DIGITÁLNI SENIORI

4

INFORMAČNÁ BEZPEČNOSŤ

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Informačná bezpečnosť

Autor: RNDr. Slavka Blichová a kol., Odbor podpory inovácií,
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Text prešiel odbornou jazykovou a typografickou korektúrou.
Za odbornú a jazykovú stránku študijného materiálu zodpovedajú autori.
Ilustrácia na titulke: Adobe Stock
Fotografie v publikácii sú ilustračné a ich obsah nemusí korešpondovať s aktuálnou verziou operačného systému digitálneho zariadenia.
Vydavateľ: Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

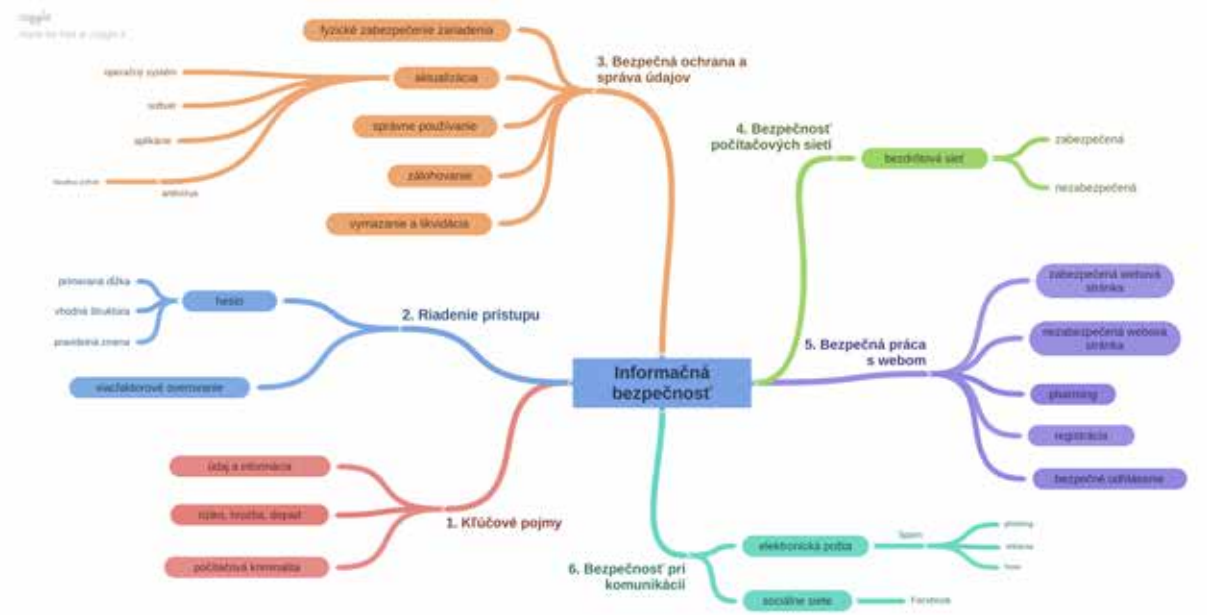
3. doplnené a revidované vydanie

ISBN 978-80-69030-05-3

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, malware, antivírusový program, zálohovanie, informačná bezpečnosť, spam, hoax, pharming, phishing, smishing, vishing, spoofing, sociálna sieť, kyberšikanovanie, grooming, falošná identita, ochrana citlivých údajov, dezinformácia, Fake News, propaganda, konšpiračná teória, mediálna gramotnosť, fakt, názor, „umelá inteligencia", deepfake

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 práci s digitálnymi technológiami. so zreteľom na zachovanie rozumnej miery nákladov v porovnaní s hodnotou chránených **informácií**. To všetko tak, aby prijaté opatrenia nebránili oprávnenému používaniu informácií. V jednotlivých častiach si vysvetlíme dôležité pojmy používané v tejto oblasti.

Aby sme získali bližšiu predstavu, skúsime na príkladoch urobiť 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 nám 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 vľavo 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 motýl"

Informácia: 1. V kníhkupectve predávajú knihu „Nočný motýl"

2. Na lúke poletuje „nočný motýl"

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 ich **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 major").

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, teda aká veľká je pravdepodobnosť, že sa daná hrozba naplní.

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)

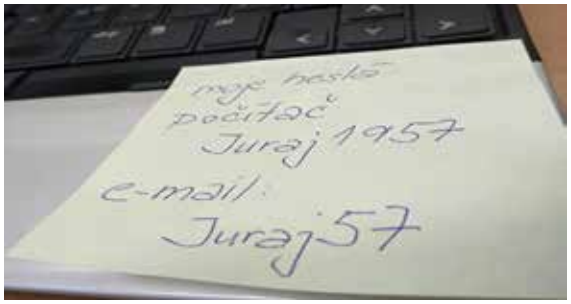
Upozornenie

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 sú sabotáž, krádež, zneužitie, neoprávnené používanie 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, internetbanking, sociálne siete). Tieto prístupy tvoria bránu do nášho súkromia.

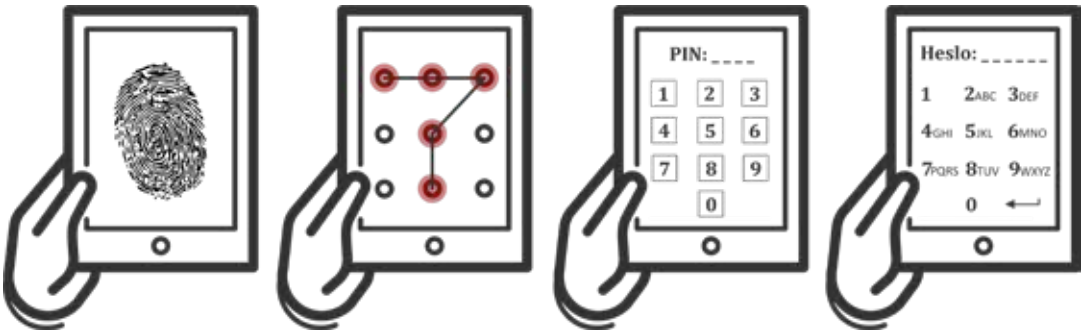


Obrázok 7 – Heslá

Napriek tomu často podceňujeme tento faktor bezpečnosti tým, že používame heslá napísané na papierikoch a nalepené na monitore, v kalendári, či veľmi jednoduché alebo ľahko prelomiteľné (odhaliteľné) 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

Pri výbere ochrany pri prihlasovaní si musíme uvedomiť klady a zápory jednotlivých možností:

- biometrické prvky–odtlačok prsta, snímka tváre
  - \+ jedinečný prvok, máme ho vždy pri sebe
  - — porušenie kože prsta, resp. úraz tváre
- grafický prvok na obrazovke (vzor)
  - \+ jednoduchý na zapamätanie
  - — ľahko odpozorovateľné ponad place (napr. v hromadnej doprave)
- PIN kód
  - \+ ľahko zapamätateľný
  - — ľahko odpozorovateľné, nepoužívať 1111, 0000, 1234,...
- klasické heslo
  - \+ bezpečné, ak je dobre vytvorené
  - — dávať pozor, aby ho člověk nezabudol

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 jeho 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 na overenie totožnosti používateľa a mal by ho poznať iba samotný používateľ. Dobré heslo nesmie byť ľahko uhádnuteľné (prelomyteľné). Preto by to nemalo 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 je treba mať dobré a rozdielne heslá pre všetky dôležité služby. Obzvlášť na prístup do počítača, e-mailu, sociálnych sietí a elektronického bankovníctva, kde sa vyskytuje najviac citlivých informácií a môže tam dôjsť k najväčším škodám. **Heslo je ako kľúč** a je potrebné si uvedomiť, že ani v reálnom živote nepoužívame jediný kľúč na otváranie viacerých dverí (napr. bytu, domu, auta, poštovej schránky, pivnice, atď.). Čím drahšie veci máme uložené „za dverami", tým bezpečnejší zámok si dávame „na dvere". 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 nám síce uľahčujú prístup, ale tento spôsob pohodlia predstavuje príliš veľké riziko, pretože jednoduché heslá sa dajú ľahko zistiť („prelomiť"). Silné a zložité heslá nám pomáhajú zabrániť nepovolaným osobám v prístupe k našim citlivým informáciám, ale často si ich nevieme zapamätať.

Ako si vytvoriť silné heslo tak, aby sme si ho vedeli zapamätať? Vytvorme si heslo z vety, ktorá nám niečo pripomína (len nám známy fakt, náš obľúbený výrok, citát z knihy, verš riekanky, básne, piesne a pod.), vďaka čomu si ho ľahko zapamätáme (napr. „NaSteneMam.3Obrazy!").

Upozornenie

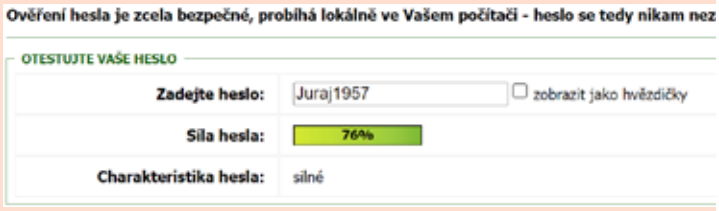
Unikátny účet – jedinečné heslo!

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

Úloha 3

Overte si silu svojho hesla. Nasnímaním QR kódu otvorte webovú stránku 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**

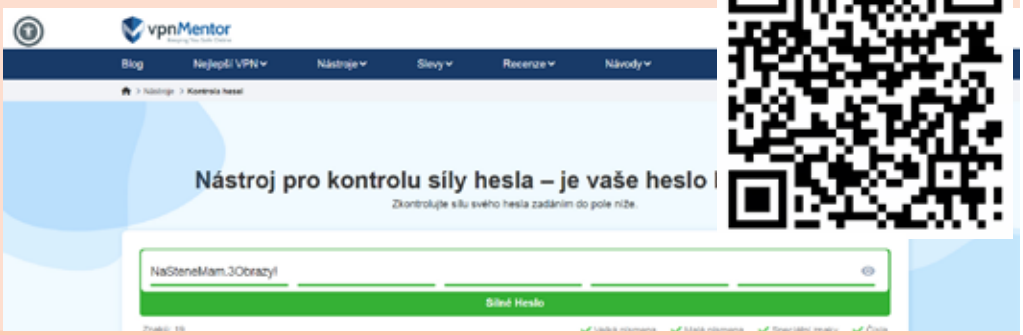


2. **https://csirt.upjs.sk/hesla/**

Na uvedenej adrese vyskúšajte silu hesla: NaSteneMam.3Obrazy!

3. **https://cs.vpnmentor.com/tools/passwordmeter**

Na uvedenej adrese (vpnMentor passwordmeter) vyskúšajte silu toho istého hesla: **NaSteneMam.3Obrazy!**



NÁŠ TIP

Na webovej stránke vpnMentor pod vyobrazeným nástrojom na kontrolu sily hesla nájdete celý rad užitočných informácií o heslách, ich spravovaní a bezpečnosti–podrobné pravidlá na vytvorenie silného hesla, praktický návod na to, ako si čo najlepšie zabezpečiť svoje heslá a online účty, čo nám hrozí, ak nám niekto heslo „hekne" (prelomí) alebo ukradne, ale aj dalšie súvisiace zaujímavosti.

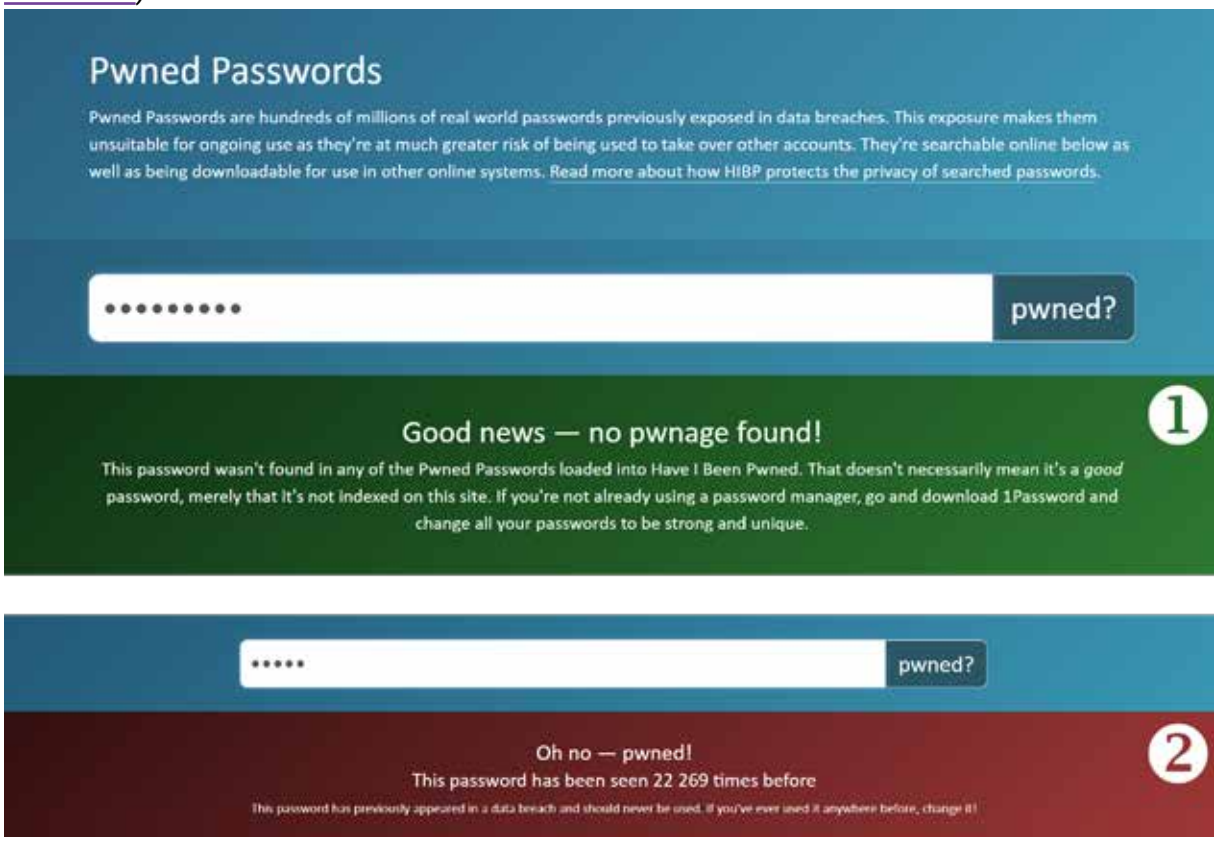
Úloha 4

Vytvorte heslo z vlastnej vety.
Príklad: Mám 4! Nádherné Vnúčatá. a Teším sa Z nich
Heslo: M4!NV.aTsZn

Vlastná veta: .....

