Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Používajú ľudia bezpečné heslá?

Predmet:	2-INF-106/00 Informatika a spoločnosť
Autor:	Jaroslava KOKAVCOVÁ, Dominika SZABOVÁ
Študijný program:	mINF
Semester:	Leto
Dátum:	Máj 2021

Abstrakt

Posledné roky narastá počet hacknutí, úniku citlivých dát a ich následné zneužitie v rôznej podobe. V ohrození už nie sú len veľké firmy, krajiny ale už aj obyčajní ľudia. Aj napriek mediálnym správam a rôznym spôsobom osvety, používajú ľudia dostatočne bezpečné heslá na ochranu svojho súkromia? Vďaka vyše 250 odpovediam sme zistili, že spoločnosť pozná zastarané spôsoby a nutnosť aktualizovať u nich tieto znalosti je viac než potrebná.

Poďakovanie

Chceme sa poďakovať všetkým respondentom dotazníka, ktorí prispeli k tejto práci svojimi odpoveďami. Rovnako veľká vďaka aj ČSOB Banke a.s., ktorá poskytla tento dotaník v rámci interného obehu a nielen nám prispela veľkým množstvom odpovedí ale rovnako to bolo užitočné aj pre samotnú spoločnosť. Ďakujeme odborníkom a kritikom, ktorí prispeli k vylepšeniu tohto dotazníka: Mgr. Ladislav Bačo, Mgr. Roman Števaňák a Mgr. Martin Daňko, PhD.
Veríme, že po vyplnení dotazníka sa väčšina respondentov zamyslela a budú si svoje dáta aj svoje súkromie lepšie chrániť.

Obsah

1 Úvod

V dnešnej dobe všetci používame rôzne aplikácie a systémy, ktoré nám uľahčujú život. Rôzny používatelia majú záujem o rôzny obsah, potrebujú rôzne práva na vykonávanie svojich činností a pod. Preto je dôležité používateľa autentifikovať a podľa toho mu zobraziť obsah.
Najčastejší spôsob autentifikácie je pomocou hesla. Je potrebné zabezpečiť bezpečný spôsob autentifikácie, aby sa nepovolený človek nemohol identifikovať ako niekto iný a preniknúť do systému. Časť tohto problému rieši samotný systém tým, ako je urobený. No zostáva tu faktor, ktorý vývojári ani správcovia systému nemajú vo svojej rukách – používatelia. Na dosiahnutie požadovanej úrovne bezpečnosti je potrebné, aby používatelia dodržiavali isté pravidlá a chránili si svoje heslá. V našej práci sme sa pozreli na to, ako bežní používatelia pristupujú k problematike hesiel. Zároveň sme im poskytli rady, ako by si mohli svoje heslá lepšie chrániť.

2 Priebeh výskumu

Hlavným pilierom nášho výskumu bol anonymný a dobrovoľný dotazník, ktorý bol verejne dostupný na webe. Dotazník bol zostavený z dvadsiatich otázok, ktoré boli kontrolované odborníkmi v danej oblasti a tiež jeho obsah bol právne konzultovaný. Dotazník bol dostupný na vyplnenie v období 29.03.2021 do 16.05.2021. Propagovanie dotazníka bolo cez sociálne siete, krúžky alebo osobné kruhy priateľov, v dvoch vlnách. Dokopy sme získali 121 odpovedí, všetky boli validne vyplnené.
Pri priebežných kontrolných stretnutiach sme objavili tendenciu nárastu odpovedí od vekovej skupiny 20-25 rokov. Vďaka Československej obchodnej banke a.s., ktorá daný dotazník zverejnila v rámci interného obehu, sa nám podarilo získať odpovede od vekovej skupiny 25-60 rokov. Dotazník podliehal úpravám pre zachovanie dôverných informácií spoločnosti, pričom každá zmena bola konzultovaná s autorkami dotazníka. Odobraté boli tieto otázky:

- Máš dve heslá, ktoré pravidelne striedaš?
- Uveď príklad tvojho hesla.
- Čo obsahuje tvoje heslo?
- Aké dlhé je tvoje heslo?
- Čo obsahuje tvoj PIN kód (akýkoľvek–mobil, NTB, SIM karta, bankomatová karta...)

Dotazník bol v obehu od 06.05.2021 a výsledky boli stiahnuté 17.05.2021. Získali sme 136 odpovedí, všetky validne vyplnené.

Vo výsledných dátach nie sú žiadne osobné údaje okrem tých, s ktorými respondenti súhlasili na začiatku jeho vyplňovania. Každá osoba, ktorá dotazník vyplnila, bola na záver oboznámená, že jej odpovede nebudú zneužité. V prípade, že respondent má podozrenie, že prezradila svoje heslo, bola upozornený, aby si heslo ihneď zmenil. V záverečnom poďakovaní sme zverejnili video, ktoré bolo stručným návodom na tvorbu nového a dostatočne silného hesla.

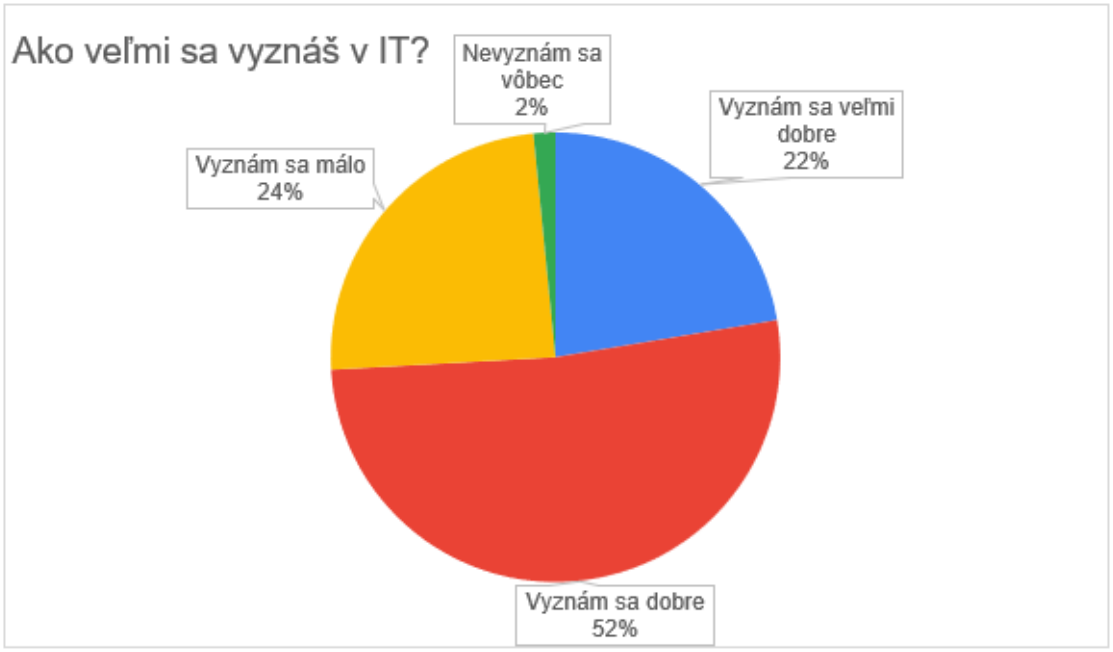
Otázky v prvej sekcií dotazníka boli povinné, ktoré sa zameriavali na vek, dosiahnuté vzdelanie respondenta, jeho vzdelanosť v informačných technológiách a skúsenosť so školením v informatickej bezpečnosti. Výsledky sú vizualizované v grafoch 1, 2, 3, 4.

V otázke vzdelanosti sme očakávali prevahu kategórie *Vysokoškolské II. stupňa* keďže je to časté najvyššie dosiahnuté vzdelanie. Napriek tomu, že skoro polovica respondentov tak odpovedala, potešilo nás, že záujem o vyplnenie dotazníka prišlo zo všetkých kategórií vzdelania.

