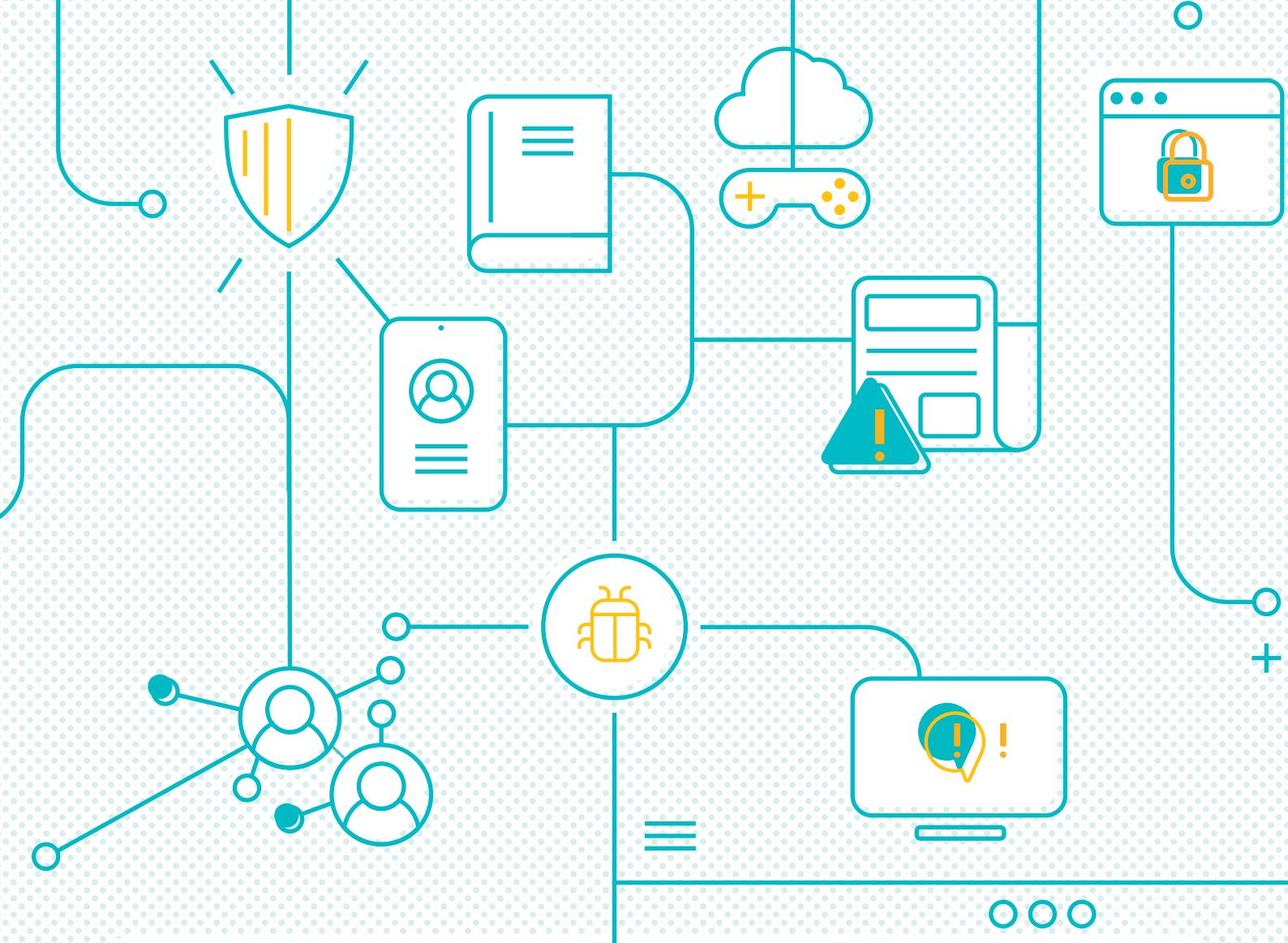


PRÍRUČKA DIGITÁLNEJ BEZPEČNOSTI

PRE UČITEĽOV
1. a 2. stupňa ZŠ

ESET | bezpečne na nete.sk

ISBN 978 – 80 – 973884 – 0 – 9

Poďakovanie

Radi by sme sa poďakovali za spoluprácu na tejto príručke **všetkým kolegom z ESETu**, ktorí nám pomáhali svojimi odbornými radami, komentármi, ale aj organizačnými schopnosťami.

Rovnako by sme sa radi poďakovali psychologičke **Jarmile Tomkovej**, ktorá zostavila viaceré kľúčové kapitoly na základe svojich odborných znalostí z praxe.

V neposlednom rade sa chceme poďakovať **všetkým učiteľom**, ktorí aj napriek nepriaznivým podmienkam vzdelávajú a pripravujú novú generáciu na život v digitálnej dobe. Mimoriadne vďační sme najmä **Petrovi Kučerovi**, ktorý si našiel čas na stretnutia s nami a dal nám užitočnú spätnú väzbu.

Obsah

Úvod

Internet a digitalizácia zmenili svet. Zásadné zmeny pritom neobišli ani deti a mládež, ktoré vyrastajú vo svete smartfónov, aplikácií či sociálnych sietí. Tieto technológie im síce otvárajú nové nevídané obzory, no prinášajú aj riziká a hrozby, ktoré predchádzajúce generácie nepoznali.

Učitelia základných škôl v tejto situácii tvoria prvú líniu, no sú často ponechaní bez potrebných materiálov či informácií. Je pritom ich úlohou učiť žiakov o digitálnom aj nedigitálnom svete a pripraviť ich na život v nich.

ESET je tu, aby pomohol.

Ako globálny líder v oblasti digitálnej bezpečnosti s viac ako 30-ročnými skúsenosťami a viac ako 110 miliónmi chránených používateľov na celom svete veríme, že je možné, aby si rodičia mohli vychutnať digitálny život bez obáv o bezpečnosť svojich detí. Na dosiahnutie tohto cieľa však musíme v prvom rade zvýšiť povedomie o dôležitosti online bezpečnosti medzi deťmi.

V rámci globálnej iniciatívy spoločnosti ESET – SaferKidsOnline sme sa rozhodli na Slovensku vytvoriť platformu Bezpečne na nete, ktorá má za cieľ vzdelávať nielen širokú verejnosť, ale špecificky sa zameriava aj na deti, rodičov a učiteľov ako dôležité články v procese vzdelávania.

Dôležitou súčasťou dlhodobého a rozsiahleho úsilia je aj táto príručka založená na vedomostiach, skúsenostiach a poznatkoch našich renomovaných oceňovaných odborníkov. Učiteľom základných škôl poskytuje základné teoretické znalosti o digitálnej bezpečnosti a bezpečnom používaní internetu.

Obsahuje praktické cvičenia, ktorými túto problematiku dokážu zaujímavo a často aj interaktívne odprezentovať svojim žiakom s dôrazom na moderné didaktické metódy. Je tiež súčasťou dlhodobej a oveľa širšej snahy spoločnosti ESET zvyšovať bezpečnosť používateľov a najmä detí na internete.

Pre viac zdrojov aj z pohľadu rodiča či samotného dieťaťa sme preto vytvorili vzdelávací portál Bezpečne na nete.

V tejto príručke sa stretávajú dva pohľady na digitálnu bezpečnosť:

- Technický – vychádzajúci z expertízy a oblasti pôsobenia spoločnosti ESET, ktorá viac ako 30 rokov vyvíja bezpečnostné technológie pre digitálne zariadenia.
- Psychologický – niektoré digitálne hrozby, ako napríklad kyberšikana, sa nedajú vyriešiť len pomocou technológií, nakoľko majú často presah z online aj do offline sveta.

Jednou z prekážok pri vzdelávaní môže byť tzv. generačná priepasť. Ide o to, že dnešné deti a mládež sú v priamom kontakte s najnovšími technológiami a majú preto oveľa detailnejšiu skúsenosť a zručnosti, ako ich využívať. To však neznamená, že s nimi učiteľ nemôže držať krok a prekonať generačnú priepasť:

- Učiteľ sa nemusí snažiť deťom vyrovnať. Zato sa môže s deťmi rozumne dopĺňať a zodpovedne koordinovať vzájomné učenie.
- Okrem učenia spoza katedry by mal využívať modernejšie metódy zážitkového vzdelávania, projektové, rovesnícke učenie a pod.
- Učiteľ môže prinášať problémové situácie, iniciovať nimi diskusiu a záujem o problém. Nemusí vždy ukázať riešenie, môže byť len moderátorom diskusie, v ktorej skupina žiakov sama nájde vhodné riešenia alebo sa minimálne zamyslí nad existenciou daných problémov.

Veríme, že táto príručka bude pre vás, učiteľov, užitočným nástrojom pri príprave a tvorbe vyučovania.

Niektoré kapitoly z teórie obsahujú praktické cvičenia, ktoré možno nájsť v dokumente Aktivity k Príručke digitálnej bezpečnosti (ďalej len „Aktivity“). Ide o sériu aktivít navrhnutých odborníkmi spoločnosti ESET, učiteľmi informatiky a detskými psychológmi, ktoré pútavou a praktickou formou prezentujú témy digitálnej bezpečnosti a bezpečného používania internetu deťmi. Zoznam aktivít nájdete v úvode kapitoly.

Bezpečnosť mobilných zariadení

Kľúčové slová

aplikácia | cloud | mobilný antivírus | mobilné bezpečnostné riešenie | mobilné zariadenie | návrat k továrenským nastaveniam (factory reset) | operačný systém | PIN kód | sledovateľ (follower) | smartfón | tablet | vývojár (developer)

Otázky, na ktoré odpovedá táto kapitola:

Aké sú základné pravidlá zabezpečenia mobilných zariadení? Prečo si zamykať obrazovku a ktorý spôsob je najbezpečnejší? Ako a prečo si udržiavať aktualizované aplikácie a operačný systém? Prečo si sťahovať aplikácie len z oficiálneho obchodu s aplikáciami pre Android/Apple zariadenia? Ako bezpečne sťahovať aplikácie a čo si na nich všímať? Potrebuje mobil/tablet antivírusovú ochranu? Prečo by si mal používateľ vytvárať zálohy a kde si ich môže bezpečne uložiť?

Praktické cvičenia k tejto kapitole:

Nastav si svoj smartfón, Modelová konferencia o sociálnych sieťach

Aké sú základné pravidlá zabezpečenia mobilných zariadení?

Jedným z prvých krokov, ktorý môže každý používateľ/žiak/študent urobiť pre svoju vyššiu bezpečnosť, je výber kvalitného mobilného zariadenia od overeného výrobcu.

Mnohé z nasledujúcich odporúčaní platia pre oba najrozšírenejšie operačné systémy Android a iOS. Pri Androide majú okrem zabudovaného zabezpečenia používatelia možnosť nainštalovať si aj bezpečnostný softvér. Zabezpečenie mobilného zariadenia (najmä tabletu, smartfónu) má niekoľko úrovní:

1. **Prístup do zariadenia:** Zariadenie by si mal používateľ vždy zamykať pre prípad straty či krádeže, no napríklad aj na ochranu uložených informácií pred neželaným prístupom inej osoby. V súčasnosti sa zariadenia zamykajú vstupným vzorom[1], PIN kódom alebo skenerom odtlačku prsta či tváre. Sken odtlačku prsta v kombinácii so štvor- až šesťmiestnym PIN kódom patrí aktuálne k najspoľahlivejším formám takejto ochrany. Ak zariadenie nemá skener odtlačku, prípadne takéto zabezpečenie neponúkne automaticky, používateľ si môže možnosti uzamykania a ich úroveň nastaviť sám v sekcii „Nastavenia".

2. **Fyzická bezpečnosť zariadenia:** Dnešné mobilné zariadenia obsahujú množstvo citlivých údajov, ktoré sa môžu v prípade straty alebo krádeže dostať do nesprávnych rúk. Používatelia by si preto mali aktivovať služby, ktoré im umožnia zariadenie na diaľku nájsť, uzamknúť či vymazať. Postup, ako si takúto službu aktivovať:

   pri Android zariadeniach

   pri Apple zariadeniach

3. **Zálohy:** Niektoré škodlivé kódy a útoky môžu narušiť fungovanie mobilného zariadenia natoľko, že je potrebný návrat k továrenským nastaveniam (v angl. „factory reset"). Tento krok automaticky vymaže **všetky údaje používateľa** vrátane jeho kontaktov, fotografií, videí alebo uložených nastavení. Práve pre podobné situácie by si používateľ mal všetky cenné dáta z mobilného zariadenia pravidelne ukladať (napríklad raz mesačne) na iné miesto a vytvárať si zálohu.

   Možností, ako to urobiť, je viacero:

   a. Jednou z používateľsky najjednoduchších je záloha v cloude, ktorú za menší mesačný poplatok umožňujú samotní výrobcovia ako Google a Apple, prípadne ďalšie aplikácie v obchodoch s mobilnými aplikáciami Google Play a App Store.

   b. Alternatívou je záloha na disku, ktorý nie je pripojený na internet, a teda neposkytuje útočníkom možnosť sa naň dostať napríklad cez zraniteľnosť alebo slabé zabezpečenie. Príkladom je externý disk, ktorý používateľ okamžite po vytvorení zálohy odpojí od počítača.

4. **Zabezpečenie citlivých aplikácií**: Kombináciou odtlačku a PIN kódu si používateľ môže zabezpečiť aj niektoré aplikácie, ako sú napríklad internetbanking či kryptopeňaženky[2]. Ide o samostatný PIN kód, ktorý by mal byť odlišný od toho, ktorý chráni vstup do zariadenia.

1 Používateľ pospája v správnom poradí niektoré z deviatich bodov zobrazených na zariadení.
2 Program v zariadení, ktorý dokáže uložiť kryptomeny ako Bitcoin, Monero, Ethereum a ďalšie.

5. **Pozor na aplikácie z neoficiálnych obchodov:** Pre čo najvyššiu bezpečnosť zariadenia odporúčame používať len aplikácie z oficiálneho obchodu s aplikáciami pre danú platformu (Google Play pre Android, App Store pre iOS). Používatelia by sa mali vyhýbať neoficiálnym obchodom a fóram, cez ktoré útočníci najčastejšie šíria škodlivé kódy.

6. **Recenzie aplikácií od iných používateľov:** Pred inštaláciou aplikácie z oficiálneho obchodu by si používateľ mal vždy prečítať recenzie ostatných používateľov. V prípade, že označujú aplikáciu za podvod, malvér či vírus, mal by používateľ jej inštaláciu odložiť a overiť si aspoň jednoduchým online vyhľadávaním, či nebola označená za nebezpečnú. Špeciálnu pozornosť by pritom mal venovať najmä negatívnym komentárom. Pozitívne si totiž útočníci často vytvárajú sami, aby zvýšili svoje šance na úspech. Podvodné aplikácie tiež často sľubujú to, čo nedokážu splniť, napr. rýchle a bezplatné zvýšenie počtu priateľov/sledovateľov (followerov) na sociálnej sieti či ľahký zárobok výmenou za inštaláciu aplikácie do zariadenia.

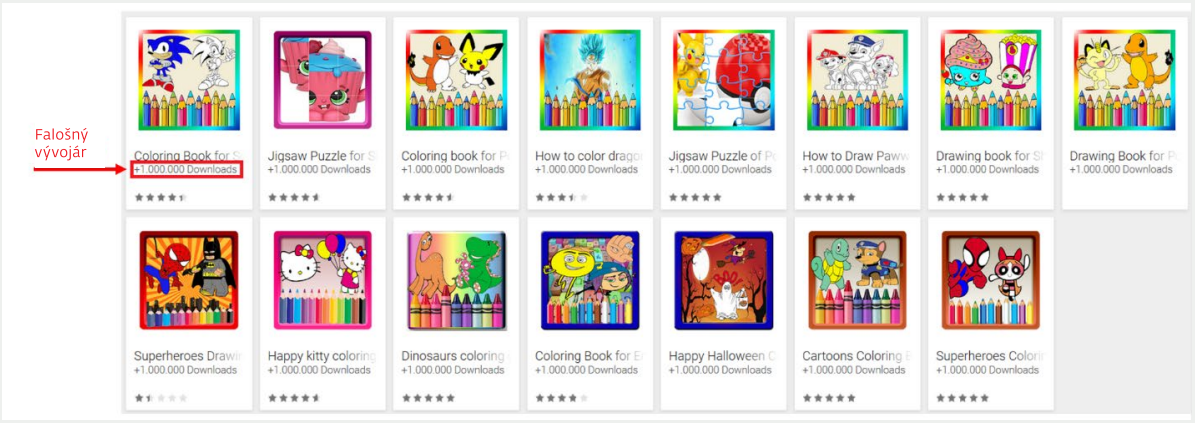
7. **Oprávnenia požadované aplikáciou:** Každá aplikácia ešte pred inštaláciou upozorní používateľa, ktoré dáta a funkcie požaduje na plnenie svojej funkcie. Podozrivé aplikácie pritom často žiadajú aj prístup k funkciám, ktoré nijako nesúvisia s ich účelom. Ak si napríklad aplikácia na prezeranie fotografií žiada prístup k mikrofónu, môže ísť o snahu sledovať používateľa.

8. **Aktualizácia operačného systému a aplikácií:** Vývojári neustále nachádzajú nové slabiny a zraniteľnosti v aplikáciách a pravidelne vydávajú aktualizácie, ktoré odstránia tieto problémy. Používateľ by sa preto mal snažiť udržiavať aplikácie aj operačný systém svojho zariadenia na čo najaktuálnejšej úrovni. V zariadení si používateľ môže nastaviť automatickú inštaláciu aktualizácií alebo možnosť, kedy mu zariadenie ponúkne aktualizácie a spustia sa až na príkaz používateľa (prostredníctvom sekcie „Nastavenia“, resp. „Settings“). Tejto téme sa bližšie venujeme aj v samostatnej kapitole Aktualizácie.

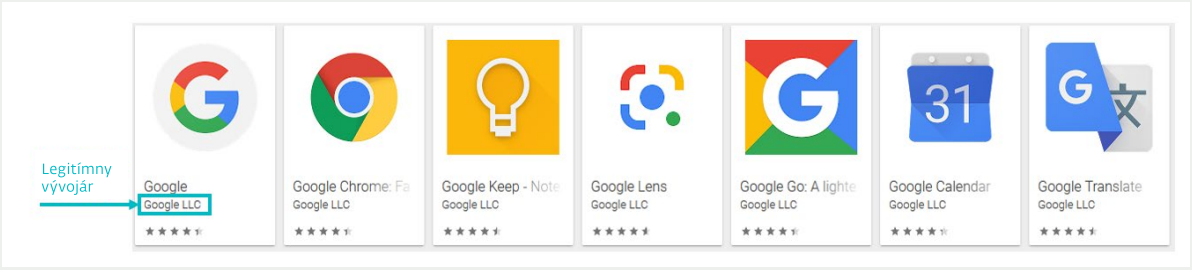
9. **Mobilné bezpečnostné riešenie (antivírus):** Pre vyššiu bezpečnosť Android zariadení odporúčame používať aj bezpečnostnú aplikáciu – bežne označovanú ako mobilný antivírus. Spoľahlivá bezpečnostná aplikácia dokáže používateľa upozorniť na škodlivú povahu či správanie aplikácie a chrániť ho tak pred infikovanými odkazmi či krádežou dát. To platí aj v prípade, že sa škodlivá povaha programu prejaví až po jeho inštalácii do zariadenia. Niektoré bezpečnostné aplikácie používateľa upozornia aj na slabé či chybné zabezpečenie a nastavenie zariadenia, prípadne mu pomôžu nájsť stratené alebo ukradnuté zariadenie. Viac sa tejto téme venujeme v časti Bezpečnostné riešenie (antivírus).

