Digit@lni seniori

4

Informačná bezpečnosť

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Informačná bezpečnosť

Autor: Slavka Blichová a kol., Univerzita Pavla Jozefa Šafárika v Košiciach,
Centrum celoživotného vzdelávania a podpory projektov
Text prešiel odbornou jazykovou úpravou.
Za odbornú a jazykovú stránku študijného materiálu zodpovedajú autori.
Ilustrácia na titulke: Adobe Stock
Fotografie v publikácií sú ilustračné a ich obsah nemusí korešpondovať s aktuálnou verziou operačného systému digitálneho zariadenia.

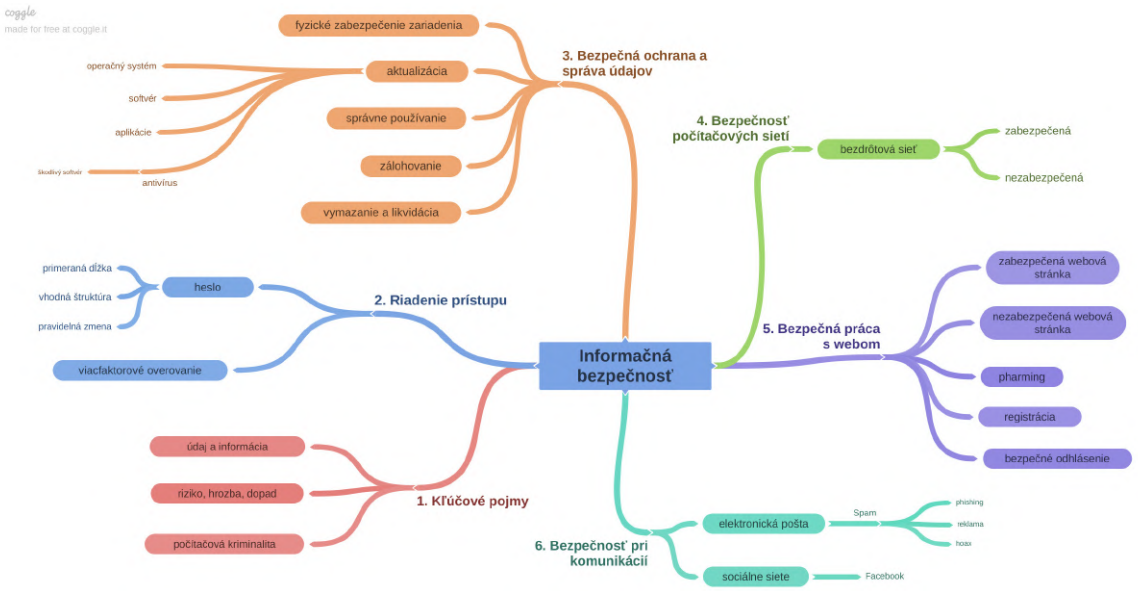
Vydavateľ: Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
2. doplnené a revidované vydanie

ISBN 978-80-974240-8-4

Obsah

Informačná bezpečnosť

Hlavným cieľom modulu je vedieť o hrozbách pri práci s digitálnymi technológiami a vedieť ako sa pred nimi chrániť.



Kľúčové slová: údaj, informácia, riziko, hrozba, dopad, počítačová kriminalita, heslo, aktualizácia, škodlivý softvér, antivírusový program, zálohovanie, bezpečnosť, hoax, sociálne siete, ochrana citlivých údajov

Hľadáte odpovede na tieto otázky?

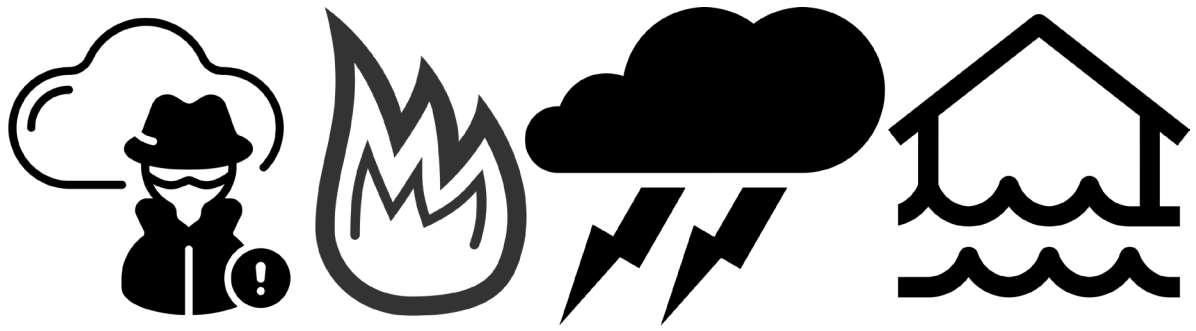
Používate silné a bezpečné heslá?
Sú potrebné aktualizácie operačného systému, softvéru a aplikácií?
Je antivírusový program dôležitý?
Zálohujete si svoje údaje (napr. rodinné fotografie)?
Poznáte prvky ochrany pri práci s webom, e-mailom?
...

1. Kľúčové pojmy

Cieľom informačnej bezpečnosti je identifikovať **hrozby** a **riziká** a na základe toho navrhovať a prijímať také opatrenia, ktoré zabezpečia minimalizáciu rizík a dopadov hrozieb pri zachovaní rozumnej miery nákladov v porovnaní s hodnotou chránených **informácií** a nebudú brániť oprávnenému používaniu informácií. V jednotlivých častiach si vysvetlíme dôležité pojmy používané v tejto oblasti.
Aby sme získali bližšiu predstavu, skúsime urobiť na príkladoch analógiu s bezpečnosťou v bežnom živote.

Príklad 1:
Vlastníme dom/byt/chatu a chceme si ich **zabezpečiť** pred vniknutím do nehnuteľnosti a krádežou, pred vandalizmom alebo poškodením, pred živelnou pohromou (povodeň, vytopenie, požiar, zásah blesku,...), prípadne zmierniť ich následky. Existuje niekoľko možností ako si svoj majetok chrániť:

a) špeciálne bezpečnostné dvere,
b) špeciálny zámok, doplnkový zámok,
c) zabezpečovací systém,
d) poistenie nehnuteľnosti.



Obrázok 1 – Hrozby

Možnosť ochrany stanovujeme podľa rizika pravdepodobnosti naplnenia danej hrozby.

Príklad 2:
Chceme prejsť cez cestu tak, aby sme sa čo najviac chránili pred prípadným úrazom. Je dôležité **dodržiavať pravidlá cestnej premávky**:

a) prechádzať cez cestu prednostne na vyznačenom úseku (priechod pre chodcov),
b) nevstupovať na vozovku, ak prichádzajúce autá idú príliš rýchlo,
c) pred vstupom na vozovku je nutné sa presvedčiť, či tak môžeme urobiť bez nebezpečenstva,
d) dodržiavať svetelnú signalizáciu pre chodcov.

Pri ich nedodržaní nám hrozí zvýšené riziko dopravnej nehody a úrazu.

Obrázok 2 – Pravidlá a riziká cestnej premávky

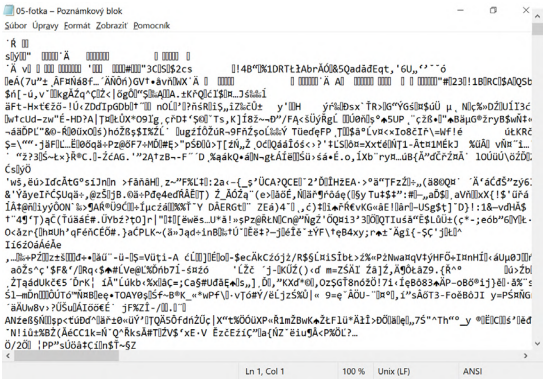
Údaj (dáta) je každá správa (alebo jej časť), bez ohľadu na to, či má alebo nemá pre nás nejakú informačnú hodnotu. Údajmi môžu byť písmená, čísla, slová, znaky, obrázky, zvuky, prípadne ich kombinácie. Údaje spracované do digitálnej formy sa nazývajú dáta.

Informácia je ľubovoľná správa, údaj, príkaz, dáta, inštrukcie a pod., ktoré prinášajú nové poznatky.
Tieto dva pojmy sa veľmi často zamieňajú. **Každá informácia je údaj, no nie každý údaj je informácia.**

Uvedieme si príklad: **70**
Toto je údaj. Sám o sebe nám nič nepovie. Ak tento údaj vidíme na váhe, na ktorú sme sa postavili, máme **informáciu** o našej **hmotnosti**.

Obrázok 3 – Údaj „70“

Ak sa pozrieme do občianskeho preukazu na rok svojho narodenia, môže to znamenať náš **vek**. Na tlakomeri to môže byť informácia o našom **tepe**.
Na pamäťových médiách máme uložené **údaje**. Pri ich správnej interpretácii z nich získame **informácie**.
Na ďalších dvoch obrázkoch máme ten istý súbor s **údajmi** (fotka) otvorený v editore na úpravu textu a v prehliadači obrázkov.



Obrázok 4 – Fotka v textovom editore

Obrázok 5 – Fotka v prehliadači obrázkov

Na obrázku je čudná zmes znakov, tieto údaje nám nedávajú žiadnu informáciu. Na obrázku vpravo máme z rovnakých údajov obrazovú informáciu, pohľad na krásnu kyticu.

Údaj: „nočný motýľ“

Informácia:
1. V kníhkupectve predávajú knihu „Nočný motýľ“
2. Na lúke poletuje „nočný motýľ“

Obrázok 6 – Nočný motýľ – jeden údaj, rôzne informácie

Úloha 1

Rozhodnite, čo je údaj a čo informácia:

STOP

Úloha 2

Uveďte aspoň jeden príklad údaja a informácie na základe vlastných skúseností:

Údaj: .....

Informácia: .....

Údaje sú ohrozené počas **prenosu, spracovania aj uchovávania**.

Hrozba je existujúca možnosť narušenia bezpečnosti.

a) **objektívne hrozby** – prírodné a fyzické, ako sú požiar, povodeň, výpadok napájania, havária a pod., spoločne označované ako vyššia moc (vis maior).

b) **subjektívne hrozby** – radíme tu hrozby od osôb.

   a. **neúmyselné** – chyby a omyly používateľov (napr. strata) a programátorov,

   b. **úmyselné** – útočníci (hackeri, crackeri, špióni, teroristi a pod.), prípadne úmyselne zavlečené chyby programátorov - nemusí sa jednať len o osoby zvonku, ale aj zvnútra (nespokojný, pomstychtivý alebo vydieraný zamestnanec).

Riziko je pravdepodobnosť naplnenia hrozby.

Dopady, hrozby sú v podstate následky toho, čo sa stane, ak sa hrozba naplní.

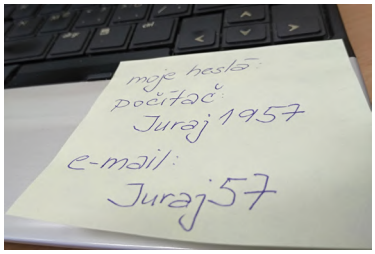
Príklad: *Študent vysokej školy píše diplomovú prácu. Má ju celú uloženú iba na USB kľúči, ktorý nosí stále pri sebe.*
Hrozba: strata USB kľúča, porucha elektroniky USB kľúča.
Riziko: dosť veľké, nakoľko v oboch prípadoch študent nebude mať k dispozícii svoju už skoro hotovú diplomovú prácu.
Dopad: ohrozenie termínu odovzdania diplomovej práce, psychické zrútenie sa študenta.
Ako tomu predchádzať?
Zálohovaním dát (diplomovej práce) na ďalšie zariadenia (aspoň 2x)

Upozornenie
Informácie majú v dnešnom svete obrovskú cenu. Prevažná väčšina dôležitých informácií je uložená v elektronickej podobe. Takéto informácie musia byť **chránené** pred neoprávneným prístupom a manipuláciou.

Počítačová kriminalita sú trestné činy zamerané proti počítačom, ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Počítače v podstate neumožňujú páchať nový typ trestnej činnosti, iba poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je sabotáž, krádež, zneužitie, neoprávnené užívanie cudzej veci, vydieranie alebo špionáž.

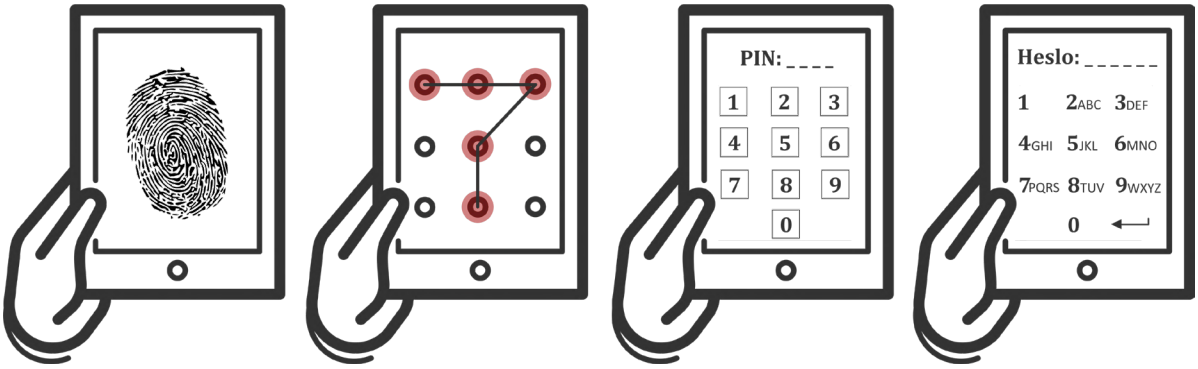
2. Riadenie prístupu

Mnohí z nás sa každý deň prihlasujú do rôznych zariadení – mobilný telefón, počítač, tablet alebo do rôznych služieb – e-mail, internet-banking, sociálne siete. Tieto prístupy tvoria bránu do nášho súkromia.



Obrázok 7 – Heslá

Napriek tomu často podceňujeme tento faktor bezpečnosti – heslá napísané na papierikoch a nalepené na monitore, v kalendári, veľmi jednoduché heslá.
Aby nedošlo k zneužitiu citlivých informácií uložených v digitálnych zariadeniach alebo v rôznych službách, je potrebné venovať prístupom náležitú pozornosť.
Pri prihlasovaní do digitálnych zariadení je k dispozícii niekoľko možností (nie v každom digitálnom zariadení sú všetky): biometrické prvky (odtlačok prsta, snímka tváre), grafický prvok na obrazovke (vzor), PIN kód alebo klasické heslo.



Obrázok 8 – Možnosti prihlasovania do digitálneho zariadenia

Upozornenie

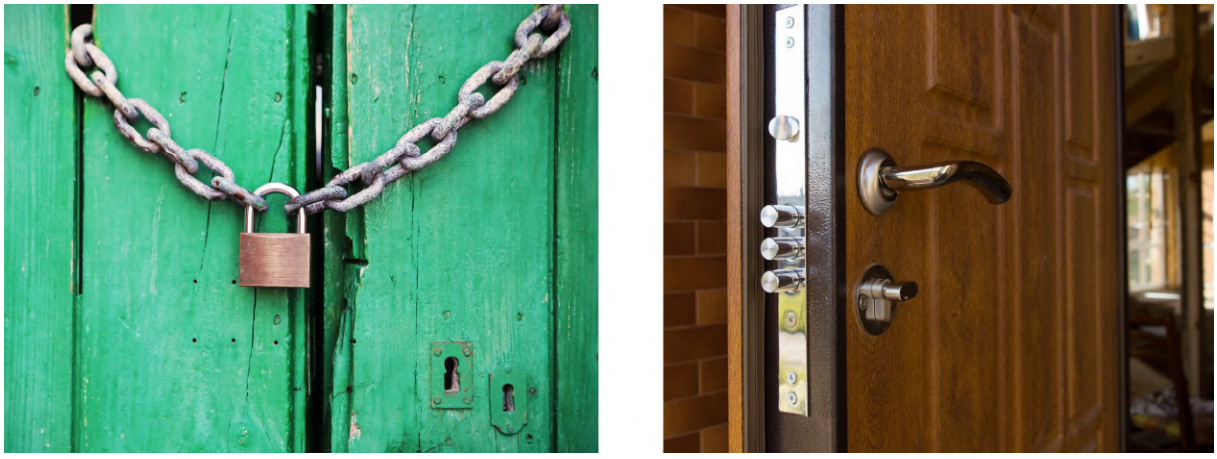
Uzamknite svoje zariadenie (tablet/mobil/počítač)!

