

6.1 $H1_0$: Neexistuje závislost mezi pohlavím a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H1_0$: Neexistuje závislost mezi pohlavím a ztrátou dat.

$H1_a$: Mezi pohlavím a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0{,}05$. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Do dalších dvou skupin byli respondenti zařazeni podle toho, zda u nich došlo ke ztrátě dat či nedošlo . Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,06165**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti, ale výsledek je krajní. Můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.(Obr. 6)

Neexistuje závislost mezi pohlavím a ztrátou dat.

6.2 $H2_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H2_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a ztrátou dat.

$H2_a$: Mezi velikostí města, odkud student pochází, a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do čtyř skupin podle velikosti jejich města původu. Do dalších dvou skupin byli respondenti zařazeni podle toho, zda u nich došlo ke ztrátě dat či nedošlo. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,17010**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi velikostí města, odkud student pochází, a ztrátou dat.

6.3 $H3_0$ Neexistuje závislost mezi předchozím vzděláním a nechtěným zformátováním dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H3_0$ Neexistuje závislost mezi předchozím vzděláním a nechtěným formátováním.

$H3_a$ Mezi předchozím vzděláním a nechtěným formátováním existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do tří skupin podle toho, jaké mají zkušenosti se zformátováním. Do dalších dvou skupin byli respondenti zařazeni podle toho, jaké bylo jejich předchozí vzdělání. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,45603**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi předchozím vzděláním a nechtěným formátováním.

6.4 $H4_0$: Neexistuje závislost mezi zaměřením předchozího studia a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H4_0$: Neexistuje závislost mezi zaměřením předchozího studia a ztrátou dat.

$H4_a$: Mezi zaměřením předchozího studia a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Do dvou skupin byli respondenti zařazeni podle toho, jaké bylo jejich předchozí vzdělání. Do dalších dvou skupin byli respondenti zařazeni podle toho, zda u nich došlo ke ztrátě dat či nedošlo. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,20647**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi zaměřením předchozího studia a ztrátou dat.

6.5 $H5_0$: Neexistuje závislost mezi používáním antivirového systému a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H5_0$: Neexistuje závislost mezi používáním antivirového systému a ztrátou dat.

$H5_a$: Mezi používáním antivirového systému a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do dvou skupin podle toho, jestli používají antivirový systém. Do dalších dvou skupin byli respondenti zařazeni podle toho, zda u nich došlo ke ztrátě dat či nedošlo. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota

testovaného kritéria je **p = 0,10257**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi používáním antivirového systému a ztrátou dat.

6.6 $H6_0$: Neexistuje závislost mezi předchozím vzděláním a zálohováním dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H6_0$: Neexistuje závislost mezi předchozím vzděláním a zálohováním dat.

$H6_a$: Mezi předchozím vzděláním a zálohováním dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Do dvou skupin byli respondenti zařazeni podle toho, jaké bylo jejich předchozí vzdělání.(Obr. 8) Do dalších dvou skupin jsem následně rozdělil respondenty podle toho, zda využívají zálohování. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,00246**. Vypočtená hodnota je nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a můžeme přijmout hypotézu alternativní.(Obr. 7) Z výsledků je zřejmé, že studenti, kteří absolvovali gymnázium, využívají zálohování podstatně více.

Mezi předchozím vzděláním a zálohováním dat existuje závislost.

6.7 $H7_0$: Neexistuje závislost mezi ztrátou dat a zálohováním dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H7_0$: Neexistuje závislost mezi ztrátou dat a zálohováním dat.

$H7_a$: Mezi ztrátou dat a zálohováním dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Do dvou skupin jsem rozdělil respondenty podle toho, zda zálohují či nezálohují svá data. Do dalších dvou skupin byli respondenti zařazeni podle toho, zda u nich došlo ke ztrátě dat či nedošlo. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,13750**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi ztrátou dat a zálohováním dat.

6.8 $H8_0$: Neexistuje závislost mezi pohlavím a zájmem o informační technologie.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H8_0$: Neexistuje závislost mezi pohlavím a zájmem o informační technologie.

$H8_a$: Mezi pohlavím a zájmem o informační technologie existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem rozdělil respondenty do deseti skupin podle toho, jaký mají zájem o informační technologie. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,00048**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé, že zájem o informační technologie je u mužů hodně rovnoměrně rozprostřený. Zájem většiny žen je průměrný a je málo žen, které mají zájem velký nebo malý.(Obr.8)

Mezi pohlavím a zájmem o informační technologie existuje závislost.

6.9 $H9_0$: Neexistuje závislost mezi pohlavím a setkáním se s phishingem.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H9_0$: Neexistuje závislost mezi pohlavím a setkáním se s phishingem.

$H9_a$: Mezi pohlavím a setkáním se s phishingem existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem respondenty rozdělil do tří skupin podle jejich odpovědí na téma phishing. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,0050**. Vypočtená hodnota je nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé že poměrově mnohem více žen nerozumí pojmu phishing.(Obr. 9) Dále se dá vyčíst, že pokud porovnáme pouze respondenty, kteří pojmu phishing rozumí, tak jsou poměry napadení u obou pohlaví téměř stejné.

Mezi pohlavím a setkáním se s phishingem existuje závislost.

6.10 $H10_0$: Neexistuje závislost mezi pohlavím a setkáním se s malwarem.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H10_0$: Neexistuje závislost mezi pohlavím a setkáním se s malwarem.

$H10_a$: Mezi pohlavím a setkáním se s malwarem existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem respondenty rozdělil do tří skupin podle jejich odpovědí na téma malware. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika

pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,00483.** Vypočtená hodnota je nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé že mnohem více žen nerozumí pojmu malware.(Obr. 10) Pokud porovnáme pouze respondenty, kteří pojmu malware rozumí je zřejmé že poměr napadení je u obou pohlaví stejný.

Mezi pohlavím a setkáním se s malwarem existuje závislost.

6.11 $H11_0$: Neexistuje závislost mezi pohlavím a zformátováním si vlastních dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H11_0$: Neexistuje závislost mezi pohlavím a zformátováním si vlastních dat.