EXTRA TIP:
Na čo by si ešte používateľ mobilného zariadenia mal dávať pozor?

Aj do oficiálnych obchodov sa občas dostanú škodlivé aplikácie a je ťažké ich rozoznať. Jedným zo znakov, ktorý môže prezradiť falošnú verziu populárnej aplikácie, je napríklad meno developera/vývojára. To sa môže od skutočného developera odlišovať len jediným znakom [nahradí veľké „I“ (ako je na začiatku mena Ivan) za malé „l“ (ako v slove lopata)]. Ďalšou taktikou útočníkov je nazvať svoj developerský účet spôsobom, ktorým si zvýši dôveryhodnosť. Príkladom sú mená, ktoré sa vydávajú za počet stiahnutí používateľmi.



OBRÁZOK 1 *„+1.000.000 Downloads" je názov falošného developera. Názvom sa snaží vytvoriť dojem, že jeho aplikácie si stiahli milióny ľudí, kým v skutočnosti si ich stiahli len desiatky alebo stovky. Zdroj: Google Play Store*



OBRÁZOK 2 *Na rovnakom mieste je bežne meno legitímneho developera, nie číslo, ako je vidieť pri aplikáciách Google. Zdroj: Google Play Store*

Pravidlá pre detských používateľov mobilných zariadení

Učitelia (a rodičia) by mali dieťa/žiakov upozorniť na riziká, ktoré sa spájajú s používaním mobilného telefónu či zneužívaním núdzových liniek:

- Deti/žiaci by nemali zneužívať núdzové linky, pokiaľ nie sú v núdzi. Blokujú totiž linku pre ľudí, ktorí naozaj potrebujú pomoc a navyše sa vystavujú riziku pokuty či vážnejšieho trestu.
- Ak dieťaťu/žiakovi volá neznámy človek, nikdy by mu nemali dávať osobné či inak citlivé informácie. Banka, technická podpora ani iný profesionál bez vyzvania používateľom nevolá, a ak áno, nikdy nevyžaduje podobné údaje.
- Človek, ktorý deťom/žiakom volá, by sa mal vždy predstaviť.

- V správe odkazovej schránky na hlasové hovory deti/žiaci nemajú uvádzať svoje ani cudzie kontaktné údaje.
- Deti/žiaci by si vždy mali rozmyslieť, komu dajú svoje telefónne číslo.
- Ak dieťaťu/žiakovi prišli nežiaduce správy cez nevyžiadané bluetooth spojenie, mali by bluetooth vypnúť a upraviť dohľadateľnosť zariadenia v „Nastaveniach".
- Ak dieťa/žiak nevie, od koho SMS správa prišla, nemalo/nemal by klikať na žiadne odkazy, ktoré obsahuje, ani na takúto správu odpovedať.

Selfies

Kľúčové slová

selfie | selfie palica (selfie stick) | virálna fotografia

Otázky, na ktoré odpovedá táto podkapitola:

Čo je selfie a aké riziká prináša? Aké pravidlá by mali používatelia dodržiavať pri tvorbe selfie?

Praktické cvičenia k tejto podkapitole:

Animália, Autoportrét, Selfie priepasť, Ja, moje druhé ja a moje selfie, CSI selfie

Selfie je fotografia samého seba, ktorú si používateľ spravidla urobí smartfónom namiereným na seba alebo s použitím selfie stick (selfie palice). Napriek modernému názvu nejde o žiadnu novinku. Stovky rokov predtým, než vznikol prvý mobilný telefón či sociálna sieť, si „selfies" – autoportréty – robili mnohí svetoznámi umelci ako Leonardo da Vinci, Rembrandt alebo Vincent van Gogh.

Na rozdiel od týchto majstrov si mnohí dnešní používatelia (bez ohľadu na vek) pri tvorbe „selfíčka" veľmi nedávajú pozor, čo všetko sa dostane do záberu, a neskontrolovaný obsah často bez rozmýšľania zverejnia na svojom profile na sociálnej sieti.

Týmto krokom sa pritom vystavujú rizikám. Na fotografii sa totiž môžu objaviť aj veci, ktoré používateľ vôbec nezamýšľal zverejniť, prípadne ho zachytia v nelichotivej póze. Recept, ako si urobiť dobrú (a najmä bezpečnú) selfie, pritom ponúkali už spomínaní Leonardo Da Vinci, Rembrandt aj Vincent van Gogh.

Keď totiž maľovali svoje autoportréty (ale aj iné diela), do detailu si premysleli, čo všetko dajú na obraz. Podobne by mali používatelia pristupovať k tvorbe selfies aj dnes a záber vždy podrobne skúmať – podobne ako by to urobil napríklad policajný vyšetrovateľ či detektív.

Nedodržanie jednoduchých pravidiel pritom môže viesť k mnohým problémom, ako je posmech od okolia či kyberšikana, zverejnenie či predaj intímnych záberov na nedostupných online fórach.

Ktoré pravidlá by mali používatelia dodržiavať pri tvorbe selfie?

1. V prvom rade si používatelia musia uvedomiť, kde sa práve nachádzajú a ako vyzerá ich okolie. Fotografia za každú cenu sa už totiž vypomstila mnohým ľuďom, čo potvrdzujú aj štatistiky. Tie ukazujú, že ročne zomrie pri tvorbe selfie viac ľudí, ako uhryzne žralok.
2. Pri tvorbe novej selfie by sa tiež mali zamerať na detaily: Čo je položené na stole, na parapete či na zemi v pozadí? Nie je v zábere niektorý z mojich preukazov (občiansky preukaz, karta poistenca, pas) alebo napríklad lístok na koncert s QR kódom? Neprezradí fotografia moju polohu niekomu, kto ju nemá poznať?
3. Predtým, než používateľ zverejní selfie, mal by si uvedomiť, že záber ostane na internete navždy a nie je možné ho úplne odstrániť. Na ilustráciu môže poslúžiť fakt, že mnohé fotografie bežných ľudí sa neúmyselne stali virálnymi, pričom ich autor, resp. majiteľ nad ich ďalším šírením nemá žiadnu kontrolu. Dobrým pravidlom je odpovedať si najprv na otázku: „Chcel by som, aby túto fotografiu/selfie videla moja stará mama, rodičia, známi alebo napríklad budúci zamestnávateľ?“
4. Používateľ by si mal chrániť súkromie a tomu prispôsobiť aj nastavenia svojho profilu. Viac o tejto téme hovoríme v kapitole o sociálnych sieťach.
5. Učitelia by mali byť v tejto oblasti pre žiakov vzorom a držať sa pravidiel, ktoré im sami odporúčajú.

BONUS:

Ak si chce používateľ urobiť selfie s iným (známym) človekom, mal by ho najprv požiadať o povolenie. Všetci máme nárok na súkromie a to platí aj pre známych youtuberov, hudobníkov či celebrity, ktoré náhodne stretneme na ulici.

Kyberšikanovanie

Kľúčové slová

strata zábran v prostredí internetu (dizinhibičný efekt) | kyberšikanovanie (cyberbullying) | happy slapping | outing | online prenasledovanie (cyberstalking) | trolling | troll | nenávistné prejavy online (cyberhate)

Otázky, na ktoré odpovedá táto kapitola:

Ako pôsobí strata zábran v prostredí internetu? Čo je kyberšikanovanie a aké sú jeho základné znaky? Čo všetko útočníci robia pri kyberšikanovaní? Čím je kyberšikanovanie odlišné od ubližovania tvárou v tvár? Prečo je potrebné vedieť o kyberšikanovaní a riešiť ho? Šikanujú častejšie chlapci alebo dievčatá? Ako môže okolie rozpoznať, že dieťa je šikanované? Ako sa dá zakročiť proti kyberšikanovaniu? Ako zareagovať, keď sa dieťa zverí so šikanovaním? V akom prostredí je vysoké riziko (kyber) šikanovania? Na čo dbať pri vzdelávacích aktivitách v prevencii (kyber) šikanovania?

Praktické cvičenia k tejto kapitole:

Džin, Čo je kyberšikanovanie, Kyberšikanovanie – zatočme s ním spoločne, Nájdi príbeh – Reportéri, Pomsta a prenasledovanie, Veselo a smutno, Kyberšikanovanie, čo s tým?, Rozhovor s hrdinom, Superhrdinovia na internete, Plagát a leták: Žiaci proti kyberšikanovaniu, Animália, Dva brehy, Konflikt slobôd

Ako pôsobí strata zábran v prostredí internetu?

Elektronická komunikácia má viacero špecifík:

- **Často prebieha s časovými odstupmi.** Platí to ako pre komunikáciu v čete, tak aj pre reakcie na obsah dostupný na sociálnych médiách či v e-mailoch. Výnimku tvoria videohovory.
- **Často prebieha s pocitom anonymity a nepostihnuteľnosti.**
- **Sťažuje empatiu.** Pokiaľ nejde o videohovor, dieťa nevidí tvár, telo, pohyby a reakciu človeka na druhej strane, a preto dostatočne nevníma dôsledky svojich činov a komunikácie.
- **Keď sa na dieťa (alebo používateľa) nikto nepozerá, dovolí si viac a správa sa uvoľnenejšie, odvážnejšie, nakoľko cíti menší tlak spoločenských noriem.** To môže byť prospešné najmä pre hanblivejších, no na druhej strane to môže zapríčiniť prehnané „uvoľnenie sa" v správaní a viesť až k agresívnym prejavom. Človek totiž prenechá voľný priechod emóciám, túžbam a správaniu, ktoré by inak bežne tlmilo jeho/jej svedomie.

Táto „prílišná online uvoľnenosť" sa tiež nazýva **dizinhibičný efekt.** Ide o znižovanie zábran a opatrnosti ľudí na internete z dôvodu pociťovanej anonymity. Práve táto uvoľnenosť je dôvodom, pre ktorý sú ľudia v komunikácii online odvážnejší a často aj agresívnejší. Dovolia si tak to, na čo by tvárou v tvár nemali odvahu. Príkladom sú agresívne prejavy a nekorektná komunikácia:

- formou jednotlivých incidentov ako trolling, nenávistné prejavy online (cyberhate),
- systematickou formou ubližovania: kyberšikanovanie (cyberbullying) či prenasledovanie online (cyberstalking).

Čo je kyberšikanovanie a aké sú jeho základné znaky?

Šikanovanie v súčasnosti môže mať offline aj online formy. Keď šikanovanie prebieha cez elektronické formy, hovoríme mu **kyberšikanovanie**, anglicky cyberbullying, **elektronické šikanovanie, mobilné a internetové šikanovanie** či **elektronická agresia**.

Výskumy ukazujú, že ak dochádza ku kyberšikanovaniu, obeť je často zároveň šikanovaná aj v offline prostredí a jej rovesnícke vzťahy sú narušené, menej uspokojivé. Kyberšikanovanie teda nie je odtrhnuté od reality zažívanej tvárou v tvár. Útočníci majú v digitálnych nástrojoch len ďalšie možnosti, ako ublížiť obeti.

Šikanovanie, či už elektronicky alebo tvárou v tvár, má nasledovné základné znaky:

- **Medzi útočníkom a obeťou je nepomer sily.** Táto prevaha či bezbrannosť obete môže byť skutočná alebo zdanlivá, prameniaca z osobnej sily, sebavedomia, pocitu menejcennosti jedinca alebo z prevahy skupiny.
- Ide o **zámerné ubližovanie** jednému alebo viacerým osobám.
- Agresor môže byť **jedno dieťa,** ale aj **skupina detí.**
- **Opakované ubližovanie**. Jednorazový agresívny čin v prostredí tvárou v tvár sa väčšinou nepovažuje za šikanovanie. Pri kyberšikanovaní je to zložitejšie, nakoľko napr. na profile obete na sociálnej sieti môže byť zdieľaný aj jeden zosmiešňujúci príspevok, ktorý môže byť podporený „lajkmi", ďalšími zosmiešňujúcimi komentármi či následným rozposielaním ďalším používateľom. Príspevok je síce len jeden, no všetky ďalšie reakcie a interakcie s ním je možné pokladať tiež za ubližovanie, pričom veľkosť publika znásobuje tento efekt.

- **Nepomer síl medzi útočníkom a obeťou.** Prevaha moci môže byť založená na rôznych faktoroch: fyzická alebo osobná sila, sebavedomie, verbálne či sociálne zručnosti, vekový rozdiel, množstvo priateľov alebo popularita v rovesníckej skupine. Prevaha môže byť reálna, ale aj subjektívna. Pri kyberšikanovaní sú prevahou aj technické zručnosti a reakcie publika na poškodzujúce činy.
- Vzniká **v dynamike skupiny**. V hre je nielen obeť a útočník, ale aj publikum či **prihliadajúci**, ktorí sú pre útočníka zdrojom spätnej väzby (obdiv, povzbudenie, odmietnutie, ignorácia) a pre obeť sú svedkami zahanbenia, napríklad na sociálnych sieťach. Pasivita/proaktívnosť svedkov ubližovania určí, či sa obeť dostane do izolácie alebo bude mať nejakých priateľov a podporu. Práve prihliadajúci svojimi postojmi a činmi môžu ubližovanie zmierniť aj celkom zastaviť šikanovanie alebo svojou pasivitou šikanovanie spoluvytvárajú a legitimizujú jeho priebeh.
- Kyberšikanovanie je podobne ako iné fyzické či psychické týranie **porušovaním práv** dieťaťa.

Kyberšikanovanie je zneužívanie internetu a digitálnych technológií, teda smartfónov, mobilných zariadení, internetu, webových stránok, aplikácií a online aktivít, pre zámerné ubližovanie druhým.

Kyberšikanovanie môže prebiehať cez tieto formy:

- **rýchle správy, SMS správy a e-maily**,
- **blogy**, zverejnené názory a postrehy ubližujúce obeti,
- **fotografie, obrázky a videá** ubližujúce obeti,
- internetové **ankety, kvízy alebo výzvy** k útoku na obeť,
- **lajk na sociálnych sieťach** – vyjadrenie súhlasu so škodlivým a ubližujúcim obsahom, čiže pridanie sa na stranu agresora,
- **urážlivé komentáre**,
- **happy slapping** tiež známe ako „fackovanie pre zábavu". Ide o nový typ ubližovania, ktorý spája šikanovanie tvárou v tvár s kyberšikanovaním. Agresor fyzicky napadne obeť a celé to nahráva na mobilný telefón. Následne zverejní nahrávku na internete alebo rozpošle rovesníkom v správe. Agresormi pri happy slappingu býva často skupina, nielen jednotlivec, a skupina sa „zabáva" a vzájomne povzbudzuje v ubližovaní. Efekt tejto formy agresie je pre psychiku obete devastujúci.

Najčastejšie sa kyberšikanovanie deje prostredníctvom:

- sociálnych sietí a četových skupín,
- správ poslaných na mobilné zariadenie obete,
- správ poslaných cez e-mail.

Čo všetko útočníci robia pri kyberšikanovaní?

Pri kyberšikanovaní chce agresor docieliť prevahu nad obeťou (aj opakovane), na čo môže využívať viaceré spôsoby ubližovania:

- **Provokuje obeť správami a príspevkami**, ktoré obsahujú urážlivý, nepravdivý, neakceptovateľný a/alebo vulgárny text. Povaha aj obsah týchto správ púta pozornosť obete, ktorá s nimi nesúhlasí a nevie ich brať na ľahkú váhu. Tým útočník vťahuje obeť do nekorektného dialógu a opakovane dokazuje svoju moc.
- **Zastrašuje a vydiera obeť**, napríklad tak, že sa nabúra do jej profilu na sociálnej sieti, zmení heslo a profil následne zneužije. Môže napríklad upravovať pôvodné správy, komunikovať s kontaktmi v mene obete, zverejňovať nevhodné príspevky poškodzujúce obeť a jej známych. Takto „ukradnutý profil" agresorovi slúži ako nástroj na následné manipulovanie a vydieranie.
- **Ponižuje a zosmiešňuje obeť** pred okolím, napríklad na sociálnych sieťach a v četových skupinách.
- **Očierňuje či ohovára obeť**, napríklad tým, že šíri klebety a poškodzujúce klamstvá s cieľom poškodiť dobré meno obete alebo jej vzťahy.
- **Vydáva sa za inú osobu/obeť (kradne jej identitu)** a v jej mene ubližuje obeti a okoliu.
- **Zverejňuje na internete informácie zo súkromia a z intímnych situácií obete (outing)** bez súhlasu obete. Uniknutými informáciami môžu byť fotografie, obrázky, videá intímneho charakteru, ktoré obeť verejne kompromitujú.
- **Zámerne vylučuje obeť z online komunity**, či už na sociálnych sieťach, v četových miestnostiach alebo v diskusiách. Takéto vylúčenie zo skupiny sa nedeje postupne, ale je rýchle a výrazné, takže je pre obeť nemožné prehliadnuť ho a vyvoláva pocit izolácie.
- **Obťažuje a prenasleduje obeť**, čím narúša jej pocit bezpečia. Agresor obeti znepríjemňuje život zahlcujúcimi interakciami, napr. spamovaním, opakovaným posielaním fotografií, správami v četoch, lajkmi a komentármi, prezváňaním. Táto pozornosť môže byť obsahom pozitívna, ale jej intenzita je obťažujúca. V niektorých prípadoch môže byť komunikácia aj negatívna a poškodzujúca, môže zahŕňať vyhrážanie sa ublížením, falošné obviňovanie, poškodzovanie dát či krádež identity, prenasledovanie offline a monitorovanie počítača obete a pod. Intenzita obťažovania sa obvykle stupňuje a neprestane ani vtedy, keď je na to útočník vyzvaný alebo keď obeť zablokuje kontakty. Z prostredia online často prechádza aj do offline prostredia.

Čím je kyberšikanovanie odlišné od ubližovania tvárou v tvár?

Pocit anonymity u agresorov uvoľňuje zábrany a spôsobuje väčšiu krutosť
V prostredí internetu sa človek cíti anonymný, akoby sa kedykoľvek mohol vydávať za inú osobu a bol nepostihnuteľný. To človeka ľahko zbaví zábran, a preto sa útočníkmi môžu stať aj ľudia, ktorí by tvárou v tvár nemali prevahu.

Kyberšikanovanie zastihne obeť kdekoľvek
Kým ubližovanie tvárou v tvár je viac-menej viazané na určité miesta, a teda je viac predvídateľné, pri kyberšikanovaní sa cez digitálne nástroje dá ublížiť hocikde, hocikedy a mnohonásobne. Touto všadeprítomnosťou obeť prichádza o akýkoľvek priestor bezpečia a pocit ohrozenia sa môže rozšíriť aj na mnohé inak bezpečné oblasti, kde sa dotyčný pohybuje.

Do kyberšikanovania sa môže zapojiť veľké množstvo agresorov
Kým offline šikanovanie má skupinu agresorov tam, kde sa dotyční stretávajú, na internete sa k aktívnemu ubližovaniu môže pridať hocikto.