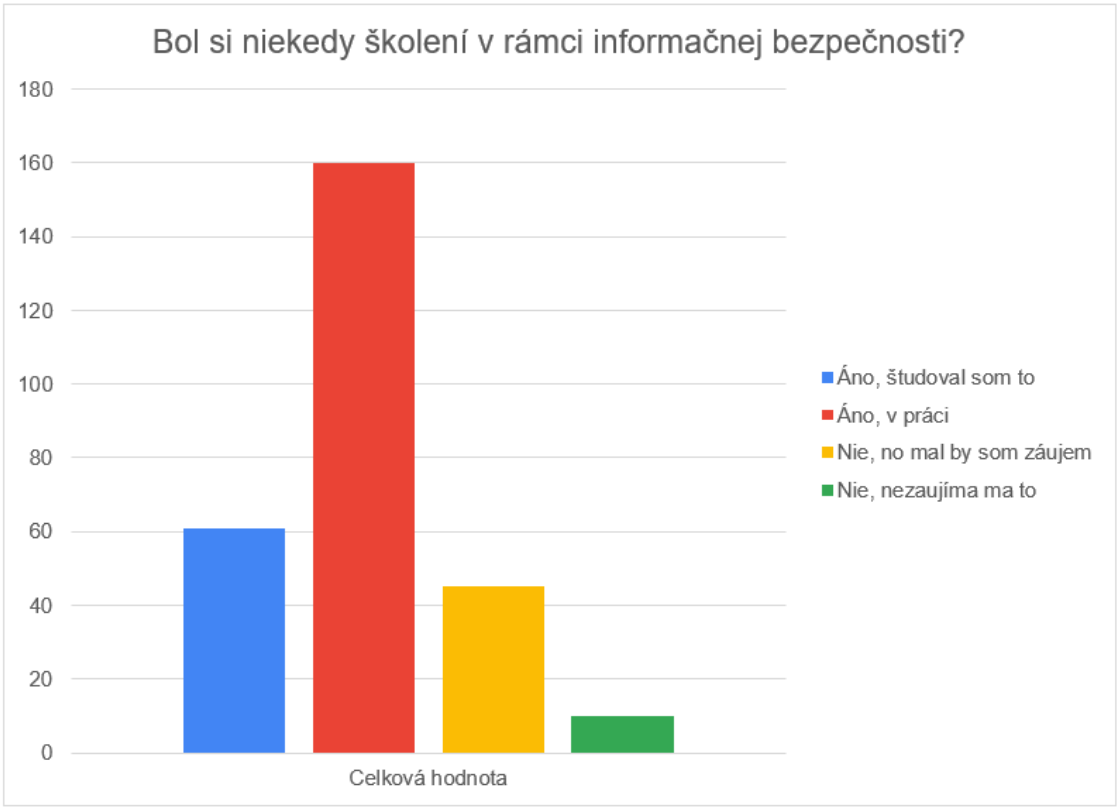
Obr. 1

Obr. 2

Vo vekovej kategórií sme získali najviac odpovedí od 26-35 ročných. Od tých je očakávané, že sa o informačné technológie budú zaujímať viac než staršia veková kategória a zároveň rozumejú viac

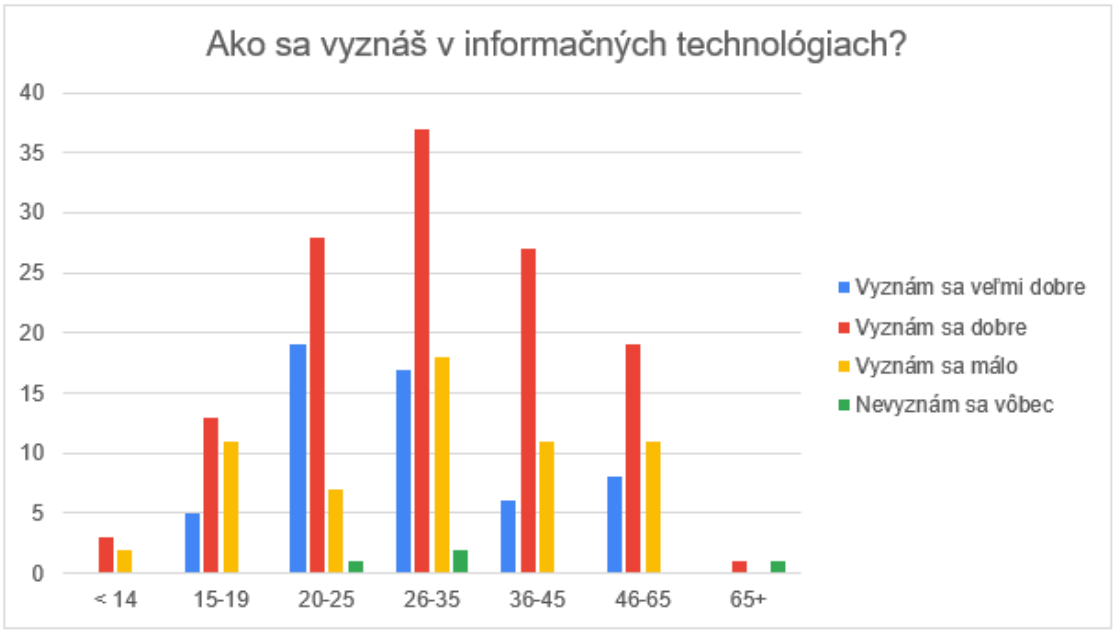

Ako veľmi sa vyznáš v IT?
Nevyznám sa vôbec 2%
Vyznám sa veľmi dobre 22%
Vyznám sa málo 24%
Vyznám sa dobre 52%

Obr. 3


Bol si niekedy školení v rámci informačnej bezpečnosti?
180
160
140
120
100
80
60
40
20
0
Celková hodnota
Áno, študoval som to
Áno, v práci
Nie, no mal by som záujem
Nie, nezaujíma ma to

Obr. 4

informatickej bezpečnosti než mladšie ročníky, ktoré ešte nemali možnosť s danou témou prísť do kontaktu. Výsledky v grafe 5 naznačujú túto domnienku.



Obr. 5: Porovnanie výsledkov pre otázku "Ako sa vyznáš v informačných technológiách?"v rámci vekových kategórií.

Našim cieľom bolo získať odpovede od skupiny ľudí, ktorá nie nutne študuje alebo vyštudovala informatické zameranie[1]. Zaujímavým výsledkom v grafe 3 je skoro rovnaký pomer ľudí, ktorí sa vyznajú málo, s tými čo sa vyznajú veľmi dobre. Preto očakávame rozmanitosť odpovedí v ďalšej sekcii.
Poslednou otázkou prvej sekcie bol prieskum vzdelanosti respondentov v informatickej bezpečnosti. Kvôli odpovediam z ČSOB, ktorá má vo svojej firemnej politike pravidelne školenie svojich zamestnancov o informatickej bezpečnosti, nám prevyšuje školenie v zamestnaní (graf 4). Vzorka respondentov prejavila záujem o takéto školenie aj vzhľadom na ich nedostatočnú vzdelanosť v tejto oblasti. Toto je určite dobrým signálom pre podporu šírenia vedomostí o bezpečnosti na internete, ochrane hesiel a potenciálnych rizikách pri nedostatočnej ochrane.
Celý dotazník si možno pozrieť v Appendix.

3 Výsledky

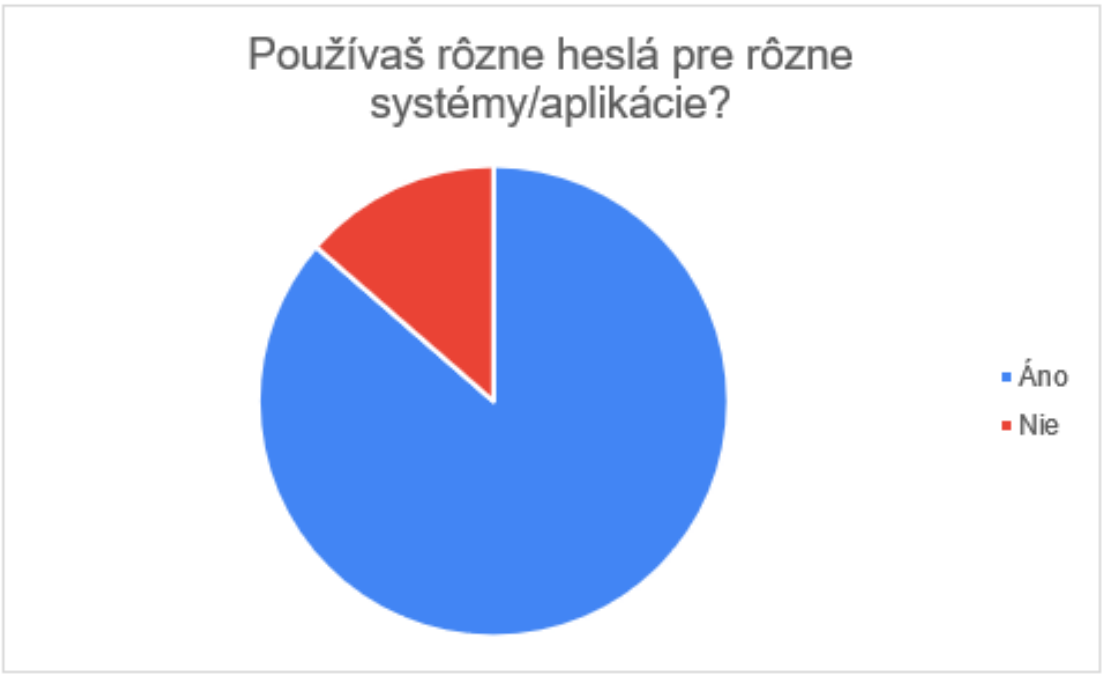
V tejto časti sa pozrieme na výsledky z nášho dotazníka.