Heslo: .....

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 5

Nasnímaním QR kódu otvorte webovú stránku **haveibeenpwned.com/Passwords** a 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 už možno využívame v praxi a ani o tom nevieme (neuvedomujeme si to).

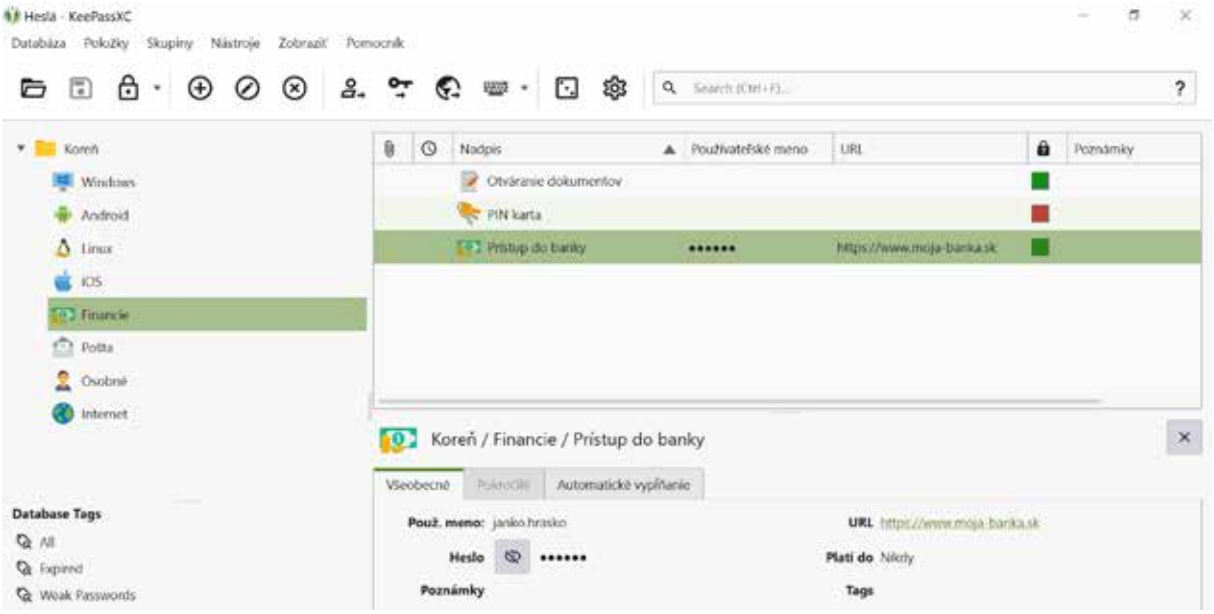
Viacfaktorové overovanie využíva prvky:

- **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 vytvoríme **zoznam hesiel**, ale mal by byť uložený na bezpečnom mieste **mimo zariadenia**. Môžeme to prirovnať k tomu, že PIN kód k platobnej karte nikdy nemáme uložený pri platobnej karte. Pre skúsenejších používateľov, 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

Zabezpečenie komplexnej ochrany našich údajov a digitálnych zariadení pozostáva z niekoľkých dôležitých krokov. Sú nimi:

1. fyzické zabezpečenie zariadenia, ktoré obsahuje údaje,
2. pravidelné aktualizácie operačného systému, softvérov a aplikácií, ktoré máme na našom zariadení nainštalované,
3. správne používanie zo strany používateľa,
4. zálohovanie údajov.

Nezanedbateľným krokom na 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** (napr. na iné zariadenie, na USB kľúč, do cloudu).

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 nefungujúce zariadenie pripojené k elektrickej sieti (počítač), alebo či nie je vybitá batéria (notebook, tablet, mobil). Niekedy pomôže zariadenie len vypnúť a opätovne zapnúť. 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 dôsledkom nehody, preto je pri manipulácii so zariadením 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),
- udržiavať 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 svoje zariadenie v aute na viditeľnom mieste, ale ani v kufri auta. Nikdy totiž nevieme, kto nás sleduje pri jeho odkladaní.

Strata zariadenia býva najčastejšie spôsobená našou nepozornosťou, pozor je potrebné dávať hlavne pri cestovaní.

Obrázok 12 – Krádež

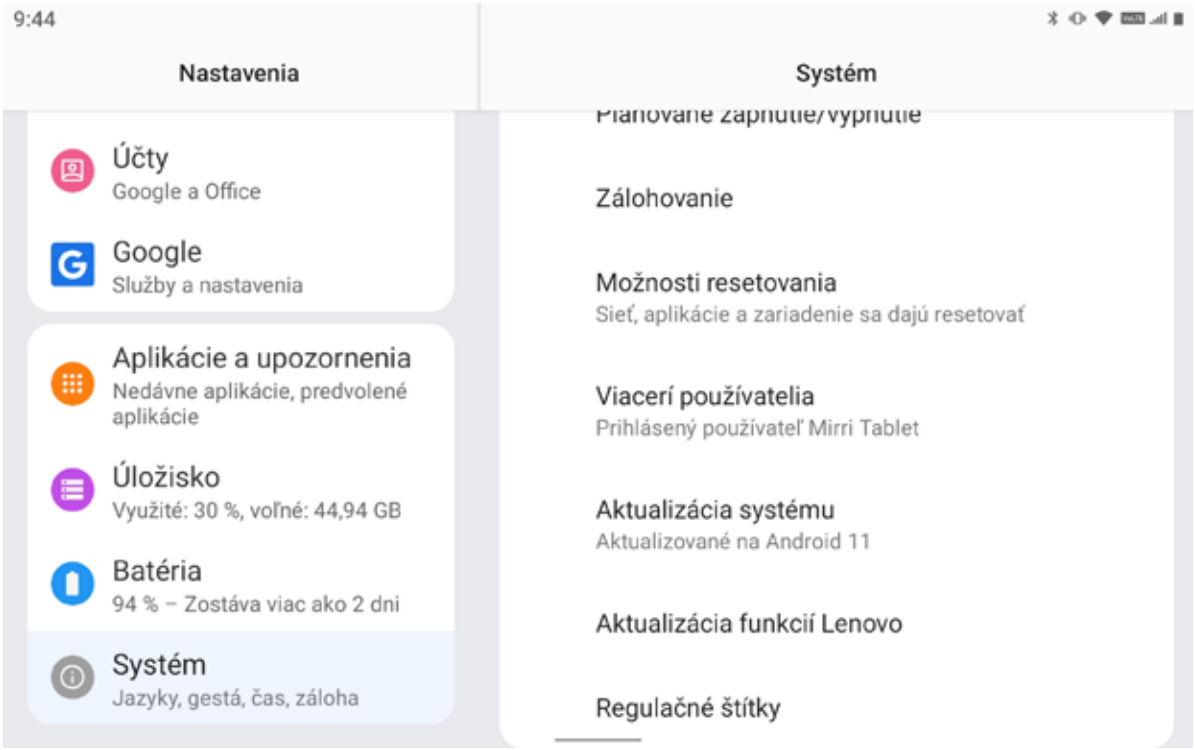
3.2. Pravidelná aktualizácia

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 však aj **opravujú chyby** (zraniteľné a slabé miesta) v operačných systémoch, softvéroch a aplikáciách, ktoré by mohli útočníci zneužiť. Tým zvyšujú bezpečnosť programu, používateľa, 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 prvom štarte zariadenia (napr. tabletu pri odsúhlasovaní podmienok použitia) môžeme dostať otázku 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
*(*vyobrazenie sa môže mierne líšiť od Nastavenia aktualizácií v našom tablete v závislosti od verzie nášho operačného systému)*

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)*

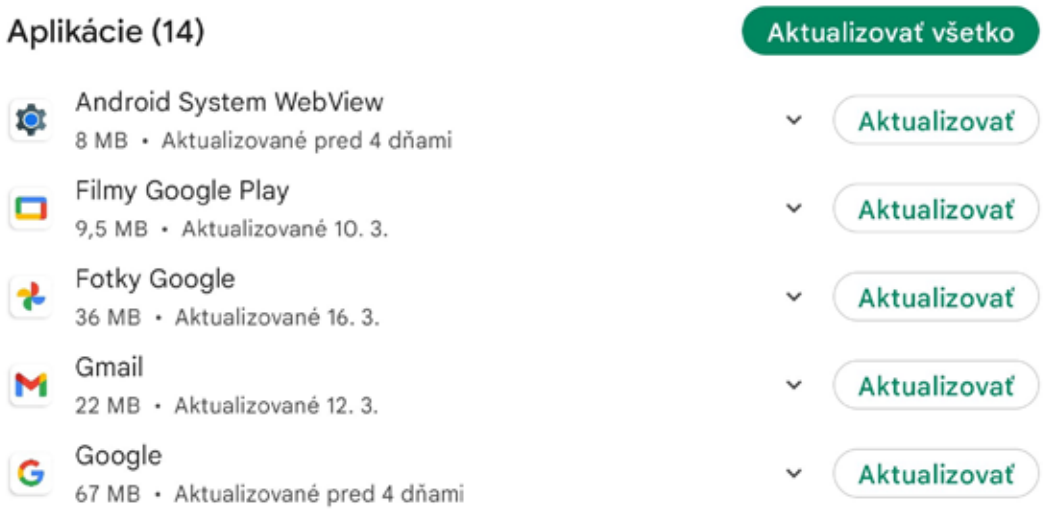
Ťuknutím na tlačidlo „Skontrolovať aktualizácie" môžeme manuálne skontrolovať dostupnosť aktualizácii pre náš tablet.

Aktualizácia jednotlivých aplikácií v tablete je ponúkaná väčšinou pri ich spustení (v závislosti od nastavení aktualizácii v našom tablete). 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)*

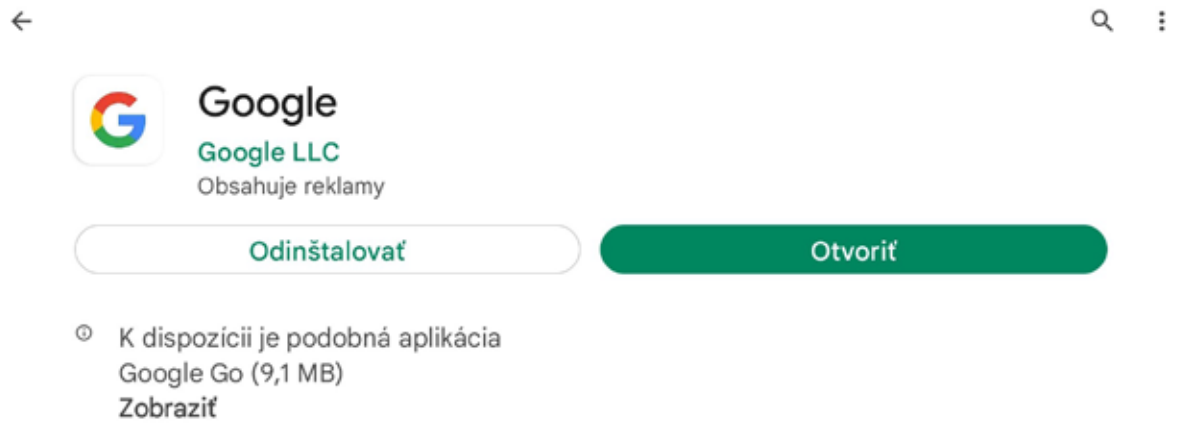
Po ťuknutí na tlačidlo „Aktualizovať" sa pripojíme na obchod s aplikáciami a môžeme spustiť samotný proces aktualizácie.

Pod tlačidlom „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 aplikácie po aktualizácii
*(*vzhľad okna v našom tablete sa môže od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému)C*

Úloha 6

Skontrolujte, či operačný systém v zariadení, na ktorom pracujete, je aktualizovaný.

Úloha 7

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

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 veľkej skupine **škodlivého softvéru**, ktorý označujeme spoločným názvom **malware**. Ten nám môže spôsobiť obrovské škody tým, že zničí našu prácu, môžeme kvôli nemu stratiť naše údaje, dokonca 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 19 – 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 20 – Ransomware

Úloha 8

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 (kontroluje optické nosiče, USB kľúče, pamäťové karty a pod.),
- Kontrola na vyžiadanie.