Tak ako zamykáte dvere a zatvárate okná do vášho príbytku, mali by ste robiť to isté s vašimi zariadeniami.

Zabezpečené zariadenie chráni vaše informácie v prípade straty alebo krádeže.

Pri prihlasovaní do rôznych účtov sa najčastejšie používa prihlasovacie meno a heslo. Na zabezpečenie potrebnej úrovne ochrany týchto používateľských účtov je dôležité stanoviť pravidlá na tvorbu hesiel.

Heslo je všeobecný prostriedok k overeniu totožnosti užívateľa a mal by ho poznať iba samotný užívateľ. Dobré heslo nesmie byť ľahko uhádnuteľné a nemalo by to byť bežné slovo, ktoré má v bežnom jazyku nejaký význam. Malo by obsahovať najmenej 12 znakov a malo by byť kombináciou veľkých a malých písmen, číslic, prípadne špeciálnych znakov. Základným pravidlom je, že treba mať dobré a rozdielne heslá pre dôležité služby. Obzvlášť na prístup do počítača, e-mailu, sociálnych sietí a elektronického bankovníctva, kde sa vyskytuje najviac informácií a môže tam dôjsť k najväčším škodám. **Heslo je ako kľúč** a je potrebné si uvedomiť, že ani v reálnom živote nemáme jediný kľúč od viacerých dverí, napr. bytu, domu, auta, poštovej schránky, pivnice, atď. Čím drahšie veci máme uložené „za dverami“, tým bezpečnejší zámok si dávame „na dvere“ a podobne by sme sa mali správať aj pri využívaní rôznych služieb a ich ochrane pomocou hesla.
Príklady hesiel:
Slabé heslá: 123456, 111111, qwertz, abc123, 123123, novak54, heslo, 0000
Silné heslá: v3S3leV1@n0c3, 1mmrdckldPC, o!3Ps?5K, C3rvn4.Ci4pock4



Obrázok 9 – „Slabé a silné heslo“

Slabé (jednoduché) heslá síce uľahčujú prístup, ale tento spôsob pohodlia predstavuje príliš veľké riziko, pretože jednoduché heslá sa dajú ľahko zistiť. Silné a zložité heslá môžu pomôcť zabrániť v prístupe k citlivým informáciám, ale často si ich nevieme zapamätať.

Ako si vytvoriť silné heslo tak, aby sme si ho aj pamätali? Vytvorme heslo z vety, ktorá nám niečo pripomína (napr. „NaSteneMam.3Obrazy!“).

Upozornenie

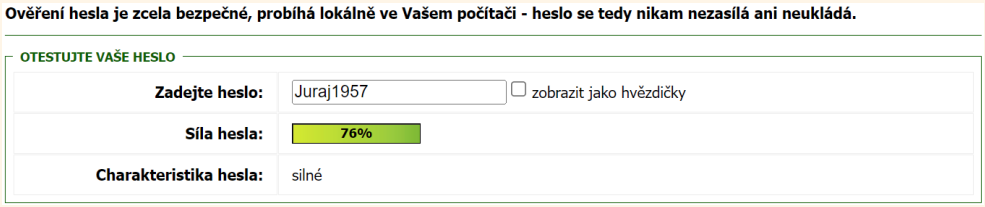
Unikátny účet – jedinečné heslo!

Samostatné heslá pre každý účet (tablet, počítač, e-mailový účet, internetbanking) pomáhajú chrániť pred zneužitím.

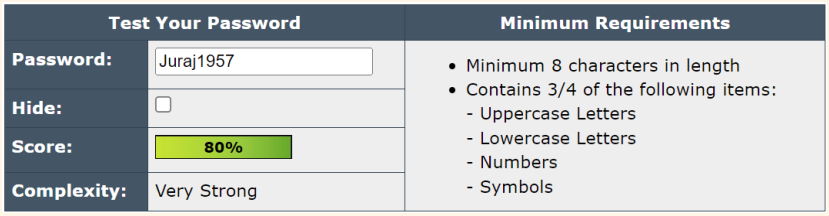
Úloha 3

Overte si silu svojho hesla. Zadajte do prehliadača webovú adresu a zadajte svoje heslá (ak nechcete zadávať svoje reálne heslá, vymyslite si heslo, ktoré sa podobá tomu vášmu – počtom znakov, veľkosťou písmen, číslic, špeciálnych znakov, napr. ak máte heslo Janka1963, vyskúšajte heslo Petra1965):

1. **www.speedweb.cz/index.php?akce=pass**



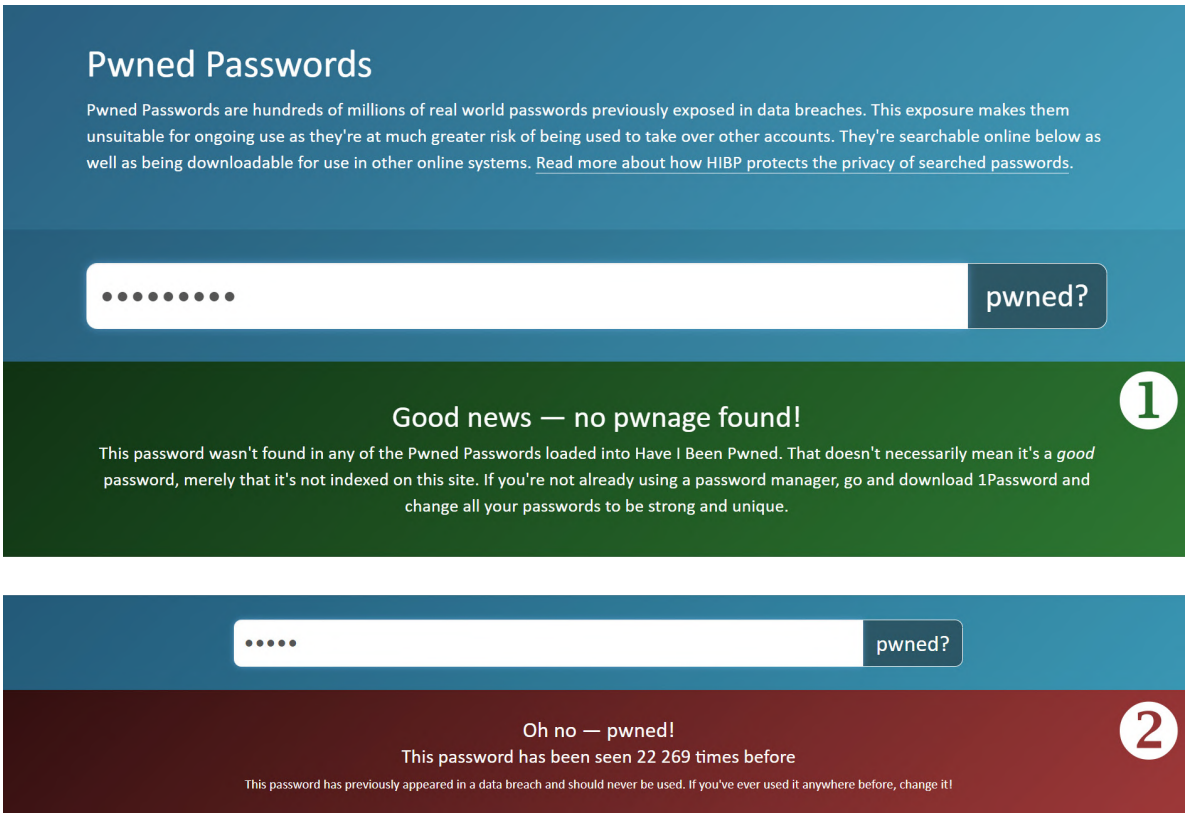
2. **www.passwordmeter.com**



3. **hesla.csirt.upjs.sk**

Na adrese **Ako bezpečné je vaše heslo?** vyskúšajte silu hesla: **NaSteneMam.3Obrazy!**

Ak chceme zistiť, či heslo, ktoré používame, nebolo odhalené pri nejakom úniku osobných údajov, môžeme si to overiť na stránke Pwned Passwords (https://haveibeenpwned.com/Passwords).



Obrázok 10 – Pwned Passwords

Úloha 4

Na webovej stránke **haveibeenpwned.com/Passwords** overte, či vaše heslo bolo odhalené pri úniku osobných údajov.

V prípade, že sa vaše heslo nachádza medzi uniknutými heslami (2), odporúčame toto heslo, čo najskôr v príslušných službách zmeniť.

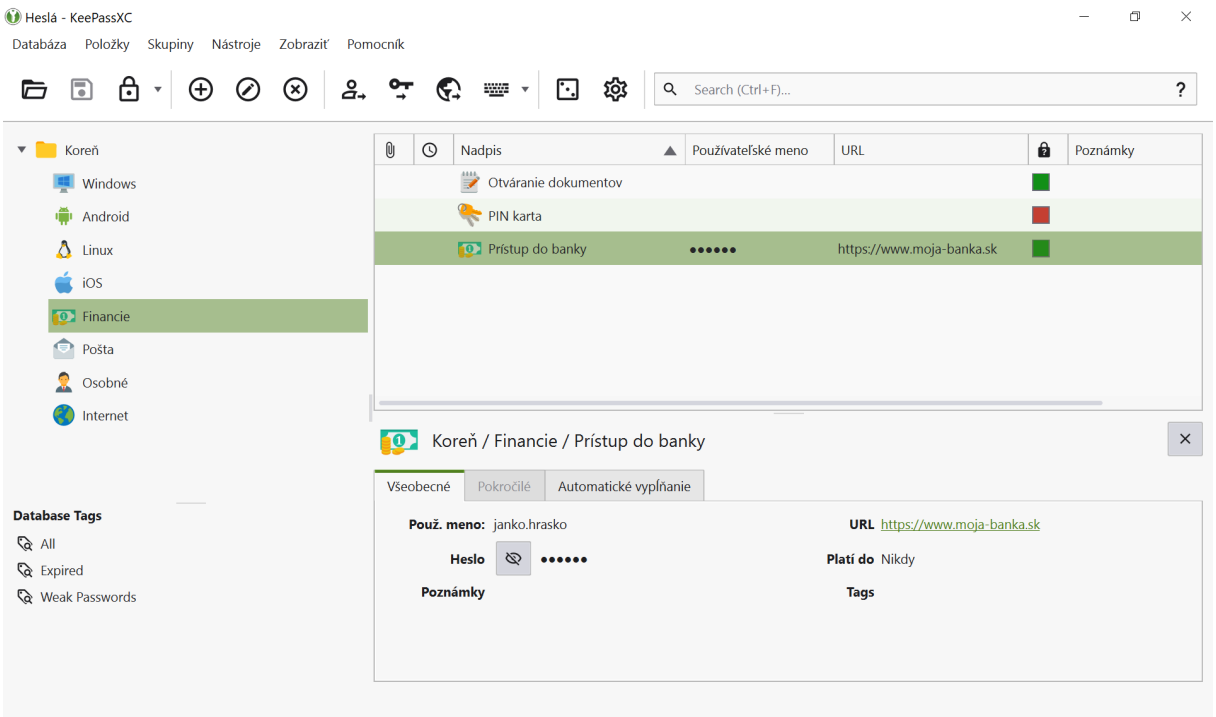
☐ Áno ☐ Nie

V súčasnosti už mnohé služby vyžadujú **viacfaktorové overovanie**, ktoré pridáva ďalšie vrstvy zabezpečenia/ochrany (môžeme to prirovnať k prídavnému zámku na dverách). Viacfaktorové overovanie využívame v praxi a možno o tom ani nevieme (neuvedomujeme si to).

Viacfaktorové overovanie využíva prvky:

- **niečo, čo mám** (telefón, občiansky preukaz, platobná karta,...)
- **niečo, čo viem** (PIN, heslo)
- **niečo, čo som** (biometrická charakteristika – odtlačok prsta, biometria tváre, oka, hlasu,...)

Príklad: **výber z bankomatu**
2 faktory overovania: **bankomatová karta** (to, čo mám) a **PIN** (to, čo viem).
Každý môže zabudnúť svoje heslo, preto je dobré, ak si udržujeme **zoznam hesiel**, ale ten by mal byť uložený na bezpečnom mieste **mimo počítača**. Môžeme to prirovnať k tomu, že PIN kód k platobnej karte nikdy nemáme uložený pri platobnej karte. Pre skúsenejších užívateľov, hlavne ak majú väčší počet účtov a častejšie obmieňajú heslá, je vhodné využitie nástroja, ktorý sa volá **manažér hesiel** (password manager). Ten uschová v bezpečí heslá na jednom mieste, pričom si stačí k nemu zapamätať jedno hlavné heslo.



Obrázok 11 – Manažér hesiel - KeePassXC

3. Bezpečná ochrana a správa údajov

Ochranu údajov a zariadení môžeme zabezpečiť dôležitými krokmi:

1. fyzickým zabezpečením zariadenia, ktoré obsahuje údaje,
2. aktualizáciou operačného systému, softvérov a aplikácií, ktoré máme na našom zariadení nainštalované,
3. správnym používaním zo strany používateľa,
4. zálohovaním údajov.

Nezanedbateľným krokom pre zabezpečenie ochrany údajov je aj ich správna likvidácia.

3.1. Fyzické zabezpečenie zariadenia

Digitálne zariadenie obsahujúce **údaje** si musíme chrániť pred **poruchou, zničením, krádežou alebo stratou**. Pri každej z týchto možností je jediná spoľahlivá prevencia krok 3 – **zálohovanie údajov mimo zariadenia**.

Napriek našej snahe sa môže stať, že nám jedného dňa prestane digitálne zariadenie pracovať. Nie je hneď dôvod na paniku. Je to obyčajné elektronické zariadenie, a v prípade **poruchy** sa väčšinou dá opraviť. Ako prvé vždy skontrolujme, či je pripojené k elektrickej sieti (počítač) alebo či nie je vybitá batéria (notebook, tablet, mobil). Niekedy pomôže vypnúť a opätovne zapnúť zariadenie. Ak nič z toho nepomáha, tak môžeme skúsiť zavolať „priateľa na telefóne“, ktorý sa na to pozrie. Ako posledný krok sú servisné strediská pre jednotlivé digitálne zariadenia.

Zničenie digitálneho zariadenia býva väčšinou nehoda, preto pri manipulácii s ním je potrebné dodržiavať niekoľko zásad:

- chrániť mobilné digitálne zariadenia pred nárazmi, napr. pádom (pomôcť môže kryt alebo obal),
- nepoužívať mobilné zariadenie pri konzumácií jedla alebo nápojov (zabránime tým napr. obliatiu tekutinou alebo zaneseniu drobných omrviniek do zariadenia),
- udržovať zariadenie v čistote (napr. prach, ale aj špinavé ruky).