3.1 Bezpečnostné návyky

Prvá otázka bola, či si respondent myslí, že používa dostatočne dobré heslá. Celkovo na otázku odpovedalo 254 ľudí, pričom 94 z nich si myslí, že má silné heslo, 138 má skôr silné, 21 má skôr slabé heslo a jeden človek sa priznal, že používa slabé heslo. Výsledky môžeme vidieť na grafe 6.
Ďalej sme sa pýtali, či ľudia používajú rôzne heslá pre rôzne systémy. Na otázku odpovedalo 257 ľudí, z toho 222 tvrdí, že používa rôzne heslá a 35 nie. Výsledky môžeme vidieť na grafe 7.

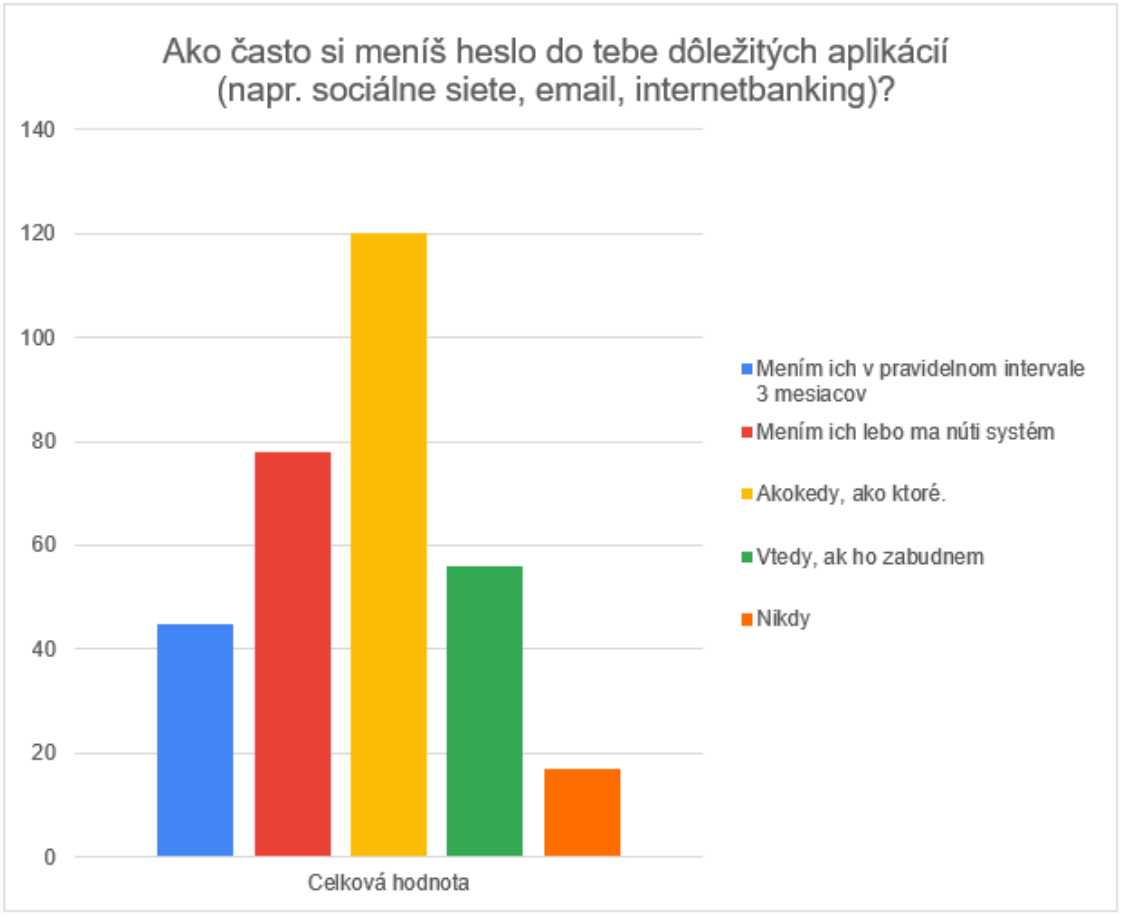
[1] čo sa nie vždy podarí, ak vaši spolužiaci a kamaráti sú informatici

Obr. 6: Graf znázorňuje, ako ľudia ohodnotili svoje heslo



Obr. 7: Používanie rôznych hesiel pre rôzne systémy/aplikácie

Taktiež nás zaujímalo, či si ľudia menia svoje heslá a ako často. Otázka umožňovala výber viacerých odpovedí. Na otázku odpovedalo 256 ľudí, pričom 45 respondentov si mení heslo pravidelne, 78 si mení heslo, pretože ich núti systém, 120 ľudí ako kedy, ako ktoré, 56 odpovedajúcich si mení heslo vtedy, keď ho zabudne, a 17 si nikdy nemenilo heslo. Výsledky môžeme vidieť na grafe 8.

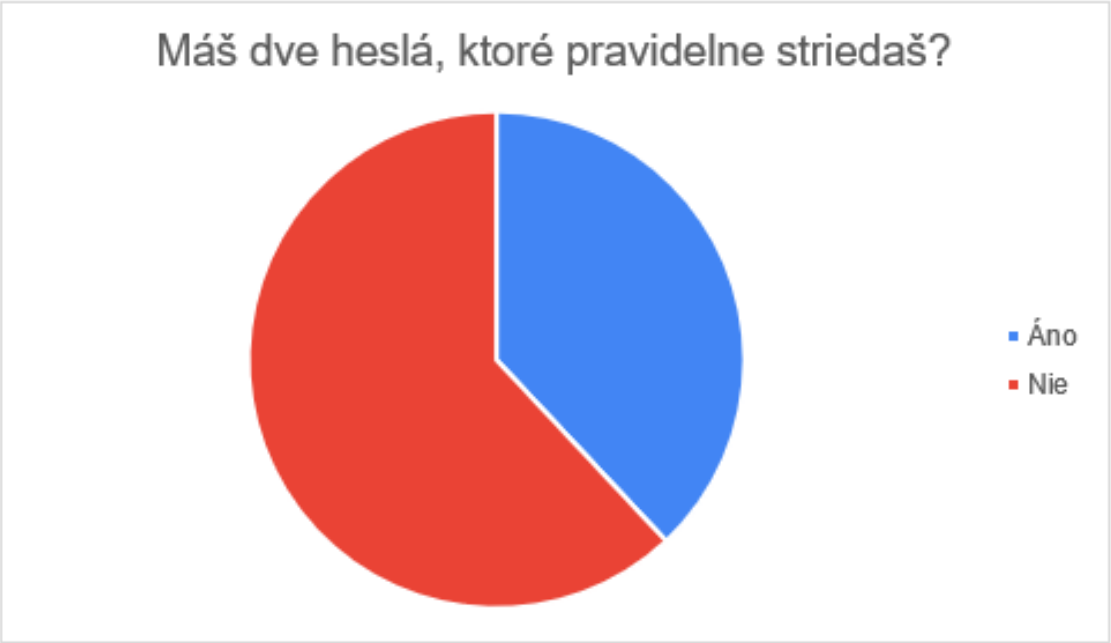


Obr. 8

Zmena hesla je dôležitá, pretože mohlo sa stať, že heslo bolo prelomené bez vedomosti používateľa a zmenou hesla znemožníme útočníkovi prístup do systému. Na druhú stranu, vyžadovať príliš často zmenu hesla môže viesť k tomu, že si používatelia budú voliť jednoduché heslá, prípadne budú striedavo používať dve heslá. Toto správanie sme skúmali aj u respondentov. Na otázku odpovedalo 121 ľudí, pričom 46 sa priznalo, že strieda dve heslá, a 75 nestrieda. Výsledky môžeme vidieť na grafe 9.