Konkrétny súbor, priečinok, USB kľúč,... si vieme kedykoľvek skontrolovať pomocou antivírusového programu. K dispozícii 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. 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 9

Spustite antivírusovú aplikáciu a skontrolujte zariadenie.

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 on klikne na neznámy odkaz alebo otvorí infikovanú 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 alebo do aplikácie, je dôležité sa z nej po ukončení svojej práce aj korektne odhlásiť** (kapitola 5.4.). Výnimkou je, keď máme zariadenie iba pre seba – vlastný telefón/tablet, alebo vlastné konto na rodinnom počítači/notebooku. Ak máme vlastné konto, nemusíme sa odhlasovať zo služieb. Je však nutné sa odhlásiť z konta, alebo aspoň uzamknúť obrazovku. Na tabletoch a mobilných telefónoch sa odhlasujeme stlačením bočného tlačidla.
2. **Bezpečná práca s webom** (kapitola 5.).
3. **Bezpečné používanie e-mailu a sociálnych sietí** (kapitola 5).
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 našom zariadení.
5. **Nezadávať prihlasovacie údaje tak, aby to niekto mohol odpozorovať.** Pozeranie ponad plece („Shoulder surfing") 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, či tabletu, mobilu 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 a pod.).
6. Vo verejne dostupných priestoroch dávať pozor, kde sú kamery – možnosť odpozorovania zadania hesla, PIN-u.

3.4. Pravidelné zálohovanie

Na **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**.

Ak svoje dáta zálohujeme pravidelne, s dostatočnou frekvenciou, je možné pri poruche systému alebo po strate údajov minimalizovať straty spôsobené nedostupnosťou, či dokonca stratou našich 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 údajov, ktoré sú pre nás dôležité, na iné médiá buď 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, pričom 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 (na ukladanie do cloudu je 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 používateľ podľa svojich preferencií. Používateľa to väčšinou obťažuje, ale zálohovanie veľmi 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 aj frekvencia ich zálohovania.

Obrázok 21 – Kópia dát

Zariadenia typu tablet a mobilný telefón využívajú služby na 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. V zariadeniach s operačným systémom Android je alternatívou využívať na zálohu tzv. „Google konto".

3.5. Bezpečné vymazanie a likvidácia

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

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.

Obrázok 22 – Vymazanie

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, diskety, CD, DVD a Blu-ray médiá.

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**, čím** úplne zlikvidujú pôvodne uložené údaje. Problémom môžu byť pamäťové médiá, na ktorých nemáme priamy prístup do všetkých ich oblastí, resp. pamäťových buniek (mobilné zariadenia ako telefóny a tablety, niektoré novšie SSD disky a pod.). Tu nám ostáva jedine možnosť fyzickej likvidácie zariadenia. Špeciálnym záznamovýjm médiom sú vzdialené úložiská, kde garantujú bezpečné zmazanie ich 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:

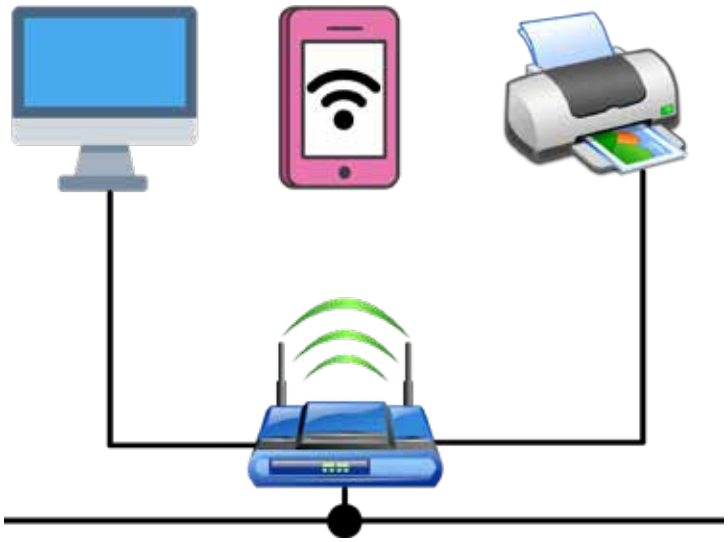
- zdieľanie údajov (spolupráca viacerých používateľov),
- zdieľanie prostriedkov (napr. tlačiarní, diskov),
- zvýšenie spoľahlivosti systému (v prípade poruchy je možné jeden zdieľaný prostriedok nahradiť iným).

Obrázok 23 – Internet

Na domáce použitie je možné vytvoriť malú osobnú sieť, v ktorej sú prepojené viaceré naše zariadenia (počítač, mobil, tablet, tlačiareň,...). Samozrejme, častejšie potrebujeme pripojiť svoje zariadenia na **internet**, čo je celosvetová/globálna 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 (predovšetkým pre mobilné a prenosné zariadenia),
3. dátové pripojenie (zväčša pre tablety a mobilné telefóny).



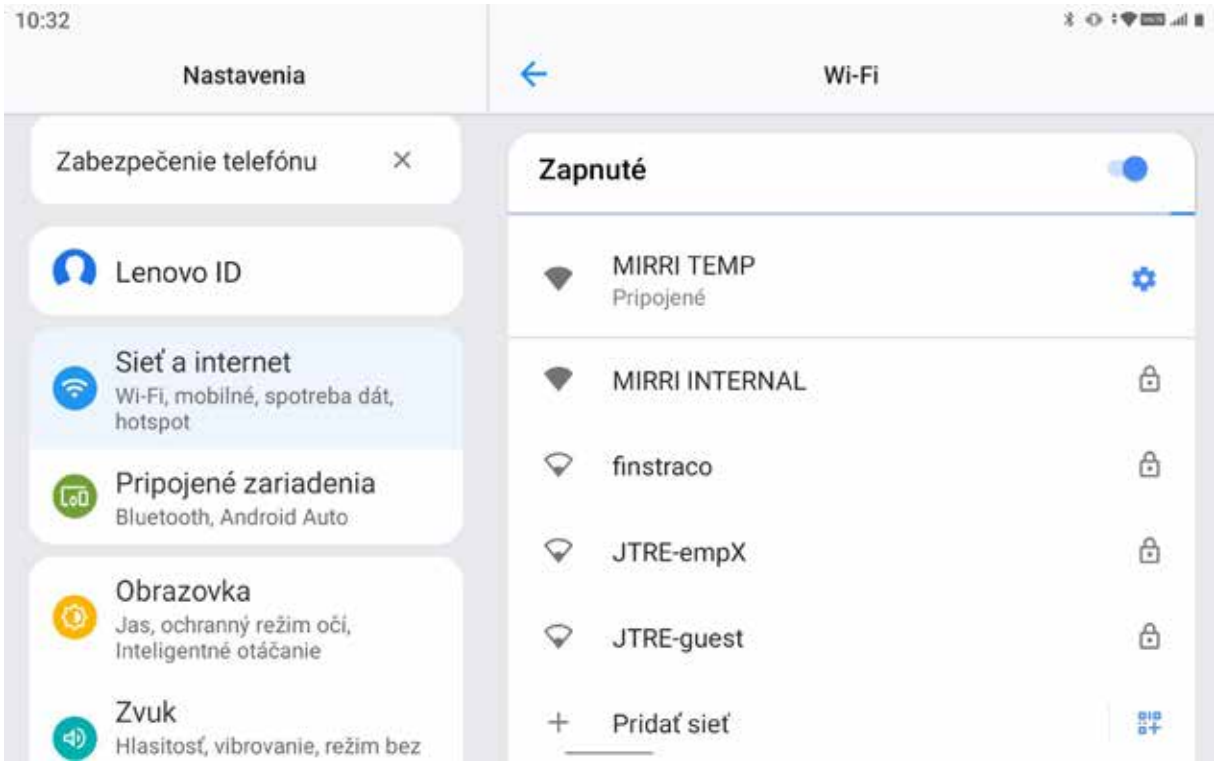
Obrázok 24 – Pripojenie na internet

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

Ak **nemáme svoj tablet alebo iné zariadenie pripojené do počítačovej siete**, útok naň môže byť zrealizovaný len priamym fyzickým kontaktom. A to tak, že sa útočník fyzicky dostane k nášmu zariadeniu, alebo sám používateľ do neho prinesie škodlivý softvér na pamäťovom médiu (napr. USB kľúč, pamäťová karta). Únik informácií z takého zariadenia bez spolupráce používateľa (nemusí to byť vedomá spolupráca, môže ísť o stratu či odcudzenie zariadenia) 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,...). Útočníci sa väčšinou snažia zneužiť zraniteľnosť nejakej sieťovej služby, prípadne využiť zle nastavenú sieťovú službu. Tak môžu získať neoprávnený prístup k informáciám uloženým v našom tablete, telefóne alebo počítači, nainštalovať do neho škodlivý softvér, alebo ovládnuť celé zariadenie. Rapídne sa tak zvyšuje možnosť úniku informácií a dát.

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



Obrázok 25 – Wi-Fi siete
*(*vzhľad okna s Wi-Fi sieťami v Nastaveniach nášho tabletu sa môžu od vyobrazenia na obrázku líšiť v závislosti od verzie nášho operačného systému)*

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

- prístup k sieti chránený heslom,
- šifrovanie komunikácie prostredníctvom siete,
- obmedzenie prístupu 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 však iba ochrana prístupu a nechráni nás 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.

Na online platby a „citlivé" operácie na internete mimo nášho domova vždy používame pripojenie na internet cez mobilné dáta. Je to oveľa bezpečnejšie, ako využívanie verených (nezabezpečených, ale aj zabezpečených) Wi-Fi sietí. **Wi-Fi v našom zariadení musí byť vtedy vypnuté** (skontrolujeme stav/farbu ikony Wi-Fi v paneli rýchleho nastavenia), pretože v snahe šetriť mobilné dáta, ak sa nachádzame na dosah dostupnej Wi-Fi siete, náš tablet (mobil) automaticky uprednostní pripojenie na dostupnú verejnú Wi-Fi sieť pred pripojením cez mobilné dáta.

Upozornenie

Byť opatrný sa vo virtuálnom priestore vypláca.

Úloha 10

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

Názov Wi-Fi siete: .....

Zabezpečená: ☐ Áno ☐ Nie

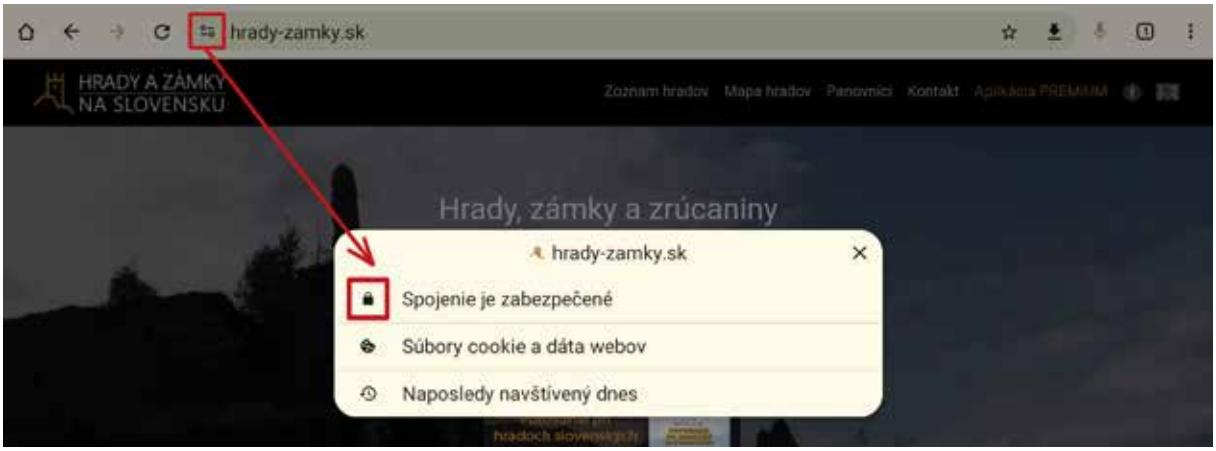
5. Bezpečná práca s webom

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

5.1. Nie všetko, čo navštevujeme, je bezpečné

Pri hľadaní informácii sa občas dostaneme na stránky, o ktorých bezpečnosti je možné pochybovať. Ak navštevujeme webové stránky, je dobré venovať pozornosť aj tomu, či sú bezpečné. Veľmi jednoduchý spôsob na to, aby sme zistili, či je webová stránka zabezpečená, je všímať si riadok adresy webovej stránky. A nepotrebujeme na to žiadne hlbšie teoretické vedomosti.

Obrázok 26a – Príklad zabezpečenej webovej stránky–riadok adresy vo webovom prehliadači obsahuje pred adresou zabezpečenej webovej stránky ikonu na otvorenie informačného okna (okno otvoríme ťuknutím na ikonku)



Obrázok 26b–Príklad zabezpečenej webovej stránky–otvorené informačné okno (okno obsahuje viacero informácií, pričom prvou v poradí je informácia o zabezpečení spojenia, označená ikonou uzamknutého visiaceho zámku–„kladky")

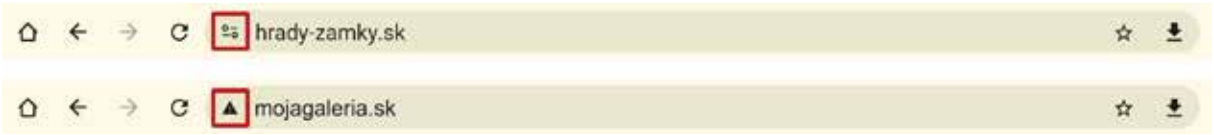
Písmenká **https** označujú súbor pravidiel (protokol), ktorými sa riadi prenos dokumentov na webe. Https je zabezpečený protokol, ktorý komunikáciu **šifruje**. Menej bezpečný je základný protokol **http** bez šifrovanej komunikácie. Tieto protokoly nemusia byť v riadku adresy webovej stránky zobrazené.