Krádež zariadenia je nemilá vec, preto je potrebné venovať pozornosť prevencii. Dôležité je nenechávať zariadenie (hlavne prenosné) bez dozoru, resp. mať ho vždy v uzamknutej miestnosti. V žiadnom prípade nenechávajme zariadenie v aute na viditeľnom mieste a nie je odporúčané ho nechávať ani v kufri auta, pretože nikdy nevieme, kto nás sleduje pri jeho odkladaní.

Obrázok 12 – Krádež

Strata zariadenia môže byť spôsobená našou nepozornosťou, pozor je potrebné dávať hlavne pri cestovaní.

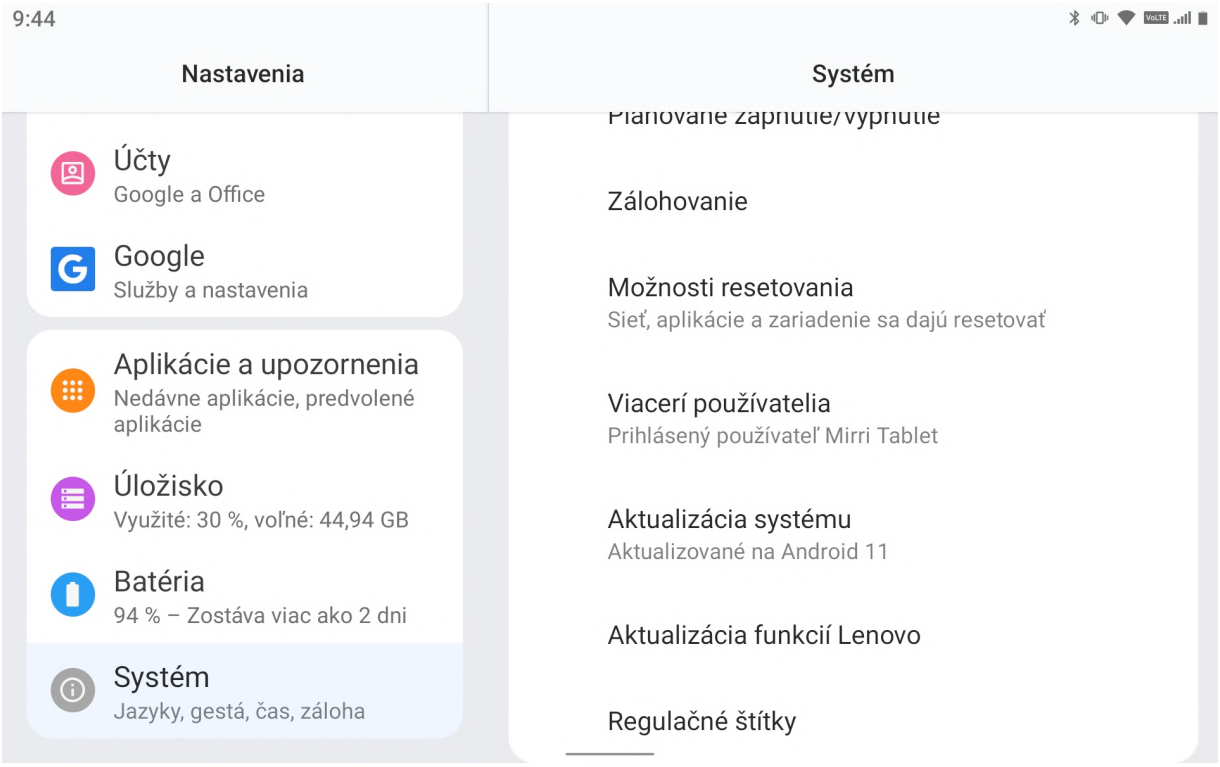
3.2. Pravidelná aktualizácia

Z hľadiska bezpečnosti údajov je **aktualizácia operačného systému, softvérov a aplikácií** nevyhnutnosťou. Aktualizácie nám prinášajú nové funkcie, zlepšenie výkonu, príjemnejší vzhľad, jednoduchšie ovládanie,.... Okrem toho **opravujú chyby** (zraniteľné či slabé miesta) v operačných systémoch, softvéroch a apli-káciách, ktoré by mohli útočníci zneužiť a tým zvyšujú bezpečnosť programu, používateľa, a aj zariadenia. Niektoré chyby softvéru (nie všetky) je totiž možné zneužiť na nejaký typ útoku alebo prieniku do počítačového systému (ide o tzv. bezpečnostné chyby).

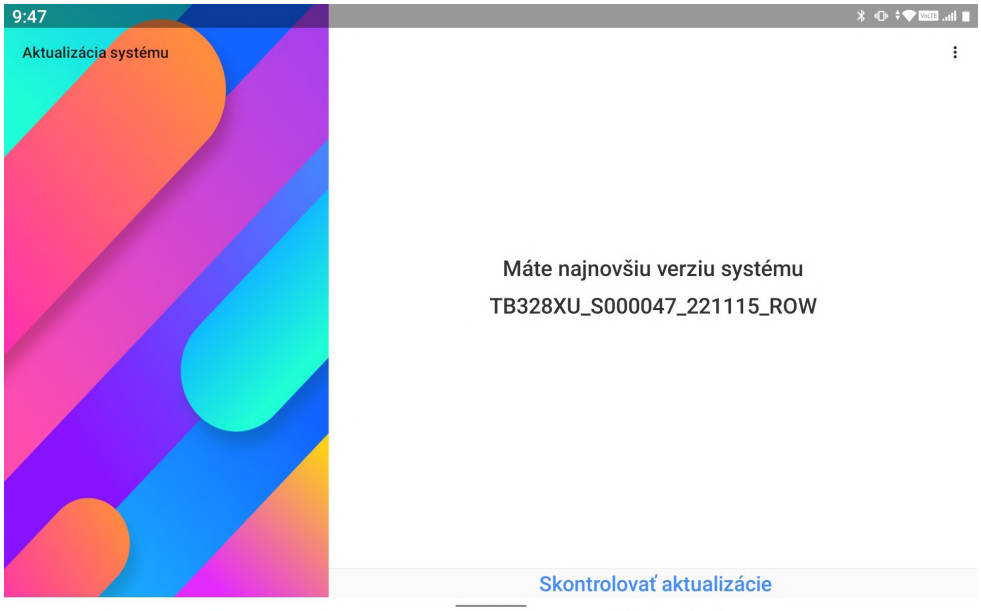
Pri štarte zariadenia (napr. tabletu pri odsúhlasovaní podmienok použitia) môžeme dostať otázky priamo od výrobcu, či súhlasíme s automatickými aktualizáciami nášho zariadenia. Tento súhlas je možné udeliť aj dodatočne. V prípade, že automatické aktualizovanie operačného systému neodsúhlasíme, môžeme aktualizovanie vykonať aj manuálne (podľa toho, kedy sa nám čas aktualizácie hodí). Manuálne aktualizovanie systému neodporúčame výrazne odďaľovať z dôvodov, ktoré sme opísali vyššie.

Obrázok 13 – Zapnutie automatických aktualizácii

Aktualizáciu operačného systému v tablete vykonáme cez aplikáciu **Nastavenia** v časti **Systém** -> Aktualizácia systému.



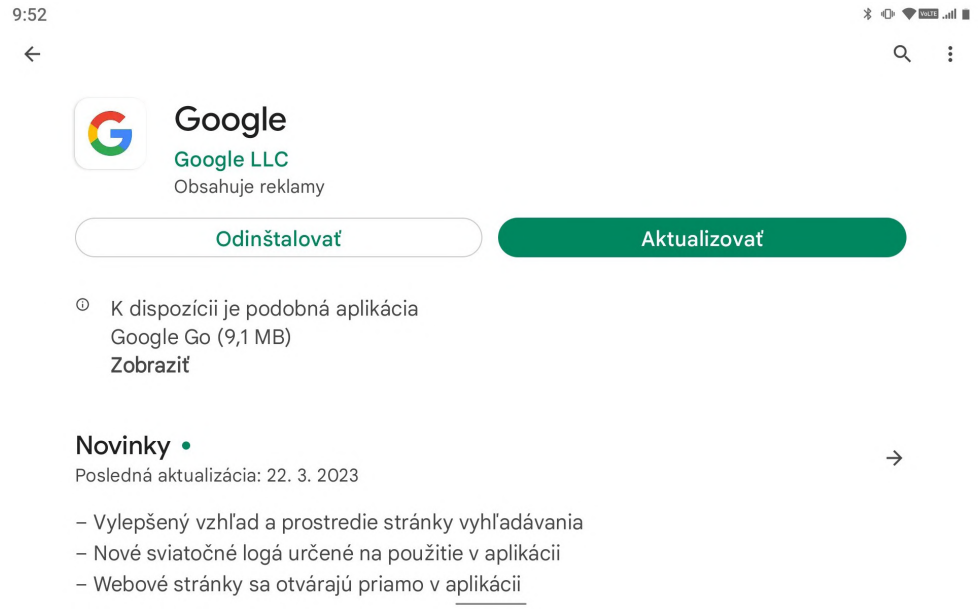
Obrázok 14 – Systém
(*systém a vzhľad obrazovky na pozadí v našom tablete sa môžu od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému a našich osobných nastavení)



Obrázok 15 – Ukážka kontroly aktualizácie operačného systému
(*vzhľad okna s hlásením o výsledkoch kontroly aktualizácie operačného systému v našom tablete sa môže od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému)

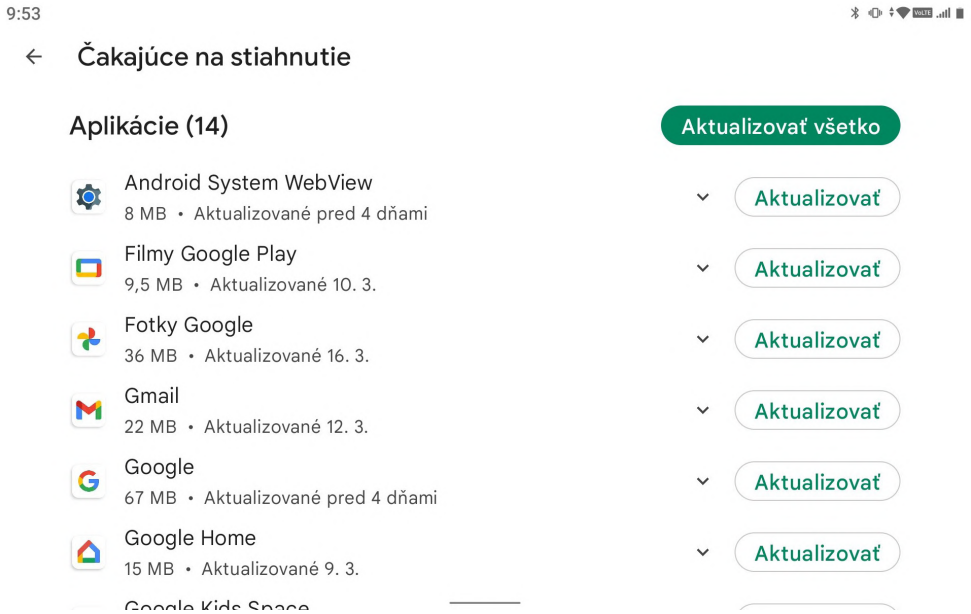
Ťuknutím na tlačidlo „Skontrolovať aktualizácie" môžeme manuálne skontrolovať dostupnosť aktualizácii na tablet.

Aktualizácia jednotlivých aplikácií na tablete je ponúkaná pri spustení. Po zobrazení upozornenia sa môžeme rozhodnúť, či aktualizáciu vykonáme okamžite alebo ju odložíme na neskôr.



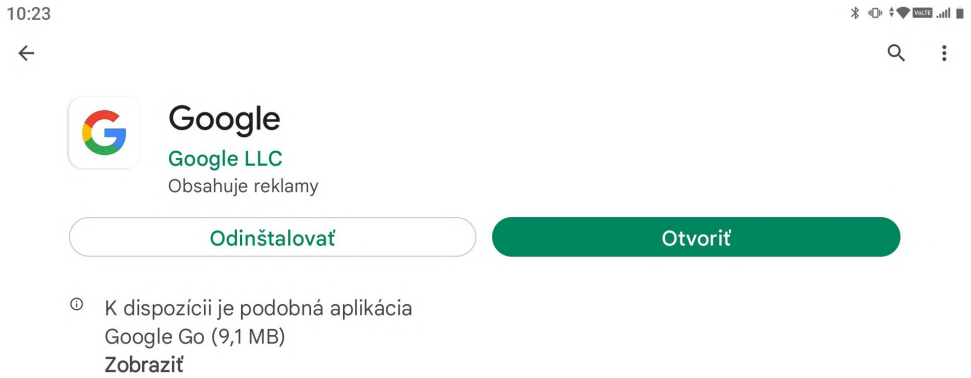
Obrázok 16 – Upozornenie na dostupnosť aktualizácie aplikácie
(*vzhľad okna s upozornením v našom tablete sa môže od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému)

Po ťuknutí na tlačidlo „Aktualizovať” sa pripojíme na obchod s aplikáciami a môžeme spustiť samotný proces aktualizácie.
V tlačidle „Aktualizovať” je zobrazená aj približná veľkosť aktualizácie (dát, ktoré sa prenesú do nášho tabletu). Ťuknutím na tlačidlo spustíme proces aktualizácie tejto aplikácie.



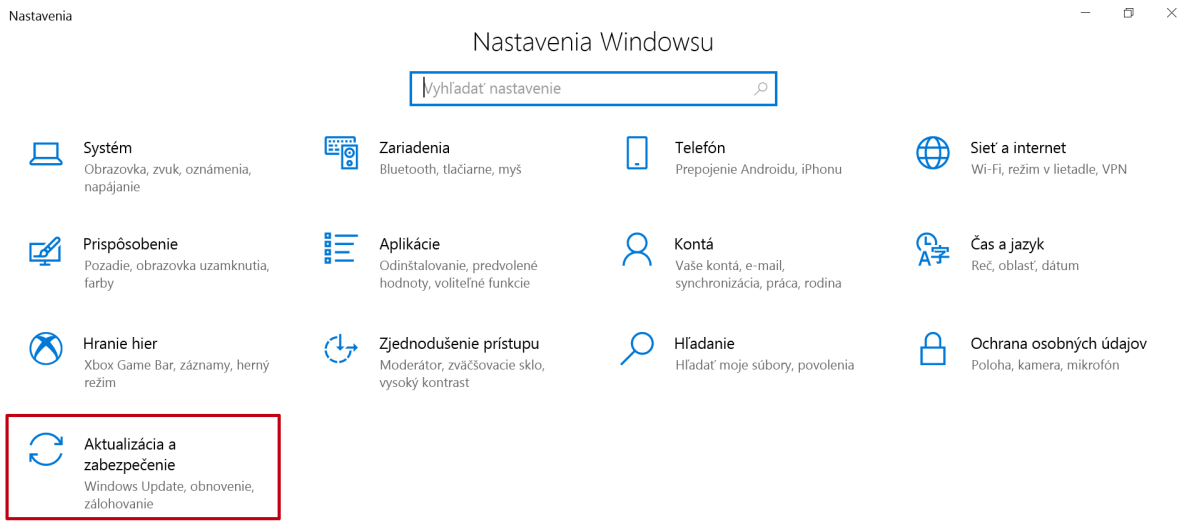
Obrázok 17 – Príprava aktualizácie

Po dokončení aktualizácie môžeme pokračovať v otváraní novej verzie aplikácie, ťuknutím na tlačidlo „Otvoriť”.