3.2 Heslá respondentov

Pokúsili sme sa zistiť, či nám respondenti prezradia svoje heslo, keď sa ich na to opýtame. Hoci otázka bola nepovinná, rovnako ako všetky ostatné otázky, odpovedalo nám 60 ľudí. Po vyškrtnutí odpovedí typu "nechcem povedať"nám zostalo 50 hesiel. V niektorých prípadoch si myslíme, že uvedená odpoveď nie je priamo heslo, len opisuje tvar hesla, no v niektorých prípadoch si myslíme, že naozaj ide o heslo daného respondenta. Uvedené heslá sme hľadali v databáze uniknutých hesiel[4] a 5 z nich sme tam našli.
Okrem samotného hesla sme sa pýtali respondentov, čo obsahuje ich heslo. Na otázku odpovedalo 97 ľudí. Otázka mala predpripravené možnosti alebo mohli respondenti uviesť vlastné odpovede. Z pôvodných odpovedí 35 ľudí zvolilo možnosť, že používajú ako heslo náhodné slová v rodnom jazyku, 22 používa náhodné slová v cudzom jazyku, 18 použije svoj login, 13 ľudí má v hesle svoje meno, 12 má meno známeho, 11 má svoj dátum narodenia, rovnako 11 používa iný významný dátum, 10 ľudí používa dátum narodenia blízkej osoby, 7 má v hesle meno svojho zvieratka, 6



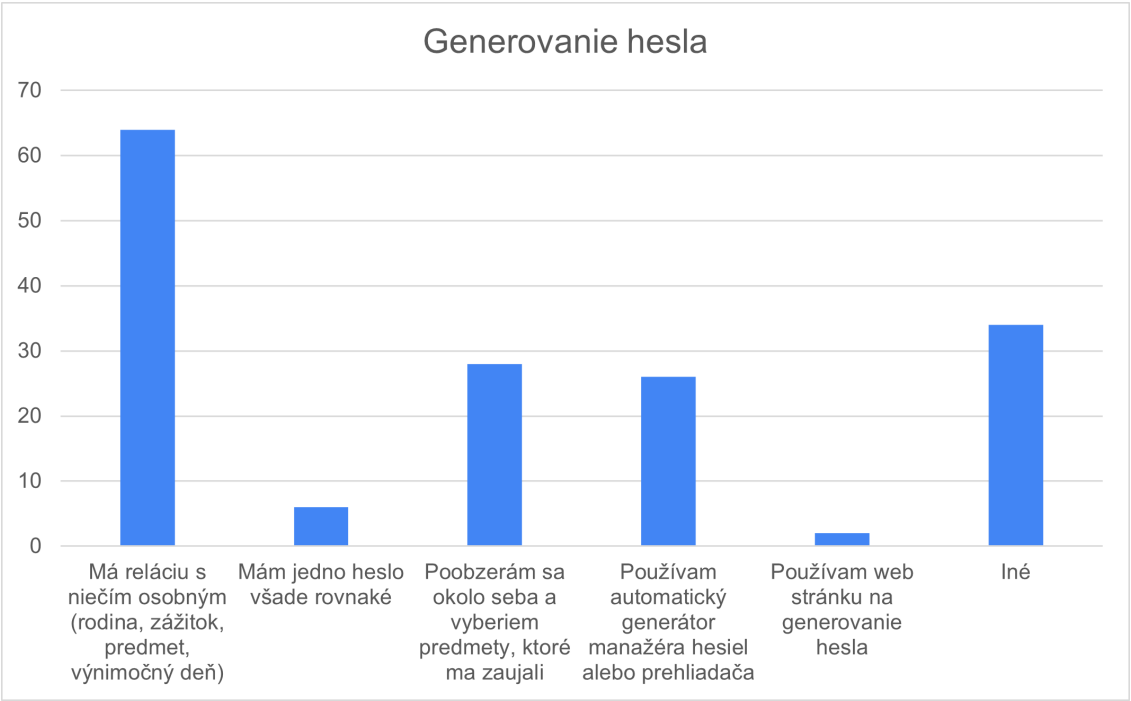
Obr. 9

významné miesto, 4 značku auta a 3 majú v hesle rok registrácie do danej služby.
Navyše 37 odpovedajúcich využilo možnosť dopísať vlastné. Medzi týmito odpoveďami sa viackrát vyskytli *náhodné písmená a čísla* , *skomoleniny slov* alebo heslá inšpirované kultúrou - texty piesní, postavy z kníh a filmov... No boli aj odpovede, ktoré nám o hesle ich autora prezradili viac, ako predchádzajúca otázka. Ak by sme vedeli, kto nám odpoveď poskytol, bez problémov by sme vedeli určiť jeho heslo.
Zisťovali sme aj samotnú dĺžku hesiel. Dostali sme 94 odpovedí. Najčastejšie sa vyskytovala hodnota 8. Priemerná hodnota bola 12.97 a medián 12. Pozreli sme sa, aká je v súčasnosti odporúčaná dĺžka hesla. Podľa [1] by mali používatelia voliť aspoň 15-znakové heslá. Túto podmienku spĺňa 33% našich respondentov. Histogram dĺžok hesiel môžeme vidieť na grafe 10.

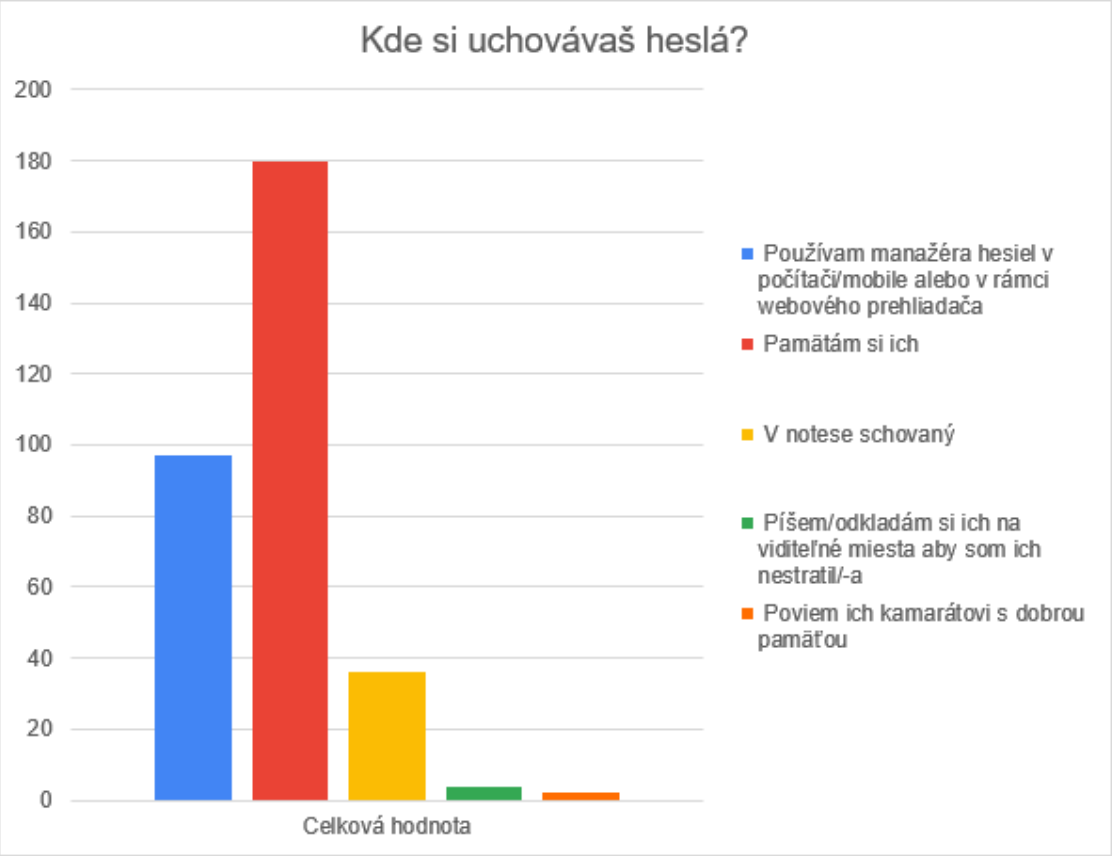
3.3 Vytvorenie a uchovávanie hesla

Pýtali sme respondentov, ako si vytvárajú svoje heslá. Odpovedalo nám 135 z nich, pričom 64 respondentov si volí heslá, ktoré majú reláciu s niečim osobným; 28 sa poobzerá po okolí; 26 používa na generovanie manažér hesiel; 6 ľudí sa priznalo, že má jedno heslo, ktoré používa všade; 2 generujú heslo pomocou webstránok a 34 ľudí uviedlo vlastné ďalšie spôsoby, pričom najčastejšie tvrdili, že si sami vymyslia náhodné heslo. Výsledky môžeme vidieť na grafe 11.
Na otázku o uchovávaní hesiel nám odpovedalo 253 respondentov, pričom 97 z nich používa manažér hesiel, 180 si heslá pamätá, 36 má heslo zapísané na papieri a ukryté, 4 majú heslo zapísané na viditeľnom mieste a 2 povedia svoje heslo kamarátovi, ktorý si ho zapamätá. Táto otázka umožňovala zadať viaceré odpovede. Najčastejšie sa vyskytovala kombinácia manažéra hesiel a pamätania si, pričom tieto dva spôsoby používa 43 našich respondentov. Výsledky môžeme vidieť na grafe 12.
Z dát môžeme vidieť, že prevláda pamätanie si hesla. Kedysi to bol odporúčaný spôsob. No s narastajúcim počtom systémov a aplikácií, ktoré potrebujú heslá, to nie je najlepšie riešenie. Keďže ľudia si nedokážu zapamätať veľa hesiel, často používajú tie isté heslá vo viacerých systémoch alebo vymýšľajú príliš jednoduché heslá. V súčasnosti existuje viacero spoľahlivých manažérov hesiel, ktoré odporúčame používať.