Obrázok 27 – Príklad nezabezpečenej webovej stránky–riadok adresy vo webovom prehliadači obsahuje pred adresou nezabezpečenej webovej stránky ikonu výstražného trojuholníka s výkričníkom

Dnešné webové prehliadače v zariadeniach (tablety, mobilné telefóny, počítače) zobrazujú adresu webových stránok aj bez protokolu. V riadku adresy je automaticky

skrytý protokol, ale zobrazuje sa iba príslušná ikona a webová adresa, prípadne pri nezabezpečenej stránke môže byť pridaný aj text „nezabezpečené".

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 jeho prevádzkovateľa. Indikátor sa zobrazí iba pri návšteve nezabezpečeného webu.



Obrázok 28 – Riadok adresy pre webovú stránku bez zobrazenia protokolu vo webovom prehliadači na tablete

Je potrebné si uvedomiť, že zabezpečená webová stránka dáva informáciu iba o tom, že pripojenie na danú stránku je zabezpečené (prevádzkovateľ danej webovej stránky si zaplatil bezpečnostný certifikát u poskytovateľa služby). Nič však nehovorí o tom, či je stránka svojím obsahom dôveryhodná, alebo nie. Aj zabezpečenú webovú stránku môže prevádzkovať deinformátor, manipulant alebo podvodník.

Upozornenie

Všetky aktivity, pri ktorých sa vyžaduje **overenie** (autentifikácia) používateľa, by sa mali vykonávať iba na **zabezpečených a zároveň 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 11

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

Zistite, či je stránka zabezpečená: ☐ Áno ☐ Nie

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

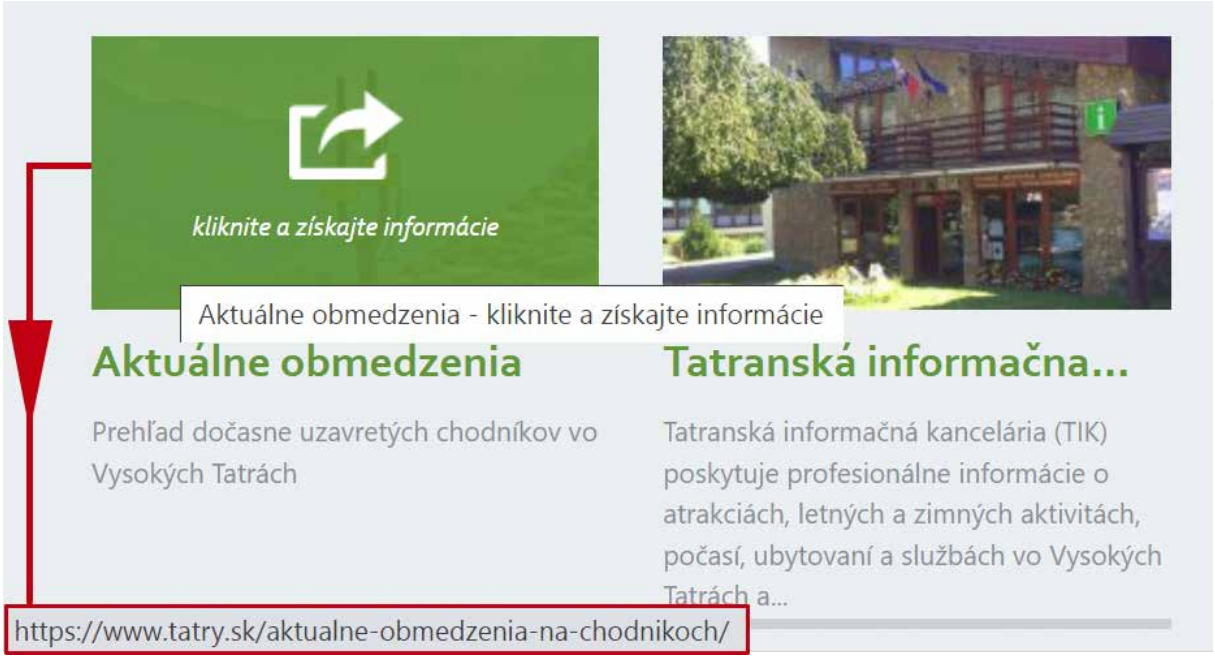
Zistite, či je stránka zabezpečená: ☐ Áno ☐ Nie

5.2. Nie všetko, na čo klikáme, je bezpečné

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

Pred každým kliknutím na internete by sme si mali dobre prečítať, na čo klikáme. Ak ide o bežné navigačné prvky, ako sú tlačidlá vo webovom prehliadači, kliknutie je bezpečné. Ak nám ale príde výzva s odkazom na neznámu webovú stránku, určite na odkaz neklikať.

Pred kliknutím na odkaz si vždy skontrolujme v ľavom dolnom rohu prehliadača webovú adresu, na ktorú budeme presmerovaný. Potrebné je dávať si pozor aj na tie najmenšie preklepy v adrese.

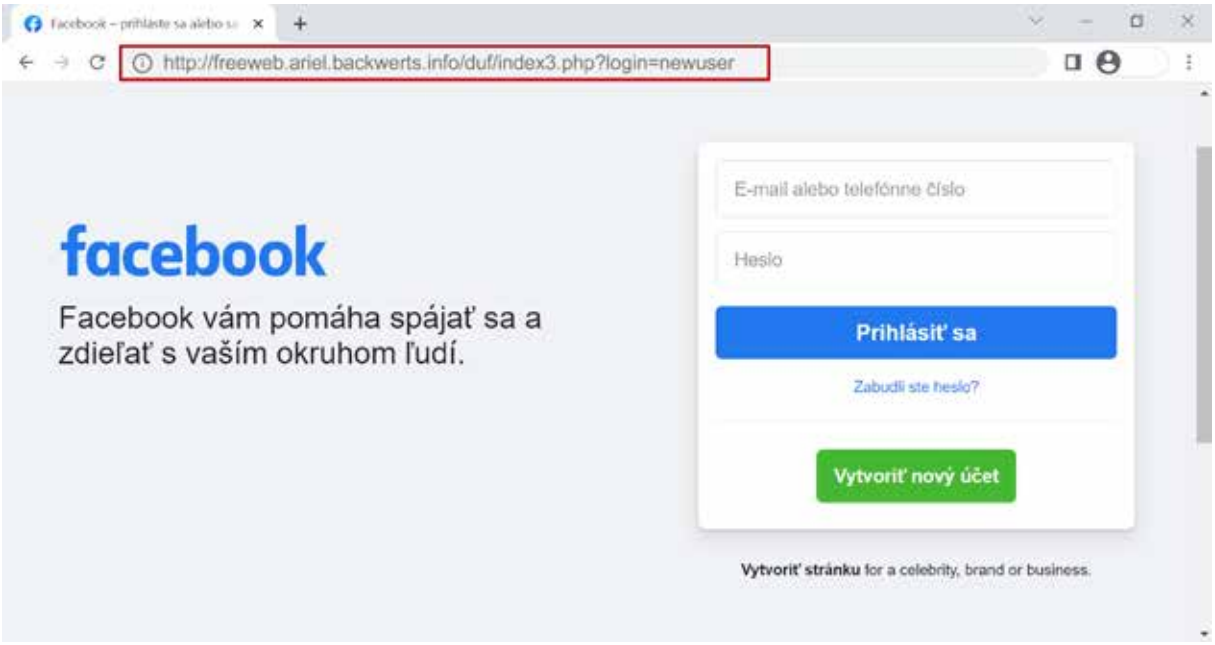


Obrázok 29 – Kontrola webovej adresy odkazu

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

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. presmeruje skutočné webové stránky inštitúcie (napr. stránky banky, sociálnych sietí, platobnej brány,...) na ním vytvorené falošné/podvodné stránky. Dizajn takýchto podvodných stránok je podobný, alebo takmer rovnaký, ako dizajn oficiálnej stránky zneužitej inštitúcie. Návštevník podvodnej stránky preto ani nemusí zistiť, že má otvorenú falošnú internetovú stránku. Rozdiel objavíme len v detailoch, napríklad v inom písmene v adrese webovej stránky (napr. www.mojabankasI.sk namiesto www.mojabankasl.sk – ide len o zámenu

podobných písmen, malého L a veľkého I, ktorú veľmi ľahko prehliadneme) alebo v odlišnej doméne (.com namiesto .sk). Táto taktika potom navedie nič netušiacu obeť, aby zadala na podvodnej stránke citlivé informácie, akými sú číslo bankového účtu, heslo, prístupové údaje do firmy, k platobnej karte alebo k platobnej bráne. Vyplnené údaje následne útočník využije vo svoj prospech.



Obrázok 30 – Príklad pharmingu–falošná stránka na prihlásenie na sociálnu sieť

Upozornenie

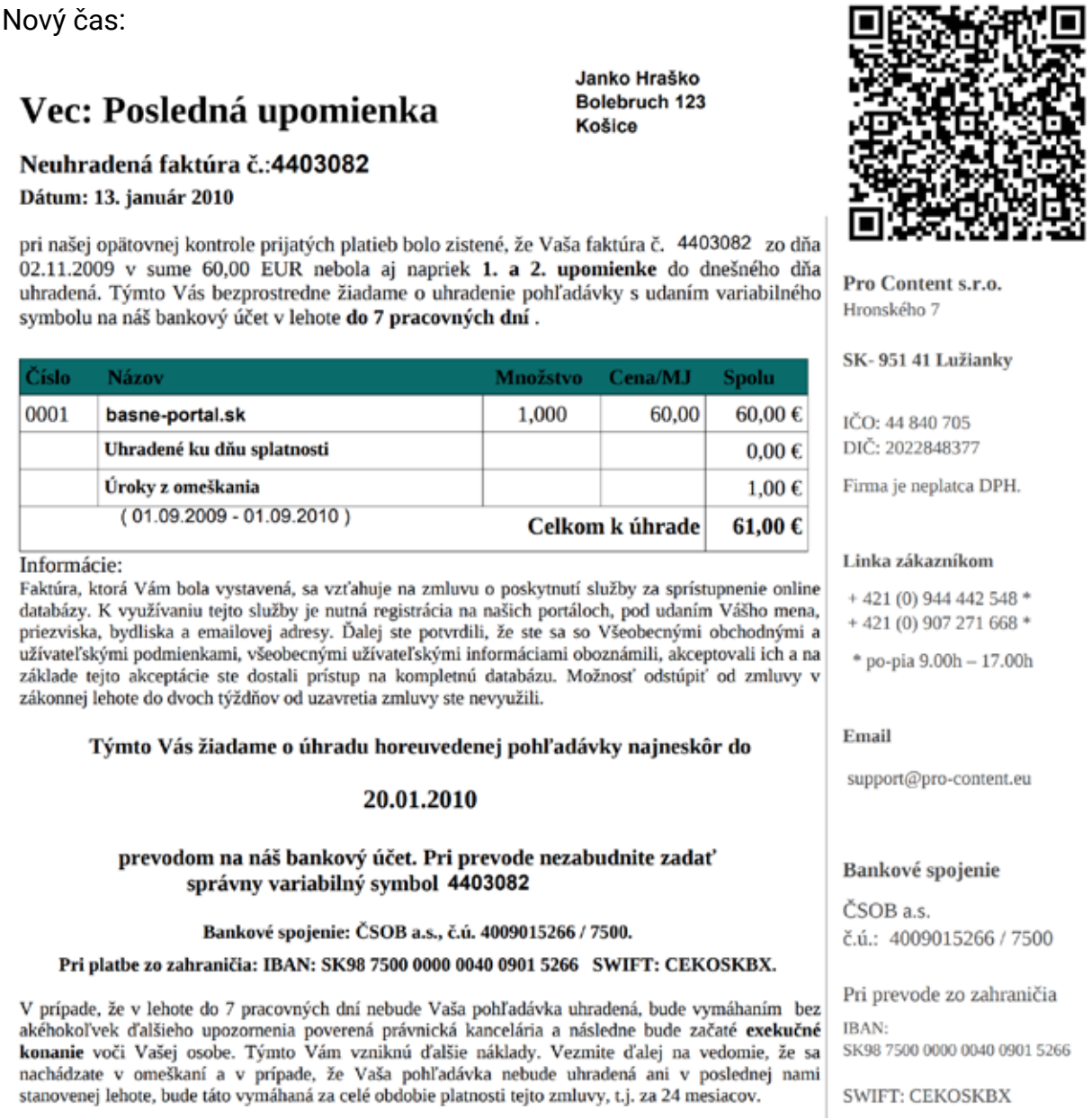
Všímajte si aj **detaily** vo webových adresách stránok, hlavne tých, kde plánujete zadávať citlivé údaje:

- 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, internetbankingu, 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. Odkaz na článok o kauze spoplatnených stránok na webe časopisu Nový čas:



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

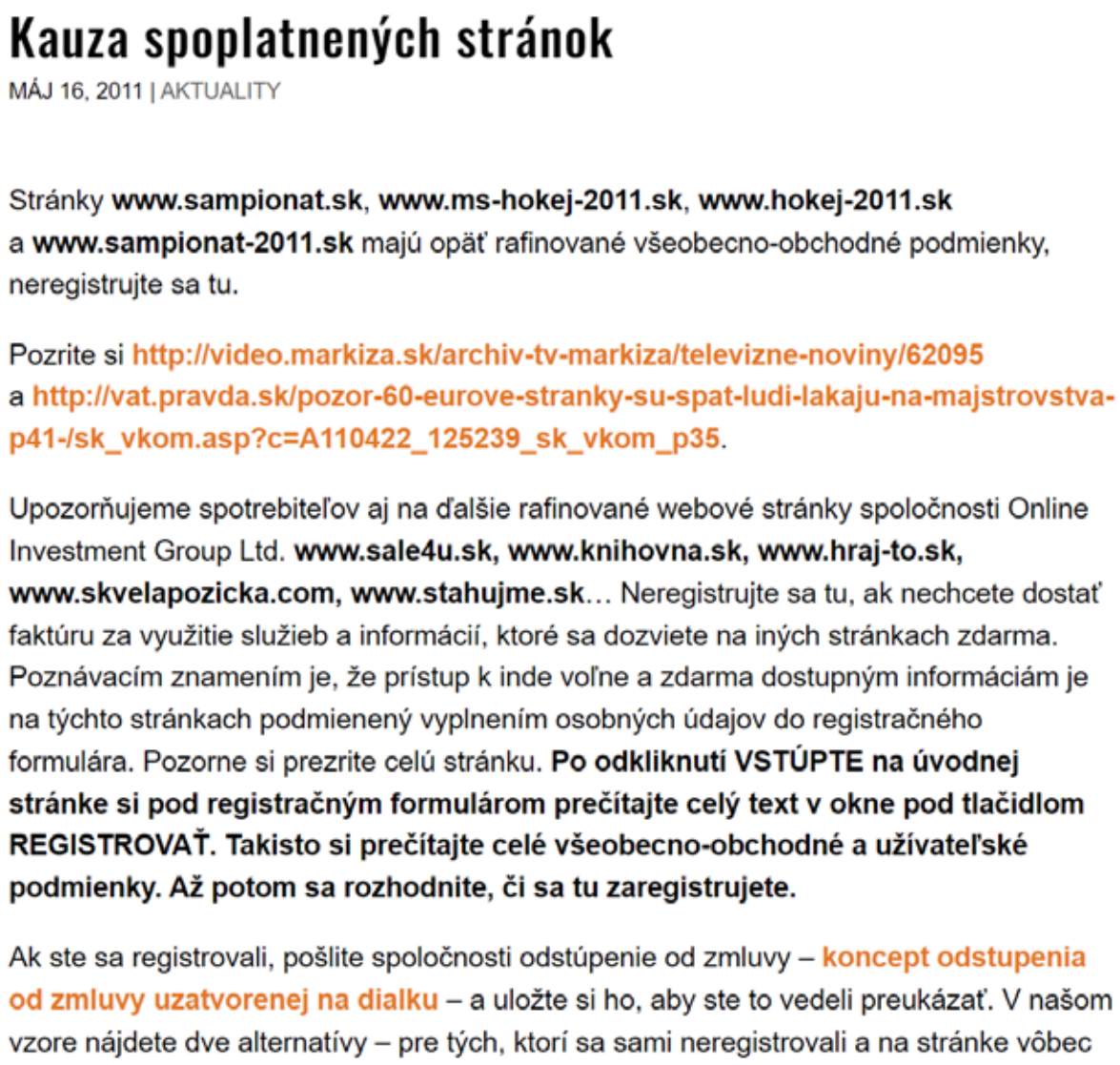
Bankové spojenie

ČSOB a.s.
č.ú.: 4009015266 / 7500

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

SWIFT: CEKOSKBX

Obrázok 31 – 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 32 – 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. Takto totiž stále ostávame prihlásení k službe a tá môže byť zneužitá. Tiež je potrebné dávať si pozor na to, či v prehliadači cudzieho zariadenia 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 33 – E-mail

Na to, aby príjemca videl, či má v schránke nejaké správy, si ju musí otvoriť. Elektronická pošta je na internete veľmi používanou službou a je určená na 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 je zaujímavým cieľom pre kybernetických útočníkov, preto pri práci s ňou musíme dodržiavať bezpečnostné pravidlá.

Najväčším nebezpečenstvom pri používaní elektronickej pošty 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 a priame, prakticky okamžité doručenie adresátovi. Reklama zasielaná e-mailom je sama o sebe legitímna, avšak len v prípade, že používateľ/adresát má záujem získavať reklamné informácie z určitej oblasti. Často si však neprajeme, aby nám 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 autori snažia 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, či 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, hoax.cz, manipulatori.cz).

hoax.sk hoax.cz manipulatori.cz

Obrázok 34 – 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 (zaplňuje e-mailovú schránku),
- dáva nebezpečné rady,
- nadbytočne zaťažuje linky a servery,
- znižuje dôveryhodnosť odosielateľa (pri odosielaní hoaxov z pracovnej adresy môže poškodiť aj zamestnávateľa),
- môže byť príčinou prezradenia dôverných informácií (pri nepoužívaní skrytej kópie pri hromadnom posielaní e-mailov môže byť zoznam adries odchytený a zneužitý na rozposielanie spamu),
- nekritickým príjmom informácií a ich ďalším šírením,
- psychickou manipuláciou (vzbudzuje pocit ohrozenia, viny,...),
- posilňuje poverčivosť (napr. rozosielaním reťazových listov šťastia).

Úloha 12

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.

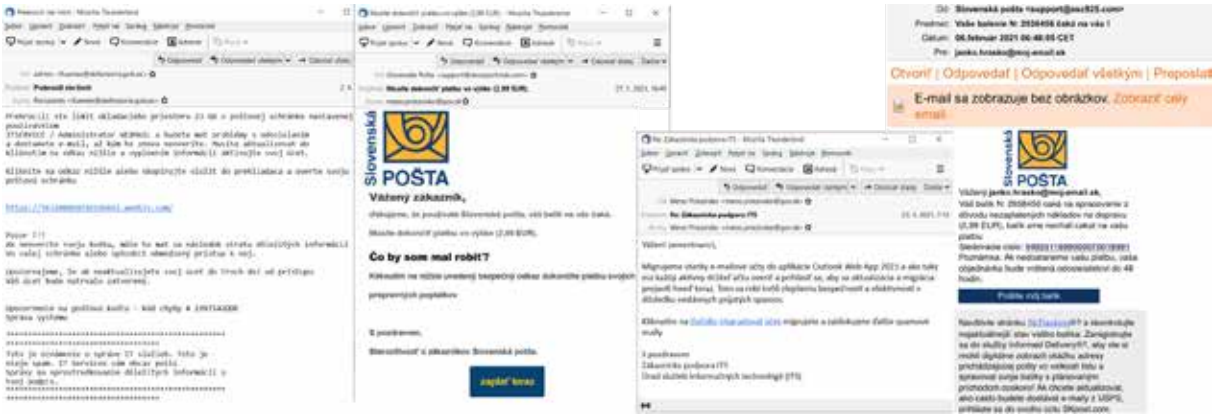
Podvodná správa – taká správa, ktorá sa snaží uviesť príjemcu do omylu a tým získať pre jej tvorcu nejaký prospech. Zámerne sme použili výraz tvorca správy, pretože odosielateľ (aspoň ten, ktorý je uvedený v správe) je spravidla falošný. Podvodné správy veľmi často obsahujú škodlivý softvér v prílohách, 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" nám oznámi zablokovanie nášho bankového účtu, falošný správca servera chce riešiť problém s naším e-mailovým kontom, falošný organizátor lotérie nám oznamuje výhru a chce nám ju odovzdať, fiktívna nešťastná vdova nás žiada o pomoc

pri prevode dedičstva z nejakej rozvojovej krajiny do Európy a pod. Pri snahe o riešenie takejto situácie sa od nás podvodníci pokúšajú získať prístupové údaje buď priamo ich vyžiadaním v e-mailovej správe (napr. Informáciou o tom, že správca servera potrebuje na riešenie problému s naším e-mailovým kontom naše prihlasovacie údaje), alebo odkazom na falošnú webovú stránku s urgentnou výzvou, aby sme sa cez zaslaný link hneď prihlásili do svojho bankového účtu. V prípade, že zareagujeme na správu, napr. o výhre, podvodníci nám postupne napíšu, čo všetko potrebujú na odovzdanie výhry a nakoniec od nás budú žiadať buď prihlasovacie údaje do nášho internetbankingu, alebo úhradu nejakého poplatku (napr. dane z výhry, aby mohli výhru vyplatiť).

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



Obrázok 35 – Ukážky podvodných e-mailov

Veľmi podobnou podvodnou praktikou je **smishing**. Na rozdiel od phishingu však v tomto prípade podvodník rozposiela odkazy na podvodné webové stránky (prípadne podvodné telefónne čísla) prostredníctvom textových správ na mobilné telefóny–SMS. Ich účel je rovnaký–získať naše osobné údaje a citlivé informácie za účelom ich zneužitia.

Viac o smishingu a podvodných SMS, aj o tom ako nenaletieť, sa dozvieme, ak si pozrieme napríklad video „Podvodné SMS" (z programu „Tohle radši nezkoušejte") na iVysíláni Českej televízie: https://www.ceskatelevize.cz/porady/16497743667-tohle-radsi-nezkousejte/424235100291008/

Okrem phishingu je veľmi častý aj tzv. **vishing**. Ide o podvodný postup s využitím telefonického rozhovoru alebo sms správy, pomocou ktorého sa útočník od nás snaží vylákať citlivé údaje (naše osobné údaje, prístupové heslá do internetbankingu, čísla platobných kariet a pod.). S vishingom a smishingom je neraz spojený ďalší, veľmi sofistikovaný druh podvodu, odborne nazývaný **spoofing**. Ide o druh kybernetického útoku, pri ktorom útočník maskuje svoju identitu tak, aby sa nám javil ako dôveryhodný. Cieľom je vyvolať v nás pocit dôvery a toho, že ide o regulárny hovor, napríklad z našej banky. Na obrazovke telefónu vidíme názov svojej banky a človek na druhej strane linky sa nám predstaví menom zamestnanca, s ktorým bežne komunikujeme. Pred týmto druhom podvodu nás ochráni len naša ostražitosť a nedôvera.


Polícia upozornila na podvodné SMS. Chcú vylákať peniaze pod zámienkou nezaplatených pokút

Tieto správy sa vydávajú za komunikáciu od polície.

Obrázok 36 – Príklad smishingu

Je treba si uvedomiť, že žiadna banka ani inštitúcia od nás nikdy nebude žiadať citlivé údaje, ani prihlásenie sa do účtu cez telefonát (ani e-mailom). Telefonát je treba okamžite zrušiť, prípadne aj nahlásiť zneužitej inštitúcii alebo polícii. Aj vtedy, ak si pravosťou telefonátu nie sme istý, hovor ukončíme a jeho pravosť si overíme spätným telefonátom, alebo osobnou návštevou pobočky. Tu si pravosť telefonátu môžeme overiť. Ak na zobrazené číslo zavoláme my, už sa nedovoláme k podvodníkovi, ale do skutočnej banky, kde spravidla zistíme, že šlo o podvod.

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: Klikanie na odkazy v e-mailoch je často spôsobom, akým útočníci získavajú prístup k našim osobným údajom. Ak e-mail vyzerá divne, najlepšie je odstrániť ho, a to aj vtedy, keď poznáme osobu, ktorá ho poslala. Prípadne môžeme osloviť jej odosielateľa a na danú správu sa ho osobne opýtať.

Ďalšie **typy podvodných e-mailov** sú také, ktorých účelom je zavedenie **škodlivého softvéru** do zariadenia 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 však príjemca správy do zariadenia nainštaluje škodlivý softvér. Ďalšou možnosťou je poslanie správy s **infikovanou prílohou**, z dôvodu čoho sa neodporúča nastavenie automatického otvárania príloh e-mailov. Otvorením

správy sa totiž automaticky otvorí aj jej príloha, čím sa spustí škodlivý softvér, ktorý nám nainfikuje tablet, mobil či počítač.