Mení sa množstvo a povaha publika „svedkov ubližovania"
Publikum pri šikanovaní tvárou v tvár je obvykle jasné: obeť vie, kto ho zbil alebo strápnil, kto to videl, a kam asi sa môže zahanbujúci chýr dostať, napr. spolužiaci a žiaci zo školy. Rozmery publika kyberšikanovania je nemožné odhadnúť, keďže obsah je možné ukladať do digitálneho sveta a znovu preposielať. Obeť preto trpí neistotou, pred kým všetkým bol/-a zahanbený/-á, čo je psychicky devastujúce a spôsobuje poškodenie vo väčšej miere.

Skrývanie sa za monitor či displej posilňuje „**fenomén sociálneho zaháľania**". Publikum pociťuje malú zodpovednosť a tlak zakročiť voči bezpráviu. Svedkovia majú pocit, že sa ich situácia osobne netýka a málokto sa zastane obete.

Agresora pri kyberšikanovaní je ťažšie identifikovať, preto je ubližovanie náročnejšie stíhať
Pre komplikované odhalenie identity agresorov kyberšikanovanie často ostáva nedoriešené, čo môže prispievať k tomu, že si jeho účastníci nemusia uvedomovať následky či svoj podiel viny. To sa týka tak agresorov, ako aj prihliadajúcich, či už ide o rovesníkov alebo o autority. Kyberšikanovanie sa navyše často deje mimo priestorov školy. Pedagógovia a školskí psychológovia tak pociťujú menší tlak zodpovednosti riešiť tieto incidenty.

Prečo je potrebné vedieť o kyberšikanovaní a riešiť ho?

Podľa viacerých medzinárodných výskumov (HBSC, EUKO, TIMSS, GSHS a PISA) sa dá tvrdiť, že s kyberšikanovaním má skúsenosť približne **každé tretie dieťa**. A jeho výskyt neustále rastie.

Neriešenie alebo nedostatočné riešenie šikanovania necháva škodlivé stopy v identite obetí, agresorov aj prihliadajúcich. Zážitok a vedomie moci či bezmocnosti, legitimizovania násilia a pasivity v medziľudských vzťahoch zostávajú silno vryté do identity každého z nich, až kým deti nezažijú skúsenosť, ktorá tieto významy „opraví". Takým opravným zážitkom je nastavenie hraníc ubližovaniu, odhalenie útočníkov, náprava vzťahov medzi rovesníkmi, udobrenie sa, spravodlivosť, odvaha zastať sa slabšieho, kamarátstvo a pod. O to sa majú spolu s deťmi postarať práve dospelí.

Kyberšikanovanie je, rovnako ako fyzické či psychické týranie, porušovaním práv dieťaťa, preto je neakceptovateľné.

Šikanujú častejšie chlapci alebo dievčatá?

Ukázalo sa, že medzi útočníkmi v šikanovaní prevažujú chlapci nad dievčatami a tieto rodové rozdiely sú prítomné vo všetkých vekových skupinách detí a dospievajúcich. Platí to pre šikanovanie online aj offline.[3]

Rodové rozdiely v počte útočníkov sa o niečo zmenšia vo veku 11 – 13 rokov, keď **v čase puberty aj dievčatá horšie kontrolujú vlastné impulzy a dokážu rovesníkom tiež značne ubližovať**; zároveň vtedy začínajú vo veľkom využívať sociálne siete, ktoré poskytujú priestor na kyberšikanovanie. Stále platí, že častejšie ubližujú chlapci ako dievčatá. Podobne ako **medzi útočníkmi, aj medzi obeťami** nájdeme **viac chlapcov ako dievčat**.

Dievčatá sú najčastejšie obeťami kyberšikanovania vo veku 12 – 17 rokov, keď sú aktívnejšie na sociálnych sieťach.

Zrejme tým, že spoločenské normy prísnejšie odsudzujú ubližovanie ženám, ako aj ženskú agresiu, dievčatá a mladé **ženy sú obeťami i útočníkmi častejšie online** než offline, kde pôsobí strata zábran a vnímanie noriem je oslabené.

Ako môže okolie rozpoznať, že dieťa je šikanované?

Je dobré, keď učiteľ v rámci vzdelávania hovorí s deťmi o tom, ako si môžu všimnúť, že niekto v ich okolí je šikanovaný, naučia sa spolu, ako to včas rozoznať, čím predídu väčším psychickým ujmám obetí.

Kyberšikanovanie je pre dieťa výrazným stresom, spôsobuje úzkosť, depresívne emočné ladenie, strach, pocity bezmocnosti. Tieto stavy majú aj vonkajšie prejavy, ktoré si **môžu všimnúť rodičia, učitelia aj rovesníci**.

V dôsledku trápenia sa môžu prejaviť:

- **psychosomatické príznaky** – bolesti brucha, hlavy, zmena chuti do jedla, poruchy spánku,
- **zneistenie, zníženie sebavedomia** a sebaúcty, pocit ohrozenia pri sociálnych kontaktoch, neurotickosť, vyhýbanie sa spoločnosti,
- **v správaní dieťaťa ubudne niečo, čo tam predtým bolo** – obmedzenie kontaktu s rovesníkmi, záujmov, činností, zvýšená apatickosť, uzatváranie sa do seba, znížený záujem o školu, horší prospech a správanie v škole,
- **v správaní pribudne niečo, čo tam predtým nebolo** – riskantné aktivity, užívanie návykových látok, sebapoškodzovanie, delikvencia, záškoláctvo,
- **stresové reakcie pri používaní počítača, smartfónu** alebo pri rozprávaní sa o ňom. Zdrojom stresu pri používaní digitálnych nástrojov však nemusí byť len kyberšikana. Môže ísť o akékoľvek iné ťažkosti mladého človeka, aj o zmeny spojené s pubertálnym obdobím. Nezabúdajte, že kyberšikanovanie je viac o vzťahoch ako o samotnom internete.

Každé dieťa reaguje na trápenie a stres špecificky, má svoje spôsoby reagovania na záťaž. Základom je, aby spolužiaci a dospelí v škole **boli navzájom k sebe vnímaví** a zaregistrovali, že niečo nie je v poriadku. V škole sú deti aj učitelia vo vzájomnom dlhodobom kontakte, a preto je šanca postrehnúť zmeny v správaní najvyššia.

3 SMITH, P.K. et al.: Consistency of gender differences in bullying in cross-cultural surveys. In LSE Research, 2018, [online]. <http://eprints.lse.ac.uk/87794/1/G%C3%B6rzig_Gender%20Differences%20in%20Bullying_Accepted.pdf>

Ako sa dá zakročiť proti kyberšikanovaniu?

Rodičia či učitelia môžu dávať dôraz na nasledovné ciele:

1. **Naučiť deti, čo je šikanovanie a kyberšikanovanie**
   - Učiteľ potrebuje naučiť deti rozpoznať hranice medzi zábavou a šikanovaním a kyberšikanovaním.
   - Učiteľ potrebuje naučiť deti, ako znížiť riziko šikanovania a kyberšikanovania.

2. **Naučiť deti, ako postupovať, keď sa stretnú so šikanovaním a kyberšikanovaním**
   - Učiteľ potrebuje deťom odporučiť konkrétne osoby, na ktoré sa môžu obrátiť v prípade problémov, ako sú rodič, starší súrodenec alebo rovesník pre emocionálnu podporu alebo učiteľ informatiky pre technickú podporu.
   - Učiteľ potrebuje naučiť deti, ako presne postupovať, keď sa im deje niečo zlé na internete.

3. **Zlepšiť sociálne zručnosti detí, podporiť ich sebaobraz a empatiu**
   - Učiteľ môže deťom pomôcť tým, že ich naučí rozoznávať vlastné pocity, aby vedeli byť citlivé voči vlastnému prežívaniu aj prežívaniu iných.
   - Učiteľ môže deťom pomôcť zlepšiť ich sebaobraz a sociálne zručnosti, aby si vedeli vytvárať a udržiavať zdravé vzťahy.
   - Učiteľ môže v triede podporiť hodnoty kamarátstva, prijatia a spolupatričnosti.

4. **Aktivizovať deti k pomoci slabšiemu**
   - Učiteľ deťom pomáha rozvíjať schopnosť aktívne brániť seba a iných pri ubližovaní.

5. **Podporiť u detí zručnosti bezpečného používania internetu**
   - Učiteľ vysvetlí deťom, ako sa lepšie chrániť pomocou technických prostriedkov.

6. **Zriadiť pre obeť bezpečnejšie miesta a zóny na internete**
   - Učiteľ pomôže zriadiť miesta, kde sa obete šikanovania môžu pohybovať bez strachu z ďalších útokov.

7. **Uistiť dieťa o tom, že je dobrým krokom zdôveriť sa**
   - Učiteľ vysvetlí žiakom, že je kľúčové, aby o probléme vedeli dospelí alebo vyspelejší rovesníci. Ak sa to totiž nedozvedia, nemôžu pomôcť.

Ako zareagovať, keď sa dieťa zverí so šikanovaním?

Postup vo vzťahu k dieťaťu, ktoré je obeťou:

Dieťa potrebuje pomoc niekoho, kto mu/jej dokáže byť sociálnou oporou a je kompetentný riešiť incident. Učiteľ má dieťaťu okrem emočnej podpory, vypočutia a pomoci vyjadriť jeho pocity, poradiť mu aj s ďalším postupom:

1. **Uložiť šikanujúcu komunikáciu** v SMS správach, čete, ponižujúce fotografie, komentáre, printscreen v online aplikácii. Ide o dôležité opatrenie, keďže dieťa môže mať logickú tendenciu všetky hanlivé obsahy a zmienky v online priestore mazať, aby sa predišlo rozširovaniu poníženia.
2. **Nerozvíjať ďalej komunikáciu s agresorom,** zablokovať ho, odstrániť ho zo zoznamu kontaktov. V tomto bode možno šikanovanie ustane, no dieťaťu následne treba pomôcť vyriešiť konflikty a viesť funkčné vzťahy s rovesníkmi.

Postup vo vzťahu k škole, rodičom, odborníkom a úradom:

1. Učiteľ nesmie prehliadať a zamlčiavať ubližovanie, ktoré sa deje medzi žiakmi, nakoľko ide o porušovanie práv dieťaťa. V podobných prípadoch by sa mal učiteľ vždy spojiť s vedením školy aj zákonnými zástupcami dieťaťa.
2. Učiteľ bezodkladne koná a snaží sa pomôcť dieťaťu v spolupráci s relevantnými článkami školského systému, teda rodičmi, dieťaťom, spolužiakmi, vedením školy, ďalšími odborníkmi v školstve ako psychológ, sociálny pedagóg či pri kontakte s políciou.

Postup vo vzťahu k triede, kde sa objavilo (kyber) šikanovanie:

1. Učiteľ pomáha okamžite aktivizovať systém pomoci v triede.
2. Učiteľ pomáha z negatívneho zážitku žiakom vytvoriť **zrozumiteľnú lekciu**, ktorá vysvetlí, čo sa udialo, v čom je konkrétne správanie (kyber) šikanovaním, prečo sa to nesmie diať, a čo s tým trieda spoločne urobí ďalej, aby sa vzťahy opäť uzdravili.
3. Učiteľ pomáha žiakom **obnoviť pocit bezpečia a zdravé vzťahy** v triede najmä s využitím skupinových aktivít. Pri kyberšikanovaní nemuseli byť páchateľmi spolužiaci, zato však spolužiaci vedia pomôcť žiakovi, ktorý trpí, cítiť sa viac zahrnutý a podporený.
4. Úspešné zapojenie sa žiakov, ktorí sa podieľali na ubližovaní, do nápravy rovesníckych vzťahov môže byť spôsobom, ako niesť zodpovednosť a zároveň spôsobom, ako znížiť trest za porušenie triednych/školských pravidiel.
5. Učiteľ odporučí aj individuálne **psychologické poradenstvo žiakom**, prípadne aj ich rodinám.
6. Je užitočné, aby bol postup riešenia šikanovania a kyberšikanovania opísaný školou v jasných krokoch a mal by zahrňovať aj **sankcie**, lebo je potrebné nastavovať hranice a viesť deti k neseniu zodpovednosti za svoje činy.

Trolling a cyberhate

Kľúčové slová

trolling | troll | nenávistné prejavy online (cyberhate)

Otázky, na ktoré odpovedá táto podkapitola:

Kto je troll? Ako sa trollom vyhnúť? Čo je cyberhate alebo nenávistné prejavy online? Ktoré ciele sledovať v prevencii trollingu a cyberhate?

Praktické cvičenia k tejto podkapitole:

Džin, Čo je kyberšikanovanie?, Kyberšikanovanie – zatočme s ním spoločne, Nájdi príbeh – Reportéri, Veselo a smutno, Kyberšikanovanie, čo s tým?, Rozhovor s hrdinom, Superhrdinovia na internete, Plagát a leták: Žiaci proti kyberšikanovaniu, Animália, Dva brehy, Konflikt slobôd

V digitálnom prostredí môžu aj bežní používatelia ľahko získať pocit, že im nič nehrozí a ich činy k ich skutočnej osobe nikto nikdy nepriradí. Tento pocit v mnohých situáciách vedie k vzájomnému osočovaniu, či dokonca agresívnym prejavom. Niektorí účastníci debát sa o vyhrotenie vášní snažia vedome a zakladajú si na tento účel napríklad falošné profily. Prostredníctvom nich potom útočia na ostatných, vyvolávajú hnev, spory a chaos. Takýmto škodlivým účastníkom v online diskusii hovoríme **trollovia**.

Kto je troll?

Troll je označenie škodlivého používateľa, ktorý:

- vyvoláva spory a hádky, provokuje čitateľov na internete,
- úmyselne zverejňuje urážlivé, dráždivé, klamlivé alebo irelevantné príspevky,
- snaží sa vyprovokovať ostatných používateľov k ostrej reakcii,[4]
- úmyselne narúša alebo marí diskusiu a odkláňa sa od témy diskusie.[5]

Pre trolla je cieľom získanie pozornosti a pocitu moci. Pre používateľa je preto najlepšie, ak ju trollovi neposkytne.

4 PCMag - Internet troll. [online]. <https://www.pcmag.com/encyclopedia/term/internet-troll>
5 University Information Technology Services - What is a troll?. [online]. [2018-01-18]. <https://uits.iu.edu/.2018.>

Výskumy ukázali, že trollovia sú častejšie narcistickí, môžu mať črty niektorých porúch osobnosti (ako psychopatia, sadizmus, machiavelizmus, schizoidná osobnosť) a bývajú impulzívnejší. Pozor na prílišné zovšeobecnenia. Nie každý človek s poruchou osobnosti musí nutne byť troll a naopak, nie každý troll musí mať nevyhnutne poruchu osobnosti – pravdepodobnosť, že ju má, je však vyššia.[6]

Ako sa vyhnúť trollom?

S trollmi sa používatelia najčastejšie stretávajú na sociálnych sieťach či v četových skupinách a individuálnych četoch. Existujú pritom možnosti, ako sa im vyhnúť:

- Správne si nastaviť súkromie na sociálnych sieťach. Pokiaľ je to možné, na žiadnej zo sociálnych sietí by používatelia nemali mať verejný profil.
- Medzi kontakty na sociálnych sieťach by si používatelia mali pridávať len ľudí, ktorých osobne poznajú alebo s nimi majú spoločných viacerých priateľov, ktorých poznajú aj osobne.
- Rozoznať falošný profil a nereagovať naň. Niekedy sa ako náš kamarát môže tváriť aj používateľ s falošným účtom, ktorý sa chce dostať do skupiny. Zbystriť pozornosť sa oplatí, ak neznámy profil na sociálnej sieti:
  - nemá na profilovej fotografii rozpoznateľnú tvár,
  - nemá s používateľom, s ktorým sa snaží spojiť, žiadne spoločné kontakty ani priateľov,
  - má na svojom profile agresívnu, podozrivú alebo škodlivú predošlú aktivitu, či znaky neznášanlivosti a nenávisti v komentároch alebo obsahoch, ktoré šíri,
  - má výrazne viac priateľov ako bežný používateľ. Pre dieťa/žiaka môže byť dobrým referenčným číslom počet priateľov populárneho rovesníka/rovesníčky,
  - nevytvára žiadny vlastný obsah, šíri len cudzie správy, videá či fotografie a pridáva neužitočné komentáre.

Ako reagovať na trollov?

V prípade kontaktu s trollom platí jednoduché pravidlo: najlepšia prvá reakcia je nereagovať. Od trolla sa totiž nikdy nedočká rozumnej debaty. Trollovi nie je možné niečo logicky vysvetliť, keďže ho teší škodiť a získavať pozornosť online. Keď sa teda používateľovi podarí rozpoznať, že má dočinenia s trollom, najlepšie urobí, keď jeho komentáre nebude rozvíjať a nebude s ním o ničom diskutovať. Každá odpoveď na obsahy trolla je totiž pre neho „odmenou".

Ak používateľ odpovie kladne, troll je rád, že s ním súhlasil. Ak používateľ reaguje záporne, troll je rád, že sa mu podarilo vzbudiť zúfalstvo či hnev. Ignorovaním mu používateľ ukáže, že sa ho jeho príspevok nedotkol ani pozitívne, ani negatívne, a tak trollovi nedá jeho vytúženú odmenu.

Ak „nereagovanie používateľa" trolla neodradí a pokračuje vo svojej škodlivej aktivite, používateľ by si mal priebežne ukladať printscreeny škodlivej aktivity a nahlásiť takéto správanie administrátorom. Zodpovedný používateľ tak urobí, či už troll obťažuje jeho alebo niekoho iného v online prostredí. Sociálne siete majú na to tlačidlo „Report"/„Nahlásiť". Nahlásením škodlivého správania používateľ prispeje ku korektnejšiemu a zdravšiemu online prostrediu pre všetkých.

6 ScienceDirect - Trolls just want to have fun. [online]. <https://www.sciencedirect.com/science/article/abs/pii/S0191886914000324>

1. Používateľ by mal následne zablokovať trolla a vylúčiť ho zo zoznamu svojich kontaktov, ak si ho tam predtým pridal.
2. Používateľ najlepšie urobí, keď sa s čímkoľvek, čo ho obťažuje online alebo offline, zverí niekomu, komu dôveruje.
3. Ak obťažovanie pokračuje cez iné „kanály", používateľ by mal pokračovať v ukladaní printscreenov a správ a okamžite osloviť dospelého alebo staršieho rovesníka. Printscreeny a ďalšie dôkazy ubližovania následne spolu zoberú na políciu.

Čo sú nenávistné prejavy online (cyberhate)?

Cyberhate alebo nenávistné prejavy online sú stereotypné predstavy a predsudky voči istým skupinám ľudí, ktoré často ústia do neznášanlivosti.

Nenávistnými prejavmi označujeme aj komunikáciu a správanie, v ktorých útočník iných diskriminuje, hanobí alebo sa snaží vylúčiť pre ich príslušnosť k rase, etniku, jazyku, národu, národnosti, farbe pleti, náboženskej viere, pohlaviu, rodu, rodovej identite, sexuálnej orientácii, politickému presvedčeniu, sociálno-ekonomickému statusu, veku a mentálnemu či fyzickému zdraviu.[7]

V správaní má mnoho prejavov ako napríklad šovinizmus, rasizmus, xenofóbia, anticiganizmus, antisemitizmus, islamofóbia a homofóbia. Školy sú zaviazané **týmto prejavom** vo výchovno-vzdelávacom procese predchádzať, viesť deti ku kultúre znášanlivosti a učiť ich o ľudských právach a ich dodržiavaní offline aj online.