Obr. 10: Histogram dĺžok hesiel



Obr. 11: Ako si ľudia vytvárajú nové heslá

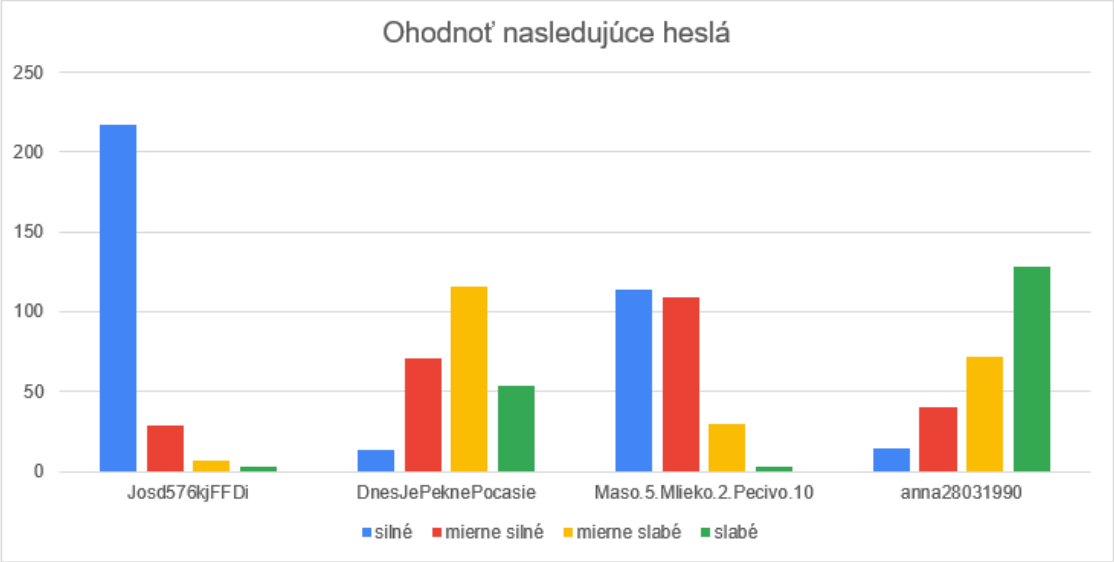


Obr. 12

3.4 Sila hesla

Významnou otázkou dotazníka bolo hodnotenie sily uvedeného hesla. Otázka bola dôležitá z dôvodu, že ešte donedávna existovalo tvrdenie, že čím heslo je náhodnejšia postupnosť znakov (písmen, čísel, špeciálnych znakov, etc.), tým je menšia šanca na jeho uhádnutie. Tento trend viedol ku zapisovaniu si hesiel do notesov alebo na viditeľné miesto, ak daná osoba nepoužívala, prípadne stále nepoužíva, manažéra hesiel. Ďalším problémom je, že ak vyžadujeme od užívateľov použitie viacerých skupín znakov (veľké písmená, malé písmená, číslice, špeciálne znaky), väčšina užívateľov si zvolí heslo, ktoré má prvé písmeno veľké a ostatné malé, a číslo alebo špeciálny znak sa vyskytne na konci.
Dnes vieme, že tento výrok nie je pravdivý. Populárny komix [8] na tento problém upozornil už pred viac než 7 rokmi. Ukazuje sa, že dĺžka hesla je dôležitejšia ako komplexnosť. Dnešným trendom pri tvorbe hesiel je takzvaný **passphrase**, teda heslo tvorené frázou zloženou z náhodných slov, prípadne vety. Je preukázané, že tieto heslá si ľudia lepšie pamätajú a taktiež je veľmi náročné ich prelomiť v prípade útoku [7].

Túto otázku zodpovedalo 254 respondentov, pričom ako najsilnejšie heslo uviedli náhodný reťazec znakov *Josd576kjFFDi*. Mierne silným až silným bol súbor slov zo slovníka obohatené špeciálnymi znakmi a číslami, teda passphrase *Maso.5.Mlieko.2.Pecivo.10*. Mierne slabá bola veta v slovenskom jazyku *DnesJePekneP ocasie* a slabým heslom bola kombinácia krstného mena, ktoré je medzinárodne používané a fiktívny dátum narodenia *anna28031990*. Výsledky sú vizualizované v grafe 13



Obr. 13: Výsledky pre otázku hodnotenia sily daných hesiel.

Silu týchto hesiel sme nechali zmerať webovými meračmi hesiel. Výsledky môžeme vidieť v tabuľke 1. Z toho vieme povedať, že silným heslom malo byť heslo *Maso.5.Mlieko.2.Pecivo.10*, mierne silným *DnesJePeknePocasie*, mierne slabým *Josd576kjFFDi* a slabým *anna28031990*. Čo nás teší, že rozdiel hodnotenia hesla *Maso.5.Mlieko.2.Pecivo.10* v kategórií mierne silné (109) a silné (114) má odchýlku len 5 hlasov.

Heslo	**CSIRT.UPJŠ** [6]	**Kaspersky**[2]	**HowSecureIsMyPassword**[5]
Josd576kjFFDi	17 minút	33 storočí	100 storočí
Maso.5.Mlieko.2.Pecivo.10	>storočie	>10000 storočí	400×10^{27} rokov
DnesJePeknePocasie	26 dní	>10000 storočí	6×10^{18} rokov
anna28031990	<1 sekunda	3 hodiny	3 roky