Obrázok 18 – Otvorenie aktualizovanie aplikácie
(*vzhľad okna v našom tablete sa môže od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému)

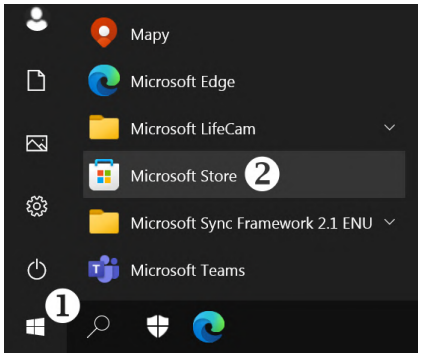
V prípade používania zariadenia so systémom Windows je vhodné nastaviť **automatické aktualizácie**.



Obrázok 19 – Aktualizácia operačného systému Windows

To, či je operačný systém aktualizovaný, zistíme v nastaveniach Windows:
Štart -> Nastavenie -> Aktualizácia a zabezpečenie -> Windows Update.

Ak chceme zapnúť aj automatické aktualizácie aplikácií nainštalovaných cez Microsoft Store, cez ponuku **Štart** (1) vyhľadáme položku **Microsoft Store** (2). V okne v pravom hornom rohu klikneme na ponuku konta (Profil) a položku **Nastavenie aplikácií**. V časti Aktualizácie aplikácií nastavíme vpravo posúvač na možnosť **Zapnutá**.



Obrázok 20 – Microsoft Store

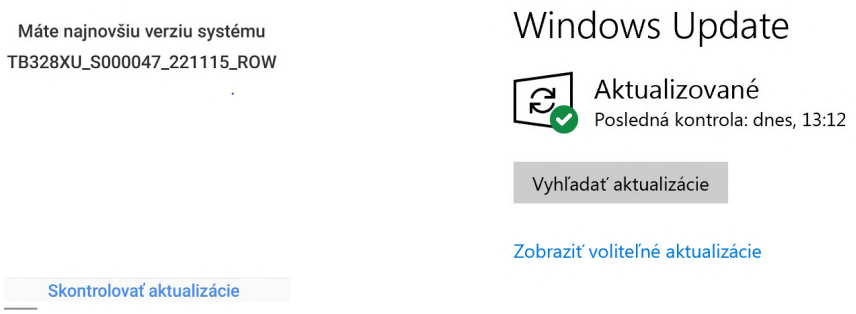
Úloha 5

Skontrolujte, či operačný systém na tablete alebo počítači, na ktorom pracujete, je aktualizovaný.

Úloha 6

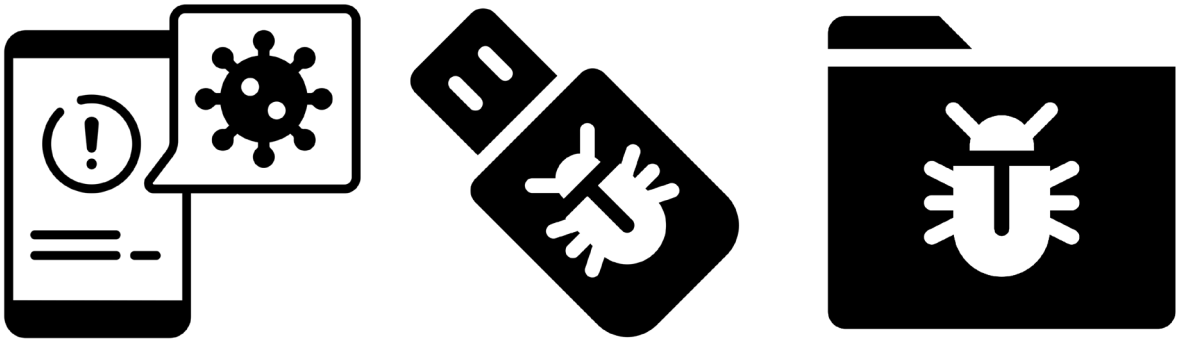
Skontrolujte, či sú v zariadení zapnuté automatické aktualizácie. Skontrolujte aktualizácie aplikácií.

Kontrola: ak je systém aktualizovaný, zobrazuje sa napr.:



Jedným z najdôležitejších softvérov, ktorý je potrebné mať stále **aktuálny**, je **antivírusový softvér**. Je to počítačový program, ktorého cieľom je identifikovať a eliminovať škodlivý softvér. V súčasnosti v online priestore je takmer každé digitálne zariadenie vystavené **škodlivému softvéru nazývaným malware**, ktorý môže spôsobiť obrovské škody. Zničí našu prácu, kvôli nemu môžeme stratiť naše údaje, dokonca aj naše osobné údaje sa môžu dostať do nesprávnych rúk.

Malware (z anglického malicious software – škodlivý softvér) je všeobecné označenie pre škodlivé softvéry akéhokoľvek typu, ktoré väčšinou bežia na digitálnom zariadení bez vedomia (a súhlasu) majiteľa. Patria sem napr. vírusy, červy, trójske kone, spyware, adware, ransomware, keylogger, backdoor, rootkit, dialer, spammer.
Majú rôzne funkcie, spôsoby šírenia a skrývania sa – škodlivý softvér využíva rôzne spôsoby maskovania, aby nebol predčasne odhalený a mohol vykonať svoju úlohu.



Obrázok 21 – Škodlivý softvér môže byť v zariadení, na USB kľúči ale aj v dokumente

Príklad: Jednou z najväčších **hrozieb pre dáta** je škodlivý softvér **ransomware**, ktorý zneprístupní údaje a žiada výkupné. Po úspešnom útoku na zariadenie, škodlivý softvér **uzamkne jeho obrazovku alebo zašifruje dáta** uložené na disku a majiteľovi infikovaného zariadenia sa zobrazí oznámenie, v ktorom sa od neho žiada zaplatenie výkupného. Súčasťou takéhoto oznámenia sú aj inštrukcie týkajúce sa realizácie platby.

Obrázok 22 – Ransomware

Úloha 7

Vo vyhľadávači zadajte slovo **„ransomware“** a nájdite nejakú aktuálnu informáciu o kyberútoku.

Pomôcka: vo vyhľadávači zadajte hľadanie iba v jazyku slovenčina a napr. posledný mesiac alebo navštívte stránku www.sk-cert.sk

Na správne fungovanie antivírusového programu je **bezpodmienečne nutné pravidelne aktualizovať vírusovú databázu**, pretože antivírus bez aktualizácií stráca na efektívnosti detekcie škodlivého softvéru. Väčšina antivírusov si sťahuje aktualizácie **automaticky**.

Antivírus na odhaľovanie škodlivého softvéru využíva niekoľko spôsobov:

- Rezidentná (trvalá) ochrana všetkých súborov (kontroluje súbory pri spúšťaní, otváraní, ukladaní),
- Ochrana prístupu na web (kontroluje obsah údajov preberaných z webu),
- Ochrana elektronickej pošty (kontroluje obsah správ a príloh pošty),
- Kontrola vymeniteľných médií (optické nosiče, USB kľúče, pamäťové karty a pod.),
- Kontrola na vyžiadanie.

Konkrétny súbor, priečinok, USB kľúč,... si vieme kedykoľvek skontrolovať pomocou antivírusového programu. K dispozícií máme buď platené antivírusové programy alebo tie, ktoré sú zadarmo. Bezplatné verzie sú spravidla bez niektorých funkcionalít.
Pre tablety a telefóny je dostupný napr. slovenský ESET Mobile Security & Antivirus, alebo český AVG Antivírus & Zabezpečenie. Pre zariadenia s operačným systémom Windows je k dispozícií Windows Defender. Väčšinou sú tieto produkty dostupné bezplatne, používateľa chránia automaticky bez toho, aby musel niečo nastavovať, systém nezaťažuje, zbytočne neotravuje a prakticky nevyžaduje žiadnu údržbu. Niektoré z produktov môžu obsahovať reklamy. Kontrola aplikácií a súborov zväčša prebieha automaticky, počas procesu práce so zariadením.

Úloha 8 (pre tablety)
Spustite antivírusovú aplikáciu a skontrolujte zariadenie.

Úloha 8 (pre počítače)
Skontrolujte jeden súbor, resp. priečinok pomocou antivírusového programu nainštalovaného v zariadení.

Malé upozornenie – škodlivý softvér je možné získať aj tým, že dovolíme niekomu (rodinnému príslušníkovi, známemu,...) prihlásiť sa cez naše zariadenie do jeho e-mailového účtu, na sociálnu sieť alebo na inú službu a ten klikne na neznámy odkaz alebo otvorí prílohu.

Upozornenie
Ak je na návšteve priateľ/niekto z rodiny a opýta sa, či si môže **pozrieť e-maily** na našom zariadení, odpovieme: **„Ano, ale neklikaj na žiadne odkazy a neotváraj prílohu."**

Pre takéto prípady je vhodné mať na svojom zariadení **hosťovské konto**, ktoré má výraznejšie obmedzené spúšťanie programov a ukladanie súborov.

3.3. Správne používanie

Aj samotný používateľ digitálneho zariadenia musí dbať na jeho správne používanie, aby tým zabránil nežiaducim problémom. Uvádzame niekoľko tipov na správne používanie:

1. **Ak sa na digitálnom zariadení (hlavne cudzom) prihlásime na webovú službu, do aplikácie, tak je dôležité sa aj korektne odhlásiť po ukončení svojej práce** (kapitola 5.4).
   Výnimkou je, keď máme zariadenie iba pre seba – vlastný telefón/tablet, vlastné konto na rodinnom počítači/notebooku,... . Ak máme vlastné konto, nemusíme sa odhlasovať zo služieb, ale máme sa odhlásiť z konta alebo aspoň uzamknúť obrazovku. Na tabletoch a mobilných telefónoch sa odhlasujeme stlačením bočného tlačidla. Uzamknutie obrazovky počítača so systémom Windows je bežný spôsob ochrany bezpečnosti a súkromia počítača (klávesy Windows + L).
2. **Bezpečná práca s webom** (kapitola 5).
3. **Bezpečné používanie e-mailu a sociálnych sietí** (kapitola 6).
4. **Neinštalovať programy a súbory z nedôveryhodných zdrojov** (ide najmä o nelegálny softvér a amatérske produkty). Tieto programy bývajú často spojené s aplikáciami, ktoré môžu ohroziť bezpečnosť práce na počítači.
5. **Nezadávať prihlasovacie údaje tak, aby to niekto mohol odpozorovať.**
   Shoulder surfing (=pozeranie ponad plece) je metóda odpozerania (nielen) prihlasovacích údajov. Pôvodne pri tom útočník stál za používateľom a sledoval ponad plece napadnutej osoby, čo píše (napr. informácie do súkromného listu, prihlasovacie údaje do e-mailu, aplikácie alebo počítača). V súčasnosti sa využívajú rafinovanejšie metódy. Útočník navodí situáciu, kedy obeť použije svoje prihlasovacie údaje (prihlásenie do sociálnej siete, internetbankingu a pod.) a tie „odsleduje“, buď klasicky pozeraním ponad plece alebo pomocou elektronických prostriedkov ako sú webové kamery, miniatúrne kamery a pod. (pozor na odomykanie mobilu v autobuse cez PIN alebo grafický vzor, zadávanie hesla v prítomnosti inej osoby,...).

6. Vo verejne dostupných priestoroch dávať pozor, kde sú kamery – možnosť odpozorovania zadania hesla, PIN-u.

3.4. Pravidelné zálohovanie

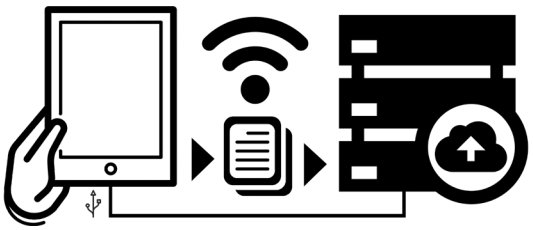
Pre **zabezpečenie dostupnosti údajov** v prípade zlyhania (porucha, neoprávnený zásah, vyššia moc a pod.) digitálnych zariadení (tablet, mobil, počítač, notebook alebo pamäťové médium) nám pomôže hlavne **zálohovanie**.

V prípade pravidelných záloh s dostatočnou frekvenciou je možné pri poruche systému alebo po strate údajov minimalizovať straty spôsobené nedostupnosťou, či dokonca stratou údajov, prípadne nedostupnosťou niektorých služieb.
Príklad: *Všetky rodinné fotografie ukladáme na jedno zariadenie (tablet, mobil, pevný disk, USB kľúč,...). V prípade neopraviteľnej poruchy tohto zariadenia strácame všetky „spomienky".*

Zálohovanie je vytváranie kópie potrebných údajov na iné médiá klasickým kopírovaním alebo pomocou špecializovaného softvéru. V prípade zálohovania (hlavne v organizáciách) by mala platiť **zásada 3-2-1**. Urobíme 3 kópie minimálne na 2 rôzne médiá a jedna kópia by mala byť mimo budovu, kde sú prvé dve.
V domácich podmienkach sa zvyknú robiť jednoduché kópie súborov, najmä fotografií a videí, kopírovaním do iného priečinka, na externé pamäťové médium (napr. externý pevný disk, USB kľúč), napaľovaním na CD-R alebo DVD-R médiá alebo uložením do cloudu (nutné internetové pripojenie).

V prípade, ak už nastane krízová situácia, je dobré mať zálohu údajov vždy k dispozícii. Pravidelná záloha údajov je dôležitý bod ochrany údajov. Pravidelnosť zálohovania si musí nastaviť každý užívateľ podľa svojich preferencií. Používateľa to väčšinou obťažuje, ale veľmi to ocení v prípade straty alebo vážneho poškodenia zariadenia.

Veľmi často sa podceňuje zálohovanie prenosných zariadení (tabletov, mobilných telefónov). Zálohy týchto zariadení nemusíme robiť denne, ale s intenzitou ich používania by mala rásť frekvencia ich zálohovania.



Obrázok 23 – Kópia dát

Zariadenia typu tablet a mobilný telefón využívajú služby pre zálohovanie cez špeciálne konto od výrobcu (je na rozhodnutí používateľa, či takúto službu využije). Cez toto konto je možné zálohovať kontakty, fotografie, správy, nastavenia aplikácií aj niektoré iné súbory. Alternatívou je, v zariadeniach s operačným systémom Android, využívať na zálohu tzv. „google konto“.

3.5. Bezpečné vymazanie a likvidácia

Veľmi často dochádza k **úniku informácií** práve neopatrným zaobchádzaním s nepotrebnými pamäťovými médiami. Ak z nejakého dôvodu potrebujeme vyradiť pamäťové médium (napr. pri výmene pamäťového média za väčšie, pokazené alebo poškodené médium a pod.), mali by sme zabezpečiť, aby sa z nich nedali údaje prečítať, ani obnoviť. Veľmi často sa zabúda na vyradené zariadenia s pamäťovými médiami, ako sú tablety, mobilné telefóny, ale aj počítače a notebooky. Pri neodbornej likvidácii uložených údajov ich môže skúsený špecialista pomerne jednoducho obnoviť, a tak získať aj citlivé údaje, ktoré boli predtým na nich uložené (rôzne doklady, výpisy z účtu, neverejné fotky a videá, citlivé údaje,...).

Je rozdiel medzi obyčajným **vymazaním údajov a trvalým odstránením**.

Vždy, keď **zmažeme** súbor alebo aj priečinok vo svojom zariadení, dôjde iba k zmazaniu cesty k týmto dátam. Preto možno obnoviť mnohé omylom zmazané fotky, dokumenty, ale napr. z mobilných telefónov spätne vytiahnuť aj správy, kontakty a osobné údaje.