$H11_a$: Mezi pohlavím a zformátováním si vlastních dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem rozdělil respondenty do tří skupin podle jejich odpovědi na téma zformátování dat. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,70368**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi pohlavím a zformátováním si vlastních dat.

6.12 $H12_0$: Neexistuje závislost mezi pohlavím a délkou hesla.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H12_0$: Neexistuje závislost mezi pohlavím a délkou hesla.

$H12_a$: Mezi pohlavím a délkou hesla existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena α = 0,05. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem rozdělil respondenty do tří skupin podle jejich odpovědi na délku hesla. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,48119.** Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi pohlavím a délkou hesla.

6.13 $H13_0$: Neexistuje závislost mezi pohlavím a složením hesla.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H13_0$: Neexistuje závislost mezi pohlavím a složením hesla.

$H13_a$: Mezi pohlavím a složením hesla existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena α = 0,05. Respondenty jsem rozdělil podle pohlaví do dvou skupin na muže a ženy. Dále jsem rozdělil respondenty do tří skupin podle toho, jak odpovídali na otázku ohledně složení hesla. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,00002**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé, že ženy používají více silná hesla než muži.(Obr. 11)

Mezi pohlavím a složením hesla existuje závislost.

6.14 $H14_0$: Neexistuje závislost mezi složením hesla a velikostí města, odkud student pochází.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H14_0$: Neexistuje závislost mezi složením hesla a velikostí města, odkud student pochází.

$H14_a$: Mezi složením hesla a velikostí města, odkud student pochází, existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle složení hesla do tří skupin. Dále jsem rozdělil respondenty do čtyř skupin podle toho, z jak velkého města pocházejí. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,40945.** Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi složením hesla a velikostí města odkud student pochází.

6.15 $H15_0$: Neexistuje závislost mezi kategorií aprobace a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H15_0$: Neexistuje závislost mezi kategorií aprobace a ztrátou dat.

$H15_a$: Mezi kategorií aprobace a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle jejich aprobace do tří skupin podle zaměření jejich aprobace. Dále jsem rozdělil respondenty do dvou skupin podle toho, jestli u nich někdy došlo ke ztrátě dat. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,65897**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi kategorií aprobace a ztrátou dat.

6.16 $H16_0$: Neexistuje vztah mezi zájmem o informační technologie a ztrátou dat.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H16_0$: Neexistuje vztah mezi zájmem o informační technologie a ztrátou dat.

$H16_a$: Mezi zájmem o informační technologie a ztrátou dat existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do deseti skupin podle jejich zájmu o informační technologie. Dále jsem rozdělil respondenty do dvou skupin podle toho, zda u nich někdy došlo ke ztrátě dat. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,35839**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje vztah mezi zájmem o informační technologie a ztrátou dat.

6.17 $H17_0$: Neexistuje vztah mezi kategorií studia a použitím antivirového systému.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H17_0$: Neexistuje vztah mezi kategorií studia a použitím antivirového systému.

$H17_a$: Mezi kategorií studia a použitím antivirového systému existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle kategorie jejich studia do tří skupin. Dále jsem rozdělil respondenty do dvou skupin podle toho, jestli používají na svém PC antivirový systém. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval

v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,00212**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé, že studenti smíšených oborů používají mnohem méně antivirové systémy

Mezi kategorií studia a použitím antivirového systému existuje závislost.

6.18 $H18_0$: Neexistuje závislost mezi kategorií studia a počtem znaků hesla ve Stagu.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H18_0$: Neexistuje závislost mezi kategorií studia a počtem znaků hesla ve Stagu.

$H18_a$: Mezi kategorií studia a počtem znaků hesla ve Stagu existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle kategorie aprobace do tří skupin. Dále jsem rozdělil respondenty do tří skupin podle toho, jaký počet znaků má jejich heslo. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,32503.** Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a můžeme přijmout hypotézu nulovou.

Neexistuje závislost mezi kategorií aprobace a počtem znaků hesla ve Stagu.

6.19 $H19_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím antivirového systému.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H19_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím antivirového systému.

H19 $_a$: Mezi velikostí města, odkud student pochází, a použitím antivirového systému existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle velikosti města, ze kterého pochází, do čtyř skupin. Dále jsem rozdělil respondenty do dvou skupin podle toho, jestli užívají antivirový systém. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,17109**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím antivirového systému.

6.20 H20$_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a nechtěným formátování.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

H20$_0$: Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím formátování.

H20 $_a$: Mezi velikostí města, odkud student pochází, a použitím formátování existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$ Respondenty jsem rozdělil podle velikosti města, ze kterého pochází, do čtyř skupin. Dále jsem rozdělil respondenty do tří skupin podle toho, jaké mají zkušenosti se zformátováním. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,90202**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi velikostí města, odkud student pochází, a použitím formátování.

6.21 $H21_0$: Neexistuje závislost mezi předchozím vzděláním a počtem znaků v hesle.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H21_0$: Neexistuje závislost mezi předchozím vzděláním a počtem znaků v hesle.

$H21_a$: Mezi předchozím vzděláním a počtem znaků v hesle existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle typu jejich středoškolského vzdělání do dvou skupin. Dále jsem rozdělil respondenty do tří skupin podle toho, jaký počet znaků mají v hesle. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,53687**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi předchozím vzděláním a počtem znaků v hesle.

6.22 $H22_0$: Neexistuje závislost mezi předchozím vzděláním a použitými znaky v hesle.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H22_0$: Neexistuje závislost mezi předchozím vzděláním a použitými znaky v hesle.

$H22_a$: Mezi předchozím vzděláním a použitými znaky v hesle existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda jednoduchá analýza rozptylu. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty

jsem rozdělil podle typu jejich středoškolského vzdělání do dvou skupin. Dále jsem rozdělil respondenty do tří skupin podle toho, jaké znaky použili v hesle. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,012388**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé, že bývalí studenti gymnázií používají častěji silnější hesla než studenti středních odborných škol.

Mezi předchozím vzděláním a použitými znaky v hesle existuje závislost.

6.23 $H23_0$: Neexistuje závislost mezi zájmem o informační technologie a setkání se s malware.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H23_0$: Neexistuje závislost mezi zájmem o informační technologie a setkání se s malware.