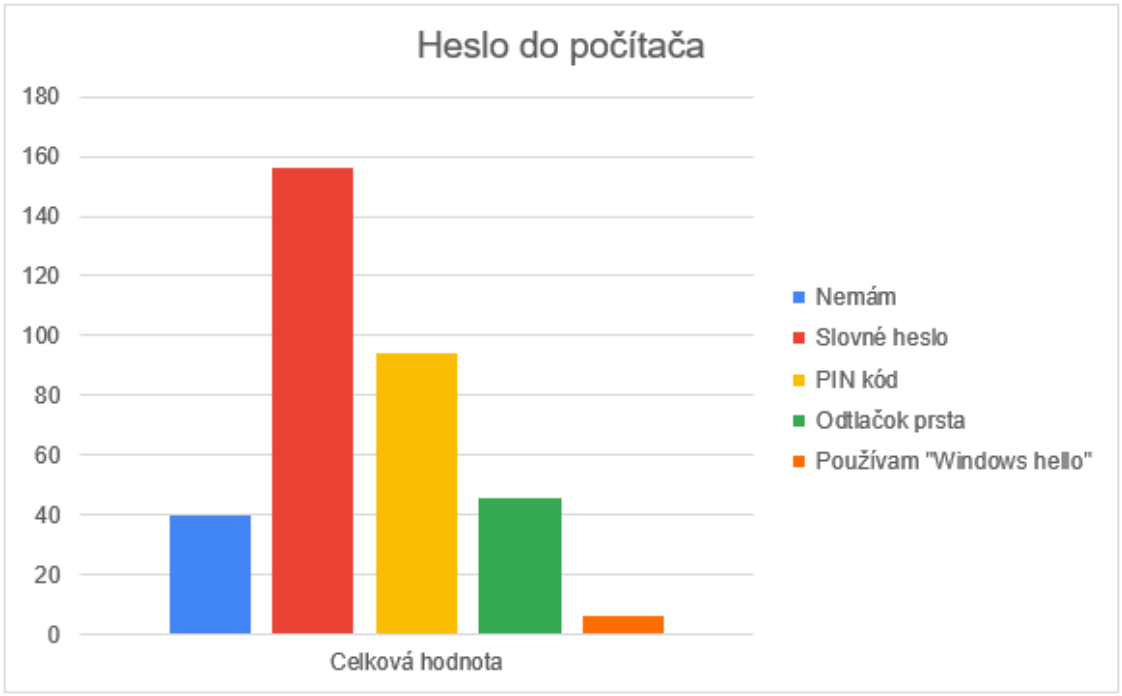
Tabuľka 1

3.5 Zariadenia

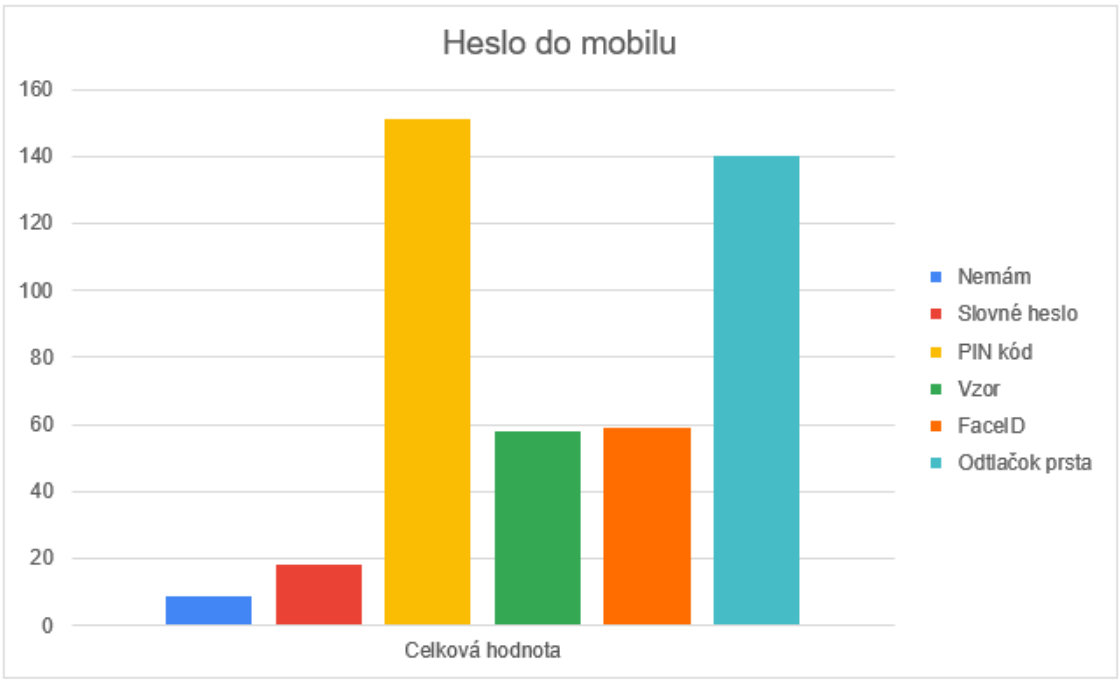
Ďalej sme sa zaujímali ako sa ľudia najčastejšie autentifikujú do počítača alebo mobilného telefónu. Na túto otázku mohli zvoliť viac menovaných spôsobov. Pri počítačoch to je, v dnešnej dobre, úplný štandard. S pribúdajúcimi funkciami našich mobilov prichádza aj väčšia potreba ich ochrany. V dnešnej dobe je na výber veľké množstvo spôsobov autentifikácie do telefónov: slovné heslo, číselný kód, vzor, biometria - odtlačok prstu alebo skenovanie tváre.
Z výsledkov prieskumu z 249 odpovedí, až 156 respondentov stále požíva slovné heslo; 94 PIN kód; 46 odtlačok prsta; 6 používa funkciu "Windows Hello" a 40 respondentov nemá žiaden spôsob autentifikácie do svojho počítača (14).
Pri spôsobe autentifikácie do mobilného telefónu, suverénne vedú PIN kód so 151 hlasmi a odtlačok prsta so 140 hlasmi. Ďalej sú populárne FaceID, 59 hlasov, a vzory, 58 hlasov. Na koniec sa dostalo slovné heslo, 18 hlasov a iba 9 respondentov označilo, že heslo do mobilu nemá (15).

3.6 PIN kód

Okrem hesiel sme sa spýtali ľudí aj na ich PIN kód. Odpovedalo nám 109 respondentov, pričom 82 uviedlo, že ich PIN kód je náhodný, 14 používa predvolené čísla, 12 má ako PIN kód dátum



Obr. 14

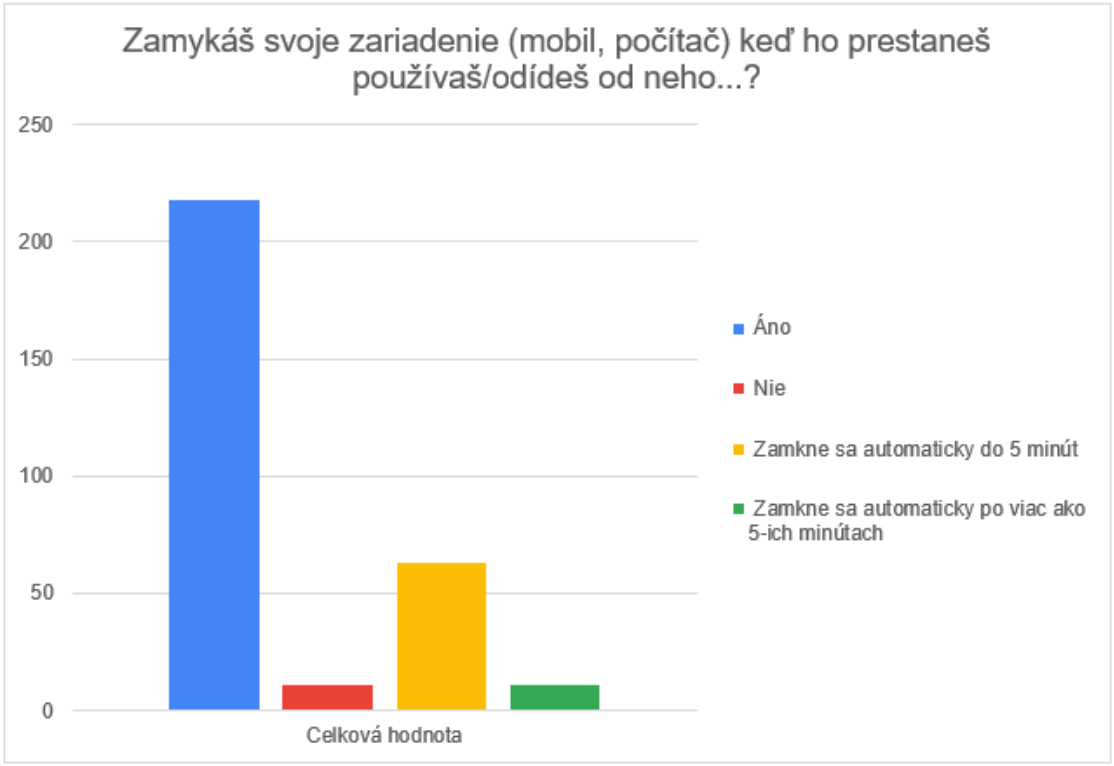


Obr. 15

narodenia seba, prípadne niekoho príbuzného a 8 ľudí používa iný významný dátum.

3.7 Ďalšie spôsoby ochrany

Keď už ľudia majú heslo akékoľvek, dbajú na to aby dané zariadenie bolo ochránené aj keď mu nevenujú pozornosť? Z 257 odpovedí sme zistili, že 218 z nich zamyká svoje zariadenie keď ho prestane používať alebo sa od neho vzdiali; 63 sa zamkne do 5 minút automaticky; 11 sa uzamkne po viac ako 5-ich minútach a rovnako 11 odpovedalo, že ho nezamykajú vôbec.