Obrázok 24 – Vymazanie

Na **trvalú likvidáciu** údajov sa používajú rôzne postupy, ktoré sa líšia podľa typu pamäťového média, požadovaného stupňa utajenia, prípadne či sa pamäťové médium má ešte dať použiť.

Asi najznámejšia forma fyzickej likvidácie pamäťových médií je **skartácia**, kedy je médium rozdelené na množstvo malých častí. V domácich alebo kancelárskych podmienkach je použiteľná na pamäťové média ako papier, platobné karty, CD, DVD a Blu-ray médiá, diskety.
Na skartáciu pevnejších médií, ako sú USB kľúče, pevné disky, mobilné telefóny, tablety a pod., sú potrebné priemyslové skartovačky, ktorými disponujú firmy špecializujúce sa na likvidáciu pamäťových médií. Čím je požadovaný vyšší stupeň utajenia, tým menšie kúsky majú vzniknúť po skartácii. Dobré skartovačky rozdelia vložené predmety na časti do veľkosti cca 5 mm.

Demagnetizácia (angl. degaussing) je metóda, ktorá je použiteľná na odstránenie údajov na všetkých pamäťových médiách, ktoré využívajú magnetický záznam.

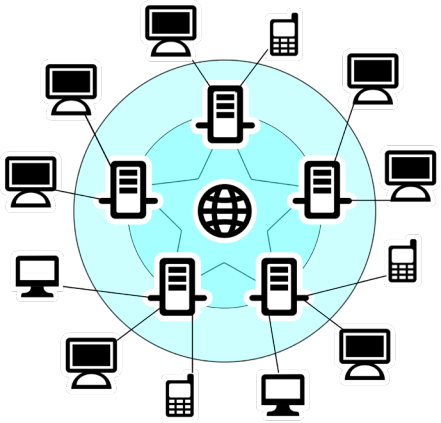
Softvérové prostriedky na likvidáciu údajov využívajú mnohonásobný prepis jednotlivých oblastí na záznamovom médiu a tým úplne zlikvidujú pôvodne uložené údaje. Problémom môžu byť pamäťové médiá, u ktorých nemáme priamy prístup do jednotlivých oblastí, resp. pamäťových buniek (mobilné zariadenia ako telefóny a tablety, niektoré novšie SSD disky a pod.), u nich zostáva jedine možnosť fyzickej likvidácie zariadenia. Špeciálnou časťou sú vzdialené úložiská, kde garantujú bezpečné zmazanie prevádzkovatelia.

4. Bezpečnosť počítačových sietí

Počítačová sieť je systém vzájomne prepojených a spolupracujúcich počítačov, medzi ktorými môžeme pohodlne a rýchlo prenášať údaje, zdieľať prostriedky (napr. tlačiareň) a komunikovať medzi používateľmi.

Význam počítačových sietí:

- zdieľanie údajov (spolupráca viacerých používateľov),
- zdieľanie prostriedkov (napr. tlačiarní, diskov),
- zvýšenie spoľahlivosti systému (v prípade poruchy je možné jeden zdieľaný prostriedok nahradiť iným).

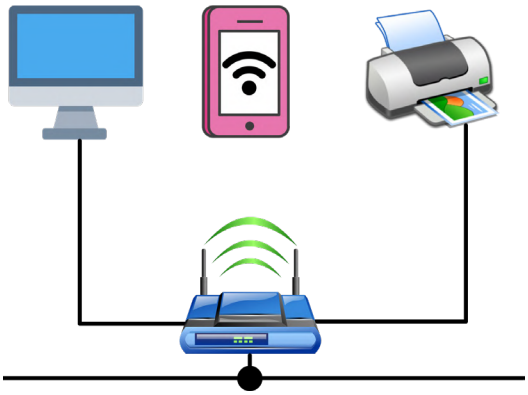


Obrázok 25 – Internet

Pre domáce použitie je možné vytvoriť malú osobnú sieť, v ktorej sú prepojené viaceré zariadenia (počítač, mobil, tablet, tlačiareň, ...). Častejšie samozrejme potrebujeme pripojiť svoje zariadenia na **internet**, čo je počítačová sieť, ktorá vznikla prepojením rôznych menších či väčších počítačových sietí.

Pripojenie na internet je možné realizovať viacerými technológiami:

1. káblové pripojenie (zväčša pre počítače),
2. bezdrôtové pripojenie – Wi-Fi (mobilné zariadenia),
3. dátové pripojenie (zväčša pre tablety a mobilné telefóny).



Obrázok 26 – Pripojenie na internet

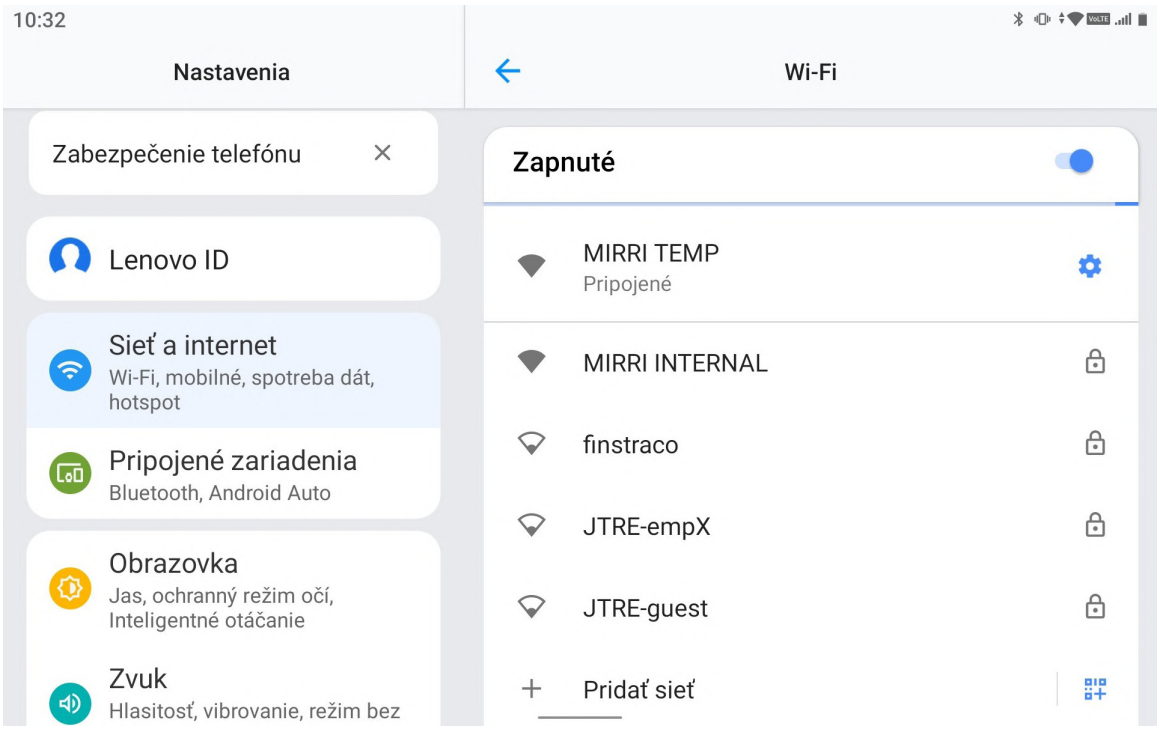
Cez bezdrôtové pripojenie môžu byť pripojené aj ďalšie zariadenia ako tlačiarne či inteligentné domáce spotrebiče.

Ak **nemáme tablet alebo počítač pripojený do počítačovej siete**, útok naň môže byť zrealizovaný len fyzickým kontaktom.

Útočník sa dostane fyzicky k zariadeniu alebo používateľ donesie škodlivý softvér na pamäťovom médiu (napr. USB kľúč, pamäťová karta). Únik informácií z takého zariadenia bez spolupráce používateľa (nemusí to byť vedomá spolupráca - strata či odcudzenie) je prakticky nemožný.

Ak **zariadenie pripojíme do počítačovej siete**, vystavujeme ho tým možným útokom po sieti (najmä po pripojení do **neznámej** alebo **verejnej** siete, napr. v obchodných centrách, hoteloch, ...), ktoré sa väčšinou snažia zneužiť zraniteľnosť nejakej sieťovej služby, prípadne využiť zle nastavenú sieťovú službu, a tak získať neoprávnený prístup k informáciám uloženým v tablete, telefóne alebo počítači, nainštalovať škodlivý softvér alebo ovládnuť celé zariadenie. Rapídne sa tak zvyšuje možnosť úniku informácií a dát.

Komunikáciu realizovanú pomocou bezdrôtovej (WiFi) siete je ľahké odpočúvať. Na rozdiel od (drôtovej) siete sa totiž netreba nikam pripájať, stačí byť v dosahu signálu.



Obrázok 27 – Wi-Fi siete
(*vzhľad okna s Wi-Fi sieťami v Nastaveniach tabletu a obrazovka na pozadí v našom tablete sa môžu od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému a osobných nastavení)

Na **ochranu bezdrôtovej siete** sa využívajú viaceré typy **zabezpečenia**:

- prístup k sieti chrániť heslom,
- komunikáciu prostredníctvom siete šifrovať,
- obmedziť prístup do siete napr. filtrovaním zariadení, ktoré majú právo sa pripojiť (cez filter fyzických adries zariadenia [MAC], keďže každé zariadenie má jedinečnú MAC adresu). Je to iba ochrana prístupu, nechráni proti samotnému odpočúvaniu.

Ak sa už **rozhodneme pripojiť so svojim zariadením na verejne prístupnú Wi-Fi sieť**, napr. v snahe ušetriť mobilné dáta, skúsme sa držať nasledujúcich zásad, ktoré zvýšia pravdepodobnosť, že naše údaje nezneužije tretia strana:

- pripájajme sa iba na stránky, ktoré začínajú označením https://, pretože takáto komunikácia je bezpečnejšia,
- majme svoje zariadenie vždy aktualizované (operačný systém, softvér, aplikácie),
- používajme iba overené aplikácie, t.j. sťahujme ich iba z overených zdrojov,
- používajme aktualizovaný antivírusový program,
- vypínajme Wi-Fi vždy, keď ju nepoužívame,
- odhlasujme sa zo svojich účtov.

Upozornenie

Byť opatrný sa vo virtuálnom priestore vypláca.

Úloha 9

Zobrazte **dostupné Wi-Fi siete** na zariadení, na ktorom pracujete, vyberte jednu z nich a zistite:

Názov Wi-Fi siete: .....

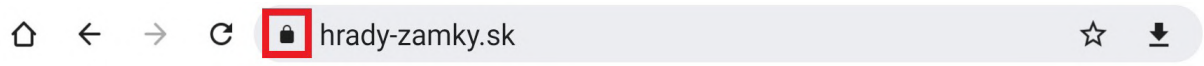
Zabezpečená: ☐ Áno ☐ Nie

5. Bezpečná práca s webom

Internet je zdrojom a archívom množstva informácii. Vlastne na ňom nájdeme takmer ľubovoľnú informáciu, ktorú hľadáme. Stačí sa len správne pýtať.

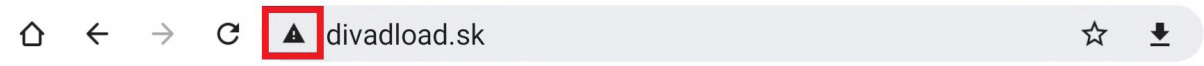
5.1. Nie všetko, čo navštevujeme, je bezpečné

Občas pri hľadaní informácii sa dostaneme na stránky, o ktorých bezpečnosti je možné pochybovať. Ak navštevujeme webové stránky, je dobré venovať pozornosť, či stránky sú bezpečné. Veľmi jednoduchý spôsob zistenia zabezpečenej webovej stránky, bez hlbších teoretických vedomostí, je všímať si riadok adresy webovej stránky.



Obrázok 28 – Riadok adresy pre zabezpečenú webovú stránku

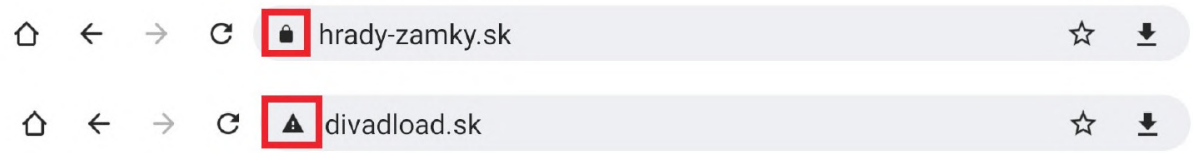
Písmenká **https** označujú súbor pravidiel (protokol), ktorými sa riadi prenos dokumentov na webe. Https je zabezpečený protokol, ktorý komunikáciu **šifruje**. Menej bezpečný je základný protokol **http** bez šifrovanej komunikácie. Tento protokol nemusí byť zobrazený.



Obrázok 29 – Riadok adresy pre nezabezpečenú webovú stránku

Dnešné prehliadače v zariadeniach (tablety, mobilné telefóny, počítače) zobrazujú adresu webových stránok aj bez protokolu. Na paneli s adresou je automaticky skrytý protokol a ostáva iba ikona zámku a webová adresa, resp. pri nezabezpečenej stránke je pridaný text „nezabezpečené“ alebo informačná ikona s výkričníkom. Spoločnosti, ktoré vytvárajú aplikácie na prehliadanie webových stránok sa v posledných rokoch viac sústreďujú na používanie protokolu https a bezpečnejší pohyb používateľov na internete. Šifrované stránky (s protokolom https) sa už stali

štandardom a prehliadače už nebudú zobrazovať, či je web, ktorý navštevujeme zabezpečený – bude to akousi povinnosťou. Indikátor sa zobrazí iba pri návšteve nezabezpečeného webu.



Obrázok 30 – Riadok adresy pre webovú stránku bez zobrazenia protokolu na tablete

Je potrebné si uvedomiť, že zabezpečená webová stránka dáva informáciu iba o tom, že pripojenie na danú stránku je zabezpečené. Nič nehovorí o tom, či je stránka (jej obsah) dôveryhodná alebo nie.

Upozornenie

Všetky aktivity, pri ktorých sa vyžaduje **overenie** (autentifikácia) **používateľa**, by sa mali vykonávať iba na **zabezpečených dôveryhodných webových stránkach**. Patria sem najmä prístup k elektronickej pošte, online nákupy, finančné transakcie, práca v informačných systémoch, komunikácia na sociálnej sieti a pod.