Nenávistné prejavy sú porušením práv a základných slobôd, ktoré sú dané ako rovné všetkým ľuďom od ich narodenia, sú chránené na globálnej úrovni a sú jasne pomenované vo Všeobecnej deklarácii ľudských práv.

Nenávistné prejavy online sú nekorektné, ale v porovnaní s trollingom sú vážnejšie tým, že porušujú ľudské práva a slobody, diskriminujú ľudí a priamo šíria extrémistické postoje a môžu preto byť kvalifikované ako priestupok alebo trestný čin.

Ktoré ciele sledovať v prevencii trollingu a cyberhate?

Učitelia môžu deti cielene viesť k aktívnemu digitálnemu občianstvu, ktorého stručné motto je: „Nesúhlas s neprávom je dôležitý, ale je to len prvý krok, zásadné sú činy." Odkaz pre deti je: „Vždy, keď zbadáte nenávistné prejavy online, je potrebné ich nahlásiť cez tlačidlo Nahlásiť/Report." Z pasívnych prihliadajúcich sa môžu deti stať aktívnymi tvorcami lepšieho online prostredia.

Školy by sa mali pri výchove detí/žiakov sústrediť na:

- budovanie vzťahov postavených na rešpekte, empatii a zdravej sebaúcte,
- vzdelávanie o ľudských právach a slobodách,
- búranie stereotypov a predsudkov,
- konštruktívne riešenie konfliktov,
- to, ako byť proaktívnym používateľom internetu a správne reagovať na cyberhate.

7 Anti-Defamation League. [online]. <https://www.adl.org/education-and-resources/resource-knowledge-base>

Sociálne siete

Kľúčové slová

čet | rozpoznávanie | šifrovanie | screenshot | sociálne siete | odkaz | FOMO | kyberšikanovanie | bubliny na sociálnych sieťach | influencer | youtuber | vloger | bloger | nenávistné prejavy | problematické používanie internetu | internetové závislosti | prenos z hráčskeho sveta | selfie dysmorfia

Otázky, na ktoré odpovedá táto kapitola:

Aké sú pravidlá bezpečného používania sociálnych sietí? Aké psychologické riziká predstavujú sociálne siete a ako ich zvládať? Kto sú influenceri a ako ovplyvňujú život detí? Skutočný vs. online svet – kedy hovoríme o problémovom používaní internetu a sociálnych sietí?

Praktické cvičenia k tejto kapitole:

Animália, Klavír, Koho vidím a koho nevidím, keď prispievam, Súboj sociálnych sietí, Nauč svoju babku používať Facebook, Influenceri, Ako si vybrať influencera?, Digitálny detox, Zdieľanie dovolenky na sociálnych sieťach, Nastavenie profilov na sociálnych sieťach, Modelová konferencia o sociálnych sieťach, Autoportrét

Sociálne siete a digitálna bezpečnosť

Kľúčové slová

čet (chat) | dohľadateľnosť | end-to-end šifrovanie | printscreen/screenshot | sociálna sieť | odkaz

Otázky, na ktoré odpovedá táto podkapitola:

Čo patrí k základnej bezpečnosti sociálnych sietí? Čo môže používateľ robiť, aby zvýšil svoju bezpečnosť na sociálnych sieťach? Ktoré prvky používateľom pomôžu zvýšiť zabezpečenie konta na sociálnej sieti? Ktoré údaje a veci by používateľ na sociálnych sieťach nemal zdieľať? Čo by mal používateľ pri výbere sociálnej siete zohľadniť? Na ktorú vlastnosť sa treba zamerať pri výbere četovej aplikácie? Na koho sa obrátiť, keď má používateľ na sociálnych sieťach problém? Ako útočníci zneužívajú sociálne siete?

Praktické cvičenia k tejto podkapitole:

Výskum používania sociálnych sietí na škole, Kto ma vytvoril?

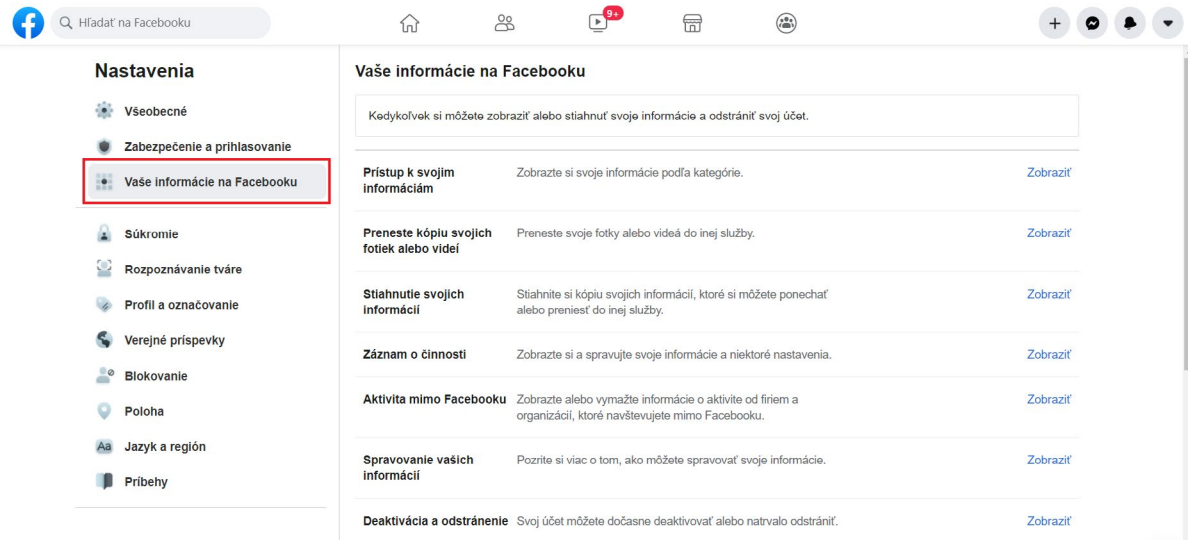
Pri sociálnych sieťach, rovnako ako pri celom internete platí, že všetko, čo používateľ raz zverejní, už navždy ostane online. Mnohé informácie sa totiž aj po odstránení z profilu na sociálnej sieti môžu objaviť v inej podobe ako snímka obrazovky (printscreen), súčasť videa alebo v inej forme digitálneho obsahu. Platí tiež, že aj keď používateľ informáciu online nenašiel, neznamená to, že už nie je na internete.

Čo môže používateľ robiť, aby zvýšil svoju bezpečnosť na sociálnych sieťach?

1. **Nastaviť si profil už v čase založenia ako súkromný** a zdieľať obsah (status, príspevok, fotografie, videá) len s obmedzenou skupinou ďalších používateľov. Čím užšia táto skupina bude, tým je vyššia bezpečnosť profilu. Vhodné je aj nastaviť si možnosť „zobraziť iba priateľom". Pri nastavení „zobraziť priateľom priateľov" už môžu obsah vidieť aj ľudia, ktorých používateľ priamo nepozná.

2. **Dôkladne vyberať obsah na zdieľanie.** Nie všetky fotografie či posty patria na internet. Fotografie, videá a príspevky by preto používateľ mal vždy zodpovedne preskúmať do najmenších detailov, podobne ako by to urobil policajný vyšetrovateľ. Tým môže predísť zverejneniu citlivých informácií o svojom súkromí. Dobré a jednoduché pravidlo je: *„Nezdieľajte nič, čo by ste neukázali (starým) rodičom."*

3. **Pravidelne kontrolovať zdieľaný obsah.** Na Facebooku si cez sekciu nastavenia používateľ môže stiahnuť všetky informácie, ktoré si o ňom uložila sociálna sieť. Podobnú možnosť ponúkajú aj iné sociálne siete ako napríklad SnapChat či Instagram. V najlepšom možnom prípade by používateľ v stiahnutých dátach mal nájsť len minimum osobných informácií. Neznámi ľudia by tak nemali získať dátum narodenia ani miesto, kde používateľ žije, pracuje či študuje.



OBRÁZOK 3 *Ako si môžete stiahnuť všetky informácie, ktoré o vás Facebook zhromaždil.*

4. **Pravidelne kontrolovať členstvo v skupinách.** Mnohé stránky (Facebook Pages a podobné) totiž mohli medzičasom zmeniť obsah či zameranie. Používatelia tiež vekom mohli zmeniť názor, čím sa ocitnú v skupine, s ktorej obsahom ani názormi nesúhlasia. Mnohé skupiny ich tvorcovia pritom založia práve s cieľom čo najrýchlejšie nazbierať členskú základňu a následne ju predať záujemcovi s najvyššou ponukou. Ten už potom jednoducho môže zmeniť jej názov a zameranie.

5. **Dvakrát merať, raz klikať.** Ak používateľ na sociálnej sieti dostane správu alebo odkaz od niektorého zo svojich priateľov, vždy by sa mal najprv zamyslieť nad tým, či by mu daná osoba posielala podobný odkaz. Ak je to možné, mal by používateľ skontrolovať, aj kam sa dostane, ak na tento obsah klikne (stačí sa presunúť myškou nad daný odkaz a ten sa aj bez kliknutia zobrazí). Ak je obsah/odkaz akokoľvek podozrivý či napísaný v jazyku, ktorý daný priateľ nepoužíva, používateľ by naň nemal klikať a mal by naň upozorniť aj priateľa, ktorý mu ho poslal.

6. **Skontrolovať a správne nastaviť dohľadateľnosť.** V nastaveniach sociálnej siete si používateľ môže nastaviť prísnejšie možnosti vyhľadávania profilu – ideálne je, aby profil používateľa vedeli dohľadať len jeho rodina, priatelia či iná vybraná skupina.

7. **Prispôsobiť správanie na sociálnej sieti.** Ak si používateľ chce byť istý, že o sebe neposkytuje priveľa informácií, môže si zvoliť prístup, pri ktorom počíta s tým, že jeho profil či zariadenie už niekto sleduje. Na také miesto by, prirodzene, nemal ukladať žiadny citlivý obsah.

Ktoré prvky pomáhajú zvýšiť zabezpečenie konta na sociálnej sieti?

Okrem správneho nastavenia a bezpečného správania je potrebné zabezpečiť si konto aj ďalšími prvkami. Hovoríme najmä o **silnom hesle** a **dvojfaktorovej autentifikácii**, ktoré dokážu ochrániť údaje uložené v profile na sociálnej sieti. Detailnejšie sa im venujeme v samostatnej kapitole Heslá.

Ktoré údaje a obsah by používateľ nemal zdieľať na sociálnych sieťach?

Používateľ by nemal zverejňovať **súkromný ani inak citlivý obsah**. Na sociálne siete, blogy a iné verejné miesta nepatrí:

- číslo ani fotografia vodičského preukazu, pasu, občianskeho preukazu či iného dokladu,
- telefónne číslo,
- školská, domáca ani pracovná adresa používateľa ani jeho blízkych či známych,
- poznávacia značka auta,
- zmluvy ani iné oficiálne dokumenty (vysvedčenia atď.)

Používatelia by tiež nemali **verejne zdieľať cestovné lístky či lístky na verejné podujatia**, nakoľko mnohé z nich používajú QR kód, ktorý si útočník môže z fotografie alebo videa jednoducho stiahnuť a použiť. Rovnakú pozornosť, akú venujete veciam, ktoré fotografujete či nakrúcate, venujte aj **pozadiu vašich nahrávok, fotografií a videí**.

Neodporúčame zverejňovať **údaje alebo iné citlivé materiály ani o blízkych ľuďoch** (vrátane rodinných príslušníkov či spolužiakov) **a známych**, keďže môže ísť o porušenie zákona o ochrane osobných údajov.

Prax tiež ukázala, že nie je vhodné zverejňovať a zdieľať cez sociálne siete aktuálnu polohu, keďže táto informácia sa dá ľahko zneužiť. Príkladom je krádež, pri ktorej prišla celebrita Kim Kardashian o šperky za milióny preto, že o sebe priveľa prezradila cez svoje príspevky na sociálnych sieťach. Polohu používateľ môže nevedome zdieľať napríklad cez zverejnené fotografie či príspevky na sociálnych sieťach, no tieto údaje o ňom môžu zbierať aj mnohé z aplikácií. Obmedziť zber lokalizačných dát môže používateľ cez „Nastavenia" zariadenia, ale aj priamo v jednotlivých aplikáciách.

Čo by mal používateľ zohľadniť pri výbere sociálnej siete?

Žiaci/študenti by mali používať len sociálne siete, pre ktoré spĺňajú vekové obmedzenie a pravidlá vymedzené ich poskytovateľom. Pri výbere by mali sledovať nielen to, koľko ľudí z ich sociálneho okruhu na danej sieti už má profil, ale aj úroveň zabezpečenia služby.

Používateľ by si tiež mal položiť nasledujúce otázky:

- Je možné nastaviť si profil ako súkromný, prípadne obmedziť, kto vidí mnou zdieľaný obsah?
- Ako je zabezpečené moje konto: menom a heslom alebo je možné pridať ďalší faktor (číselný kód, overenie cez aplikáciu alebo SMS, odtlačok)?

V prípade, že sa chcú pripojiť aj na sociálnu sieť s horším zabezpečením, mali by tomu prispôsobiť obsah, ktorý v rámci nej zdieľajú.

Na ktorú vlastnosť sa treba zamerať pri výbere četovej aplikácie?

Ak žiaci/študenti používajú četové služby, mali by sa zamerať na tie, ktoré ponúkajú **end-to-end šifrovanie**[8]. Táto technológia chráni ich komunikáciu a sprístupňuje jej obsah len osobám na jej koncoch (preto end-to-end) a výrazne komplikuje snahy o jej sledovanie „na ceste". Aj pri týchto službách platí, že akýkoľvek zdieľaný obsah sa môže bez vedomia a súhlasu používateľa ocitnúť online (ak ho zverejní druhá strana).

Pri výbere četovej aplikácie by si používateľ mal vždy pozrieť aj spôsob, akým poskytovateľ služby pracuje s jeho/jej dátami, kde a ako sú uložené, aj ako sa ďalej využívajú. Podmienky sa väčšinou dajú nájsť na webovej stránke aplikácie, no v niektorých prípadoch sú uložené aj priamo v samotnej aplikácii v rámci nastavení či opisu jej funkcií. Ak s niektorou z uvedených podmienok služby používateľ nesúhlasí, mal by sa jej radšej vyhnúť.

Pri sťahovaní aplikácie by si používateľ vždy mal overiť, či si sťahuje aplikáciu z oficiálnej stránky alebo dôveryhodného obchodu a najmä z profilu skutočného developera (viac v kapitole Bezpečnosť mobilných zariadení). Najmä pri platforme Android sa totiž často objavujú falošné verzie a napodobeniny populárnych četových aplikácií (WhatsApp, Messenger, SnapChat, Hangouts atď.), ktorých cieľom je zber a krádež citlivých dát používateľov.

Na koho sa obrátiť, keď má používateľ na sociálnych sieťach problém?

Používateľ by mal požiadať o pomoc osobu, ktorej verí. U detí sú to spravidla rodičia, starší súrodenci či učiteľ. Podľa závažnosti potom spoločne môžu vyhľadať pomoc, prípadne sa môžu obrátiť na políciu.

Ako útočníci zneužívajú sociálne siete?

1. Vyhľadávajú a sledujú budúce obete.
2. Zbierajú citlivé dáta.
3. Šíria reklamy a hoaxy.
4. Šíria škodlivý kód (cez príspevky, fotografie, skupiny, odkazy v správach).

8 Dá sa overiť cez Google, prípadne v opise aplikácie v Google Play alebo App Store obchode.

Sociálne siete a psychická odolnosť

Kľúčové slová

strach z vynechania (FOMO = Fear Of Missing Out) | kyberšikanovanie | bubliny na sociálnych sieťach

Otázky, na ktoré odpovedá táto podkapitola:

Aké psychologické riziká vytvárajú sociálne siete a ako ich deti môžu zvládať? Ako na deti vplýva negatívna alebo nedostatočná spätná väzba na sociálnych sieťach? Ako môžu učitelia podporiť odolnosť detí voči tomuto riziku? Prečo niektoré deti využívajú sociálne siete slobodne a niektoré problematicky či závislo? Ako na deti cez sociálne siete vplýva tlak na krásu a životný štýl? Ako sa môže detský používateľ chrániť voči tomuto riziku? Čo je strach z vynechania a ako súvisí s používaním sociálnych sietí? Ako môžu učitelia podporiť odolnosť detí voči strachu z vynechania?

Praktické cvičenia k tejto podkapitole:

Digitálny detox

Aké psychologické riziká vytvárajú sociálne siete a ako ich používatelia môžu zvládať?

Sociálne siete sú pre používateľov – a najmä tínedžerov – veľmi lákavé. Prezentovanie sa cez profil sa im zdá bezpečnejšie, navyše môžu zdieľať rôzne typy obsahu, byť v kontakte, prezentovať sa a zároveň nestáť pred rovesníkmi tvárou v tvár. Taktiež tam môžu zverejniť len to, na čo sú hrdé a aj to vo vylepšenej podobe, čím sa dokážu vyhnúť trápnym situáciám.

Pozitívne reakcie okolia (napr. formou „lajkov" a interakcií) pomáhajú dočasne podporiť sebavedomie. Je veľmi ľahké si na to navyknúť, či dokonca sa od tejto formy uznania stať závislým. Rovnako môže ublížiť, keď spätná väzba nie je pozitívna alebo je slabšia oproti očakávaniam. Používateľ tiež môže nadobudnúť dojem, že ostatní vyzerajú na sieti ešte úžasnejšie a šťastnejšie. Deti treba učiť, ako chápať fenomény sociálnych médií, a pomôcť im vybudovať si psychickú odolnosť voči nasledujúcim rizikám:

1. Negatívna alebo nedostatočná spätná väzba
2. Nutkavé, problematické a závislé používanie sociálnych médií
3. Tlak na krásu a životný štýl
4. Strach z vynechania (FOMO)
5. Počet priateľov a popularita
6. Bubliny sociálnych sietí

Negatívna alebo nedostatočná spätná väzba

V extrémnom prípade môže ísť o šikanovanie, trolling a hate-speech na sociálnych sieťach.

Deti, ktoré používajú sociálne siete, sa častejšie stretávajú s kyberšikanovaním ako tie, ktoré sociálne siete nepoužívajú. Sociálne siete sú v tomto ohľade často platformou, na ktorej dokážu deti rovesníkov zosmiešniť verejne a pred širším publikom, ako by to bolo možné „tvárou v tvár". Agresor tak chce ukázať svoju moc verejne.

Učiteľ by mal deti viesť k tomu, aby tvorili publikum, ktoré agresorovi túto moc nedá a nepridá sa k zosmiešňovaniu, ale naopak, zastane sa obete online aj offline. Deti by sa tiež mali naučiť, že ak vedia o podobnom čine, mali by o ňom povedať niekomu dospelému. Viac v kapitole Kyberšikanovanie.

Vysoko rizikovým prostredím sú sociálne siete, ktoré umožňujú, aby obsah (napr. fotografie a videá) z platformy po krátkom čase „zmizol" (napr. SnapChat). Používateľa táto skutočnosť môže zvádzať k rizikovému správaniu s vedomím, že po ňom nezostanú zaznamenané žiadne stopy. Takým rizikovým správaním na sociálnych sieťach je posielanie intímnych fotografií, sexting, ale aj nekorektné a šikanujúce obsahy.