$H23_a$: Mezi zájmem o informační technologie a setkání se s malware existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do deseti skupin podle jejich zájmu o informační technologie. Dále jsem rozdělil respondenty do tří skupin podle toho, jaké mají zkušenosti s malwarem. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p < 0,00001**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé, že většina lidí co nerozumí pojmu malware má podprůměrný zájem o informační technologie.

Mezi zájmem o informační technologie a setkání se s malware existuje závislost.

6.24 $H24_0$: Neexistuje závislost mezi zájmem o informační technologie a setkání se s phishingem.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H24_0$: Neexistuje závislost mezi zájmem o informační technologie a setkání se s phishingem.

$H24_a$: Mezi zájmem o informační technologie a setkání se s phishingem existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do tří skupin podle jejich zkušeností s phishingem. Dále jsem rozdělil respondenty do deseti skupin podle toho, jaký mají zájem o informační technologie. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **$p < 0,0001$**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a přijmout hypotézu alternativní. Z výsledků je zřejmé že většina respondentů, kteří se zajímají o informační technologie průměrně i přesto nerozumí pojmu phishing.

Mezi zájmem o informační technologie a setkání se s phishingem existuje závislost.

6.25 $H25_0$: Neexistuje závislost mezi zájmem o IT a zálohováním.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H25_0$: Neexistuje závislost mezi zájmem o IT a zálohováním.

$H25_a$: Mezi zájmem o IT a zálohováním existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil podle toho, zda využívají zálohování do dvou skupin. Dále jsem rozdělil respondenty do deseti skupin podle toho, jaký mají zájem o informační technologie. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval

v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,02016**. Vypočtená hodnota je tedy nižší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu nulovou a můžeme přijmout hypotézu alternativní. Z výsledků je zřejmé, že většina respondentů využívajících zálohování má nadprůměrný zájem o informační technologie.

Mezi zájmem o IT a zálohováním existuje závislost.

6.26 $H26_0$: Neexistuje závislost mezi zájmem o IT a nechtěným smazáním.

Byla stanovena nulová a alternativní hypotéza a provedeno statistické zpracování tak, aby bylo zjištěno, která ze dvou hypotéz je platná.

$H26_0$: Neexistuje závislost mezi zájmem o IT a nechtěným smazáním.

$H26_a$: Mezi zájmem o IT a nechtěným smazáním existuje závislost.

Pro ověření této hypotézy byla použita statistická metoda chí-kvadrát test. Hladina významnosti u této metody byla stanovena $\alpha = 0,05$. Respondenty jsem rozdělil do tří skupin podle toho, zda u nich někdy došlo ke zformátování dat. Dále jsem rozdělil respondenty do deseti skupin podle toho, jaký mají zájem o informační technologie. Na základě tohoto rozdělení jsem vytvořil kontingenční tabulku četností, kterou jsem zpracoval v softwaru statistika pomocí statistické metody. Vypočtená hodnota testovaného kritéria je **p = 0,36899**. Vypočtená hodnota je tedy větší než hodnota stanovené hladiny významnosti a proto můžeme odmítnout hypotézu alternativní a přijmout hypotézu nulovou.

Neexistuje závislost mezi zájmem o IT a nechtěným smazáním.

7 Diskuze

Z výsledků je zřejmé, že velice vlivným faktorem na chování respondentů je pohlaví. Ženy jsou celkově více náchylné ke ztrátě dat, což nejspíš souvisí i s dalším ověřeným faktem a to tím, že mají většinou průměrný zájem o informační technologie. Odpověď na otázku o zájmu o informační technologie byla často volena jako zájem průměrný, protože respondentky nevěděly co přesně na otázku odpovědět a tak zvolily střední cestu. Jejich zájem může být tedy ve skutečnosti ještě menší než průměrný. Dále je zřejmé, že většina žen i přes svůj průměrný zájem nerozumí pojmu malware a phishing. Obecně těmto pojmům nerozuměla velká část obou pohlaví, ženy však na tom byly prokazatelně hůře. Pokud porovnáme pouze respondenty, kteří pojmu malware a phishing rozumí, je zřejmé, že poměr napadení je u obou pohlaví stejný.

Na rozdíl od mužů však ženy volí silnější hesla, přestože délka hesla není významně odlišná. Použití silnějších kombinací znaků by se dalo přisoudit tomu, že ženy jsou obecně považovány za důslednější.

Věk jako ovlivňující faktor nakonec nebyl použit, protože většina respondentů byla ve stejné věkové kategorii a jejich věk se většinou lišil pouze o jednotky. Věkové rozmezí respondentů bylo primárně mezi 20 – 25 roky a pouze zlomek respondentů dosahoval většího stáří.

Nebyla zjištěna žádná závislost mezi městem původu a chováním respondentů v e-bezpečnosti. To bych přisuzoval tomu, že výuka na základních školách se v informatice nejspíš příliš neliší. Více informací pak nejspíš respondenti načerpají až na středních školách a na které je často nutné dojíždět do větších měst.

Z hlediska předchozího vzdělání se studenti gymnázií odlišovali ve dvou oblastech: 1.používají silnější hesla, 2.více využívají možnost zálohy dat. V ostatních parametrech se chování studentů gymnázia nijak nelišilo.

Velký vliv na náchylnost respondentů k ohrožení má jejich zájem o informační technologie. Celkově nejvíce respondentů mělo o informační technologie průměrný zájem. Je ale prokazatelné že lidé s podprůměrným zájmem mnohem méně rozumí dvěma největším hrozbám, kterými jsou malware a phishing. Zároveň tito respondnti

s menším zájmem o informační technologie prokazatelně méně zálohují svá data. Zajímavé však je, že nebyla prokázána závislost mezi zájmem o informační technologie a nechtěným zformátováním vlastních dat. Může to být způsobeno tím, že u většiny uživatelů k nechtěnému zformátování vůbec nedošlo. Dalším možným vysvětlením je že IT gramotnost není jediným faktorem, který ovlivňuje náhodné zformátování.