Úloha 10

V prehliadači zariadenia zadajte do adresného riadka webovú adresu **www.divadlo.sk**

Zistite, či je stránka zabezpečená: ☐ Áno ☐ Nie

V prehliadači zariadenia zadajte do adresného riadka webovú adresu **www.krizovkarsky-raj.sk**

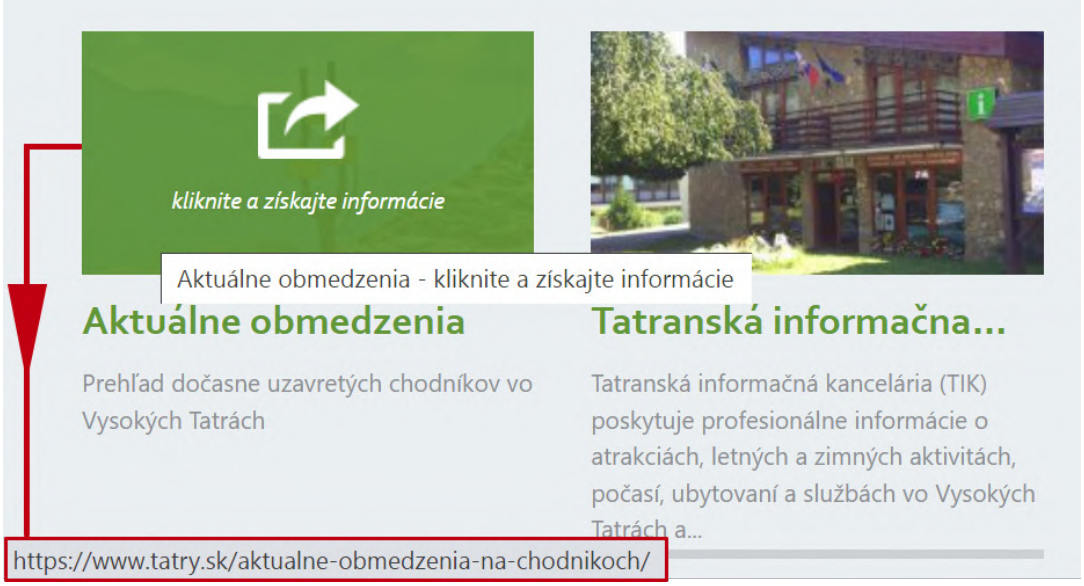
Zistite, či je stránka zabezpečená: ☐ Áno ☐ Nie

5.2. Nie všetko, na čo klikáme, je bezpečné

Bezpečnosť na internete je podmienená psychikou, a to najmä pocitom bezpečia. Každý útočník chce, aby sa užívateľ, ktorého chce napadnúť, cítil pohodlne a mal dôveru voči zdrojom, ktoré používa/sťahuje. Najväčšou hrozbou je naivita, s ktorou používateľ internet využíva a hlavne myšlienka, že jemu sa nemôže nič zlé stať.

Pred každým kliknutím si treba prečítať, na čo klikáme. Ak sú to bežné navigačné prvky, ako tlačidlá vo webovom prehliadači, kliknutie je bezpečné. Ak nám, ale príde výzva s odkazom na neznámu stránku, určite neklikať.

Pred kliknutím na odkaz si skontrolujme v pravom dolnom rohu prehliadača adresu, na ktorú budeme presmerovaný. Pozor je potrebné dávať aj na drobné preklepy v adrese.

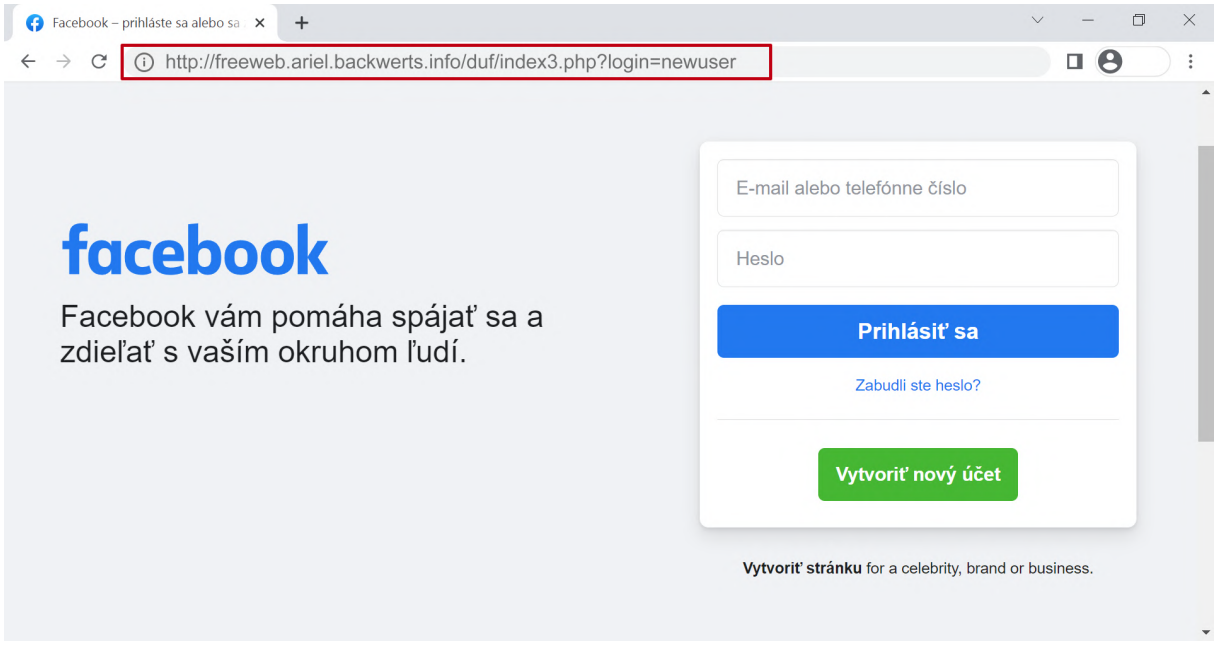


Obrázok 31 – Kontrola webovej adresy odkazu

V prípade, že sa na stránkach zobrazujú rôzne reklamy, neklikáme na nich, nakoľko môžu obsahovať škodlivý softvér, ktorý by sa mohol uložiť bez nášho vedomého pričinenia do zariadenia.

Jednou z hrozieb pri návšteve webových stránok, hlavne takých, kde zadávame citlivé údaje (napr. prihlasovacie meno a heslo, údaje k bankomatovej karte,...) je tzv. **pharming**. Ide o podvodnú techniku, keď páchateľ ovládne resp. presmeru-

je skutočné webové stránky inštitúcie (napr. stránky banky, sociálnych sietí, platobnej brány,...) na ním vytvorené falošné/podvodné stránky. Dizajn stránok je podobný alebo takmer rovnaký ako dizajn oficiálnej stránky inštitúcie. Návštevník stránky preto ani nemusí zistiť, že má otvorenú falošnú internetovú stránku. Rozdiel objavíme v detailoch. Napríklad v inom písmene v adrese webovej stránky (napr. www.mojabankasl.sk namiesto www.mojabankasI.sk – zámena podobných písmen malého L a veľkého I) alebo v odlišnej doméne (.com namiesto .sk). Táto taktika potom navedie nič netušiacu obeť, aby zadala citlivé informácie, akými je číslo bankového účtu, heslo, prístupové údaje do firmy, k platobnej karte alebo k platobnej bráne. Vyplnené údaje následne využije útočník vo svoj prospech.



Obrázok 32 – Príklad pharmingu - falošná stránka na prihlásenie na sociálnu sieť

Upozornenie

Všímajte si aj **detaily** vo webových adresách stránok, hlavne tých, kde plánujete zadávať citlivé údaje:

- internetbanking vašej banky,
- nákup v internetových predajniach,
- stránky zdravotných poisťovní a štátnych inštitúcií.

5.3. Registrácia na rôzne služby

Na webových stránkach sa často prihlasujeme cez portály na rôzne služby, napr. do e-mailovej schránky, do internetbankingu, do poisťovne, na sociálnu sieť, do internetového obchodu,... Do väčšiny služieb sa musíme najprv registrovať. Pri **registrácii** je veľmi dôležité **prečítať si všeobecno-obchodné podmienky**, aby sme presne vedeli, za akých podmienok budeme danú službu využívať. Ak si ich neprečítame, môže sa stať, že budeme nemilo prekvapení, ako tomu bolo napr. pri kauze spoplatnených stránok. Prevádzkovateľ služby v podmienkach uviedol, že služba je spoplatnená a po registrácii vystavil faktúru. Majitelia týchto stránok sa neštítia ani zastrašovania – vyhrážajú sa súdom a exekúciou (https://www.cas.sk/clanok/359836/spoplatnene-registracie-na-internete-co-ked-pride-necaka-na-faktura/).

Janko Hraško
Bolebruch 123
Košice

Vec: Posledná upomienka

Neuhradená faktúra č.:4403082
Dátum: 13. január 2010

pri našej opätovnej kontrole prijatých platieb bolo zistené, že Vaša faktúra č. 4403082 zo dňa 02.11.2009 v sume 60,00 EUR nebola aj napriek **1. a 2. upomienke** do dnešného dňa uhradená. Týmto Vás bezprostredne žiadame o uhradenie pohľadávky s udaním variabilného symbolu na náš bankový účet v lehote **do 7 pracovných dní** .

Číslo	Názov	Množstvo	Cena/MJ	Spolu
0001	**basne-portal.sk**	1,000	60,00	60,00 €
	Uhradené ku dňu splatnosti			0,00 €
	Úroky z omeškania			1,00 €
	(01.09.2009 - 01.09.2010)		**Celkom k úhrade**	**61,00 €**

Informácie:
Faktúra, ktorá Vám bola vystavená, sa vzťahuje na zmluvu o poskytnutí služby za sprístupnenie online databázy. K využívaniu tejto služby je nutná registrácia na našich portáloch, pod udaním Vášho mena, priezviska, bydliska a emailovej adresy. Ďalej ste potvrdili, že ste sa so Všeobecnými obchodnými a užívateľskými podmienkami, všeobecnými užívateľskými informáciami oboznámili, akceptovali ich a na základe tejto akceptácie ste dostali prístup na kompletnú databázu. Možnosť odstúpiť od zmluvy v zákonnej lehote do dvoch týždňov od uzavretia zmluvy ste nevyužili.

Týmto Vás žiadame o úhradu horeuvedenej pohľadávky najneskôr do

20.01.2010

prevodom na náš bankový účet. Pri prevode nezabudnite zadať správny variabilný symbol 4403082

Bankové spojenie: ČSOB a.s., č.ú. 4009015266 / 7500.

Pri platbe zo zahraničia: IBAN: SK98 7500 0000 0040 0901 5266 SWIFT: CEKOSKBX.

V prípade, že v lehote do 7 pracovných dní nebude Vaša pohľadávka uhradená, bude vymáhaním bez akéhokoľvek ďalšieho upozornenia poverená právnická kancelária a následne bude začaté **exekučné konanie** voči Vašej osobe. Týmto Vám vzniknú ďalšie náklady. Vezmite ďalej na vedomie, že sa nachádzate v omeškaní a v prípade, že Vaša pohľadávka nebude uhradená ani v poslednej nami stanovenej lehote, bude táto vymáhaná za celé obdobie platnosti tejto zmluvy, t.j. za 24 mesiacov.

Pro Content s.r.o.
Hronského 7

SK- 951 41 Lužianky

IČO: 44 840 705
DIČ: 2022848377

Firma je neplatca DPH.

Linka zákazníkom

+ 421 (0) 944 442 548 *
+ 421 (0) 907 271 668 *

* po-pia 9.00h – 17.00h

Email

support@pro-content.eu

Bankové spojenie

ČSOB a.s.
č.ú.: 4009015266 / 7500

Pri prevode zo zahraničia
IBAN:
SK98 7500 0000 0040 0901 5266

SWIFT: CEKOSKBX

Obrázok 33 – Kauza spoplatnených stránok - upomienka

Kauza spoplatnených stránok

MÁJ 16, 2011 | AKTUALITY

Stránky **www.sampionat.sk**, **www.ms-hokej-2011.sk**, **www.hokej-2011.sk** a **www.sampionat-2011.sk** majú opäť rafinované všeobecno-obchodné podmienky, neregistrujte sa tu.

Pozrite si **http://video.markiza.sk/archiv-tv-markiza/televizne-noviny/62095** a **http://vat.pravda.sk/pozor-60-eurove-stranky-su-spat-ludi-lakaju-na-majstrovstva-p41-/sk_vkom.asp?c=A110422_125239_sk_vkom_p35**.

Upozorňujeme spotrebiteľov aj na ďalšie rafinované webové stránky spoločnosti Online Investment Group Ltd. **www.sale4u.sk, www.knihovna.sk, www.hraj-to.sk, www.skvelapozicka.com, www.stahujme.sk**… Neregistrujte sa tu, ak nechcete dostať faktúru za využitie služieb a informácií, ktoré sa dozviete na iných stránkach zdarma. Poznávacím znamením je, že prístup k inde voľne a zdarma dostupným informáciám je na týchto stránkach podmienený vyplnením osobných údajov do registračného formulára. Pozorne si prezrite celú stránku. **Po odkliknutí VSTÚPTE na úvodnej stránke si pod registračným formulárom prečítajte celý text v okne pod tlačidlom REGISTROVAŤ. Takisto si prečítajte celé všeobecno-obchodné a užívateľské podmienky. Až potom sa rozhodnite, či sa tu zaregistrujete.**

Ak ste sa registrovali, pošlite spoločnosti odstúpenie od zmluvy – **koncept odstupenia od zmluvy uzatvorenej na dialku** – a uložte si ho, aby ste to vedeli preukázať. V našom vzore nájdete dve alternatívy – pre tých, ktorí sa sami neregistrovali a na stránke vôbec

Obrázok 34 – Kauza spoplatnených stránok – informácia v médiách

5.4. Bezpečné odhlásenie

V prípade prihlasovania sa do svojich účtov (e-mail, sociálne siete, internetbanking,...) na verejných počítačoch (internetové kaviarne, počítačové miestnosti v školách,...) alebo u známych, t. j. z cudzích zariadení, je veľmi dôležité dbať na **korektné odhlásenia sa z účtu**. V žiadnom prípade nezatvárame webovú stránku, na ktorej sme boli prihlásení, len zatvorením prehliadača cez „krížik“ ☒ v pravom hornom rohu (štandardne pre počítače) alebo zatvorením aplikácie v prípade tabletov a mobilných telefónov, pretože stále ostávame prihlásení k službe a tá môže byť zneužitá. Tiež je potrebné dať pozor na to, či nie je nastavené automatické ukladanie hesla.

6. Bezpečnosť pri komunikácii

V tejto časti sa budeme venovať bezpečnosti dvoch najrozšírenejších spôsobov komunikácie na internete – elektronickej pošte a komunikácii cez sociálne siete.

6.1. Elektronická pošta (E-mail)

Elektronická pošta vznikla ešte pred vznikom internetu v druhej polovici šesťdesiatych rokov. Je to tzv. off-line komunikácia, ktorá funguje podobne ako klasická pošta. Odosielateľ odovzdá správu svojmu poštovému serveru („podacia pošta“), ten ju podľa adresy prijímateľa nasmeruje cez sieť poštových serverov až na server, na ktorom má príjemca správy zriadenú schránku („doručovacia pošta“), a ten mu ju doručí do jeho schránky.

Obrázok 35 – E-mail

Príjemca si musí schránku otvoriť, aby videl, či má v nej nejaké správy.
Elektronická pošta je veľmi používanou službou na internete, ktorá je určená pre rýchlu písomnú komunikáciu. Okrem samotných textových správ je možné prostredníctvom elektronickej pošty súčasne prenášať aj ľubovoľné súbory, ako sú obrázky, fotografie, formátovaný text v samostatnom súbore, zvukové, či video záznamy. Pri používaní elektronickej pošty sme limitovaní len objemom prenášaných dát.

Elektronická pošta predstavuje stále zaujímavý cieľ pre kybernetických útočníkov, preto pri práci s ňou musíme dodržiavať bezpečnostné pravidlá.

Najväčším nebezpečenstvom sú nevyžiadané e-maily – **SPAM**. Spam šíri nevyžiadanú reklamu, falošné správy (hoax) alebo škodlivý softvér.

Reklama – ponuky zasielané prostredníctvom e-mailu sú jednou z foriem internetovej reklamy. Ich hlavnou výhodou sú takmer nulové náklady, priame a okamžité doručenie adresátovi. Reklama zasielaná e-mailom je sama o sebe legitímna, ak užívateľ má záujem získavať reklamné informácie z určitej oblasti. Často si však nepraje, aby mu reklama bola zasielaná, ale napriek tomu sa tak deje. V takomto prípade sa reklamný e mail stáva zároveň nevyžiadanou poštou – spamom.