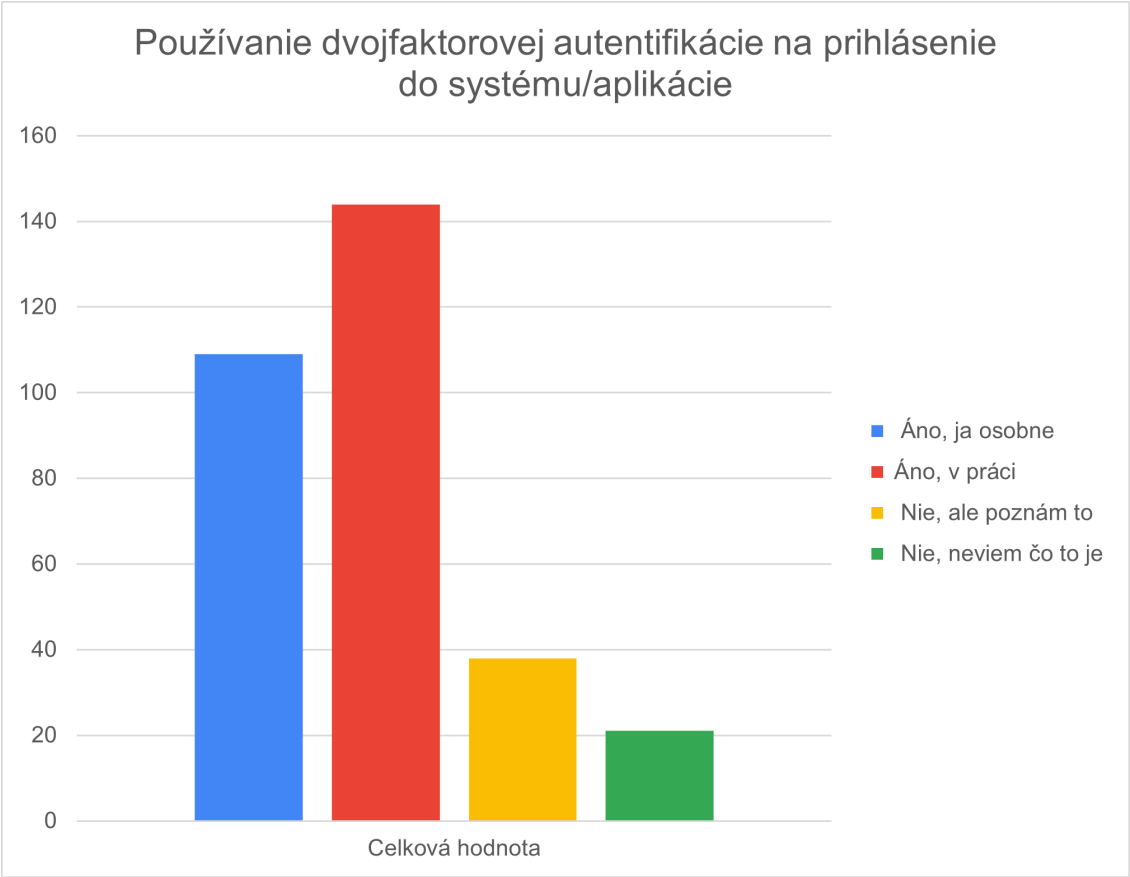


Obr. 16

Ďalej sme zisťovali, či si respondenti chránia prístup do systémov pomocou dvojfaktorovej autentifikácie (2FA). Z 254 respondentov, 109 používa 2FA osobne; 144 na pracovisku; 38 to síce nepoužíva, ale pozná to; 21 to nepoužíva a nepozná vôbec. Dvojfaktorovú autentifikáciu ponúka už množstvo aplikácií na webe alebo je štandardom v spoločnostiach, ktoré pracujú s citlivými informáciami. V prípade prezradenia hesla máme ešte ďalší prostriedok, ktorý nás ochráni pred prístupom útočníka. Poznáme ho vo forme SMS, overenie cez otázky alebo aj softwareový/hardvérový token generujúci číselný kód. Je to jedna z metód posiľňujúca bezpečie dát.

3.8 Úniky dát

Položili sme našim respondentom otázku, ako sa zachovajú, keď sa dozvedia, že unikli heslá z aplikácie, ktorú používajú. Dostali sme 250 odpovedí, pričom 53 ľudí si zmení heslá do všetkých účtov; 118 do tých, ktorých sa únik dát týka; 34 si overilo, že únik dát sa ich netýka, a tak si heslo nezmenili; 19 ľudí si heslo nezmení, lebo si ho mení pravidelne a 37 ľudí sa cíti bezpečne, pretože nevedia o takýchto situáciach. Výsledky môžeme vidieť na grafe 18.
Tým, ktorí používajú rôzne heslá pre rôzne účty, stačí, aby si zmenili heslo v dotknutej aplikácií. Ak používa rovnaké heslo aj v iných systémoch, je potrebné zmeniť si ho všade. Určite chválime, že si respondenti pozrú, či sa útok týka priamo ich alebo nie a podľa toho sa rozhodnú, či zmeniť heslo. No vzniká otázka: Veríme prevádzkovateľovi, keď povie, že útok sa týkal iba nejakej časti

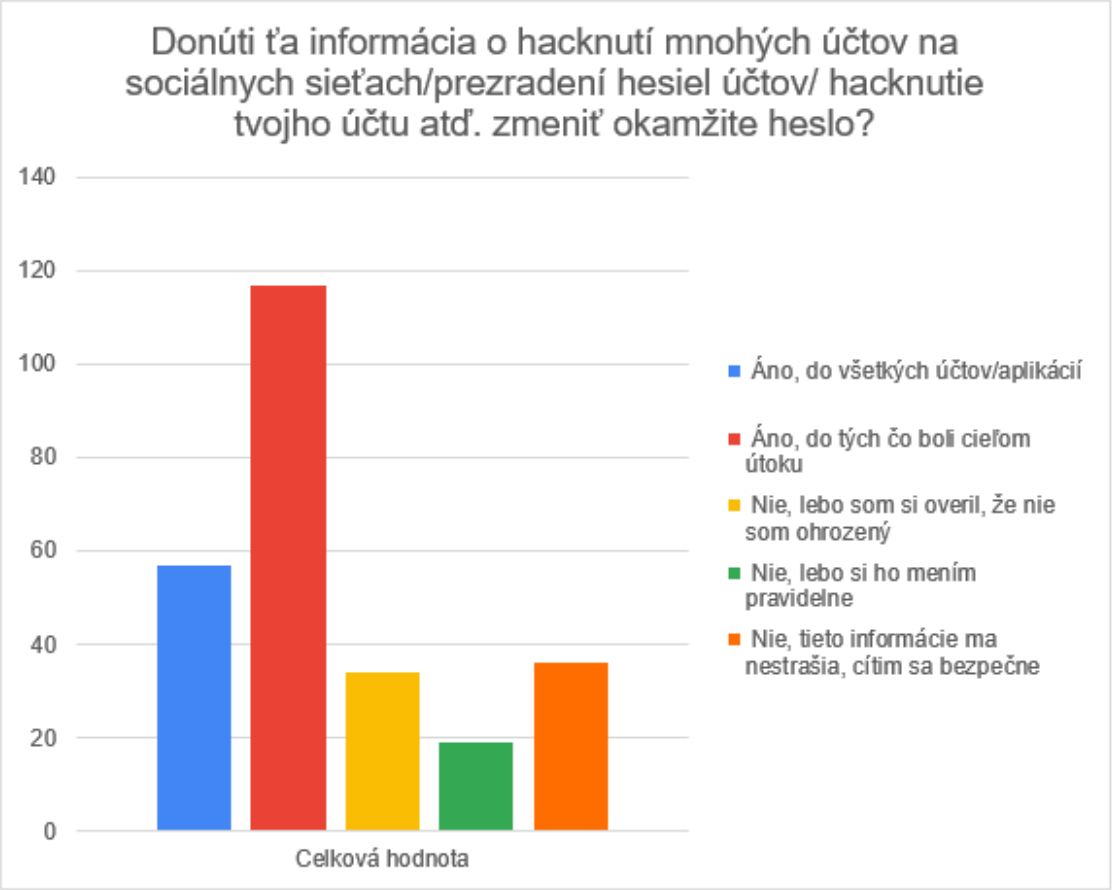


Obr. 17

používateľov? Pravidelné menenie hesla nás uchráni pred neznámymi únikmi dát, ale ak o tom vieme, odporúčame si zmeniť heslo znova.
Špeciálne sme sa zamerali na respondentov, ktorí v jednej z predchádzajúcich otázok uviedli, že nepoužívajú rôzne heslá pre rôzne systémy. Takých respondentov, ktorí zároveň odpovedali na túto otázku, bolo 34, no iba 3 z nich si zmenia heslá do všetkých účtov. Trinásti si zmenia iba do tej aplikácie, z ktorej dáta unikli; 6 si overili, že nie sú ohrození, 1 si mení heslo pravidelne a 11 majú pocit, že sa ich to netýka.

4 Záver

V tejto práci sme sa pozreli na to, ako ľudia pristupujú k problematike hesiel. Zistili sme, že viacero z nich nemá problém na internete vyzradiť informácie, ktoré by mohli viesť k uhádnutiu hesla. Narazili sme aj na ďalšie príklady nevhodného správania sa, ktoré znižuje bezpečnosť.
Taktiež sme zistili, že ľudia stále uprednostňujú komplikované heslá pred dlhými, čo sa ukazuje ako nie úplne bezpečné.
Pozitívnym zistením bolo, že ľudí zaujíma informačná bezpečnosť. Len 10 respondentov uviedlo, že neboli školení v tejto oblasti a ani o to nemajú záujem. Naopak viacero respondentov sa nám ozvalo, že ich téma veľmi zaujala a chceli by sa dozvedieť viac. Dúfame, že sa aj vďaka nášmu dotazníku a videu na konci niečo nové naučili.



Obr. 18

5 Fun facts

Každý prieskum prináša rôzne odpovede, niektoré smutné ale aj úsmevné. Nižšie si prečítajte výber najlepších odpovedí z tohto prieskumu.

Odporúčanou metódou ako vytvoriť heslo je *prúd myšlienok*, nech myslíte na čokoľvek, je tu pravdepodobnosť silného hesla. Ďalší respondent používa na generovanie hesla manažér hesiel, ale pravdepodobne si nastavil, nech jeho heslá obsahujú iba písmená, pretože ako sám uviedol, nechce používať čísla, aby nemal rôzne heslo na slovenskej a anglickej klávesnici. Ako riešenie by sme odporučili kolegovi kúpiť si klávesnicu s numerickou časťou. A na záver chceme pozdraviť respondenta, ktorý aj napriek super zvyku používať manažéra hesiel na ich ukladanie, ešte sa uistí, že heslo vie jeho kamarát. Toto veru nie je dobrá taktika.

Literatúra

[1] Catalin Cimpanu. Fbi recommends passphrases over password complexity. Dostupné na `https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/`.

[2] Kaspersky. Kaspersky password checker. Dostupné na `https://password.kaspersky.com/`.

[3] KPBI Kraje pro bezpečný internet. Bezpečná hesla. Dostupné na https://www.youtube.com/watch?v=sUpGHM_Adxo.

[4] Have I Been Pwned? Pwned passwords. Dostupné na https://haveibeenpwned.com/Passwords.

[5] Security.org. How secure is my password? Dostupné na https://howsecureismypassword.net/.