Zdánlivě překvapivé je zjištění, že neexistuje závislost mezi používáním antivirového systému a ztrátou dat. To je však pravděpodobně dáno skutečností, že prakticky všichni uživatelé mají antivirový systém. Podobně překvapivé je, že neexistuje závislost mezi ztrátou dat a zálohováním dat. To může znamenat, že data mnohých uživatelů nejsou příliš cenná. Pravděpodobnější vysvětlení je, že většina respondentů je příliš pohodlná měnit své zažité návyky. Přijetí nulové hypotézy 16 také ukazuje, že neexistuje vztah mezi zájmem o informační technologie a ztrátou dat. Zde se otvírá prostor pro působení osvěty v informatice a vedení k pravidelnému zálohování dat.

Kategorie aprobace nemá na chování vliv, pouze z hypotézy 17 bylo zjištěno, že studenti smíšených aprobací méně využívají antivirový systém. Není proto zjevný důvod a to by si mohlo vyžádat další výzkum. Dále bylo zjištěno, že neexistuje závislost mezi kategorií aprobace a počtem znaků hesla ve Stagu. Tento jev by se dal přisoudit tomu, že si možná většina studentů nechává své původně přidělené heslo.

8 Závěr

Ženy jsou celkově více náchylné ke ztrátě dat, což nejspíš souvisí s jejich menším zájmem o IT problematiku. Dále méně rozumí pojmům malware a phishing. Na rozdíl od mužů však ženy volí silnější hesla, přestože délka hesla není významně odlišná.

Nebyla zjištěna žádná závislost mezi městem původu a chováním respondentů v e-bezpečnosti. Rovněž obor studia většinou neprokázal žádné průkazné vlivy na sledované parametry IT gramotnosti.

Z hlediska předchozího vzdělání se studenti gymnázií odlišovali ve dvou oblastech: 1.používají silnější hesla, 2.více využívají možnost zálohy dat.

Velký vliv na náchylnost respondentů k ohrožení má jejich zájem o informační technologie. Celkově nejvíce respondentů mělo o informační technologie průměrný zájem. Je ale prokazatelné že lidé s podprůměrným zájmem mnohem méně rozumí dvěma největším hrozbám, kterými jsou malware a phishing.

Práce naznačila oblasti, kam stojí za to soustředit úsilí při zlepšování IT gramotnosti studentů. Je třeba zvýšit povědomí o hrozbách typu malware nebo phishing a zejména o způsobech prevence a ochrany před nimi. Uživatele je třeba vést k tomu, aby si uvědomili, že zálohování dat musí ve vlastním zájmu zařadit mezi základní operaci při práci s počítačem

9 Seznam citací

[1] Cyber crime costs global economy $445 billion a year: report | Reuters. Business & Financial News, U.S & International Breaking News | Reuters [online]. Copyright © [cit. 12.07.2017]. Dostupné z: http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

[2] SIKORSKI, Michael. a Andrew. HONIG. *Practical malware analysis: the hands-on guide to dissecting malicious software*. San Francisco: No Starch Press, c2012. ISBN 978-1-59327-290-6.

[3] HOFFMAN, Lance J. Rogue programs: viruses, worms, and Trojan horses. New York: Van Nostrand Reinhold, c1990. ISBN 978-0442004545.

[4] What is malware and why should i be concerned? | McAfee Blogs. Securing Tomorrow. Today. | McAfee Blogs [online]. Copyright © 2017 McAfee LLC [cit. 12.07.2017]. Dostupné z: https://securingtomorrow.mcafee.com/consumer/family-safety/malware/

[5] Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code. Indianapolis: Wiley, c2011. ISBN 978-0-470-61303-0.

[6] Type of Computer Viruses (Names and Definitions) - pctechguide.com. Pctechguide.com - We Share What We Learn [online]. Dostupné z: https://www.pctechguide.com/virus-removal/popular-computer-virus-types-and-their-effects

[7] What is a Trojan Horse? Is it Malware or a Virus?. [online]. Copyright © 2017 AVG Technologies. All rights reserved. [cit. 12.07.2017]. Dostupné z: https://www.avg.com/en/signal/what-is-a-trojan

[8] The Difference Between a Virus, Worm and Trojan Horse - Webopedia. Webopedia: Online Tech Dictionary for IT Professionals [online]. Dostupné z: http://www.webopedia.com/DidYouKnow/Internet/virus.asp

[9] Trojan.Zbot | Symantec. Symantec - Global Leader In Next-Generation Cyber Security [online]. Copyright ©1995 [cit. 12.07.2017]. Dostupné z: https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

[10] Computer Worm Information and Removal Steps | Veracode. Application Security | Veracode [online]. Copyright © 2017 VERACODE, All Rights Reserved [cit. 12.07.2017]. Dostupné z: https://www.veracode.com/security/computer-worm

[11] ELISAN, Christopher C. Malware, rootkits & botnets: a beginner's guide. New York.: McGraw-Hill, c2013. ISBN 978-0071792066.

[12] Ransomware-5 Dos And Donts. NORTON™ - Antivirus Software and Spyware Removal [online]. Copyright ©1995 [cit. 12.07.2017]. Dostupné z: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[13] Co je to adware a jak jej odstranit. Jak odstranit počítačové viry - odstranitvirus.cz [online]. Copyright © [cit. 12.07.2017]. Dostupné z: https://odstranitvirus.cz/adware/

[14] The Radicati Group, Inc. [online]. Copyright ©rj [cit. 12.07.2017]. Dostupné z: http://www.radicati.com/wp/wp-content/uploads/2010/04/Email-Statistics-Report-2010-2014-Executive-Summary2.pdf

[15] What is... Punycode Phishing? Part 1. FraudWatch International Blog [online]. Copyright © Copyright [cit. 12.07.2017].

Dostupné z: https://blog.fraudwatchinternational.com/expert-explanations/what-is-punycode-phishing-part-1

[16] Firewally | Antivirové Centrum. ESET, Kaspersky, Avira, AVG, Avast antivirus včetně verzí ke stažení zdarma | Antivirové Centrum [online]. Copyright © 1998 [cit. 12.07.2017]. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[17] DAVIS, Michael, Sean. BODMER a Aaron. LEMASTERS. Hacking exposed malware & rootkits: malware & rootkits security secrets & solutions. New York: McGraw Hill, c2010. ISBN 978-0071591188.