Fáma – hoax – je internetom (veľmi často cez elektronickú poštu) masovo šírená správa. Ide buď o falošnú poplašnú správu, žart alebo mystifikáciu – správa sama o sebe sa nezakladá na pravde. Medzi často rozšírené fámy patria správy, ktoré upozorňujú na neexistujúce nebezpečenstvá alebo sľubujú rýchle zbohatnutie. Pri niektorých poplašných správach sa snažia autori zaistiť čo najväčšie rozšírenie správy výzvami na ďalšie preposielanie pod rôznymi zámienkami. Časté sú fámy o mobilných telefónoch, falošné alebo neaktuálne prosby o pomoc, reťazové listy šťastia, ponuky na veľké čiastky peňazí zo zahraničia. V zásade platí pravidlo, že pokiaľ správa obsahuje výzvu k ďalšiemu hromadnému rozosielaniu, ide s najväčšou pravdepodobnosťou o hoax. Na internete existuje niekoľko špecializovaných stránok s databázou fám (hoaxov), na ktorých si vieme overiť pravosť takejto správy predtým, ako ju prepošleme ďalej (napr. hoax.sk, www.facebook.com/hoaxPZ/, hoax.cz).

Obrázok 36 – Ukážky hoaxov zo stránky hoax.cz

Ak zistíme, že ide o hoax, mali by sme **slušne upozorniť iba odosielateľa** (hlavne ak to je niekto známy – z rodiny, priateľ,...), aby správu nešíril a **poslať mu prípadne odkaz na webovú stránku hoaxu**.

Ako môže hoax škodiť:

- obťažuje príjemcov (zaplňovanie e-mailovej schránky),
- nebezpečné rady,
- nadbytočné zaťažovanie liniek a serverov,
- strata dôveryhodnosti odosielateľa (pri odosielaní hoaxov z pracovnej adresy je možné poškodiť aj zamestnávateľa),
- prezradenie dôverných informácií (nepoužívanie skrytej kópie pri posielaní, zoznam adries môže byť odchytený a zneužitý na rozposielanie spamu),
- nekritický príjem informácií a ich ďalšie šírenie,
- psychická manipulácia (vzbudzujú pocit ohrozenia, viny,...),
- posilňovanie poverčivosti (reťazové listy šťastia).

Úloha 11

Na webovej stránke **www.hoax.cz** v časti Aktuality zistite, ktorý hoax bol **druhý v poradí** medzi TopTen českých hoaxov a reťazových správ za konkrétne obdobie (konkrétny mesiac).

Názov hoaxu: .....

Mesiac: .....

Upozornenie

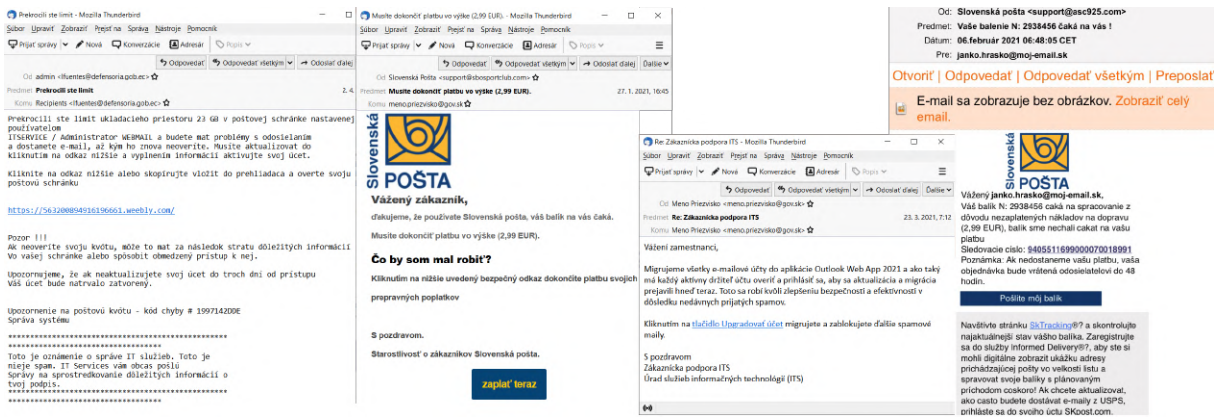
Vždy si **skontrolujte masovo rozposielanú správu**, ktorá obsahuje ponuky, prosby, informácie o zdraví,... aj keď príde od známeho.

Podvodná správa – taká správa, ktorá sa snaží uviesť príjemcu do omylu a tým získať pre jej tvorcu nejaký prospech. Zámerne sme použili výraz tvorca správy, pretože odosielateľ (aspoň ten, ktorý je uvedený v správe) je spravidla falošný. Podvodné správy veľmi často obsahujú škodlivý softvér v prílohách, prípadne sa snažia získať prihlasovacie údaje (tzv. **phishing**).

Phishing (z anglického password fishing – doslova rybolov hesiel) je činnosť, pri ktorej sa podvodník snaží vylákať od používateľa **prístupové údaje**, napr. do elektronickej pošty, do internetbankingu, k platobnej karte.

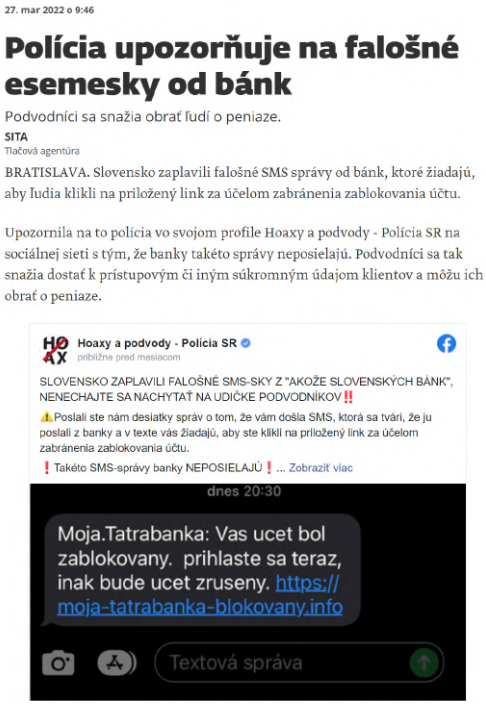
Väčšinou sa takéto podvodné správy snažia dostať príjemcu do neštandardnej situácie. Napr. banka oznámi zablokovanie bankového účtu, správca servera chce riešiť problém s e-mailovým kontom, organizátor lotérie oznamuje výhru a chce ju odovzdať, nešťastná vdova žiada o pomoc pri prevode dedičstva z nejakej rozvojovej krajiny do Európy a pod. Pri snahe o riešenie takejto situácie sa pokúsia získať prístupové údaje buď priamo vyžiadaním v správe (správca servera potrebuje na riešenie problému s e-mailovým kontom prihlasovacie údaje) alebo odkazom na falošnú stránku (aby sme sa hneď prihlásili do banky). V prípade, že zareagujeme na správu, napr. o výhre, postupne napíšu, čo všetko potrebujú na odovzdanie výhry a nakoniec môžu žiadať buď prihlasovacie údaje do banky alebo úhradu nejakého poplatku (napr. dane z výhry, aby mohli výhru vyplatiť).

Pokusy o phishing je možné nahlásiť organizáciám, v ktorých mene útočník vystupuje.



Obrázok 37 – Ukážky podvodných e-mailov

Okrem phishingu je veľmi častý aj tzv. **vishing**, čo je podvodný postup s využitím telefonického rozhovoru alebo sms správy, pomocou ktorého sa útočník snaží získať citlivé údaje (osobné údaje, prístupové heslá do Internetbankingu, čísla platobných kariet a pod.).


27. mar 2022 o 9:46

Polícia upozorňuje na falošné esemesky od bánk

Podvodníci sa snažia obrať ľudí o peniaze.

SITA
Tlačová agentúra

BRATISLAVA. Slovensko zaplavili falošné SMS správy od bánk, ktoré žiadajú, aby ľudia klikli na priložený link za účelom zabránenia zablokovania účtu.

Upozornila na to polícia vo svojom profile Hoaxy a podvody - Polícia SR na sociálnej sieti s tým, že banky takéto správy neposielajú. Podvodníci sa tak snažia dostať k prístupovým či iným súkromným údajom klientov a môžu ich obrať o peniaze.

Obrázok 38 – Príklad vishingu

Zamyslime sa predtým, ako konáme: Ignorujme e-maily alebo komunikácie, ktoré vytvárajú pocit naliehavosti a vyžadujú, aby sme reagovali na krízu, ako napríklad problém s bankovým účtom alebo daňami.
Pri tomto type správ pravdepodobne ide o podvod.

Ak máme pochybnosti o správe, vyhoďme ju: Kliknutím na odkazy v e-mailoch je často spôsobom, akým útočníci získavajú prístup k našim osobným údajom. Ak e-mail vyzerá divne, aj keď poznáme osobu, ktorá ho poslala, najlepšie je odstrániť ho. Prípadne osloviť odosielateľa a opýtať sa ho na danú správu.

Ďalšie **typy podvodných e-mailov** sú také, ktorých účelom je zavedenie **škodlivého softvéru** do počítača príjemcu. Typicky to bývajú správy, v ktorých je príjemca upozornený na kritickú chybu nejakého softvéru, a výrobca mu posiela **odkaz** na aktualizáciu, ktorá túto chybu odstráni. Namiesto aktualizácie si príjemca správy nainštaluje škodlivý softvér. Inou možnosťou je poslanie správy s **infikovanou prílohou**. Z tohto dôvodu sa neodporúča nastavenie automatického otvárania príloh, keď otvorením správy sa otvorí príloha, čím sa spustí škodlivý softvér a nainfikuje počítač.

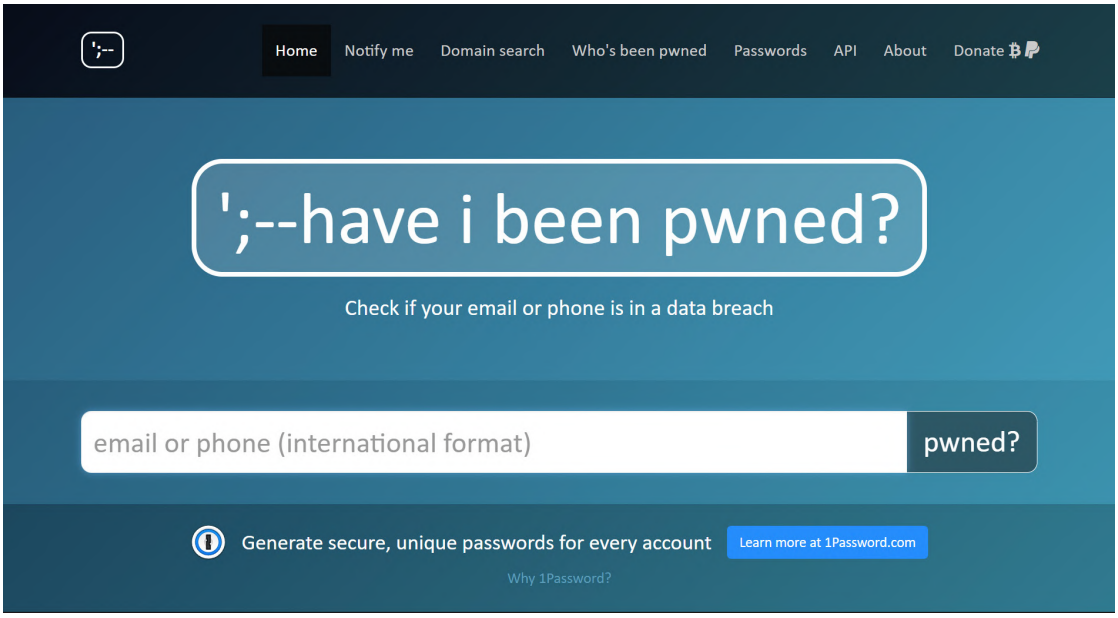
Upozornenie

Nikdy neposkytujte citlivé údaje vo forme odpovede na e-mail, aj keď sa zdá, že prišiel od známej dôveryhodnej inštitúcie (napr. banky).

Nikdy neklikajte na odkazy v podozrivých e-mailoch.

Nikdy neotvárajte prílohy nevyžiadaných e-mailových správ.

Napriek opatrnosti pri práci s elektronickou poštou je možné, že účet bol skompromitovaný pri úniku osobných údajov. Stránka **HIBP (Have I Been Pwned) – https://haveibeenpwned.com** bola vytvorená ako bezplatný zdroj pre každého, kto by chcel zistiť, či jeho účet mohol byť vystavený tomuto riziku pri úniku údajov.



Obrázok 39 – Over svoj e-mail

Úloha 9

Na webovej stránke https://haveibeenpwned.com/ overte, či vaša e-mailová adresa bola skompromitovaná.

☐ Áno ☐ Nie

6.2. Sociálne siete

Sociálna sieť je sieťová služba prístupná cez webovú stránku alebo aplikáciu určenú na nadväzovanie a udržiavanie kontaktov medzi ľuďmi. Každý používateľ si vytvorí vlastný profil, v ktorom napíše o sebe základné informácie.

Obrázok 40 – Sociálne siete

Na základe týchto informácií sa nadväzujú vzťahy medzi používateľmi, ktorí sa spájajú do skupín. Vzájomnými prepojeniami používateľov a skupín vzniká sieť vzťahov. Nevýhodou sociálnych sietí je fakt, že používatelia nemusia do svojho profilu vložiť pravdivé informácie, a je to takmer nemožné zistiť.
Príklady sociálnych sietí: Facebook, LinkedIn, Twitter.

Asi najrozšírenejšia sociálna sieť **Facebook** mala mať skôr súkromný charakter. Napr. už samotný profil v porovnaní s profesionálne zameranými portálmi (napr. LinkedIn) umožňuje zadať **množstvo osobných údajov** (napr. dátum narodenia, rodinní príslušníci, vzťahy, politická a náboženská príslušnosť), ale súčasne umožňuje **zvoliť, kto môže jednotlivé informácie vidieť** (verejnosť, priatelia mojich priateľov, len priatelia,...). Na všetkých portáloch však môžu užívatelia priradiť k svojmu profilu fotografiu, ktorá sa zobrazí verejne.