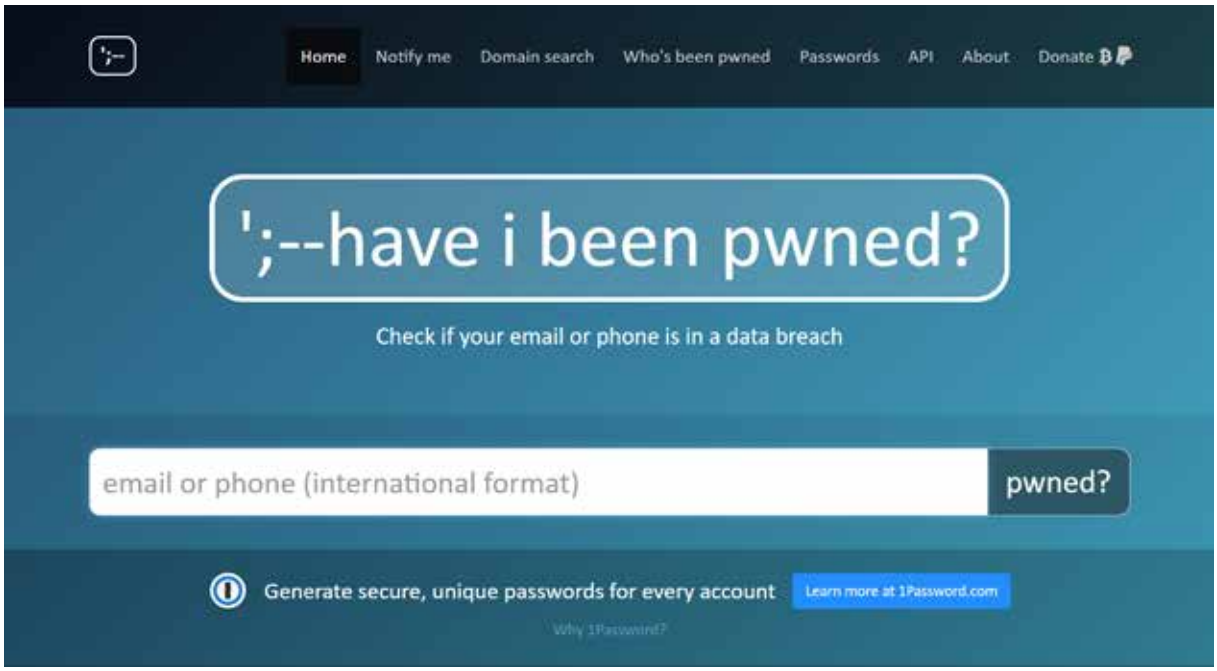
Upozornenie

Nikdy neposkytujte citlivé údaje vo forme odpovede na e-mail, aj keď sa zdá, že prišiel od známej a 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 náš 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 si chcel overiť, či jeho účet mohol byť pri úniku údajov vystavený tomuto riziku.



Obrázok 37 – Over svoj e-mail

Úloha 13

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

☐ Áno ☐ Nie

6.2. Sociálne siete

Obrázok 38 – Sociálne siete

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

Na základe týchto informácií sa v sociálnej sieti nadväzujú vzťahy medzi používateľmi, ktorí sa môžu spájať do skupín. Vzájomnými prepojeniami používateľov a skupín vzniká sieť vzťahov. Nevýhodou sociálnych sietí je fakt, že používatelia nemusia do svojho profilu vložiť pravdivé informácie, čo je takmer nemožné zistiť.

Príklady sociálnych sietí: Facebook, Instagram, LinkedIn, X (predtým Twitter), Telegram (ruská sociálna sieť), TikTok (čínska sociálna sieť na vytváranie a zdieľanie krátkych videí, veľmi populárna hlavne medzi mládežou), YouTube (sociálna sieť fungujúca na prezeranie aj bez registrácie a špecializovaná na zdieľanie videí).

Medzi strednou a staršou generáciou asi najrozšírenejšia sociálna sieť **Facebook** mala mať pôvodne skôr súkromný charakter. Napr. už samotný profil v nej, na rozdiel od profesionálne zameraných portálov (napr. LinkedIn), umožňuje zadať **množstvo osobných údajov** (napr. dátum narodenia, rodné mesto, súčasné bydlisko, kontaktné údaje, členovia rodiny, vzťah, vzdelanie, práca, politická a náboženská príslušnosť, záujmy, životné udalosti,...), ale súčasne nám umožňuje **zvoliť, kto môže jednotlivé informácie a príspevky vidieť** (verejnosť, priatelia mojich „priateľov", len moji „priatelia", iba ja). Na všetkých sociálnych sieťach však môžu používatelia priradiť k svojmu profilu fotografiu, ktorá sa zobrazí verejne.

Tak, ako v skutočnom živote človek nezdieľa všetky informácie o sebe 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 jej zobrazovania:

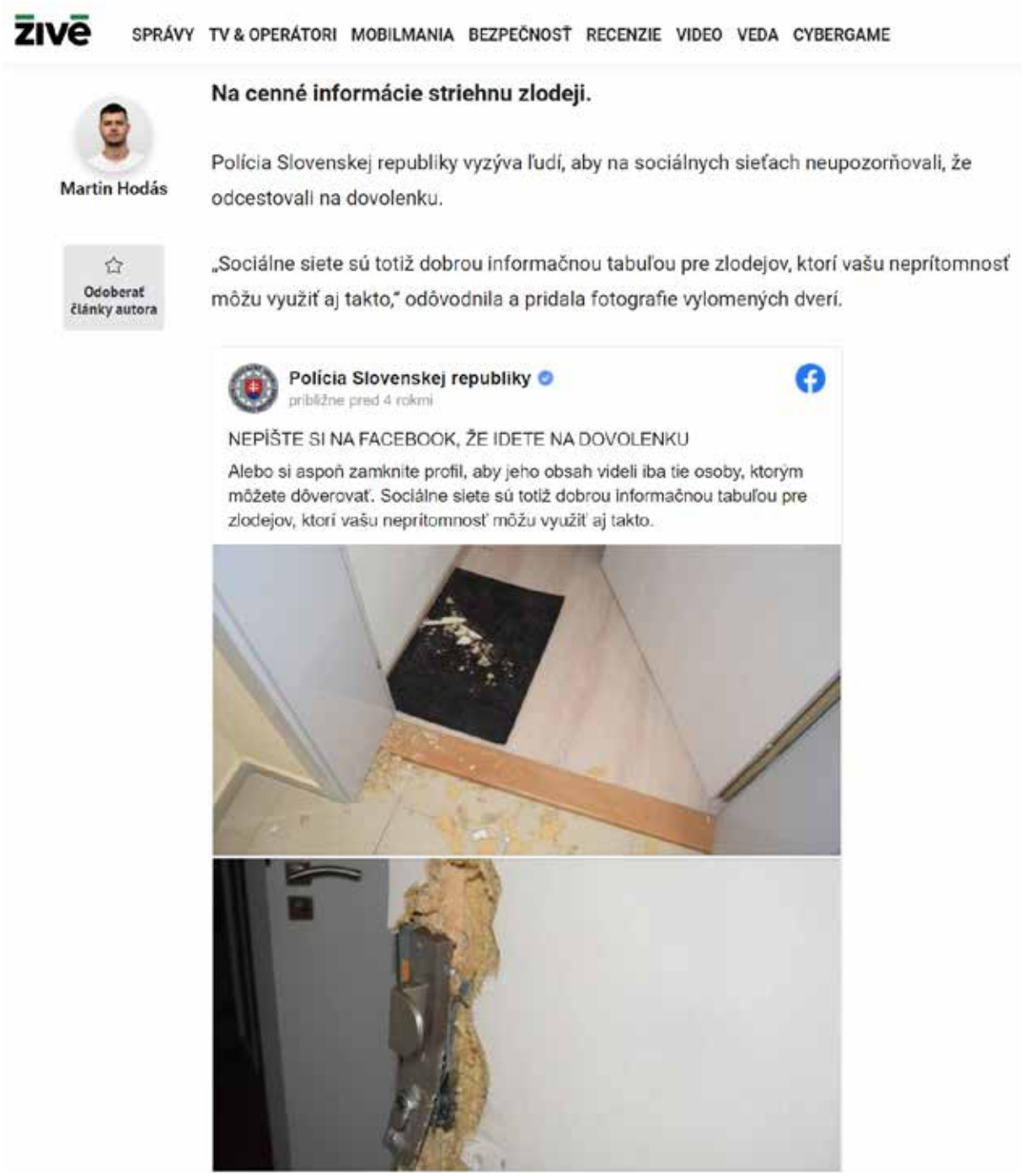
- **verejné** – pre kohokoľvek s účtom aj bez účtu na Facebooku = žiadne súkromie.
- **„priatelia", „priatelia" okrem ..., konkrétni „priatelia"** – informácie sú dostupné pre tých, ktorých sme označili za „priateľov". Základnou otázkou býva, či sú „moji priatelia" (na sieti) naozaj moji priatelia.
- **iba ja** – ochrana súkromia pre používateľov, ktorí si svoje súkromie chránia. Pri tomto nastavení, nemá okrem vlastníka (a správcu/administrátora sociálnej siete) 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 povoliť prístup len istej skupine ľudí, ktorí tak budú môcť pristupovať k našim informáciám a obsahu, ktorý na sociálnych sieťach zdieľame. Pre našu bezpečnosť na internete je dôležité mať čo najviac informácií o možnostiach nastavení ochrany súkromia a zabezpečenia našich údajov v používateľských účtoch na obľúbených webových stránkach a v sociálnych sieťach, kde sme zaregistrovaný. Prekonajme svoju prirodzenú lenivosť a venujme **nastaveniam súkromia a zabezpečeniu svojich používateľských účtov čas náležitú pozornosť**. Pomôže nám to predchádzať nemilým prekvapeniam a problémom spojeným s únikom našich súkromných dát a ich možným zneužitím.

V každej voľnej chvíľke, každý deň, milióny ľudí hľadajú na sociálnych sieťach nových priateľov, alebo komunikujú so starými kamarátmi. Pri tom neraz zdieľajú aj intímne udalosti svojho života, dokonca 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, pričom si neuvedomujú, 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 naše dieťa alebo vnúča 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 práve balia na dovolenku, čakajú na lietadlo, prileteli do slnečnej destinácie, atď., čo je ideálnou informáciou napríklad pre zlodeja, ktorý nám môže počas dovolenky vykradnúť opustený byt alebo dom.

Starostlivosť o svoju „digitálnu identitu" by mala byť základnou zručnosťou každého, kto sa pohybuje na internete. O tom, čo je a čo nie je vhodné verejne zdieľať a aké dopady na náš reálny život môže mať naše nevhodné správanie sa na internete a sociálnych sieťach, sa môžeme dozvedieť viac vo videu „Digitální identita" (z programu „Tohle radši nezkoušejte") na iVysíláni Českej televízie: https://www.ceskatelevize.cz/porady/16497743667-tohle-radsi-nezkousejte/424235100291010/



Obrázok 39 – Jeden z dôsledkov zverejňovania informácií na sociálnej sieti

Pri používaní rôznych služieb ako sú 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 niekto neskopíroval. Tiež je známym faktom, že niektoré sociálne siete obsah nemažú, na ich serveroch zostáva uložený aj naďalej. Informácie o používateľoch sociálnych sietí sú tak zhromažďované a strojovo spracované na ďalšie použitie v budúcnosti.

To, čo **uverejníme, bude uverejnené navždy:** Musíme si byť vedomí 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. Tie sú schopné o sebe prezradiť všetko. To často zneužívajú zločinci, ktorí si na sociálnych sieťach pod falošnou identitou hľadajú mladých „kamarátov”.

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. Čoraz častejšie je na tieto účely zneužívaná aj „umelá inteligencia”. Dávajme si pozor na to, čo zverejňujeme na sociálnych sieťach, aj na zasielanie intímneho obsahu, hlavne neznámym ľuďom. Často býva zneužitý na kyberšikanu a vydieranie.
- **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 svoj profil nepravdivými údajmi. Ďalšou skupinou sú osoby, ktoré chcú komunikovať na sociálnej sieti, ale nemajú záujem vyzradiť svoju vlastnú identitu. Preto použijú vymyslenú, alebo ju niekomu ukradnú. Falošná identita býva zneužívaná pri groomingu, na šírenie nepravdivých informácií a hlavne na romatické podvody s láskou s cieľom zmanipulovať svoju obeť a obohatiť sa.

Vojak alebo lekár na misii–atraktívny človek, ktorý nás na sociálnej sieti denne zahŕňa láskou. Vidinu spoločného života však naruší nečakaný problém, na vyriešenie ktorého sú nevyhnutné naše peniaze... To je typický scénar internetového podvodu s láskou. Viac informácií o tomto type podvodov, aj s osobnou výpoveďou reálneho vojaka–občana Českej republiky slúžiaceho v americkej armáde, ktorý sa stal obeťou krádeže identity na sociálnej sieti za účelom romantických podvodov s láskou, obsahuje video „Láska mezi kontinenty” (z programu „Tohle radši nezkoušejte”) na iVysíláni Českej televízie:

https://www.ceskatelevize.cz/porady/16497743667-tohle-radsi-nezkousejte/424235100291007/

Okrem toho podvodné správy, ktorými sa podvodníci od nás snažia vylákať naše prístupové údaje, sa objavujú aj na sociálnych sieťach.

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

Dokument nám ukazuje, ako naozaj fungujú sociálne siete. Ako 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 to najdôležitejšie, aby sme to posunuli ďalej zdieľaním. Pre falošné správy sa sociálne siete stali priam rajom. Čím viac času tu strávime, čím viac ich obsahu vidíme, tým vzniká väčší priestor na predaj reklamy a produktov a tým viac dolárov tečie do vreciek ich akcionárov a majiteľov.

Obrázok 41 – Netflix – film Sociální dilema

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

Na záver je však 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, či riešiť spoločne na diaľku problémy. Každý deň vznikajú sociálne siete a stránky zamerané na určitý koníček. Ich používatelia hľadajú ľudí z celého sveta, s ktorými majú rovnaké záujmy a celá ich komunikácia 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.

6.3. Dezinformácie a mediálna gramotnosť

Dezinformácia je overiteľne nepravdivá, zavádzajúca alebo manipulatívne podaná informácia–klamstvo, polopravda alebo fakt vytrhnutý z kontextu. Ide o správu, ktorá bola vytvorená zámerne a je šírená s úmyslom klamať alebo zavádzať. Často obsahuje aj fakt, ktorý je na prvý pohľad pravdivý, čo jej dodáva na dôveryhodnosti. To sťažuje jej odhalenie.