Deťom je dôležité zdôrazniť, že ten, kto chce zneužiť fotografie zdieľané na sociálnej sieti, z nich dokáže urobiť printscreen skôr, než fotografia zmizne, prípadne fotografiu zaznamenať z iného digitálneho príslušenstva. Následne obsahy môžu byť kedykoľvek zneužité napr. na zosmiešnenie obete alebo na vydieranie. Ako záťaž deti vnímajú nielen ubližovanie, ale aj slabú odozvu na ich príspevky.

Ako môžu učitelia podporiť odolnosť detí voči tomuto riziku?

Učitelia vedú deti k tomu:

- aby sa sústredili na dobré vzťahy medzi rovesníkmi,
- aby sa naučili riešiť konflikty a po hádke sa vedeli zmieriť, udobriť,
- aby nezdieľali nič, čo nechcú, aby sa stalo stredobodom posmechu; čím menej digitálnych stôp, tým menej materiálov, ktoré sa dajú zneužiť,
- aby vedeli, ako a prečo si dôsledne nastavovať súkromie svojich príspevkov,
- aby vedeli, ako postupovať v prípade, že sa im udeje niečo nepríjemné na sociálnych sieťach.

Nutkavé, problematické a závislé používanie sociálnych médií

Dieťa môže používať sociálne médiá slobodne, aj keď na nich trávi veľa času. Vždy záleží aj na tom, čo presne tam robí a prečo, či je samo spokojné s tým, koľko času tomu venuje alebo s množstvom času nie je spokojné, ale nedarí sa mu to kontrolovať.

Prečo niektoré deti využívajú sociálne siete slobodne a niektoré problematicky?

To, či sa dieťa priveľmi pripúta k sociálnym médiám, určuje jeho širšia životná situácia. To, ako je spokojné so sebou a svojimi vzťahmi. Čím je dieťa vnútorne zraniteľnejšie, menej spokojné a menej začlenené medzi rovesníkov, tým viac môže závisieť jeho pohoda od toho, čo mu pomáha zlepšiť vlastný sebaobraz, napríklad aj úspech na sociálnych sieťach. Viac v kapitole Skutočný svet verzus online svet.

Príliš neisté a úzkostlivé deti môžu nutkavo kontrolovať reakcie na vlastné príspevky, inokedy dieťa odbieha k sociálnym médiám z pocitu vnútornej nudy, osamelosti alebo pre rozptýlenie pozornosti, keď sa trápi.

TLAK NA KRÁSU A ŽIVOTNÝ ŠTÝL

Ako na deti cez sociálne siete vplýva tlak na krásu a životný štýl?

Sociálne médiá niekedy pripomínajú výstavu dokonalej vizáže a veľmi vzrušujúcich životov, porovnaním s ktorými sa tínedžer neraz cíti byť nedostatočne dobrý. Ide najmä o sociálne siete založené hlavne na fotografiách, napr. Instagram. Keď je dieťa obzvlášť zraniteľné a používa tieto sociálne siete často, hrozí väčší pocit úzkosti, zlý pocit ohľadom výzoru a strach z vynechania. Sociálne siete založené na zdieľaní videí, ako YouTube, majú menej negatívny vplyv na osobnú pohodu a deti v mnohom obohacujú.

Tlak sociálnych médií na duševnú pohodu je výrazný až pri ich nadmernom používaní a zraniteľné sú nimi najmä deti, ktoré ani pred ich používaním neboli šťastné.

Ako sa môže detský používateľ chrániť voči tlaku na krásu a životný štýl?

- Používateľ by si mal vybrať veku primerané sociálne médiá podľa odporúčaní veku od odborníkov vývojárov.
- Používateľ by mal byť na sociálnych médiách skôr v interakcii, než len pasívne prehliadať cudzie príspevky. Aj na Instagrame, sociálnej sieti typickej práve spomínaným pasívnym prehliadaním, je možné napríklad vytvárať príbehy a pod., čo je vyššia miera interaktívnosti s ďalšími používateľmi.
- Používateľ skôr profituje zo sociálnych médií, ktoré poskytujú rôznorodý a realistickejší obsah (ako napr. YouTube).
- Pri menej interaktívnych sociálnych médiách (ako napr. Instagram) by mal byť používateľ aktívnym a prezieravým vo výbere a množstve priateľov a povahe odoberaných príspevkov. Okrem influencerov je možné sledovať aj príspevky z oblasti záľub, cestovania, umenia, športu a pod. To, aké odbery si mladý človek zvolí, je v jeho rukách a ovplyvní to potom to, čo vidí, čím sa obklopuje.

STRACH Z VYNECHANIA (FOMO)

Čo je strach z vynechania a ako súvisí s používaním sociálnych sietí?

Strach z vynechania (FOMO, Fear of missing out) je strach, že niečo zaujímavé alebo dôležité sa môže objaviť, prihodiť a dotyčný to premešká. Strach z vynechania sa týka aj zážitkov offline, človek skrátka chce byť tam, kde sa niečo deje a chce byť v obraze. Na internete sa strach z vynechania môže týkať mnohých vecí, nielen sociálnych sietí. Niekto napríklad dookola kontroluje správy zo sveta, aby mu neušlo nič zo spoločenského diania. Deti a dospievajúcich však neraz zaujíma viac než ekonomická a politická situácia práve to, čo sa deje medzi rovesníkmi alebo na ich vlastnom profile, a nechcú to prepásť.
Na sociálnych sieťach teda strach z vynechania vzniká ľahko, keďže sociálne statusy a interakcie je možné kontrolovať neustále.

Používatelia sú tiež pravidelne upozorňovaní na udalosti a akcie, ktoré by ich mohli zaujímať, prípadne na udalosti, o ktoré prejavili záujem oni a ich priatelia. Neustále prehliadanie toho, čo robia alebo plánujú robiť ich kamaráti v porovnaní s tým, čo robia oni, vyvoláva často tlak na výkon a pocit nedostatočnosti. Keby sa človek nedozvedel o množstve aktivít, na ktorých sa zúčastňujú kamaráti, možno by mu/jej ani neprišlo čudné zostať doma a oddychovať po svojom.

Ako môžu učitelia podporiť odolnosť detí voči strachu z vynechania?

- Učiteľ môže viesť deti k sebapoznaniu, k vedomosti o tom, aké sú ich skutočné potreby a preferencie.
- Učiteľ môže deťom vysvetliť, čo je strach z vynechania, a tým znížiť dosah tohto fenoménu. Mladým používateľom tiež treba zdôrazňovať, že sociálne siete sú výstavou zhustených exkluzívnych momentov, ktoré nereprezentujú komplexný obraz o živote jednotlivca vrátane zlých chvíľ a bežných povinností.

POČET PRIATEĽOV A POPULARITA

Mladým sa môže zdať úžasné, keď má človek široký zoznam kamarátov. Sú to však skutoční kamaráti? Alebo sú to len pridaní používatelia do okruhu ľudí, s ktorými je dotyčný „akože kamarát"? Je dobré, aby aj oni videli všetko to, čo používateľ chce zdieľať s okruhom svojich najbližších a priateľov? Odpoveď na túto otázku veľmi pravdepodobne znie „nie", čo si však mladý používateľ nemusí uvedomovať pri písaní jednotlivých príspevkov. Zdieľanie sa často deje v určitej nálade, keď sa používateľ nezastaví a nezamyslí nad možnými dôsledkami. Navyše podvedome môže fungovať logika: keď to viac ľudí vidí, je väčšia šanca na (dobrú) odozvu, čo nemusí byť najlepšie riešenie.

Koho vpustiť medzi svoje kontakty na sociálnej sieti?

- Základné pravidlo pre všetkých používateľov sociálnych sietí je pridávať si do zoznamu kontaktov len ľudí, ktorých človek pozná aj naživo, alebo tých, s kým má aspoň niekoľko spoločných priateľov v skutočnom živote.
- Ak používateľa zaujímajú názory inej osoby, ale nepozná sa s ňou osobne, existuje aj možnosť „sledovať" jej aktivity bez toho, aby sa navzájom stali kamarátmi na sociálnej sieti (napr. Facebook), resp. bez toho, aby umožnil druhej osobe sledovať svoj obsah (napr. Instagram). „Sledovanie" umožňuje používateľovi inšpirovať sa postrehmi iných, no zároveň nezdieľať priveľa zo svojho súkromia.

- Podobne, bez vedomia používateľa, môže niekto iný začať sledovať jeho/jej aktivity na sociálnych sieťach aj bez žiadosti o priateľstvo. Takým človekom môže byť osoba, ktorá nemusí mať len dobré úmysly. Používateľ sa tomu môže vyhnúť nastavením dohľadateľnosti napr. na Facebooku v „Nastavenia" → „Súkromie" → „Kto ma môže kontaktovať?" a „Kto ma môže vyhľadať?"

Priateľ na sociálnej sieti nie je automaticky blízky priateľ

- Na tých sociálnych sieťach, kde je to možné (napr. Facebook), by si mal používateľ dopriať dostatok času na vytvorenie kategórií kontaktov. Vzťahy s ľuďmi sa prirodzene vyvíjajú a s niekým, s kým si dieťa rozumelo v 13 rokoch, sa ako 15-ročné už nemusí vôbec kamarátiť. Preto je dobre tento zoznam priateľov a „kategórie blízkosti" pravidelne aktualizovať. Na Facebooku je pre každého v zozname priateľov možné nastaviť jednu z možností: „Blízki priatelia", „Známi", „Pridať do ďalšieho zoznamu".

OBRÁZOK 4 *Kategórie priateľov na Facebooku.*

- Facebook tiež ponúka možnosť nastaviť si, keď používateľ chce „dostávať upozornenia" o tom, čím niektorý z jeho kontaktov práve prispel do sociálnej siete. To si používateľ obvykle nastaví pre tie kontakty, o ktorých chce byť obzvlášť v obraze a informovaný. Pre iných facebookových kamarátov je zas možné „zrušiť priateľstvo". Keď používateľ zruší s niekým priateľstvo na Facebooku, deje sa to diskrétne, teda dotyčný sa o jeho vyradení zo zoznamu nedozvie a nemôže sa ho to dotknúť. Používateľ si teda nemusí robiť výčitky svedomia a môže sa v nastaveniach kontaktov rozhodovať slobodne.

Používateľ by mal pri pravidelnej revízii svojich kontaktov na sociálnej sieti zvážiť:

- Som s touto osobou stále kamarát?
- Zaujíma ma ešte stále to, čo robí?
- Obohacuje ma to?
- Chcem sa naďalej obklopovať jeho/jej názormi alebo mi nerobia veľmi dobre?
- Je dobré, aby vedel/-a o mne všetko to, čo mám bežne chuť zdieľať?

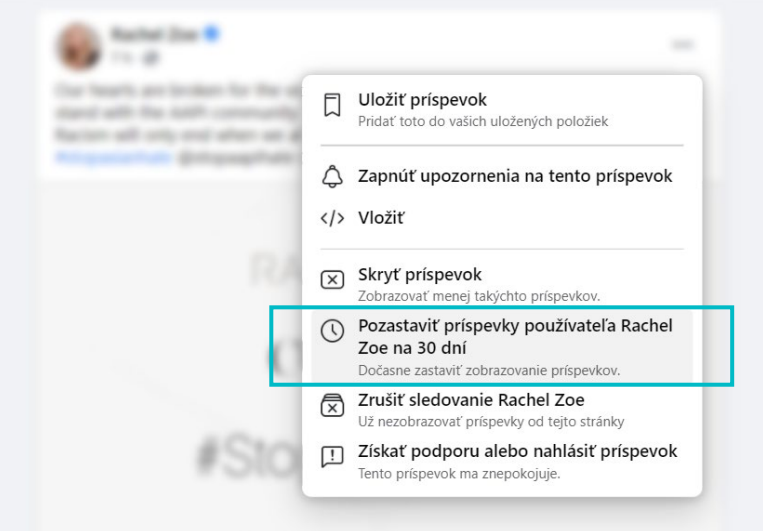
Bubliny na sociálnych sieťach
Algoritmus zobrazovania obsahov v Novinkách (ang. News feed) sa vytvára podľa toho, s ktorými príspevkami používateľ najčastejšie interaguje, na aké (a čie) príspevky kliká, hodnotí ich, komentuje ich. Algoritmus sociálnej siete to vyhodnocuje a následne používateľovi tieto a podobné príspevky zobrazuje v Novinkách na úkor iných typov príspevkov, s ktorými v minulosti neinteragoval.

To vytvára jednostranný výber určitého typu príspevkov, ktoré sa používateľovi zobrazujú. V tomto smere sa hovorí o vytváraní sociálnych bublín na sociálnych sieťach. Znamená to, že používateľ sa väčšinovo obklopuje tým, čo ho/ju zaujíma, a to tak obsahovo, ako aj názorovo. Iné názory či obsah sa mu zobrazuje menej a témy strácajú rôznorodosť, čím sa uzatvára do vlastnej bubliny. To tiež vyvoláva pocit, že názory používateľa sa stávajú pravdou potvrdenou aj používateľovým okolím.

Vyplýva z toho riziko oslabeného kritického myslenia, v dôsledku ktorého používateľ ľahšie podľahne dezinformáciám a hoaxom.

Riziko uzatvárania sa v bubline je možné znížiť:

- Vlastným regulovaním toho, čím sa na sociálnych sieťach používateľ obklopuje.
- Častejším vystupovaním z elektronických interakcií na sociálnych sieťach a udržiavaním rozmanitých medziľudských vzťahov offline.
- Zámerným vyhľadávaním tém a priateľov, s ktorými používateľ v poslednom čase veľmi nebol v kontakte, keďže algoritmus sociálnej siete ich príspevky nezaradil do používateľových Noviniek.
- Na Facebooku aj občasným (dočasným) vypnutím zobrazovania príspevkov od určitých osôb. Ak sa používateľovi zdá, že má v Novinkách priveľa príspevkov určitého typu, má možnosť priateľa buď zablokovať, skryť všetky jeho príspevky alebo požiadať sociálnu sieť, aby sa mu od neho v Novinkách mesiac nezobrazovali príspevky. Ak tuší, že chce od neho dlhšiu pauzu, môže zrušiť jeho „sledovanie" alebo tematicky obmedzí zobrazovanie určitého typu príspevkov. Urobí tak cez možnosti pri konkrétnom príspevku, nie v nastaveniach priateľstva.



Influenceri

Kľúčové slová:

influencer | youtuber | vlog | vlogovanie | blog | blogovanie | bloger | nenávistné prejavy

Otázky, na ktoré odpovedá táto podkapitola:

Kto je to influencer a ako zasahuje do života detí? V čom spočíva moc influencera? Ako hľadieť na psychologickú pomoc od influencerov? Ako vplývajú influenceri na sebaobraz a identitu detí? Ako si vybrať správneho influencera? Ako môžu deti rozpoznať reklamu, ktorú spoluvytvárajú influenceri? Ako si deti môžu udržať kritické myslenie pri sledovaní svojich obľúbených influencerov? Čo znamená byť influencerom?

Praktické cvičenia k tejto podkapitole:

Animália, Kto ma vytvoril, Influenceri, Ako si vybrať influencera?, Byť influencerom, Internetové celebrity

VIDEO PRE UČITEĽOV:

Po načítaní QR kódu si môžete pozrieť video s expertkou spoločnosti ESET Danielou Buján Havranovou o tom, že túžba stať sa influencerom so sebou prináša enormný stres.

Kto je to influencer a ako zasahuje do života detí?

Influencer je osoba, ktorá sa stala populárnou na sociálnych médiách, má veľa fanúšikov a vysokú sledovanosť. Dokáže tak svojimi príspevkami výraznejšie ovplyvňovať názory a správanie ostatných.

Deti objavujú vlastnú identitu a pomáha im v tom identifikovanie sa s niekým iným v ich veku. Influencer býva často niekto spomedzi tínedžerov, kto hovorí o tom, čo mnohé deti zaujíma a čo cítia, no nevyznajú sa v tom až tak dobre. Tým deťom pomáha pomenovať mnohé veci, inšpiruje ich, dá im radu. Zároveň jeho príspevky môžu byť trendy a zábavné, a preto ich sledovanie skrátka prináša deťom relax.

Influenceri na svoje príspevky využívajú viacero foriem:

1. **Fotografie**, ako napr. na sociálnej sieti Instagram a SnapChat, ktorá je založená hlavne na zdieľaní a hodnotení fotografií, okrem zdieľania videopríbehov.

2. **Blog** – je webová stránka, ktorá umožňuje registrovaným používateľom (blogerom) zverejňovať chronologicky ich príspevky vo forme článkov, ktoré môžu obsahovať aj ďalší multimediálny obsah, napríklad fotografie a videá. Obsah, teda téma blogu môže byť rôznorodá – od úvah o spoločnosti cez vedecké články, praktické tipy, denník až po školský či firemný blog. Obvykle je na blogu umožnené komentovať, hodnotiť a zdieľať jednotlivé príspevky, čím sa zvyšuje ich sledovanosť a možnosť, že ovplyvnia verejnosť.

3. **Videá** zdieľané na sociálnych sieťach – tieto videá sa tiež nazývajú **vlogy**. Vlog (skrátené označenie pre videoblog) je blog, pri ktorom sa používateľ (**vloger**) nevyjadruje písomne, ale ústne; a to tak, že natáča seba alebo svoje okolie a pri tom niečo rozpráva. Natočené videoblogy (vlogy) sú najčastejšie zdieľané na sociálnej sieti YouTube, a preto sa vlogeri, ktorí tam svoje príspevky zdieľajú, nazývajú aj **youtuberi**.

Pre niektorých používateľov je jednoduchšie a príjemnejšie natáčať vlogy než písať text. Podobne tak pre niektorú cieľovú skupinu môže byť sledovanie videa lákavejšie ako čítanie textu. Influenceri vlogujú na rôzne témy, čím vytvárajú svoj špecifický obsah a identitu influencera. Môže ísť o špecifické témy, napríklad inštruktážne videá, skúsenosti z videohier, humorné či vzdelávacie videá alebo pravidelné zhrnutia noviniek, cestovanie, fitness a pod.

Sledovať influencerov znamená zároveň čeliť rizikám, ktoré to prináša, a preto je nevyhnutné rozvíjať schopnosti detí čeliť rizikám. To vyžaduje v prvom rade vedomosti o rizikách, aby ich detský používateľ mohol „prekuknúť" a nepodliehal im. Vyžaduje to tiež kritické uvažovanie a mediálnu gramotnosť, takže tieto témy a aktivity je užitočné prepájať.

V čom spočíva moc influencera?

Pre svojich fanúšikov sú influenceri nositeľmi hodnôt, trendov, ideálov krásy a životného štýlu. To, čo robia a o čom hovoria, si deti následne viac všímajú tak na sebe, ako aj vo svojom okolí. To je skrytá moc, ktorou influenceri disponujú, keď nadobudli popularitu. To je možné využiť na hodnotné ciele, ako napr. šírenie dobra, búranie predsudkov alebo podporovanie zdravých či ekologických postojov, pomoci iným. Tiež sa to využíva na propagovanie produktov od značiek, s ktorými influenceri spolupracujú.

Ako hľadieť na psychologickú pomoc od influencerov?