[18] What is Anti-Virus Software?. [online]. Copyright © Copyright 2004 [cit. 12.07.2017]. Dostupné z: https://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software

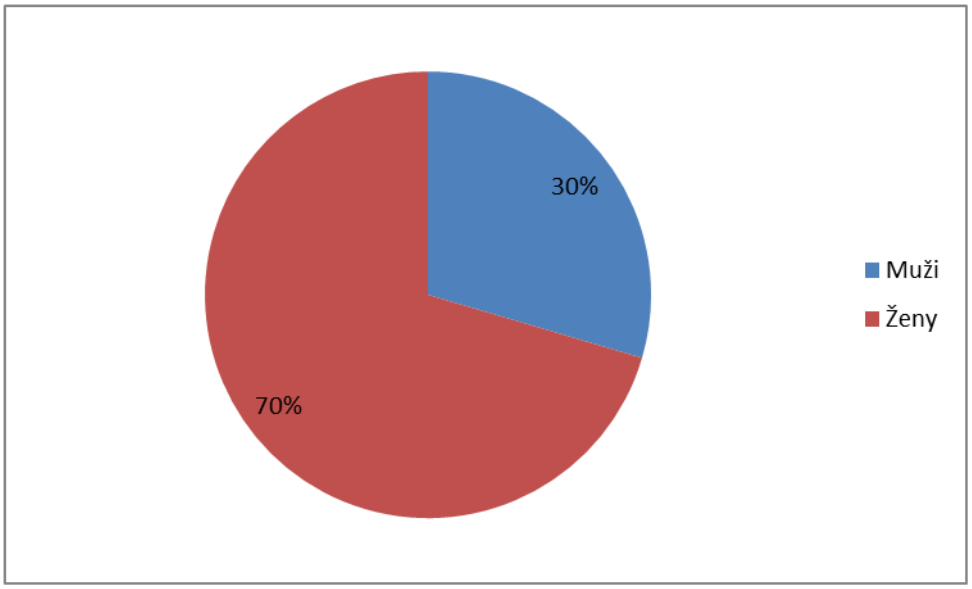
[19] How to Create a Strong Password (and Remember It) . How-To Geek - For Geeks, By Geeks. [online]. Copyright © 2006 [cit. 12.07.2017]. Dostupné z: https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

[20] V. [online]. Dostupné z: http://www.kge.zcu.cz/pesonal/PERSON/svoboda/vyuka/typy_otazek.htm

10 Seznam obrázků

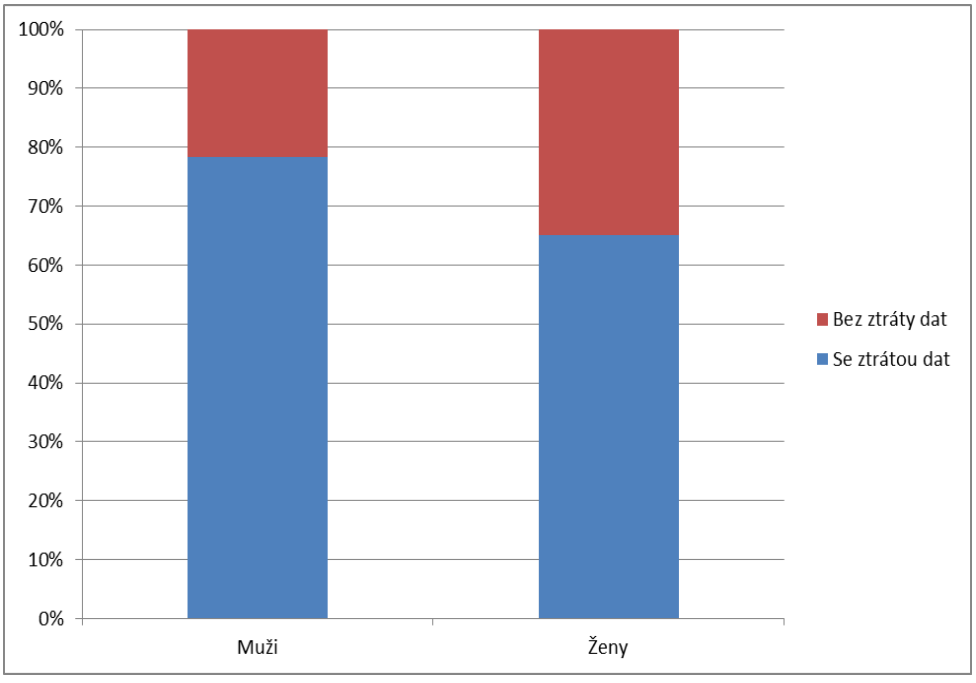
11 Přílohy

Pohlaví respondentů:



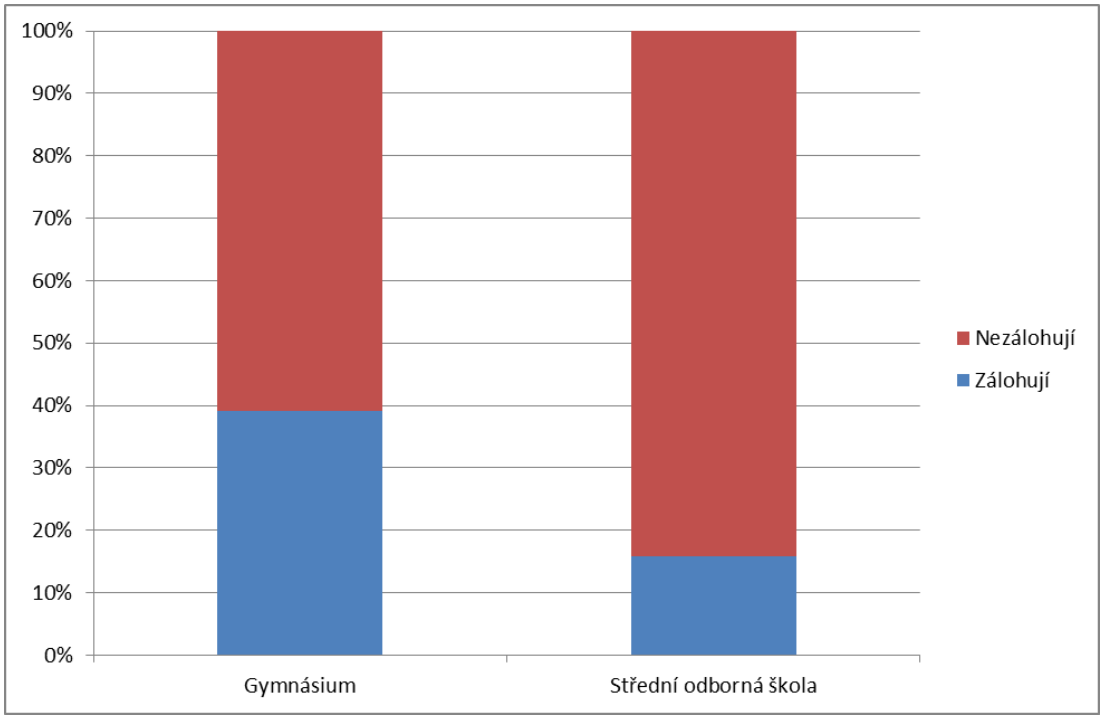
Obrázek 5: Pohlaví respondentů

$H1_0$:

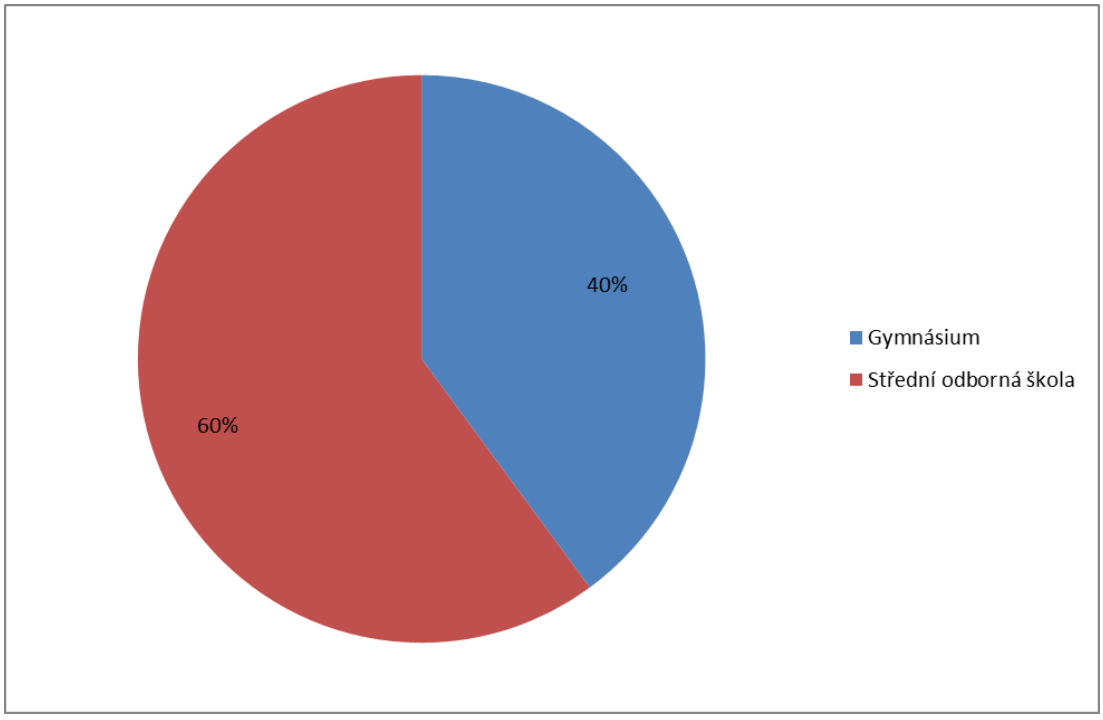


Obrázek 6: Porovnání ztráty dat z hlediska pohlaví

$H5_0$:

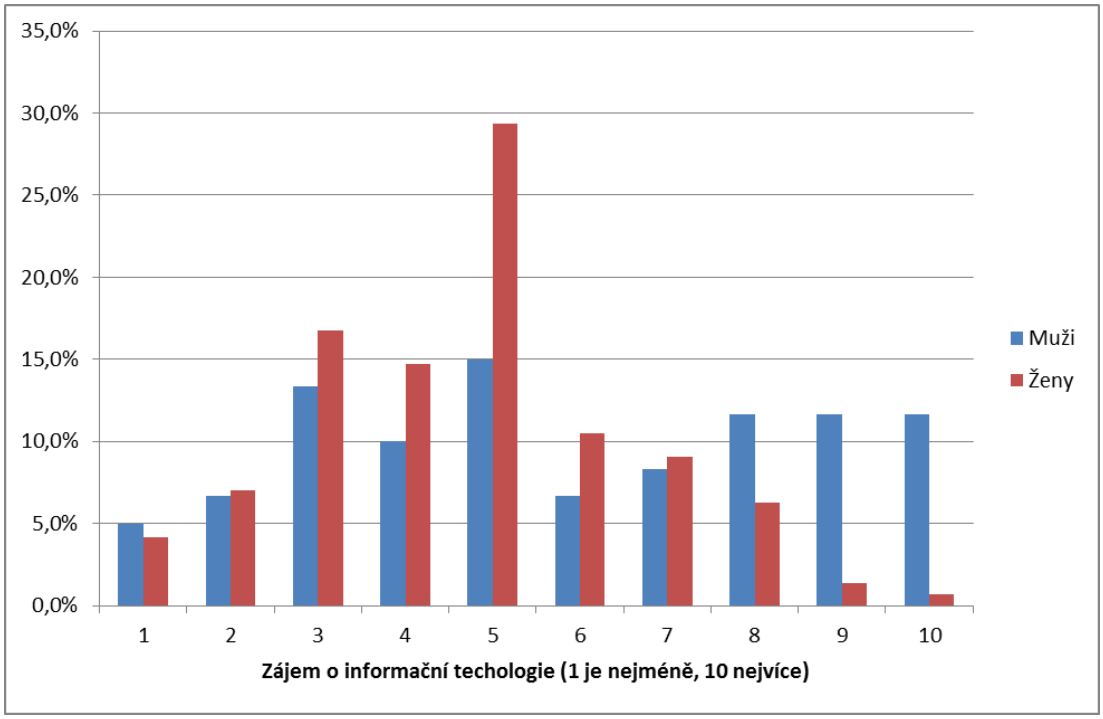


Obrázek 7: Zálohování vzhledem k předchozímu vzdělání



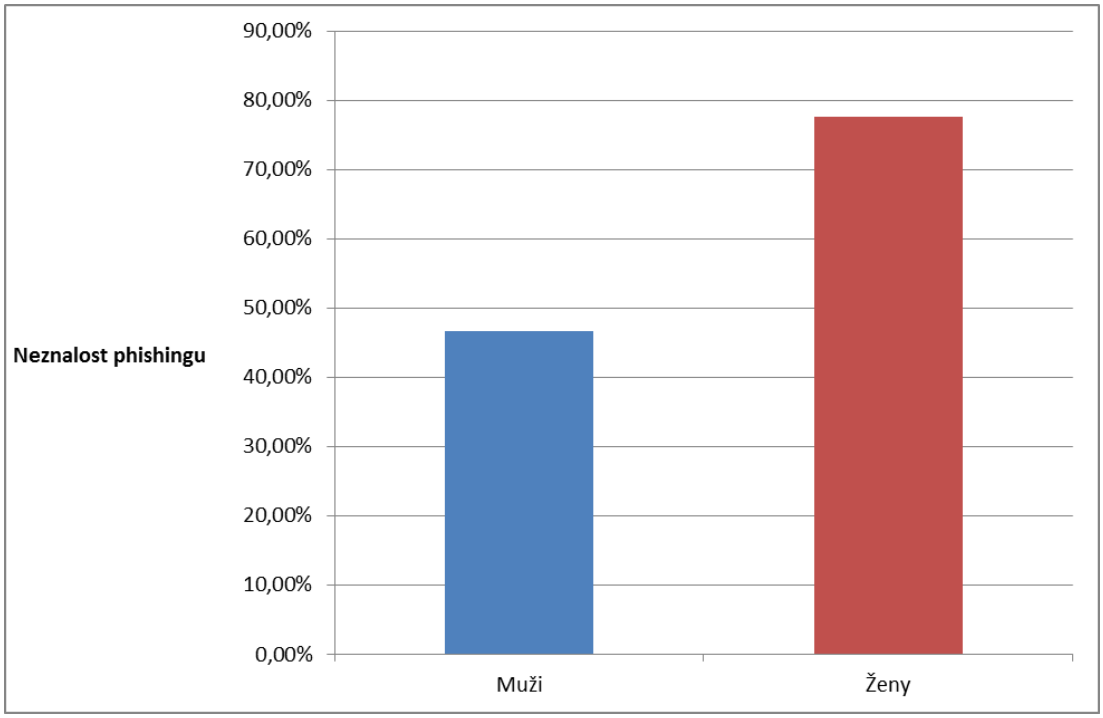
Obrázek 8: Respondenti podle předchozího vdělání

H8:



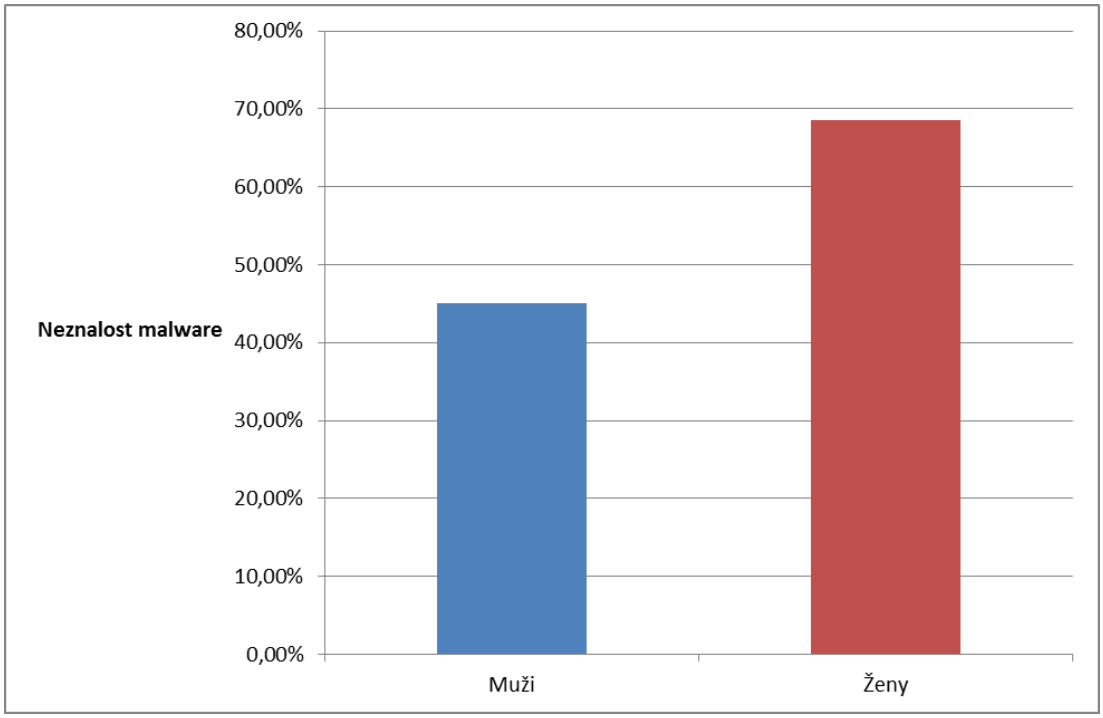
Obrázek 9:Vztah mezi pohlavím a zájmem o informační technologie

H9:



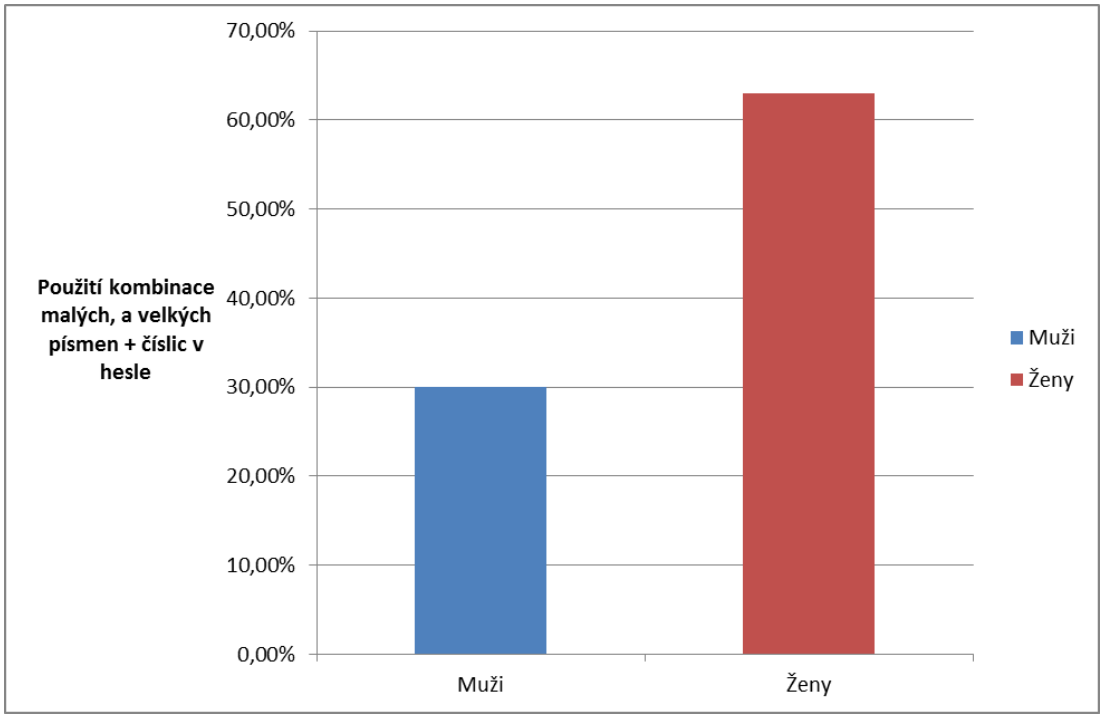
Obrázek 10: Porovnání neznalosti phishingu u žen a mužů

H_{10}:



Obrázek 11: Porovnání neznalosti malware u žen a mužů

H13:



Obrázek 12: Porovnání síly hesla u žen a můžů

Dotazník:

Faktory ovlivňující chování studentů učitelství v e-bezpečnosti

Dotazník by měl prozkoumat, jaké faktory jsou relevantní z hlediska hrozeb úniků dat. Dotazník je anonymní a je klíčové aby ho každý vyplňoval sám bez pomoci ostatních. Může se stát, že některé pojmy nebudete znát, proto zvolte příslušnou odpověď. Pokud má otázka nějaké podotázky a vy jste už v otázce vyplnil, že jste se s daným pojmem nesetkal tak podotázky přeskočte. Správné odpovědi zakroužkujte, popřípadě vypište.

1. Jaké je vaše pohlaví?

Muž Žena

2. Kolik let vám je?

3. Napište zkratku aprobace, kterou na pedagogické fakultě studujete.

4. Jak byste nejvýstižněji charakterizovali velikost města, odkud pocházíte?

a) Obec b) Městys c) Město (pod 30 000 obyv.) d) Město (nad 30 000 obyv.)

5. Jaká byla vaše střední škola?

a) Gymnázium b) Střední odborná škola c) Speciální střední škola d) Odborné učiliště

e) Jiná

6. Jak byste na stupnici od 1 do 10 (1 je nejméně) charakterizovali svůj zájem o informační technologie?

1 2 3 4 5 6 7 8 9 10

7.1. Stalo se vám někdy, že jste přišli o svá elektronická data? Jako ztráta dat se počítá cokoliv od nechtěného vymazání flash disku až po krádež dat formou hackerského útoku.

a) Ano b) Ne

7.2. Kolikrát u vás ke ztrátě dat došlo?

a) 1-2 b) 3-5 c) 5-10 d) více jak 10x

7.3 Jak byste charakterizovali závažnost ztráty na stupnici od 1 do 10 (10 je nejzávažnější).

1 2 3 4 5 6 7 8 9 10

8. Používáte ve vašem PC antivirový systém?

a) Ano b) Ne

9. Využíváte možnosti zálohování svých dat?

a) Ano b) Ne

9.1. Na stupnici od 10 do 100 zaznamenejte kolik % dat, která jste vytvářel, zálohujete.

10 20 30 40 50 60 70 80 90 100

10. Setkali jste se někdy phishingem?

a) Ano, byl na mě proveden phishingový útok. b) Ano, ale phishingový útok na mě proveden nebyl.

c) Nevím, co je phishing.

10.1. Měl phishing za následek únik nějakých dat nebo narušení soukromí vašeho účtu?

a) Ano, přišel jsem o svá data nebo mi byl narušen účet.b) Ne, o nic jsem nepřišel.

10.2. Na stupnici od 1 do 10 zaznamenejte závažnost napadení phisingem (10 je nejvyšší závažnost).

1 2 3 4 5 6 7 8 9 10

11. Setkali jste se s malwarem?

a) Ano, s malwarem jsem se setkal. b) Ne, nikdy jsem se s ním nesetkal.

c) Nevím co je malware.

13) Přišli jste někdy o data nechtěným smazáním nebo zformátováním paměťového média?

a) Ano, ale data jsem obnovil. b) Ano, data jsem už neobnovil. c) Ne, o data jsem nepřišel.

14) Jaký počet znaků vaše heslo od STAGu má?

a) 0 - 4 b) 5 - 10 c) více jak 10

14.1. Z jakých znaků je heslo složeno?

a) Používám jen písmena nebo jen číslice b)Používám číslice i písmena

c) Používám kombinaci malých a velkých písmen a číslic

14.2. Z jakých znaků je vaše heslo složeno?

1 2 3 4 5 6 7 8 9 10