Tak, ako v skutočnom živote človek nezdieľa všetky informácie verejne, ale niektoré len v istom okruhu ľudí, tak isto, možno aj opatrnejšie, by mal narábať s informáciami, ktoré poskytuje vo virtuálnom svete sociálnych sietí. Pri (takmer) každej informácii na sociálnej sieti je možné nastaviť úroveň zobrazovania údajov:

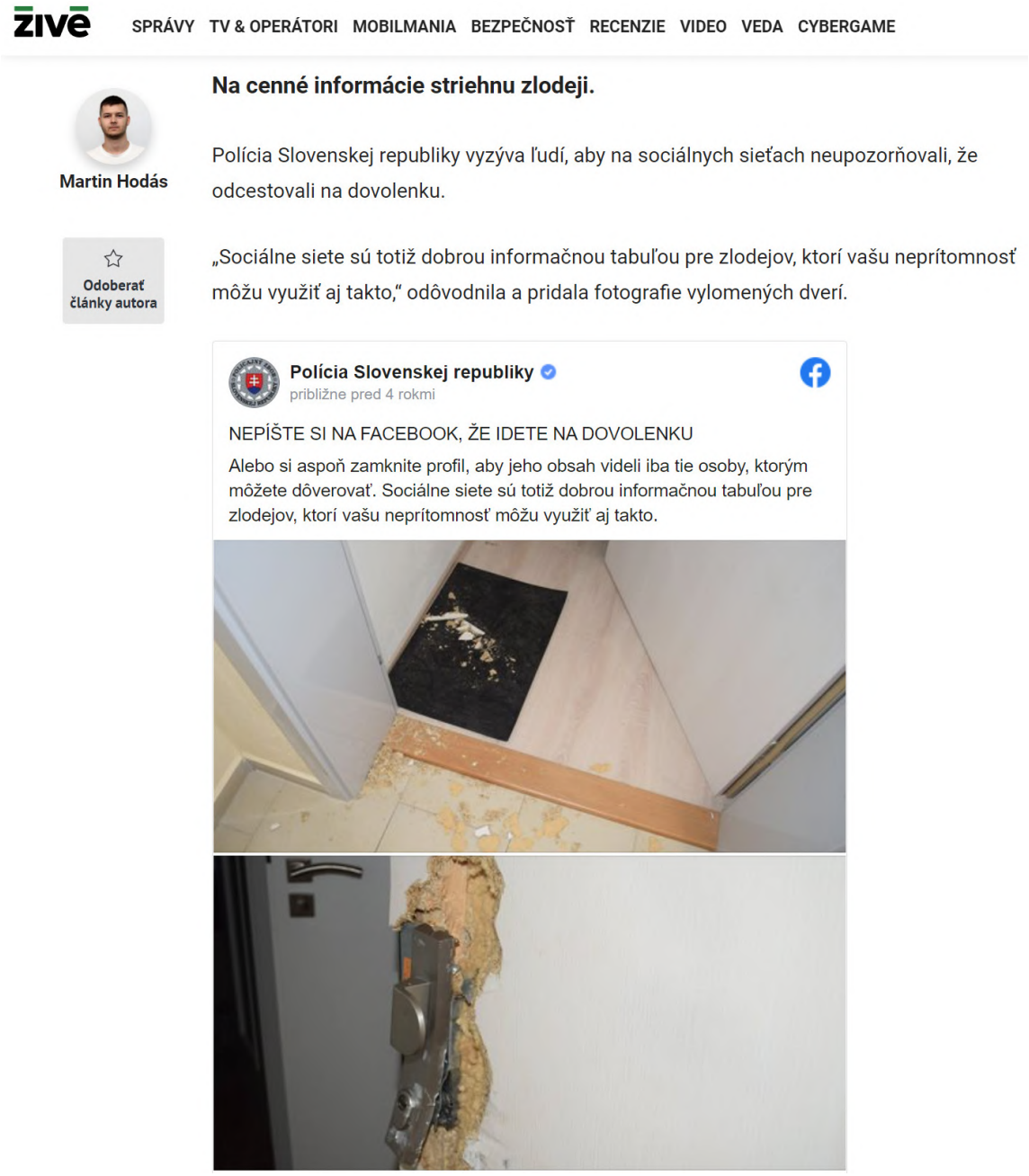
- **verejné** – pre kohokoľvek s účtom aj bez účtu na Facebooku = žiadne súkromie.
- **priatelia, priatelia okrem ..., konkrétni priatelia** – informácie sú dostupné pre tých, ktorých sme označili za „priateľov“. Základnou otázkou býva, či sú „moji priatelia“ (na sieti) naozaj moji priatelia.

- **iba ja** – ochrana súkromia pre používateľov, ktorí si svoje súkromie chránia. Pri tomto nastavení, nemá okrem vlastníka nik iný prístup k zverejneným informáciám.
- Najzložitejším, ale najlepším riešením je definovanie vlastných pravidiel pre úrovne súkromia – **Vlastné** (pre jednotlivcov, skupiny, ...).

Vlastnime svoju online prítomnosť: Je v poriadku obmedziť prístup len istej skupine ľudí, ktorí môžu pristupovať k našim informáciám a obsahu, ktorý zdieľame. Získajme viac informácií o nastaveniach ochrany osobných údajov a zabezpečenia na našich obľúbených webových stránkach.

V každej voľnej chvíľke, každý deň, milióny ľudí hľadajú na sociálnych sieťach nových priateľov alebo komunikujú so starými kamarátmi. Zdieľajú aj intímne udalosti svojho života. A mnoho vecí v živote robia hlavne preto, aby o nich mohli dať vedieť na sociálnych sieťach. Ľudia často zverejňujú zneužiteľné osobné informácie, napr. fotografie, časové plány, osobné údaje. Neuvedomujú si, kto všetko k nim má prístup, a čo všetko sa z nich dá zistiť a zneužiť.

Jedným z **najväčších omylov** na sociálnych sieťach je **zverejňovať o sebe príliš mnoho informácií**. Používanie skutočného mena, zverejňovanie fotografií, adresa bydliska alebo školy, do ktorej dieťa chodí, môže viesť až k obťažovaniu alebo útoku aj v reálnom svete. Úplne bežné je na internete zverejňovať fotografie seba a svojich kamarátov, problematické sú aj takzvané „statusy“, kde sa ľudia radi podelia s kamarátmi o rôzne aktuálne informácie. Mnohí ľudia na sociálnych sieťach verejne uvádzajú, že sa balia na dovolenku, čakajú na lietadlo, prileteli do slnečnej destinácie, atď., čo je ideálnou informáciou napríklad pre zlodeja, ktorý môže dovolenkárom vykradnúť opustený dom.



Obrázok 41 – Dôsledok zverejňovania informácií na sociálnej sieti

Pri používaní rôznych služieb ako sociálne siete, blogy, internetové fóra a iné cloud služby si musíme uvedomiť **fakt**, že **všetky informácie, ktoré** na týchto službách **zadáme už nikdy nebude možné trvale zmazať**. Aj v prípade, že nahrané dáta neskôr zmažeme totiž nemôžeme mať istotu, že si ich medzitým nikto neskopíroval. Tiež je známym faktom, že niektoré sociálne siete obsah nemažú, zostáva uložený aj naďalej. Informácie o používateľoch sú takto zhromažďované a strojovo spracované pre ďalšie použitie v budúcnosti.

To, čo uverejníme, bude uverejnené navždy: Musíme si byť vedomý toho, že keď uverejníme na internete obrázok alebo správu, môžeme tiež neúmyselne zdieľať osobné údaje o sebe a svojich rodinných príslušníkoch – napríklad miesto, kde žijeme.

Upozornenie

Ako by povedali naše staré mamy: **„Ak nechceš, aby sa niekto niečo dozvedel, tak to nehovor nikomu“** Toto možno aplikovať aj v súčasnosti. **Ak nechcete, aby sa niekto dostal k vašim súkromným fotkám alebo iným dôverným informáciám, tak ich nezverejňujte v online prostredí.**

Ešte nezodpovednejšie ako dospelí sa tu však správajú deti, ktoré sú schopné o sebe prezradiť všetko. To často zneužívajú zločinci, ktorí si hľadajú mladých kamarátov pod falošnou identitou.

Potenciálne nebezpečenstvá spojené s používaním sociálnych sietí:

- **Kyberšikanovanie** – šikana realizovaná prostredníctvom informačných a komunikačných technológií, hlavne prostredníctvom internetu a mobilného telefónu. Najčastejšie ide o zasielanie obťažujúcich, urážajúcich či útočných e-mailov a SMS, vytváranie dehonestujúcich stránok a blogov, prípadne zverejňovanie fotografií a videí s cieľom ublíženia inej osobe.
- **Grooming** – vytváranie dôverného vzťahu s cieľom zneužiť neplnoletú osobu.
- **Falošná totožnosť/identita** – bežný jav na sociálnych sieťach. Veľkou skupinou sú maloletí, ktorí si vytvorili účet na sieti aj keď nespĺňajú podmienku minimálneho veku a naplnili profil nepravdivými údajmi. Ďalšia skupina sú osoby, ktoré chcú komunikovať na sociálnej sieti, ale nemajú záujem vyzradiť vlastnú identitu, tak použijú vymyslenú. Falošná identita sa zneužíva aj na šírenie nepravdivých informácií.

Podvodné správy sa objavujú aj na sociálnych sieťach. Podvodníci sa snažia vylákať od používateľa prístupové údaje.

Tragická nehoda? Len navonok. Podvodníci našli nový spôsob ako od Slovákov ukradnúť údaje k FB

MATÚŠ MITRO 26. FEBRUÁRA 2021

Odcudzenie prihlasovacích údajov k účtom prostredníctvom falošných odkazov je už pomerne starým trikom podvodníkov. V nových prípadoch ľudia zdieľajú príspevky s tragickými dopravnými nehodami, ktoré navodzujú dojem, že sa stali na Slovensku. Priložený odkaz ľudí navedie na falošnú stránku, ktorá môže ukradnúť prihlasovacie údaje. Na takéto prípady **upozornila** členka skupiny Internetové podvody, útoky a bezpečnosť na Facebooku.

Najčítanejšie články

24 HOD 48 HOD 7 DNÍ

1 Dotknú sa aj teba. Zlatá éra Netflixu skončila, gigant narazil na realitu a prichádza s radikálnymi krokmi

2 Polovodičová kríza je iba „predjedlo". Automobilový priemysel čaká niečo ešte oveľa horšie

3 Páni Zeme? Omyl, ľudstvo nie je ani len civilizáciou "typu I". Môžeme sa ňou však stať

4 Netflix má nového kráľa sledovanosti, suverénne ho milujú aj Slováci

5 Rusko skúsilo superzbraň. Podľa Putina dokáže zabiť všetko živé, západní odborníci vidia divadlo

Obrázok 42 – Podvodná správa na Facebooku

Čo všetko o nás sociálne siete vedia? Kontrolujeme sociálne siete alebo sociálne siete kontrolujú nás?

Viac sa môžeme dozvedieť, ak si pozrieme dokumentárny film **The Social Dilemma** (Sociální dilema), ktorý trafil klinec po hlavičke. Ukážku je možné pozrieť na webovej stránke https://www.netflix.com/sk-cs/title/81254224.

Dokument nám ukazuje, ako naozaj fungujú sociálne siete. Sociálne siete nám servírujú to, čo chceme vidieť, vo forme, v akej to chceme vidieť. Všetko na striebornom podnose. Len aby to vyvolalo reakciu, otvorenie, lajk, komentár a najdôležitejšie, aby sme to posunuli ďalej zdieľaním. Pre falošné správy sa stali priam rajom.

Čím viac času tu strávime, čím viac obsahu vidíme, tým vzniká väčší priestor na predaj reklamy a produktov, tým viac dolárov tečie do vrecka akcionárov a majiteľov.

Obrázok 43 – Podvodná správa na Facebooku

A práve o to tu ide. V dokumente na problém upozorňujú aj tvorcovia a poprední predstavitelia, ktorí nám sociálne siete priniesli, tak je jasné, že ide o vec, pred ktorou si už nemožno zatvárať oči. Približuje nám špinavé triky, ktoré dnes sociálne siete používajú na to, by nás k obrazovke pripútali na čo najdlhší čas.

Ale na záver je potrebné povedať, že **silu a možnosti sociálnych sietí vieme využívať aj v prospešných oblastiach života**. Vo vzdelávacích sieťach sú zoskupení najmä študenti s cieľom spolupracovať s ostatnými študentmi na akademických projektoch, komunikovať s učiteľmi, riešiť spoločne na diaľku problémy. Každý deň vznikajú sociálne siete a stránky zamerané na určitý koníček, ich užívatelia hľadajú ľudí z celého sveta, s ktorými majú rovnaké záujmy, celá komunikácia všetkých v sieti sa točí okolo ich najobľúbenejšej činnosti. Ďalším príkladom prospešnej siete sú profesijné siete; vytvárajú sa vo firmách a slúžia na komunikáciu medzi zamestnancami a zamestnávateľom, no taktiež medzi firmou a zákazníkmi.

7. Zhrnutie

Na záver skúsme zhrnúť, čo sme sa mali naučiť, a či sme to zvládli.

Kognitívne (vzdelávacie) ciele

porozumieť kľúčovým pojmom z oblasti informačnej bezpečnosti	
poznať opatrenia na zamedzenie neautorizovaného prístupu k údajom	
poznať odporúčané politiky pre výber hesiel	
rozumieť dôležitosti pravidelnej aktualizácie softvéru	
rozumieť pojmu škodlivý softvér (malware)	
rozumieť princípom fungovania antivírusového softvéru	
poznať zásady správneho zálohovania	
rozlišovať či je bezdrôtová sieť zabezpečená alebo nie	
rozpoznať zabezpečené webové stránky	
rozumieť pojmu pharming (presmerovanie na podvrhnuté webové stránky)	
rozumieť, že k používateľskému účtu v počítačovej sieti sa pristupuje cez používateľské meno a heslo a účet má byť zamknutý alebo používateľ má byť odpojený, keď sa na účte nepracuje	
rozumieť dôvodom na ochranu osobných údajov/informácií	
rozumieť pojmu phishing (odchytávanie prístupových údajov)	

Afektívne (postojové) ciele

vnímať nutnosť zabezpečenia digitálnych zariadení a dát uložených v nich	
chápať, aký vplyv na bezpečnosť môže mať pripojenie sa do siete: škodlivý softvér, neoprávnený prístup k údajom, narušenie súkromia	
kriticky vyhodnotiť nutnosť vytvárania rôznych účtov na rôzne služby (online nákupy, finančné transakcie, sociálne siete,...)	
uvedomiť si dôsledky vykonávania niektorých činností pri nezabezpečenom pripojení do siete (napr. verejné bezdrôtové siete) alebo na nezabezpečených webových stránkach	
kriticky vyhodnotiť bezpečnosť svojich hesiel pri prístupe do zariadenia, siete, rôznych účtov pre rôzne služby	
chápať, že je dôležité neuvádzať dôverné alebo osobné identifikačné informácie na stránkach sociálnych sietí	
uvedomovať si možnosť dostať nevyžiadanú, podvodnú elektronickú správu	
uvedomovať si nebezpečenstvo nakazenia počítača vírusom pri otváraní elektronickej správy alebo prílohy správy	
chápať dôležitosť existencie záložných postupov v prípade straty údajov zo zariadenia	

Psychomotorické (výcvikové) ciele

analyzovať používané heslá z pohľadu bezpečnosti	
skontrolovať silu používaných hesiel	
navrhnúť nové heslo spĺňajúce kritéria silného a bezpečného hesla	
vedieť pomocou antivírusového programu skontrolovať konkrétnu pamäťovú jednotku, priečinok alebo súbory	
vedieť zálohovať údaje na určené miesto	
vedieť skontrolovať pripojenie cez bezdrôtovú sieť a určiť, či je zabezpečené alebo nie	
rozpoznávať možnú podvodnú, nevyžiadanú správu elektronickej pošty	
vyhodnotiť možné zneužitie e-mailovej adresy	
vyhodnotiť konkrétnu webovú stránku ako zabezpečenú alebo nezabezpečenú	

Digit@lni seniori

Na webovej stránke projektu „Zlepšovanie digitálnych zručností seniorov a distribúcia Senior-tabletov“ **www.digitalniseniori.gov.sk** nájdete:

- Užitočné informácie o projekte
- Informácie o školeniach
- Online školiace materiály
- Online školiace aktivity
- Spriatelené organizácie podporujúce vzdelávanie seniorov

Pre viac informácií o projekte a školeniach, taktiež ako technickú podporu pre vaše digitálne zariadenie kontaktujte telefonickú linku počas pracovných dní v čase od 08:00 do 16:00 h.

Call Centrum: 02/35 80 30 80

Kontaktujte nás aj e-mailom na digitalni.seniori@mirri.gov.sk

Projekt „Zlepšovanie digitálnych zručností seniorov a distribúcia Senior-tabletov“ je financovaný z Plánu obnovy a odolnosti SR ako investícia č.7 Komponentu 17 (Digitálne Slovensko).

ISBN 978-80-974240-8-4