Je užitočné, keď influenceri pomáhajú deťom vnímať, že sú O. K. také, aké sú. Influenceri k tomu môžu pomôcť tým, že hovoria nielen o pozitívnych zážitkoch, ale aj o tých menej radostných, a o tom, ako to zvládli. Niektorí influenceri otvorene hovoria o tom, aké je to čeliť nenávistným prejavom na internete (hate-speech) alebo šikanovaniu, psychickej kríze a ťažkostiam, rozchodu, vlastným obavám, a ako si s tým poradili. Takéto príspevky pomôžu deťom nehanbiť sa za to, čím prechádzajú, niekedy tam nájdu aj tipy na to, ako to zvládnuť. Ich príspevky však rozhodne nemôžu slúžiť ako univerzálne rady.

Ako si deti môžu udržať kritické myslenie pri sledovaní svojich obľúbených influencerov?

Pravidelné sledovanie influencerov a známych osobností je bežnou voľnočasovou aktivitou, podobne ako to bolo i v predošlých generáciách. Zmenili sa len médiá, forma a frekvencia, v ktorých ich môžu dnešné deti sledovať – vďaka smartfónom vlastne nonstop. Na sociálnych médiách je stále častejšie vidieť zhustenú verziu štylizovaných a retušovaných príspevkov, prototypy úžasného života a dokonalej vizáže ostatných používateľov a influencerov.

Tínedžerom pri predstave života influencerov pravdepodobne napadnú úžasné fotografie a videá z dovoleniek, výletov alebo spolupráce so známymi značkami, produkty zadarmo. Detskí používatelia sociálnych sietí dokonca môžu nadobudnúť dojem, že vo svete ich idolov neexistujú žiadne problémy.

Riziko pre detského používateľa spočíva v tom, že také príspevky idú cez médium, ktoré bez kritického uvažovania budí dojem autentickosti.

Video v porovnaní s fotografiami prináša deťom viac podnetov, o čosi konzistentnejší obraz ako štylizovaná a upravená fotografia. Je v ňom zahrnutá neverbálna komunikácia, a teda je bližšie realite. Influencer vo videu občas urobí niečo nedokonalé, zasmeje sa na sebe, nie je stopercentný v každom momente.

Ako vplývajú influenceri na sebaobraz a identitu detí?

- **Sebavedomie**
  Deti si možno neuvedomujú, že video či iný príspevok je len výsekom zo života influencera. Influencer nie je vždy len pekne oblečený a vtipný, aj on vie byť znudený, depresívny a obyčajný. Vtedy sa však obvykle nefotí či nenatáča. Keď deti podliehajú tomuto skresleniu a neuvedomujú si to, môžu si pripadať, že nie sú dosť dobré a výnimočné.
  - Deťom je potrebné pripomínať, že príspevky influencerov nie sú celá realita, že videá sú zostrihané, fotky sú štylizované a mnohí influenceri dávajú verejnosti len šľahačku na torte.
- **Napodobňovanie**
  - Počas dospievania je prirodzené, že sa deti chcú podobať na svoje idoly. Je dôležité pripomínať im, že sú jedinečné osobnosti a túto výnimočnosť by bola škoda stratiť. Deťom tiež treba pomáhať k lepšiemu sebapoznaniu, teda uvedomiť si, čo ich robí jedinečnými.

Ako si vybrať správneho influencera?

Influenceri majú veľkú moc a silu ovplyvňovať názory a hodnoty verejnosti. Nie je to moc samozvaná, práve naopak, čímsi sa publiku zapáčili a páčia, a toto „niečo“ pomohlo vytvoriť ich popularitu a základňu fanúšikov. A čím viac fanúšikov majú, tým silnejšie ovplyvňujú verejnosť a tým aj ľudí, ktorí možno ani nevedia, čo je na influencerovi „to jedinečné príťažlivé“, skrátka ho odoberajú, lebo sledujú trendy a idú s dobou.

Sledovať influencerov len preto, že sú populárni a trendy, nemusí byť pre používateľa to najrozumnejšie. Influencer má totiž podprahovo vplyv na názory, vkus, hodnoty mladých ľudí, a preto je dôležité vybrať si toho správneho influencera. Niektoré známe osobnosti môžu deti inšpirovať k športu, zdravému životu, odvahe, dobročinnosti, iné zas ponúkajú kontroverzný príklad životného štýlu spojeného s rôznymi rizikami.

Učiteľ so žiakmi vedie diskusiu o tom,

- názormi, vyjadrovaním a vyžarovaním ktorých ľudí sa chcú žiaci pravidelne obklopovať?
- čo je pre nich hodnotné?
- čo chcú u svojho influencera vidieť a počuť?
- čím by ich influencer sklamal a čo mu už rozhodne nebudú tolerovať?

Ako môžu deti rozpoznať reklamu, ktorú spoluvytvára influencer?

Úspešní influenceri spolupracujú s určitými značkami a z ich propagovania majú zárobok. Tým sa ich príspevky stávajú reklamou. Keď diváci vidia reklamu v televízii, napríklad na kozmetiku, uvedomujú si jasne, že je to reklama. No ak povie obľúbená influencerka v jednom z jej videí, ako jej nejaký značkový krém pomohol, tak to pôsobí ako jej skúsenosť a realita. Pre fanúšika to môže vyzerať, že nejde o reklamu, ale o fakt. Fanúšik má rád influencerku, dôveruje jej, a tak skôr uverí prezentovaným produktom. Táto neexplicitnosť reklamy robí z influencerov silné reklamné nástroje. Zastúpenie medzi propagovanými produktmi majú módne značky, nápoje, zdravá výživa, fitness produkty, elektronika, hry, šperky, cestovné agentúry. A, samozrejme, vlastné značky a produkty influencerov, ak také majú (oblečenie, hudobné albumy a pod).

Čo znamená byť influencerom?

Deti a tínedžeri často vidia len benefity influencerstva a nezamýšľajú sa nad záťažou a rizikami, ktorým ich vzory čelia. Mnohí túžia po takejto lákavej a zdanlivo pohodlnej kariérnej ceste. Globálny prieskum vysnívaných povolaní 11- až 16-ročných detí ukazuje, že stále ešte najpopulárnejším povolaním je lekár (18 %), ale tesne za ním je influencer (17 %) a youtuber (14 %). Táto zmena v obľúbenosti povolania je prirodzená vzhľadom na to, čo prináša digitálna doba a existencia sociálnych médií.[9]

Názor detí skresľuje aj to, že pred očami majú hlavne známych influencerov, teda výsledok dlhodobého snaženia sa tých niekoľko ľudí, ktorým sa podarilo uspieť. Okrem nich je veľa tých, ktorým sa to nepodarilo alebo „ich to omrzelo" po prvých mesiacoch vyčerpávajúcej práce na sociálnych médiách s neuspokojivými výsledkami. Preraziť totiž nie je jednoduché. Známi influenceri sa nestali populárnymi počas prvého týždňa a so záujemcami sa roztrhlo vrece. Navyše, aj keď už sú populárni, v úlohe influencera je naďalej mnoho **odvrátených stránok, ktoré si fanúšikovia neuvedomujú**:

1. **Tlak na výkon**. Influencer potrebuje byť stále aktívny a kreatívny. Na to, aby si udržal sledovanosť, potrebuje mať dôkladne navrhnutý koncept a zámer, plán, na čo sa bude zameriavať a ako to svojimi príspevkami dosiahne. Potrebuje svoje vízie pravidelne napĺňať obsahom a netreba zabúdať na to, že pripravovať, tvoriť a šíriť príspevky je reálna práca, ktorá si vyžaduje čas a energiu. Treba ju robiť aj vtedy, keď influencer nemá úplne dobrú náladu.

2. **Tlak na odozvu**. Napriek veľkej snahe influencera môže byť odozva na príspevky slabá alebo priemerná, niekedy neprimerane nízka vzhľadom na investovanú energiu.

9 PAPADATOU, A.: 1 of 5 British children want a career as a social media influencers. Publikované 31.1.2019. [online]. <https://www.hrreview.co.uk/hr-news/1-of-5-british-children-want-a-career-as-social-media-influencers/114597>

3. **Šikanovanie a trolling**. Zrejme všetci influenceri zažívajú na sociálnych médiách aj negatívne spätné väzby, kyberšikanovanie a trolling.

4. **Hrozba vyhorenia.** Po niekoľkých mesiacoch či rokoch influenceri neraz zažívajú syndróm vyhorenia, stratia energiu pokračovať, sú z toho unavení alebo znechutení z negatívnych reakcií.

5. **Strata súkromia.** Pri všetkej popularite a nadmernom zdieľaní obsahov o svojom živote môže človek strácať súkromie, čo ohrozuje osobnú pohodu, ako aj bezpečnosť.

6. **Problémy vo vzťahoch v skutočnom živote**. Sústredenie sa na prácu smerujúcu k fanúšikom uberá z času, pozornosti a energie venovanej blízkym priateľom a rodine. Niektoré priateľstvá môžu byť preverené alebo aj ohrozené záťažou popularity a žiarlivosťou kamarátov. A tu netreba zabúdať, že zástupy fanúšikov ešte neznamenajú dostatok blízkych priateľov a tí sú predsa nedoceniteľní.

Skutočný svet verzus online svet

Kľúčové slová:

problematické používanie internetu | závislosť od internetu | prenos z hráčskeho sveta | selfie dysmorfia

Otázky, na ktoré odpovedá táto podkapitola:

Existuje závislosť od internetu? Čo považujeme za problematické používanie internetu? Kedy už ide o závislosť od online aktivít? Ako môže spozorovať učiteľ, že dieťa prepadlo online aktivitám? Hrozí, že sa dieťa častým hraním stratí vo virtuálnej realite? Kedy hovoríme o problematickom používaní sociálnych sietí? Sú deti samými sebou alebo viac tými, akí sa prezentujú na sociálnych médiách? Čo u detí spôsobuje strach z vynechania? Ako tlak na krásu vplýva na sebaobraz detí? Vnímajú deti autentický zážitok alebo vyberajú kulisy pre „fotoshooting"? Hrozí deťom zahltenie komunikáciami?

Praktické cvičenia k tejto podkapitole:

Klavír, Návrh kampane za používanie internetu bez závislostí, Digitálny detox

Existuje závislosť od internetu?

Závislosť od internetu, teda od samotného média, neexistuje. Online a offline svet sú len prostredia, kde človek zažíva rôzne veci a podobne, ako neexistuje nič také ako závislosť od „bytia offline", tak nie je ani závislosť od „bytia online". Existuje len závislosť od konkrétnych online aktivít alebo ich nadmerné/problematické používanie. U detí a tínedžerov ide hlavne o tieto online aktivity:

- hranie hier,
- vyhľadávanie informácií,
- používanie sociálnych sietí a četovanie,
- nadmerné pozeranie videí,
- online nakupovanie.

Čo považujeme za problematické používanie internetu?

Existuje mnoho činností na internete, ktoré si môže človek užívať, ale za určitých okolností im môže prepadnúť až do takej miery, že ich robí opakovane a škodlivým spôsobom, avšak nedarí sa mu tieto činnosti obmedziť. Vtedy ide o tzv. problematické používanie internetu, teda také, ktoré narúša osobný a sociálny život, zhoršuje výkon v práci alebo v škole.

Problematické používanie internetu ešte nie je závislosť, je však akousi šedou a kritickou zónou, ktorá sa môže pri lepšej online životospráve zas upraviť a nemusí mať žiadne následky. Sú aj prípady, keď problematické používanie prerastie do závislosti, podobne ako napríklad pri pití alkoholu. Už pri problematickom používaní je potrebné spozornieť a snažiť sa, aby sa nerozvinula závislosť. Najväčší výskyt nadmerného používania internetu je vo veku dospievania a mladšej dospelosti (13 – 20 rokov).

Čo však urobí z obľúbenej online aktivity problematické používanie či závislosť? Nejde len o intenzitu a čas, ktorý dieťa venuje aktivite, ale aj o širšiu životnú situáciu a zraniteľnosť.

Rizikovými faktormi problematického používania internetu sú:

- genetická zraniteľnosť (závislosti v rodine),
- aktuálna psychická zraniteľnosť (náročné obdobie, veľa záťaže, depresívnosť),
- celková spokojnosť v živote, rodinná situácia, kvalita rovesníckych a iných vzťahov,
- psychická odolnosť dieťaťa, stratégie zvládania stresu a konfliktov,
- situačné faktory (rozchod, hádky, strata bezpečia, výrazný negatívny zážitok),
- nízka rozmanitosť aktivít, ktoré dieťaťu prinášajú radosť v offline svete,
- povaha online aktivity.

Kedy už ide o závislosť od online aktivít?

Množstvo investovaného času ešte nevypovedá o závislosti. Najpodstatnejší je vzťah dieťaťa k danej aktivite, teda či je tento vzťah relatívne slobodný alebo od neho dieťaťu „závisí život". Rozhoduje priorita, ktorú človek dá online aktivite, a to, či ho/ju daná činnosť oberá o iné dôležité oblasti života.

Tak ako pri všetkých závislostiach, aj v závislosti od online aktivity musí byť prítomných 6 znakov:

1. **Dôležitosť.** Daná online aktivita je v živote človeka prioritou číslo jeden a odsúva iné činnosti a hodnoty na vedľajšiu koľaj. Väčšinu svojej energie človek investuje do tejto činnosti alebo myslenia na ňu. V prípade dieťaťa si okolie môže všimnúť, že klesá počet a rozmanitosť záujmov a činností, ktoré predtým boli v jeho živote.

2. **Zmeny nálad.** Nálada človeka sa odvíja od ne/prítomnosti aktivity, od ktorej je závislý.

3. **Rastúca potreba** človeka vykonávať danú aktivitu. Na to, aby aktivita ďalej prinášala dostatočné potešenie, potrebuje ju človek opakovať čoraz častejšie a vo väčšej intenzite.

4. **Abstinenčné príznaky**. Ide o nepríjemné stavy, ktoré nastúpia, ak nie je možné vykonávať aktivitu alebo ak je potrebné obmedziť jej vykonávanie. Sprievodnými znakmi – podobne ako pri látkových závislostiach – sú zhoršená nálada, podráždenosť, agresivita, nervozita, nesústredenosť.

5. **Konflikt**. Ide o nevyhnutný príznak závislosti. Opakované závislé správanie človeku spôsobuje ťažkosti vo vzťahoch, vo fungovaní v škole môže dochádzať aj k vnútornému konfliktu (pocity viny, sebanenávisť).

6. **Strata kontroly**. Po období snahy o obmedzenie online aktivity prídu epizódy, keď človek naplno prepadne závislosti a stratí sebakontrolu.

Najzásadnejším rozlišovacím znakom závislostí od online aktivít je konflikt a strata kontroly. To znamená, že človek si uvedomuje, že dané správanie mu spôsobuje problémy, ale napriek všetkej snahe sa nevie dobre ovládnuť a opakovane prepadne aktivite. Veľmi často sú symptómy závislosti od internetu príznakmi iných duševných ťažkostí, ktoré si tiež vyžadujú pozornosť.

Takáto nelátková závislosť od online aktivít je však zriedkavá, obvykle ide o tzv. „problematické používanie internetu", ktoré sa týka pomerne veľkej časti populácie a najmä mladých ľudí.

Ako môže spozorovať učiteľ, že dieťa prepadlo online aktivitám?

Dieťa za učiteľom asi nikdy nepríde s tým, že mu online aktivity prerastajú cez hlavu. Rovnako nie je ľahké tento problém rozoznať, keďže internet a digitálne technológie sú v súčasnosti prirodzenou súčasťou našich životov. Deti o nich navyše veľa rozprávajú, takže táto téma je takmer všadeprítomná. Učiteľ si môže všimnúť niektoré z nasledujúcich zmien v správaní dieťaťa:

- je častejšie nevyspaté a nesústredené,
- zhoršuje sa jeho prospech a stráca predošlý záujem o školu,
- je častejšie mrzuté, podráždené, agresívne alebo je mysľou niekde inde,
- výrazne klesne počet jeho/jej kamarátov,
- o ničom inom nerozpráva,
- stráca akékoľvek predošlé záujmy,
- teší sa len na to, kedy sa znovu dostane k svojej obľúbenej online aktivite.

Tieto zmeny v správaní dieťaťa učiteľovi môžu pomôcť identifikovať online závislosť. To, o akú online závislosť ide, je možné odhadnúť z toho, o čom dieťa najviac rozpráva, napríklad hranie hier, sociálne siete atď.

Nakoľko môže ísť aj o iné duševné ťažkosti, učiteľ by mal situáciu konzultovať priamo s rodičmi, ktorí obvykle najlepšie vedia, čo sa deje s ich dieťaťom. Vhodné je obrátiť sa na školského psychológa a rodičom odporučiť pre žiaka či rodinu terapeutickú pomoc.

Čo môže urobiť učiteľ?

- vybudovať si dobrý vzťah s deťmi založený na rešpekte a dôvere,
- primerane sa zaujímať o to, ako sa deti majú a čo robievajú aj vo voľnom čase,
- byť všímavým pozorovateľom, aby postrehol/postrehla zmeny v správaní dieťaťa,
- aj pri menšom podozrení sa porozprávať s rodičmi o tom, že si o dieťa robí starosti. Ďalej je na rodičovi, aby stanovil doma pravidlá ohľadom online aktivít a digitálnych nástrojov,
- robiť so žiakmi na hodinách aktivity, ktoré ich upozornia na možné riziká,
- zvyšovať povedomie o závislostiach od online aktivít,
- využívať jednoducho koncipované rovesnícke preventívne programy,
- zvyšovať vlastné vedomosti a kompetencie a udržiavať si prehľad o používaní jednotlivých online aktivít a aplikácií,
- naučiť žiakov vnímať vlastné používateľské návyky v širšom kontexte – napríklad to, ako súvisia s ich náladami, zaangažovanosťou do činností offline, úspechov i neúspechov, životných situácií a podobne. Vedomý používateľ internetu je lepšie pripravený mať svoj online život vo vlastných rukách.

Problematické hranie videohier

Dnes takmer všetky deti hrajú nejaké videohry, či už na počítačoch, tabletoch, herných konzolách, telefónoch alebo inak. Záujem o elektronickú zábavu je približne rovnaký u chlapcov i dievčat. Rodičia i učitelia by určite preferovali, aby sa deti hrali prevažne vzdelávacie hry, ale realita je taká, že deti sa túžia hrať hlavne pre zábavu. Ak sa deti hrajú hry vhodné pre ich vek a stráži sa rozsah a dôležitosť, aké má hranie v ich životoch, takáto zábava je neškodná. Avšak, nájdu sa aj deti, ktoré sa hrajú nadmerne, odmietajú robiť čokoľvek iné, a pre ktoré sa hranie stalo prioritou číslo jeden. Vtedy môže ísť o závislé hranie. Podobných prípadov je málo, hovorí sa približne o 3 – 5 %.

Najčastejšie sú hráči závislí od hier MOBA (multiple online battle arena), čo sú krátke sekvencie bitiek, ktoré hrajú prevažne chlapci (napr. League of Legends, War of Tanks).

Druhými najrizikovejšími hrami sú MMORPG (multiple online role playing games), teda online hry pre mnoho hráčov, kde je hra postavená na vylepšovaní vlastného avatara (War of Warcraft).