Dezinformácie sú staré ako ľudstvo samé. Boli a sú využívané vo všetkých politických režimoch ako nástroj tzv. „psychologickej vojny" a „hybridnej vojny" na nekalý politický boj, spravodajské hry a politickú propagandu, prípadne môže ísť o lživú reklamu či „antireklamu". Autori dezinformácií využívajú rôzne manipulatívne techniky. Ich zámer je klamstvom a zavádzaním šíriť strach, nenávisť, rozoštvávať a manipulovať (protivníkom, skupinou ľudí, verejnosťou) s cieľom niekomu poškodiť, alebo pre niekoho zabezpečiť politický či finančný zisk. Na tieto účely sa neštítia zneužívať ani národné, vlastenecké alebo kultúrne cítenie, či náboženské presvedčenie.

Psychologická vojna–snaha o zmenu postoja ľudí k faktom, ktoré sú neodškriepiteľné a zmeniť ich nie je možné (snaha zmeniť ich názor / pohľad na daný fakt).

Hybridná vojna–konflikt, ktorý kombinuje tradičné vojenské operácie s rôznymi nevojenskými metódami, vrátane kybernetických útokov (v čase otvoreného ozbrojeného konfliktu alebo „studenej vojny").

S nástupom moderných digitálnych technológií a internetu dosiahli dezinformácie veľkého rozmachu. Šíria sa na sociálnych sieťach, cez reťazové e-maily, dezinformačné weby, niektorých „influencerov" a ich propagandistické a dezinformačné internetové kanály, ale aj mimo internetu cez dezinformačné médiá (tlač, rozhlas, televízia).

Influencer–verejne známa osoba (herec, hudobník, športovec, redaktor, politik,...), ktorá má vplyv na svojich priaznivcov a sledovateľov (je ich vzorom, čím dokáže ovplyniť ich názory a rozhodovanie sa pri nakupovaní, voľbách,...).

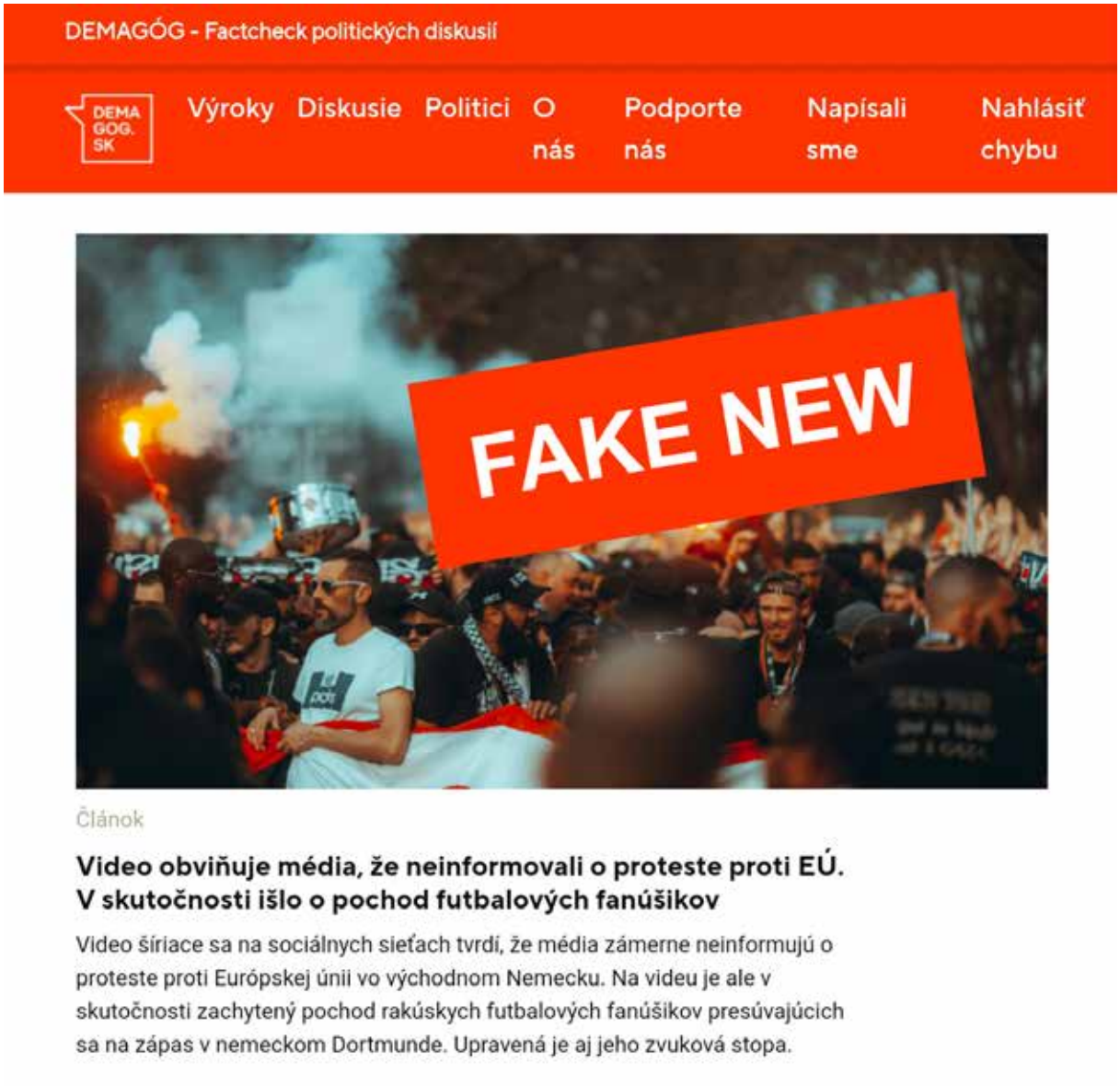
Najčastejšie využívané formy dezinformácií:

• **Falošné správy / Fake News** – úmyselne vytvorené a cielene šírené klamstvá a zavádzajúce správy, ktoré napodobňujú spravodajstvo alebo iný novinársky žáner.

• **Hoaxy / Fámy** – „naliehavá" správa, často poplašná, s výzvou na jej preposlanie ďalej (pozri kapitolu 6.1. Elektronická pošta–E-mail).

• **Propaganda** – informácie, myšlienky, názory, vizuálny materiál–(fotografie, videá), ktorých cieľom je nie informovať verejnosť, ale manipulovať – prostredníctvom skresľovania pravdivých faktov presviedčať a meniť názory ľudí a vyvolať či posilniť u nich určité postoje alebo konanie (tzv. „vymývanie mozgov" v prospech určitej skupiny ľudí, politickej strany alebo názoru, často na úkor a bez rešpektovania názoru iných). Vytvára zdanie vyššieho cieľa (napríklad boj za práva občanov a ich vlasti, národnú hrdosť, jednostranne prezentované „ľudské práva", právo na život a pod.), na čo využíva ľudské vášne, strach a nenávisť.

• **Konšpiračná teória** – vysvetľuje udalosť alebo súbor okolností ako výsledok tajného sprisahania (konšpirácie) malou mocnou skupinou osôb (vláda, tajný spolok, organizácia, spravodajská služba, firma,... či dokonca mimozemská civilizácia). Odmieta pri tom všeobecne akceptované vysvetlenie danej udalosti, aj vedecky podložené dôkazy.



Obrázok 41 – Príklad falošnej správy (Fake New)

Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira, paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené.

Šírenie dezinformácií internetom je rýchle a má obrovský dosah. Zorientovať sa v obrovskom množstve informácií a nájsť ich dôveryhodný zdroj nie je pre laika jednoduché. Vyžaduje si to kritické myslenie a ochotu sa nad správami analyticky zamýšľať.

Ako si overiť, či je správa pravdivá?

1. Naučme sa rozlišovať, či ide o fakt alebo názor (nieči osobný / subjektívny):

fakt – skutočnosť popisuje (je objektívny, neutrálny a overiteľný),

názor – skutočnosť interpretuje (je subjektívny, zaujatý a neoveriteľný).

2. Zvážme / overme si dôveryhodnosť správy a média – pomôžu nám pri tom odpovede na 4 základné otázky: Poznám autora článku? Kto je šéfredaktor média, kde článok vyšiel? Kto toto médium vlastní? Poznám pôvod informácií?

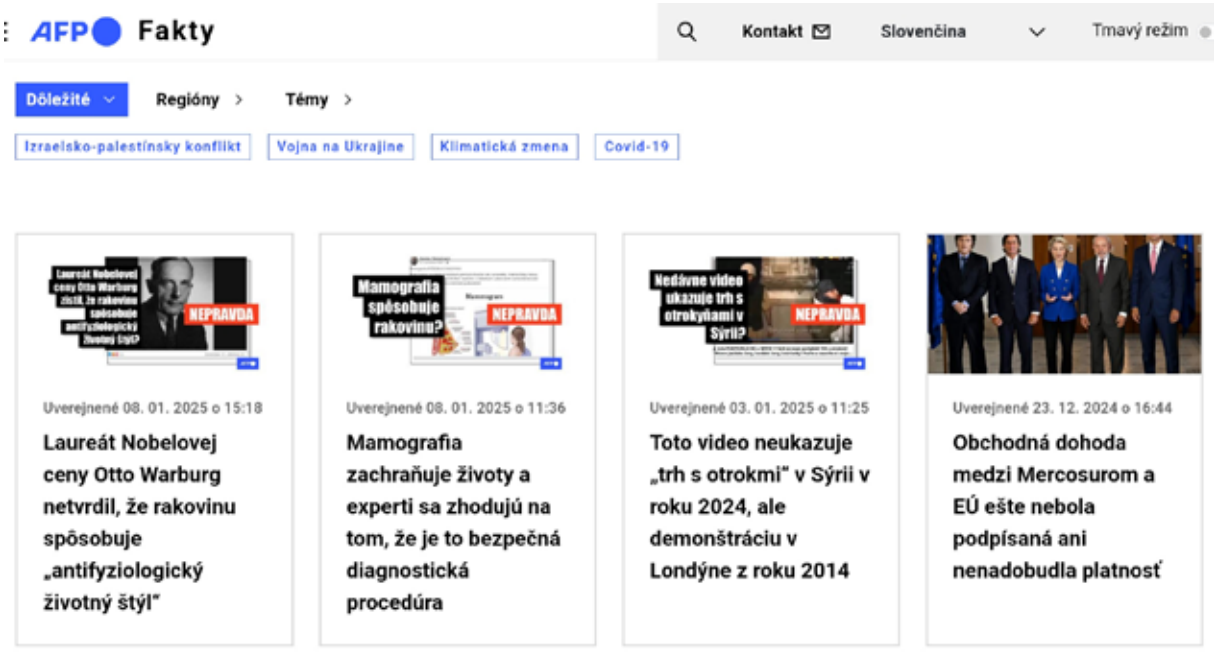
Mediálna gramotnosť–schopnosť informácie a médiá nielen konzumovať, ale aj zmysluplne a zodpovedne s nimi pracovať.

O tom, ako správne overovať informácie a rozpoznať dôveryhodné zdroje sa môžeme dozvedieť viac vo videu „Dezinformace" (z programu „Tohle radši nezkoušejte") na iVysíláni Českej televízie: https://www.ceskatelevize.cz/porady/16497743667-tohle-radsi-nezkousejte/424235100291001/

Kurzy a kvíz mediálneho vzdelávania (nielen) pre seniorov nájdete na českých webových stránkach Kurzy „Fakt, jo?" (https://www.faktjokurz.cz/):

Pravdivosť populárnych správ zdieľaných na internete, ale aj pravdivosť mnohých výrokov (nielen) politikov, je možné si overiť na stránkach venujúcich sa hoaxom (pozri odkazy v kapitole 6.1.) a tiež napríklad na špecializovaných webových stránkach:

demagog.sk demagog.cz fakty.afp.com



Obrázok 42 – Webová stránka na overovanie informácií fakty.afp.com

Boj proti dezinformáciám začnime u seba. Nenechajme sa manipulovať dezinformáciami a neprispievajme k šíreniu strachu a nenávisti ich preposielaním a zdieľaním. Buďme zodpovední, otvorení diskusii, ochotní prijímať cudzie argumenty a zdieľajme len správy z dôveryhodného zdroja. Internet je neregulovaný priestor a zďaleka nie všetko, čo na ňom nájdeme, je pravda.

Upozornenie

Dezinformácia ako taká nie je trestná. Jej šírením sa však môžeme dopustiť iných trestných činov–ohovárania, šírenia poplašnej správy, krivého obvinenia, či schvaľovania a podnecovania k trestnému činu. Dávajme si preto pozor, čo na internete píšeme a zdieľame.

Neznalosť zákona nás neospravedlňuje.

Úloha 14

Na webovej stránke demagog.sk (https://demagog.sk/) vyhľadajte výroky svojho obľúbeného politika a potom politika, ktorému dôverujete najmenej. Prezrite si ich výroky, ktoré prešli overovaním pracovníkmi webu a poznačte si, koľko z nich je pravda, koľko nepravda, koľko je zavádzajúcich a koľko z nich sa nedá overiť (výsledné čísla nám pomôžu zistiť, do akej miery sme manipulovateľní a či máme tendenciu podliehať dezinformáciám).

Môj obľúbený politik:

☐ Pravda ☐ Nepravda ☐ Zavádzajúce ☐ Neoveriteľné

Politik, ktorému najmenej dôverujem:

☐ Pravda ☐ Nepravda ☐ Zavádzajúce ☐ Neoveriteľné.