[6] CSIRT UPJŠ. Ako bezpečné je vaše heslo? Dostupné na https://hesla.csirt.upjs.sk/.

[7] Johannes Weber. Password strength/entropy: Characters vs. words. Dostupné na https://weberblog.net/password-strengthentropy-characters-vs-words/.

[8] xkcd936. Password strength comic. Dostupné na https://xkcd.com/936/.

Appendix

Používajú ľudia bezpečné heslá?

Ahoj,
sme študentky Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. V rámci projektu na predmet Informatika a spoločnosť sme sa rozhodli zistiť, ako na bezpečnosť hesiel dbajú bežní používatelia.

Dotazník je anonymný a dobrovoľný. Skladá sa z dvoch častí. V prvej z nich sa nachádzajú všeobecné otázky, ktoré sú povinné. Otázky z druhej časti sa zameriavajú na heslá, pričom odpovedať na ne je NEPOVINNÉ. Výsledky dotazníka budú použité len na účely výskumu. Odoslaním dotazníka súhlasíš s účasťou.

Vopred ďakujeme za tvoje odpovede.

Dominika a Jarka

* Povinné

Všeobecné otázky

1. Aké je tvoje najvyššie dosiahnuté vzdelanie? *

Označte iba jednu elipsu.

- ◯ Neukončené
- ◯ Základoškolské
- ◯ Stredoškolské bez maturity
- ◯ Stredoškolské s maturitou
- ◯ Vysokoškolské I. stupňa
- ◯ Vysokoškolské II. stupňa
- ◯ Vysokoškolské III. stupňa

2. Aká je tvoja veková kategória? *

Označte iba jednu elipsu.

- < 14
- 15-19
- 20-25
- 26-35
- 36-45
- 46-65
- 65+

3. Ako sa vyznáš v informatike/technológiach? *

Označte iba jednu elipsu.

- Vyznám sa veľmi dobre
- Vyznám sa dobre
- Vyznám sa málo
- Nevyznám sa vôbec

4. Bol si niekedy školený v rámci informačnej bezpečnosti? *

Začiarknite všetky vyhovujúce možnosti.

- [ ] Áno, študoval som to/zaujímam sa o túto tému
- [ ] Áno, v práci
- [ ] Nie, no mal by som záujem
- [ ] Nie, nezaujíma ma to

Preskočiť na 5. otázku

Otázky o heslách

Otázky v tejto sekcií sú nepovinné.

5. Považuješ svoje heslo za silné?

Označte iba jednu elipsu.

- ◯ Áno
- ◯ Skôr áno
- ◯ Skôr nie
- ◯ Nie

6. Používaš rôzne heslá pre rôzne systémy/aplikácie?

Označte iba jednu elipsu.

- ◯ Áno
- ◯ Nie

7. Ako často si meníš heslo do tebe dôležitých aplikácií (napr. sociálne siete, email, internetbanking)?

Začiarknite všetky vyhovujúce možnosti.

- ☐ Mením ich pravidelne v intervale 3 mesiacov
- ☐ Mením ich lebo ma núti systém
- ☐ Ako kedy ako ktoré
- ☐ Vtedy, ak ho zabudnem
- ☐ Nikdy

8. Máš dve heslá, ktoré pravidelne striedaš?

Príklad: heslo1 > heslo2 > heslo1 > heslo2

Označte iba jednu elipsu.

- ◯ Áno
- ◯ Nie

9. Uveď príklad svojho hesla:

_____

10. Čo obsahuje tvoje heslo?

Začiarknite všetky vyhovujúce možnosti.

- [ ] Moje meno
- [ ] Meno blízkej osoby/známeho
- [ ] Meno domáceho zvieratka
- [ ] Moju prezývku alebo login
- [ ] Môj dátum narodenia
- [ ] Dátum narodenia blízkej osoby
- [ ] Dátum významného dňa
- [ ] Miesto môjho narodenia/krajinu, iné obľúbené miesto
- [ ] Značku auta
- [ ] Rok registrácie do aplikácie/stránky/systému
- [ ] Náhodné predmety/slová v rodnom jazyku
- [ ] Náhodné slová v cudzom jazyku

Iné: ☐ _____

11. Aké dlhé je tvoje heslo?

_____

12. Ako si vytvoríš heslo?

Začiarknite všetky vyhovujúce možnosti.

- [ ] Používam automatický generátor manažéra hesiel alebo prehliadača
- [ ] Používam web stránku na generovanie hesla
- [ ] Poobzerám sa okolo seba a vyberiem predmety, ktoré ma zaujali
- [ ] Mám jedno heslo všade rovnaké
- [ ] Má reláciu s niečím osobným (rodina, zážitok, predmet, výnimočný deň)

Iné: ☐ _____

13. Kde si uchovávaš heslá?

Začiarknite všetky vyhovujúce možnosti.

- [ ] Používam manažéra hesiel v počítači/mobile alebo v rámci webového prehliadača
- [ ] Pamätám si ich
- [ ] V notese schovaný
- [ ] Píšem/odkladám si ich na viditeľné miesta aby som ich nestratil/-a
- [ ] Poviem ich kamarátovi s dobrou pamäťou

14. Ohodnoť nasledujúce heslá:

V každom riadku označte iba jednu elipsu.

	silné	mierne silné	mierne slabé	slabé
Josd576kjFFDi	◯	◯	◯	◯
DnesJePeknePocasie	◯	◯	◯	◯
Maso.5.Mlieko.2.Pecivo.10	◯	◯	◯	◯
anna28031990	◯	◯	◯	◯

15. Heslo do počítača:

Začiarknite všetky vyhovujúce možnosti.

- [ ] Nemám
- [ ] Slovné heslo
- [ ] PIN kód
- [ ] Odtlačok prsta
- [ ] Používam 'Windows Hello' (snímanie tváre, obrázok)

Iné: ☐ _____

16. Heslo do mobilu:

Začiarknite všetky vyhovujúce možnosti.

- [ ] Nemám
- [ ] Slovné heslo
- [ ] PIN kód
- [ ] Vzor
- [ ] FaceID
- [ ] Odtlačok prsta
- [ ] Iné: _____

17. Čo obsahuje tvoj PIN kód?

Akýkoľvek PIN kód - mobil, počítač, SIM karta, bankomatová karta.

Začiarknite všetky vyhovujúce možnosti.

- [ ] Obsahuje dátum narodenia mňa alebo môjho blízkeho
- [ ] Je to pre mňa významný deň
- [ ] Sú to náhodné čísla
- [ ] Sú to predvolené čísla

18. Zamykáš svoje zariadenie (mobil, počítač) keď ho prestaneš používaš/odídeš od neho...?

Začiarknite všetky vyhovujúce možnosti.

- [ ] Áno
- [ ] Nie
- [ ] Zamkne sa automaticky do 5 minút
- [ ] Zamkne sa automaticky po viac ako 5-minútach

19. Používaš ty alebo vo svojom zamestnaní dvojfaktorovú autentifikáciu (dvojstupňové overenie) na prihlásenie do systému/aplikácie?

Začiarknite všetky vyhovujúce možnosti.

- [ ] Áno, ja osobne
- [ ] Áno, v práci
- [ ] Nie, ale poznám to
- [ ] Nie, neviem čo to je

20. Donúti ťa informácia o hacknutí mnohých účtov na sociálnych sieťach/prezradení hesiel účtov/ hacknutie tvojho účtu atď. zmeniť okamžite heslo?

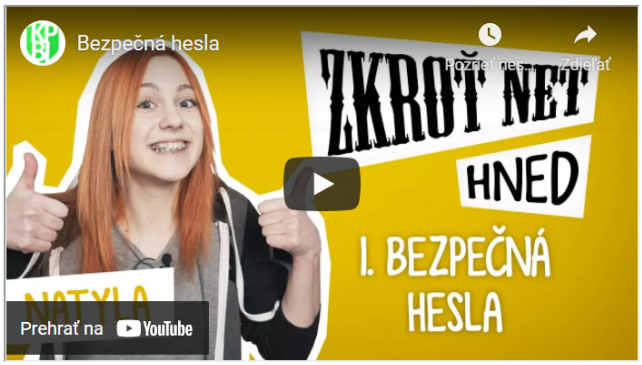
Začiarknite všetky vyhovujúce možnosti.

- [ ] Áno, do všetkých účtov/aplikácií
- [ ] Áno, do tých čo boli cieľom útoku
- [ ] Nie, lebo som si overil, že nie som ohrozený
- [ ] Nie, lebo si ho mením pravidelne
- [ ] Nie, tieto informácie ma nestrašia, cítim sa bezpečne

Ďakujeme za tvoju odpoveď :)

NIKDY NIKOMU NEHOVOR SVOJE HESLO!
Ak si nám ho práve prezradil, **OKAMŽITE SI ZMEŇ SVOJE HESLO!**

Ak sa chceš dozvedieť viac o tom, ako bezpečne používať heslá, pozri si nasledujúce video:



Video[3]