Obľúbenými medzi menšími deťmi sú aj tvorivé budovateľské hry ako Minecraft. Hráč v nich vytvára prostredie, do ktorého vstupuje v role postavy. Pri Minecrafte je menšia pravdepodobnosť závislosti aj preto, že je to tvorivá, neagresívna hra, sekvencie pohybov v hre sú pomalšie a preferujú ju menšie deti. V ranom veku sú online závislosti navyše zriedkavé, pokiaľ rodičia dbajú o rozmanitosť aktivít a záujmov.

Hrozí, že sa dieťa častým hraním stratí vo virtuálnej realite?

Pri častom hraní online hier alebo počítačových hier sa môže stať, že po ukončení hrania dotyčný stále vníma vonkajšie podnety tak, akoby boli z hráčskeho sveta. Každodenné situácie dotyčnej osobe môžu pripomínať výzvy, ktorými prechádzala v hre, a tak na ne aj odpovedá. Či už ide o odpoveď emočnú, teda že mu/jej stúpne adrenalín a miera pripravenosti konať, podobne ako v hre, alebo ide o odpoveď slovnú či mentálnu. Môže sa stať, že človek sám seba vníma tak, akoby bol hrdinom hry a pozeral sa cez hráčsku optiku. Môže si predstavovať nad hlavami ľudí políčka symbolizujúce počet ich životov či očakávať ukryté hráčske poklady a bonusy za najbližším rohom.

To však ešte stále nutne neznamená, že je závislým hráčom. Môže ísť len o prirodzené prispôsobenie sa mysle na dlho využívaný spôsob vnímania. Vtedy sa častejšie objavujú aj vtieravé opakujúce sa myšlienky súvisiace s hrou alebo čosi ako „flešbeky" – živé záblesky – z hry. Objavuje sa to pri dlhých sekvenciách hrania alebo pozeraní mnohých dielov seriálu „na jedno posedenie". Po prestávke od týchto aktivít sa opäť myseľ nanovo nastaví na prostredie, kde sa bude dlhodobo nachádzať.

Rizikom je túžba vyskytovať sa čo najviac v prostredí, na ktoré sa takto myseľ prispôsobila. Neraz to tvorí podstatu nadmerného hrania, v niektorých prípadoch je to hnacím motorom závislosti. Nie každé dieťa, ktoré trávi hraním veľa času, je od hrania závislé, môže si to užívať, no treba mať v celkovom živote stále rozmanitosť a nebyť závislými.

Kedy hovoríme o problematickom používaní sociálnych sietí?

Dieťa môže používať sociálne médiá slobodne, aj keď na nich trávi veľa času. Vždy záleží aj na tom, čo presne tam robí a prečo, či je spokojné s tým, koľko času tomu venuje. Alebo s množstvom času nie je spokojný/-á, ale nedarí sa mu/jej to kontrolovať. Čím je dieťa vnútorne zraniteľnejšie, menej spokojné a menej začlenené medzi rovesníkov, tým viac môže závisieť jeho/jej nálada a pohoda od úspechu na sociálnych sieťach.

Príliš neisté a úzkostlivé deti môžu nutkavo kontrolovať reakcie na vlastné príspevky, inokedy dieťa odbieha k sociálnym médiám z pocitu vnútornej nudy, osamelosti alebo pre rozptýlenie pozornosti, keď sa trápi.

Ako tlak na krásu vplýva na sebaobraz detí?

Publikum často nerozozná, kedy sú fotografie retušované. To má negatívny vplyv na sebahodnotenie používateľov, ktorí si popri retušovaných fotografiách pripadajú škaredí a nedokonalí. Príliš časté používanie sociálnych médií, hlavne Instagramu, tak môže vytvárať rozladenosť, pocit nedostatočnosti a osamelosti u dospievajúcich.

Posúva to tiež ideál krásy smerom k nerealistickým obrazom. Ak sú deti menej v kontakte s tým, čo je prirodzené, reálne a autentické, môžu postupne začať vnímať pozmenenú vizáž za normu a robiť všetko preto, aby sa k nej priblížili.

Sú deti samými sebou alebo viac tým, čím sa prezentujú na sociálnych médiách?

Niektorí ľudia internet využívajú najmä na to, aby ukázali, čo radi robia, no nájdu sa aj takí, ktorí sa online vydávajú za úplne iných ako v skutočnosti. Takáto pretvárka môže nepriamo vytvárať úzkosť a viesť k vnútorným konfliktom a odmietaniu seba samého. Keď sa človek prezentuje príliš „retušovane", vytvára na seba tlak a vyvoláva v sebe pocit sklamania pri zážitkoch, ktoré sa s touto retušovanou predstavou nezhodujú.

Vnímajú deti autentický zážitok alebo si len vyberajú kulisy?

Robiť si selfie fotografie je pre mladých zábava. Mnohým sa však stáva, že zabudnú na samotný zážitok a príliš sa sústredia na výslednú fotografiu. Napríklad pri prechádzke mestom sa tínedžer viac sústredí na to, čo bude vhodná kompozícia pre jeho fotografiu než na samotnú prechádzku alebo na spoločnosť priateľov. Existujú dokonca prípady, keď sa mladí stali závislí od robenia a zdieľania retušovaných selfie.

Čo u detí spôsobuje strach z vynechania (FOMO)?

Strach z vynechania je strach, že človek premešká niečo zaujímavé alebo dôležité, napr. koncerty, oslavy kamarátov, výlety, tréningy atď. To môže spôsobovať úzkosť a negatívne pocity. Podobné pocity môže vyvolať aj strach používateľa/dieťaťa, že premešká najčerstvejšie pikošky na sociálnych sieťach. Prejavom je príliš časté kontrolovanie svojho zariadenia a nervozita.

Hrozí deťom zahltenie komunikáciou?

„Byť neustále k dispozícii“ na dvoch-troch platformách naraz dáva tínedžerom vytúžený pocit zahrnutia do komunity a prehľadu, je to však psychicky vyčerpávajúce. Láka to k nutkavému kontrolovaniu smartfónov a rozptyľuje to pozornosť, zahlcuje a vyvíja tlak. Priemerne sa školáci pozrú na svoj telefón každé tri minúty. Miera tlaku závisí aj od počtu sledovaných platforiem a ich povahy.

Dospelí môžu pomôcť deťom nadobudnúť vnútornú rovnováhu, podporiť ich sebavedomie, posilniť ich rovesnícke zručnosti, aby mali dostatok kvalitných kamarátstiev offline či pomôcť im nájsť si zmysluplné trávenie voľného času. Ak sa dieťa opakovane dostáva do konfliktov a problémov v rodinnom prostredí či s kamarátmi, je potrebné s ním viesť dôverný rozhovor a pomôcť mu vyhľadať pomoc, podporu alebo aj psychológa.

Dezinformácie, hoaxy a falošné správy

Kľúčové slová:

hoax | dezinformácie | falošné správy | spravodajské vojny | skresľovanie | konšpirácie | dezinformačné médiá vs tradičné médiá | analytické myslenie

Otázky, na ktoré odpovedá táto kapitola:

Čím sa líši misinformácia od dezinformácie? Kto a prečo produkuje dezinformácie? Čo sú dezinformačné médiá? Ktoré informácie sa šíria rýchlejšie a prečo? Čo je konfirmačné skreslenie? Ako naša myseľ hľadá odpoveď na neznáme otázky? Čo sú to hoaxy? Aké podoby majú dezinformácie a hoaxy? Podľa čoho identifikujeme hoax/falošnú správu? Ako sa chrániť pred hoaxmi? Ako zastaviť falošné správy? Kde si môžeme overiť správy? Čo spraviť s falošnou správou? Akú hrozbu predstavujú hoaxy?

Praktické cvičenia k tejto kapitole:

Rozpoznávanie pravdivých a falošných správ, Rozoznáš klamstvo?

Čím sa líši misinformácia od dezinformácie?

Tieto dva pojmy sa často zamieňajú, no nemajú rovnaký význam. Obe šíria nesprávne či vymyslené informácie, no v prípade misinformácie je jej šíriteľ úprimne presvedčený o jej pravdivosti a nemá v úmysle ňou škodiť. Dezinformácia je rovnako fakticky nesprávna, no jej tvorca a často aj šíriteľ to vie, a napriek tomu ju vedome rozširuje a snaží sa tým ublížiť.

Dezinformácie môžu byť aj informácie, ktoré sú vo svojom jadre pravdivé, ale sú šírené bez súvislostí – sú kumulované na jeden portál alebo profil a vytvárajú skreslený pohľad na problematiku. Vyberajú sa napríklad ojedinelé prípady, ktoré sú však kumulované. Dezinformácia vedie k nesprávnym záverom alebo rozhodnutiam. Je aj nástrojom tzv. psychologickej vojny – propagandy.

Kto a prečo produkuje dezinformácie?

Dezinformácie sú bežné v nekalom súperení politických strán, v spravodajských hrách medzi rôznymi politickými systémami, medzi znepriatelenými štátmi. Predstavujú aj prvok vojenského súperenia. Cieľom dezinformácie je oklamať protivníka a doviesť ho k záverom, ktoré sú prospešné autorovi dezinformácie. Často stačí, že dezinformácie vytvoria atmosféru chaosu, pochybnosti o tom, čo je pravdivé, a teda znížia dôveru v autority, ktoré riadia spoločnosť, alebo v systém. A narušenie funkčnosti nejakého systému môže byť práve zámerom tvorcov dezinformácií.

Dôvodom môže byť aj biznis – na trhu existuje priestor na informácie, ktoré tradičné médiá neposkytujú. Dôvodom nepokrývania tohto priestoru nie je to, že by chceli niečo zamlčať, ale to, že tie informácie sú buď nepravdivé, alebo nekvalitné, resp. neoveriteľné. Vyplnením tohto prázdneho priestoru môže vzniknúť dezinformačné médium s relatívne vysokou sledovateľnosťou, čo im umožní zarobiť na reklame.

Čo sú dezinformačné médiá?

Dezinformačné alebo konšpiračné médiá sa zameriavajú na šírenie dezinformácií. Zvykneme ich nazývať aj pojmom konšpiračné médiá. Ich cieľom je šíriť konšpiračné teórie, hoaxy, neoverené alebo zmanipulované informácie. Ich tematika je väčšinou zameraná jedným smerom – v súčasnosti najmä na tému utečencov, proti COVID-19, proti EÚ.

Formálne sa snažia podobať na tradičné médiá, viaceré napríklad publikujú aj reálne správy. No kým tradičné médiá opisujú svet komplexne a ucelenejšie, dezinformačné sa najviac venujú vybraným témam, v ktorých chcú negatívne ovplyvňovať myslenie čitateľov. Častejšie preberajú správy z iných zdrojov alebo ich prekladajú, dajú im šokujúcejší titulok. Ak robia rozhovory, tak väčšinou s osobami, ktoré majú rovnaké názory a podporujú ciele média. Neriešia otázky etiky a serióznosti. Ich cieľom nie je informovať a kontrolovať verejnú moc, ale viesť kampaň proti demokratickému systému. Chyby v správach sú úmyselné, zamlčiavajú časť informácie a vytrhávajú správy z kontextu.

Veľkú skupinu dezinformačných médií tvoria nielen spravodajské portály, ale aj médiá venujúce sa zdraviu. Populárnym článkom na českom internete bol článok „Rakovina sa dá vyliečiť peroxidom vodíka" a na Slovensku napríklad článok: „Tajomstvo odhalené: Rakovina nie je choroba, ale biznis. Takto s ňou zatočíte."

Takmer v každej krajine sveta fungujú okrem štandardných aj dezinformačné médiá. Napriek riziku, ktoré predstavujú, je dobré ich poznať, aby sme sa im vyhli a nešírili správy z nich ďalej.

Ktoré informácie sa šíria rýchlejšie a prečo?

Výskum, ktorý v marci 2018 zverejnil časopis Science, potvrdil, že falošné správy sa na internete šíria rýchlejšie ako pravdivé. Autori porovnávali šírenie informácií na sociálnej sieti Twitter a zistili, že nepravdivé informácie sa šírili šesťkrát rýchlejšie. Ľudia radi ďalej šíria informácie, ktoré pôsobia senzačne. Pred svojím okolím, ale aj samým sebou tak vyzerajú byť informovanejší a tí, čo sú „v obraze" a pri zdroji informácií.[10]

Na mnohé otázky existujú odpovede, pravdivé informácie sú však pre mnohých ľudí menej zaujímavé a nudnejšie na rozdiel od nepravdivých informácií. Overené informácie, ktoré vysvetľujú alebo vyvracajú nepravdy, sa šíria oveľa ťažšie a často sa nedostanú k ľuďom, ktorí si prečítali pôvodnú senzačnú informáciu. Napraviť tak škody po dezinformátoroch je ak nie nemožné, tak veľmi ťažké. Nepravdivé informácie bývajú populistické, ľahko sa šíria aj vďaka internetu a tiež vďaka nižšej dôvere ľudí v autority.

Ďalším dôvodom je, že ľudia uprednostňujú informácie, ktoré zapadajú do ich videnia sveta, do ich jestvujúcich názorov, vzniká tzv. konfirmačné skreslenie.

Čo je konfirmačné skreslenie?

Je to prirodzená vlastnosť nášho myslenia, teda chyba v úsudku. Je to tendencia uprednostňovať, hľadať, z pamäti si prednostne vyvolávať také informácie, ktoré potvrdzujú naše presvedčenie alebo hypotézu. Menšiu pozornosť venujeme alternatívnym možnostiam.

Z experimentov vieme, že ľudia nehľadajú informácie, ale názory, ktoré potvrdzujú to, čo si už dopredu myslia – konfirmácie (konfirmujú – potvrdzujú ich predstavy). Efekt konfirmačného skreslenia je silnejší pri emocionálne nabitých otázkach a hlboko zakorenených presvedčeniach. Je to zameranie sa na posudzovanie myšlienok jednostranným spôsobom a ignorovanie alternatív. Vďaka konfirmačnému skresleniu sme presvedčení aj o pravdivosti nepravdivej informácie a v dobrej viere ju šírime ďalej v domnienke, že je pravdivá. Šírime misinformáciu. Keďže o pravdivosti správy sme presvedčení, nevidíme dôvod na jej overovanie. Preto je veľmi dôležité poznať konfirmačné skreslenie a neustále pochybovať o pravdivosti a následne si ju overovať. Len neustále overovanie a porovnávanie informácií s viacerými dôveryhodnými zdrojmi je cestou, ako sa vyhneme šíreniu nepravdivých správ.

10 VOSOUGHI, S. et al.: The spread of true and false news online. In Science, 2018, [online]. <https://science.sciencemag.org/content/359/6380/1146>

Ako naša myseľ hľadá odpoveď na neznáme otázky?

Pri vytváraní úsudku preferujeme jednoduchšie a ľahšie riešenie problémov pred riešením, ktoré si vyžaduje viac premýšľania a snahy. Sme leniví prečítať si komplexnejšie informácie.

Ak dostaneme otázku, na ktorú nepoznáme odpoveď, naša myseľ si ju transformuje na takú otázku, ktorú vieme rýchlejšie vyhodnotiť. Pri vyhodnocovaní si vybavujeme v pamäti situácie, na ktoré si vieme čo najrýchlejšie spomenúť. Skúste si odpovedať na otázku: Ktoré povolanie je nebezpečnejšie – policajt alebo morský rybár? Pravdepodobne väčšina ľudí odpovie policajt, lebo sa im v pamäti vybavia akčné filmy, v ktorých vystupujú policajti v rôznych prestrelkách. V skutočnosti odpovedáme na otázku, v koľkých nebezpečných situáciách ste videli policajta a v koľkých morského rybára. Podľa štatistických údajov morský rybár patrí medzi najrizikovejšie povolania na svete. Podrobnejšie o fungovaní nášho myslenia a chybách v myslení sa dočítate v knihe Myslenie rýchle a pomalé (Daniel Kahneman).

Experti (**Gordon Pennycook a David Rand**), ktorí skúmajú ľudské myslenie, potvrdili teóriu, že náchylnosť uveriť falošným správam vychádza z nedostatočne rozvinutého analytického myslenia.

Čo sú to hoaxy?

Hoax je správa s klamlivým, falošným či inak vedome nesprávnym obsahom (a teda dezinformáciou), ktorá sa snaží vyvolať negatívnu emóciu a zmanipulovať príjemcu, aby správu preposielal a ďalej masovo šíril. Hoax je špecifický typ dezinformácie, obsahuje požiadavku na ďalšie šírenie. V podstate ďalší šíritelia hoaxu môžu byť vďaka manipulácii presvedčení o pravdivosti obsahu, a teda ho šíria ako misinformáciu. Autor hoaxu sa často vydáva za dôveryhodný zdroj (firmu, štátnu inštitúciu alebo zneužíva ich meno na podvodné citácie, ako napr.: „americkí vedci zistili“, „podľa zistení Interpolu“) a varuje pred katastrofickými následkami fiktívnej udalosti. Používa pritom tvrdenia, ktoré nemajú oporu vo vedecky overených alebo overiteľných dátach. Cieľom tvorcu hoaxu je vyvolať strach, úzkosť či pocit ohrozenia a donútiť tak obeť, aby konala nepremyslene.

Aké podoby majú dezinformácie a hoaxy?

Dezinformácie a hoaxy môžu mať viacero podôb, na ilustráciu uvádzame jedny z najrozšírenejších.

- **Zneužívajúce súcit** – Tento druh hoaxov sa snaží zneužívať súcit prijímateľa a za ďalšie šírenie, lajkovanie či popularizáciu sľubuje nereálnu finančnú odmenu, záchranu ohrozeného života či iné výhody.
- **Falošné správy a dezinformácie (Fake news)** – snažia sa pomocou upravených, prekrútených či vymyslených informácií manipulovať masy a ich názory, najčastejšie s politickým alebo ideologickým cieľom. Ich silu zvyšujú aj sociálne siete, ktoré podobný obsah neregulujú a pre jeho vysokú virálnosť ho ich algoritmy šíria ešte intenzívnejšie.
- **Vymyslené citáty známej osobnosti** – autor informáciu šíri ako citát (vyjadrenie) známej osobnosti, ktorá má v danej krajine (lokalite) dôveru a jej názory môžu byť mienkotvorné. Takáto správa/informácia sa pre zvýšenie hodnovernosti doplní aj fotografiou osobnosti. Môže ísť o známu osobu, ktorá je staršia a nie je, alebo je menej aktívna na sociálnych sieťach, preto je správa ťažšie overiteľná.