6.4. „Umelá inteligencia” a jej zneužívanie

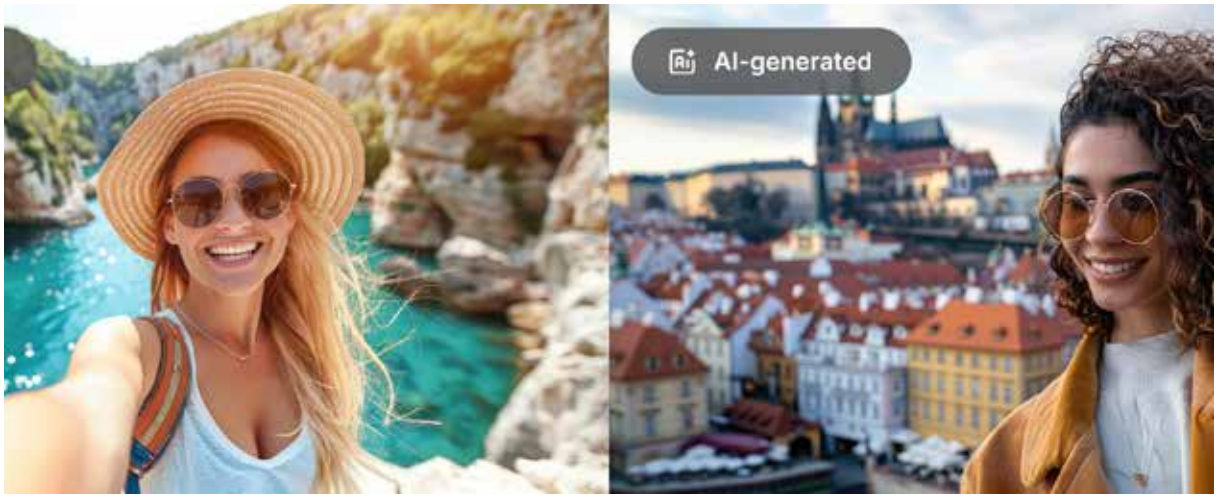
„Umelá inteligencia” (AI) je tak fascinujúca, ako aj desivá, keďže sa dá využiť tak na dobré, ako na zlé účely. O možnostiach jej praktického využitia a o tom, ako nám vie byť užitočná, si povieme viac v Module 5 (kapitola 4.6. „Umelá inteligencia” a jej využitie v každodennom živote). V tejto kapitole sa zacielime na najčastejšie spôsoby jej zneužívania na kybernetické podvody.

Napodobenie hlasu (manipulácia s hlasom) niekoho, koho dobre poznáme a dôverujeme mu, je zákerná podvodná praktika, ktorá je už dnes alfou a omegou pri mnohých kybernetických útokoch. S využitím „umelej inteligencie” zaberie podvodníkom len pár minút. Stačí im k tomu akákoľvek hlasová nahrávka danej osoby – odpočúvaný telefonát, video alebo hlasový záznam zverejnený na internete. Podobným spôsobom môže byť pomocou „umelej inteligencie” manipulované aj s fotkami a videom.

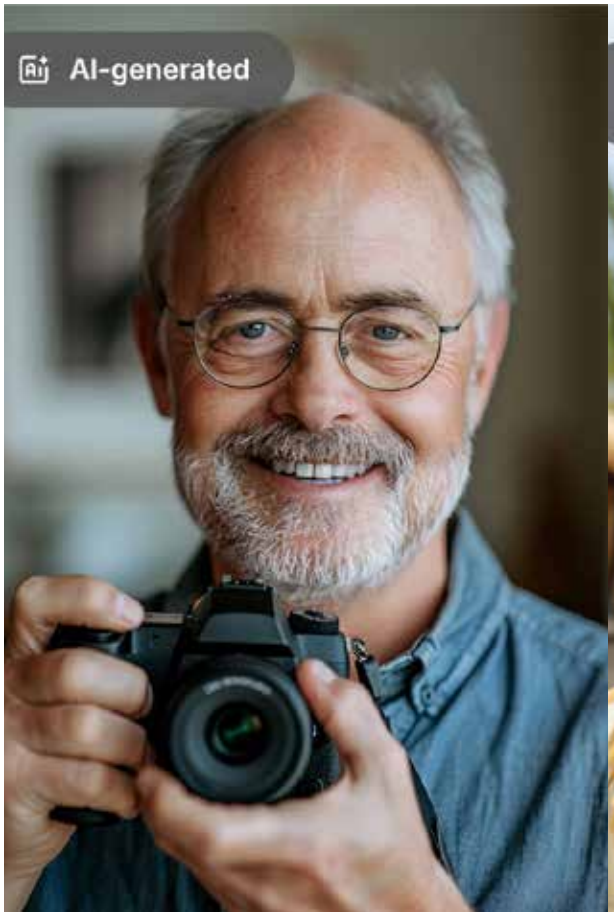
Podvodníci veľmi dobre vedia, ako im vie „umelá inteligencia” uľahčiť prácu a vedia aj to, že s ňou môžu byť pri kybernetických útokoch a podvodoch oveľa efektívnejší. Je treba si však uvedomiť, že „umelá inteligencia” je len algoritmus (počítačový program) a zneužíva ju človek.

Deepfakes (falzifikáty) sú obrázky, videá alebo hlasové nahrávky, ktoré sú upravované alebo generované pomocou nástrojov „umelej inteligencie”. Môžu zobrazovať skutočné alebo neexistujúce osoby, k napodobenému hlasu môžu pridať aj podvrhnuté video a do úst nám dokážu vložiť to, čo sme nikdy nevyslovili. Deepfakes videá môžu byť zneužité na vydieranie, šikanu, na šírenie dezinformácií a manipuláciu voličov pri politických kampaniach (hlavne pred voľbami), alebo na podvodnú reklamu. Takmer každý z nás sa už mal možnosť stretnúť so zneužívaním známych osobností a politikov v reklamách napríklad na pochybné produkty alebo falošné / podvodné investície.

Odhaliť deepfake (falzifikát), predovšetkým pre bežného laika, nie je ľahké, aj keď existujú nástroje, ktoré dokážu analyzovať video či zvukovú nahrávku a zistiť, či s nimi bolo manipulované. Obranou pre nás je preto predovšetkým vzdelávanie sa a kritické myslenie.

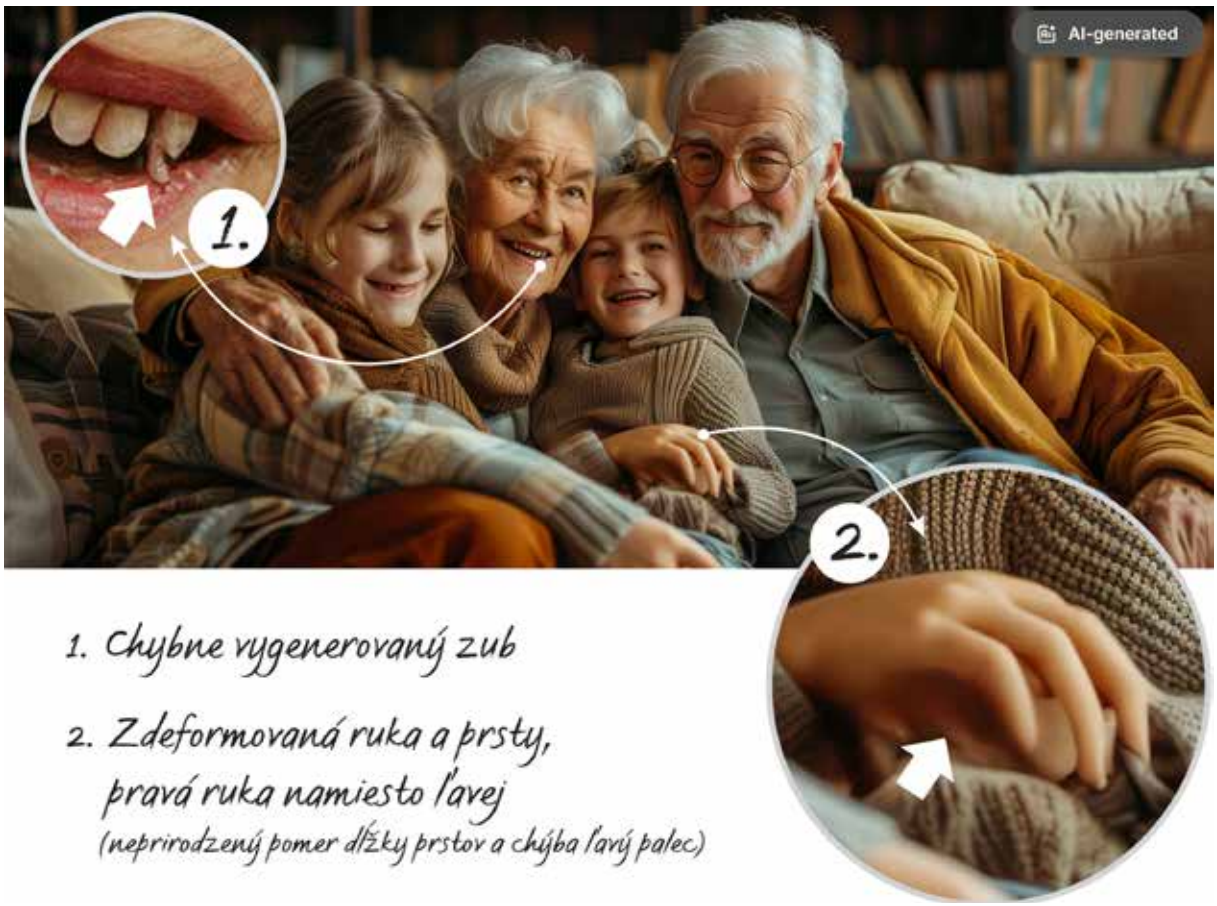


Obrázok 43 – Deepfake – Fiktívne zábery z dovolenky (nie realita) / „fotografie" vygenerované („nakreslené") „umelou inteligenciou", ktoré laik (a nielen on) na pohľad nerozozná od skutočných (Ešte stále ste presvedčený, že všetko, čo vidíte na sociálnych sieťach, sa skutočne stalo?)–zdroj ilustračných obrázkov: freepik.com



Obrázok 44 – Deepfake – „Portrét" fiktívneho človeka (v reáli neexistuje) / bezchybný „fotoportrét" vygenerovaný „umelou inteligenciou" (Ešte stále ste presvedčený, že každý človek, ktorého vidíte na profilovej fotografii na sociálnej sieti a požiadal vás o „priateľstvo", naozaj reálne existuje?))– zdroj ilustračného obrázka: freepik.com

Obrázok 45 – Deepfake – To, že na tejto „fotografii" niečo nesedí, udrie do očí väčšine z nás už na prvý pohľad. Nenechajme sa nikým nachytať. Jej „autor" nás chcel len pobaviť a žirafa „s úsmevom leva" nie je žiadnou hračkou prírody, ale opäť len výtvorom „umelej inteligencie"– zdroj ilustračného obrázka: freepik.com



Obrázok 46 – Deepfake – Odhaliť falzifikát fotografie, ktorý vygenerovala „umelá inteligencia", len pohľadom naň je spravidla veľmi ťažké, pri dokonalom deepfake priam nemožné aj pre odborníka. Napriek tomu sa na mnohých z nich dajú nájsť drobné nedostatky, z ktorých niektoré si máme šancu všimnúť až pri ich detailnom skúmaní, často až „pod lupou" (drobné neprirodzené „chybičky krásy", neprirodzené proporcie alebo črty tváre, zdeformované ruky, prsty a pod.)–zdroj ilustračného obrázka: freepik.com

Obrázok 47a

Obrázok 47b
Deepfakes – Neprirodzené osvetlenie a tiene, chybičky v textúre, neprirodzená poloha tela, ale aj až prílišná dokonalosť snímky bez typického „zrna" sú signálom toho, že „fotografia" môže byť vygenerovaná nástrojmi AI, alebo sa ňou inak manipulovalo–zdroj ilustračných obrázkov: freepik.com

Viac informácii o „umelej inteligencii" a jej zneužívaní podvodníkmi, ale aj o tom, ako pomáha bankám chrániť naše financie na našich bankových účtoch, sa môžeme dozvedieť, ak si pozrieme video „Umělá inteligence" (z programu „Tohle radši nezkoušejte") na iVysíláni Českej televízie:

https://www.ceskatelevize.cz/porady/16497743667-tohle-radsi-nezkousejte/424235100291004/

Upozornenie

Neverme všetkému len preto, že to odporúča niekto slávny. Overujme si informácie z relevantných zdrojov a rozlišujme medzi faktami a dojmami.

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 pojmom phishing (odchytávanie prístupových údajov), smishing (rozposielanie odkazov na podvodné stránky cez SMS), vishing (snaha vylákať citlivé údaje cez telefonát), spoofing (maskovanie identity útočníka s cieľom pôsobiť dôveryhodne)	
rozumieť pojmom dezinformácia, falošné správy (Fake News), hoax, propaganda, konšpiračná teória	
rozumieť pojmom mediálna gramotnosť, vedieť rozlíšiť fakt a názor a poznať pravidlá overovania si pravdivosti informácií	
poznať pravidlá zodpovedného narábania s informáciami	
rozumieť pojmom „umelá inteligencia" a deepfakes, zoznámiť sa so spôsobmi zneužívania „umelej inteligencie" pri kybernetických podvodoch	

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	
osvojiť si kritické myslenie pri práci s informáciami na internete	

DIGITÁLNI 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 978-80-69030-05-3