- **Dezinformácie šírené známym človekom** – niekedy šíreniu nezmyslov pomáha známy človek, ktorý má veľa fanúšikov, ale nie je odborníkom v danej oblasti. Môže to byť spevák, politik, ale aj známy lekár. Napríklad nezmyselné informácie o ochorení COVID-19 šíril známy lekár venujúci sa životospráve. Donald Trump navrhoval bojovať s pandémiou COVID-19 pomocou dezinfekčného prostriedku, čo malo za následok aj otravu u jednej osoby.
- **Technologické hoaxy** – väčšinou sa šíria pomocou e-mailov a upozorňujú na vymyslený vírus alebo technologickú hrozbu. Často nás vyzývajú k aktivite, ktorá nám poškodí funkčnosť technológie. Napr. nás vyzývajú na vymazanie konkrétneho súboru v operačnom systéme (ktorý je bežnou súčasťou) a tvrdia, že ak tam taký súbor nájdeme, naše zariadenie je už napadnuté vírusom.
- **Zábavné hoaxy, hoaxy vytvorené pre príležitosti, keď sa považujú za spoločensky vhodné** – zväčša sú vytvárané napr. k 1. aprílu ako kanadské žartíky s cieľom dobehnúť používateľa. Niekedy sa nájdu používatelia, ktorí informácii uveria a ešte ju dlho šíria ďalej. Táto forma hoaxu je v podstate neškodná.
- **Reťazové správy** – v minulosti sa šírili listami klasickou poštou, dnes sa presunuli na internet. Adresáta nabádajú na ďalšie šírenie a využívajú poverčivosť ľudí. Napríklad tvrdia, že ak správu nepošlete aspoň piatim ďalším ľuďom, budete mať nešťastie, v prípade, že správu prepošlete, sľubujú vám rôzne výhody.
- **Upravené alebo staré fotografie (video)** – pri tvorbe dezinformácie sa často používa aj stará fotografia, ktorá je reálna, ale viaže sa k inej udalosti. Fotografia sa niekedy aj upraví, dorobia sa v nej veci, čím vznikne falošná fotografia. Autor k nej pripojí text, ktorý je napríklad kompilátom názorov kontroverzného servera, ktorý šíri hoaxy pravidelne. Typickým príkladom je fotografia z roku 1991 s loďou Vlora, ktorá sa použila v roku 2018 v Európe v súvislosti s migračnou krízou.

Voľne dohľadateľné obrázky v Google prehliadači. Zdroj: Google.com

Doplniť klamlivý text k starému obrázku je jednoduchá a veľmi účinná metóda zavádzania. Obrázok netreba nijako zmanipulovať, sám osebe vyzerá dôveryhodne.

Podľa čoho identifikujeme hoax/falošnú správu?

Mnohé z falošných správ majú charakteristické znaky, ktoré ich dokážu prezradiť. Často pochádzajú zo zdrojov s pochybnou alebo kontroverznou povahou, prípadne zdroj nie je vôbec uvedený. Na stránkach, ktoré šíria falošné správy, väčšinou chýba kontakt na redakciu či konkrétneho autora, prípadne majú nízku úroveň gramatiky a štylistiky.

Objavujú sa aj texty a weby, ktoré sú profesionálne a kvalitne spracované. V takom prípade je jedinou možnosťou, ako odhaliť ich falošný pôvod, neustále overovanie a porovnávanie informácií s viacerými dôveryhodnými zdrojmi. Dôveryhodné sú najmä štandardné médiá, ktoré robia svoju prácu transparentne, overujú si fakty a dodržiavajú etický kódex. Dobrým zdrojom môžu byť aj nezávislé (medzinárodné) organizácie, mimovládne inštitúcie, univerzity či vedecké ústavy demokratických štátov.

Za podozrivé by sme mali označiť aj príspevky, ktoré nemajú uvedený dátum a miesto udalosti, ktorú opisujú. Zbystriť by sme mali aj v prípade príspevkov, ktoré sa zaoberajú politicky citlivými témami a snažia sa pri tom pôsobiť senzačne a poburujúco.

Čím je správa šokujúcejšia, tým je pravdepodobnejšie, že je to dezinformácia. Nezabúdajme, že počet lajkov a zdieľaní nehovorí nič o pravdivosti a dôveryhodnosti správy.

Ako sa chrániť pred hoaxmi? Ako zastaviť falošné správy?

Je dôležité učiť sa rozpoznávať pravdivé a falošné správy. Nielen preto, aby sme my sami poznali pravdu, ale aj preto, aby sme dezinformácie nešírili ďalej. V nasledujúcom postupe uvádzame kroky, ktoré nám pomôžu identifikovať falošnú správu a následne zastaviť jej šírenie.

- **Zvážte zdroj** – preskúmajte účel stránky, pozrite si zverejnené kontakty, overte si ich vo vyhľadávači. Je to tradičné seriózne médium alebo ste ho našli v zozname dezinformačných médií?
- **Preverte si autora** – vyhľadajte si informácie o autorovi. Je dôveryhodný? Akým témam sa venuje? Je to reálny autor alebo ide o vymysleného/fiktívneho autora?
- **Skontrolujte si dátum** – je v správe uvedený dátum? Ide o nový alebo starý článok? Dávajte si pozor na staré správy, to, že boli pravdivé v minulosti, neznamená, že sú relevantné a pravdivé aj dnes. Medzičasom mohlo výrazne pokročiť vedecké poznanie v danej oblasti.
- **Zamyslite sa, či nie ste zaujatí** – aké je vaše presvedčenie? Podporuje správa to, čo si už vopred myslíte? Pozor na konfirmačné skreslenie.
- **Čítajte celú správu, nielen nadpis** – nadpis správy môže byť šokujúci, aby vás motivoval na ňu kliknúť (clickbait). Aký je celý príbeh? Nie je nepravdivý len nadpis, aby vás článok zaujal?
- **Pozrite si kvalitu zdrojov** – obsahuje správa odkazy na iné zdroje? Overte si, či uvedené zdroje nie sú v rozpore s tvrdeniami v danej správe.
- **Zamyslite sa, či nejde o vtip** – nie je obsah čudný? Zamyslite sa, či to nie je satira alebo irónia. Skontrolujte si stránky a autora, aby ste sa uistili, či nejde o vtip.
- **Spýtajte sa experta** – spýtajte sa odborníka, konzultanta alebo stránky, ktorá je zameraná na kontrolu faktov.

Kde si môžeme overiť správy?

Pravdivosť správ si môžeme overiť aj cez špecializované webové stránky, ktoré sa zaoberajú odkrývaním hoaxov. Napríklad stránky: snopes.com alebo stopfake.org, FactCheck.org, hoax.cz.

Na Slovensku zverejňuje aktuálne hoaxy aj Polícia SR na sociálnej sieti Facebook.

Ak príspevok/správa obsahuje obrázok, jeho pravdivosť môžeme overiť aj pomocou spätného vyhľadávania (reverse search) obrázkov cez Google.

Čo spraviť s falošnou správou?

Ak správu vyhodnotíme ako falošnú, nešírme ju ďalej. Ak poznáme šíriteľa správy (často je to okruh našich známych), je vhodné ho upozorniť na fakt, že správa je falošná. Na falošné správy, hoaxy a dezinformácie šírené na sociálnych sieťach môžeme upozorniť nástrojmi sociálnej siete priamo prevádzkovateľov sociálnej siete. Priamo v ponuke pri príspevku nájdeme možnosť „Nahlásiť príspevok" a tam môžeme uviesť dôvod nahlásenia – Falošná správa.

Akú hrozbu predstavujú hoaxy?

Hoaxy a dezinformácie už nie sú výmyslom, ktorý môžeme len tak písať a hovoriť hocikomu. Neospravedlňuje nás ani to, ak je našou motiváciou na šírenie nezmyslov drobná zábava či recesia. Dezinformácie môžu narobiť veľké škody na majetku i na zdraví. Hoax vás môže obrať o peniaze, stačí, keď uveríte nejakej bizarnosti, alebo len vďaka šíreniu hoaxov na sociálnej sieti sa neznáma osoba dostane k vašim citlivým údajom, napríklad k číslu bankovej karty.

Šírenie hoaxov v zdravotníckej oblasti je veľmi nebezpečný fenomén. Ak uveríme hoaxom a následne odmietneme liečbu, očkovanie, môže nám, ale aj celej spoločnosti hoax ublížiť aj na zdraví.

A nezabúdajme, že vytváranie a šírenie poplašnej správy a dezinformácie môže napĺňať aj prvky trestného činu. Na sociálnej sieti ste sa mohli stretnúť s tým, že polícia hľadá aj autorov poplašných správ – napríklad žiada používateľov sociálnej siete o pomoc pri identifikácii hlasu v nahrávke poplašnej správy.

Digitálna identita a súkromie

Kľúčové slová:

cloud | digitálne občianstvo | digitálna stopa | e-mailový účet | lokalita

Otázky, na ktoré odpovedá táto kapitola:

Čo je digitálna identita? Čo je to digitálna stopa a aké druhy digitálnych stôp poznáme? Dá sa digitálna stopa odstrániť? Môže používateľ zistiť, kde a akú digitálnu stopu zanechal? Čo je digitálne občianstvo? Čo je digitálny podpis? Budeme v budúcnosti voliť online?

Praktické cvičenia k tejto kapitole:

Animália, Koho vidím a koho nevidím, keď prispievam?, Súboj sociálnych sietí, Nauč svoju babku používať Facebook, Autoportrét, Selfie priepasť, Ja, moje druhé ja a selfie, CSI selfie, Kto ma vytvoril?

Čo je digitálna identita?

Používateľ si na internete môže vytvoriť prakticky neobmedzené množstvo digitálnych identít. Niektoré z nich sa môžu vo veľa ohľadoch zhodovať s jeho skutočným ja – napríklad profil na Facebooku či Instagrame – ale môžu sa aj výrazne odlišovať – profil hráča na serveroch Fortnite či Steam, skrytý za vymyslenou prezývkou. Niektoré identity dokonca používateľ môže vytvoriť zámerne odlišné, aby nebolo možné vystopovať ich originálneho majiteľa – falošný e-mail, pod ktorým sa používateľ prihlási na odoberanie reklamných letákov.

Kľúčovou pri digitálnej identite je reputácia. Tú si človek buduje svojím správaním a interakciami s inými používateľmi na danej platforme. Ak ju má dobrú, umožňuje mu to pôsobiť dôveryhodnejšie, uzatvárať obchody či dohody online, prípadne získať výhodnejšie podmienky. Príkladom je používateľ, ktorý ponúka svoj byt na krátkodobý prenájom (napr. Airbnb). Pokiaľ je spoľahlivý, jeho byt je vždy čistý a ochotne návštevníkom poradí, dostane vysoké hodnotenie od svojich zákazníkov. Keď má veľa takýchto referencií, buduje si tým reputáciu a môže získať výhody od tejto online služby a priláka aj lepších zákazníkov. Rovnako to platí aj o samotných zákazníkoch. Ak sú známi tým, že po sebe nechajú neporiadok alebo sa snažia vyhnúť plateniu, ich reputácia klesá a tým aj šance, že si nájdu ubytovanie.

Čo je digitálna stopa a aké druhy digitálnych stôp poznáme?

Ak má používateľ e-mailový účet, je prihlásený na sociálnej sieti, hráva online hry alebo len surfuje po rôznych zábavných, spravodajských či iných stránkach, vytvára pritom digitálne stopy. To však automaticky neznamená, že niekto pozná jeho/jej identitu v skutočnom svete. Digitálna identita je anonymným odrazom jeho/jej správania v digitálnom svete, ktorý v spojení s inými informáciami – digitálnymi stopami – môže viesť ku konkrétnemu človeku.

Dáta tvoriace digitálnu stopu môže používateľ poskytovať buď **aktívne**, alebo **pasívne**:

- **Pasívnu digitálnu stopu** tvoria informácie, ktoré používateľ zanecháva v online priestore nevedome a ktoré nie sú priamo viditeľné. Príkladom pasívnej digitálnej stopy môže byť typ prehliadača, zariadenia, použitého jazyka, operačný systém či IP adresa uložená v databáze poskytovateľa internetového pripojenia alebo na serveroch prevádzkovateľa online služby, ktorú používateľ navštívil. IP adresa pomáha identifikovať používateľovu približnú lokalitu či poskytovateľa internetu, no môže byť často nespoľahlivá, keďže sa dá cielene maskovať.
- **Aktívna digitálna stopa** zahŕňa všetky vedome poskytnuté a zverejnené údaje na internete. Ak používateľ pošle e-mail, zverejní blog, dá lajk fotografii/komentáru, zdieľa video alebo text na sociálnej sieti, alebo si píše cez čet, všetky tieto a im podobné informácie sa stávajú aktívnou digitálnou stopou. Používateľ by si tiež mal uvedomiť, že veľkí hráči ako napríklad Google či Facebook majú na množstve webových stránok svoje kódy, ktoré majiteľovi stránky pomáhajú analyzovať návštevnosť. Okrem toho gigantom pomáhajú zbierať rozsiahlejšie spektrum digitálnych stôp a tým aj presnejší obraz o správaní používateľa online.

To, či sa daná stopa považuje za aktívnu alebo pasívnu, často závisí od technickej úrovne používateľa. Skúsenejší používateľ si je totiž vedomý, že jeho správanie na webe môže byť sledované, a preto sa vedome vyhýba určitým stránkam či online službám alebo používa nástroje, ktoré bránia sledovaniu.

Dá sa digitálna stopa odstrániť?

Digitálna stopa je trvalá a nezmazateľná súčasť našej online existencie. Na základe General Data Protection Regulation (GDPR) síce má každý občan EÚ právo požiadať „o zabudnutie", no ide o pomerne zdĺhavý proces. Navyše, aj keď na konci tohto procesu daná služba či prevádzkovateľ už nemá údaje používateľa, mohli sa zachovať v inej databáze či byť súčasťou balíka dát, ktorý už medzičasom skončil v rukách inej organizácie. Nevhodný e-mail alebo zahanbujúca fotografia používateľa sa navyše môže zachovať aj na disku iného človeka, ktorý si z nej urobí printscreen. Týmto spôsobom sa informácia aj napriek vymazaniu môže opätovne objaviť na internete a v budúcnosti skomplikovať používateľovi napríklad prijímací pohovor či nadviazanie nového vzťahu.

Môže používateľ zistiť, kde a akú digitálnu stopu zanechal?

Vďaka legislatíve je to možné, no stále pomerne náročné. Firmy, ktoré o svojich používateľoch zbierajú dáta, majú totiž podľa regulácie GDPR (platí len pre občanov EÚ) povinnosť mu tieto údaje poskytnúť v prípade, že o to požiada. Aj preto sociálne siete či iné veľké online služby majú často priamo v používateľských nastaveniach zabudovanú možnosť, vďaka ktorej si jednotlivec môže vyžiadať všetko, čo o ňom vie daný prevádzkovateľ.

Čo je digitálne občianstvo?

Rovnako ako sme občanmi krajiny vo fyzickom svete, postupne sa nimi stávame aj v tom digitálnom. Príkladmi európskych krajín, ktoré už poskytujú mnohé služby štátu online, sú Estónsko, Holandsko či Anglicko. Prináša to mnohé výhody, ako je nonstop dostupnosť služieb, ušetrený čas, ktorý by inak občania strávili čakaním na úradoch, ušetrené zdroje, ktoré by štát vynaložil na úradníkov, ale aj nižšia chybovosť a neúnavnosť automatizovaných systémov. Výhody fungovania a dostupnosti online služieb občania tiež mohli pocítiť napr. v čase šírenia koronavírusu.

Občania vďaka elektronizácii nemusia úradom opakovane poskytovať svoje údaje, nakoľko sú dostupné v centralizovaných systémoch štátu. Digitalizované služby úradov tiež zjednodušujú administratívne úkony, ako je prepis vozidla, zmena adresy pobytu či napríklad založenie firmy. Namiesto cestovania na úrad, čakania na časenku a odovzdávania papierov pri okienku tak občania môžu z domu vyplniť online formulár, podpísať ho vďaka čipu v občianskom preukaze a kliknutím ho zaslať úradníkom.

Centralizácia a automatizácia však majú aj tienistú stránku. Aj pri IT systémoch môžu nastať výpadky či obdobia, keď budú systémy preťažené, čo môže obmedzovať služby štátu. Ďalším rizikom je, že systémy nebudú dostatočne chránené a bezpečné pred útokmi zvonka, či môžu pre nesprávne nastavenia umožniť únik citlivých dát. Takým prípadom bol aj masový únik informácií 6,5 milióna izraelských voličov, ktoré boli dostupné online pre chybu v aplikácii vládnej strany.

Ak si občan založí firmu, mal by tiež myslieť na to, že pravdepodobne bude pracovať s dátami svojich zákazníkov a musí preto dodržiavať prísne pravidlá stanovené legislatívou (napr. GDPR). Tá určuje nielen spôsob, akým dáta majú byť zbierané, uchovávané a chránené, ale aj vysoké pokuty v prípade ich úniku či krádeže.

Čo (nie) je digitálny podpis?

Keď svetu vládli králi, kniežatá a monarchie, na svoju poštu dávali voskové pečate, do ktorých vytlačili svoj erb alebo iný charakteristický znak. Ak list dorazil k adresátovi s odstránenou alebo poškodenou pečaťou, bolo jasné, že list niekto „po ceste" otvoril a čítal ho, alebo dokonca zmenil jeho obsah.

Podobný mechanizmus funguje aj v digitálnom svete, kde sa správy, e-maily či citlivé dokumenty označujú tzv. digitálnym podpisom.

Pozor! Digitálny podpis neznamená, že si používateľ napíše alebo „nakreslí" svoje meno v digitálnej podobe v niektorom z grafických programov či napíše v textovom editore (napr. Word), alebo naskenuje svoj podpis napísaný rukou. Ak by si ho totiž iba nakreslil/napísal/naskenoval, útočník by ho dokázal ľahko napodobniť, a teda podpisovať za neho zmluvy, dokumenty či ukradnúť mu identitu.

Skutočný digitálny podpis je matematická schéma, ktorá dokáže potvrdiť pravosť dokumentov a správ. Digitálny podpis zároveň zaručí, že dáta (dokumenty, správy a pod.) pochádzajú od konkrétneho odosielateľa a neboli po ceste pozmenené (resp. je možné identifikovať, že ich niekto zmenil) podobne, ako to kedysi zaručovala vosková pečať.

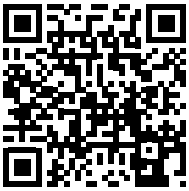
Digitálny podpis (jeho šifrovací mechanizmus) tvoria dve časti:

- **súkromný kľúč**, ktorý je tajný a pozná ho iba samotný používateľ,
- **verejný kľúč**, ktorý je verejne dostupný, no zároveň spárovaný so súkromným kľúčom používateľa.

Príklad: Alica chce digitálne a zároveň spoľahlivo a nezameniteľne podpísať svoju správu, čo dosiahne tým, že ju zašifruje svojím súkromným (tajným) kľúčom. Bob (alebo ktokoľvek iný) si chce prečítať správu, môže použiť Alicin verejný kľúč (ktorý je spárovaný s jej súkromným kľúčom) na dešifrovanie. Keďže súkromný kľúč pozná len Alica, nikto iný nedokázal dokument podpísať tak ako ona, takže Bob si môže byť istý, že správa pochádza od Alice a nebola cestou nikým iným pozmenená.

Tento princíp, samozrejme, funguje aj opačne. Ak by Bob zašifroval svoju správu Aliciným verejným kľúčom, tak si jej obsah dokáže otvoriť a prečítať jedine Alica. Tým je zaručené, že obsah správy poznajú len oni dvaja a že sa do ich komunikácie nikto po ceste nenabúral, a ani ju nepozmenil.

Táto matematická schéma úzko súvisí s takzvaným asymetrickým šifrovaním:



Vysvetľujúce video 1

Vysvetľujúce video 2

Budú občania v budúcnosti voliť online?

Jedna z oblastí, ktorá dodnes odoláva digitalizácii, sú voľby do politických funkcií. Aj keď sa na prvý pohľad môžu javiť ako jasný kandidát na presun do online sveta, prípadné výhody v podobe vyššej volebnej účasti či „ľahšieho" hlasovania majú hneď niekoľko závažných rizík, pre ktoré je papierová alternatíva zatiaľ bezpečnejšou možnosťou.

Fyzické voľby sú transparentné, no zároveň slobodné a tajné. Volič totiž musí navštíviť vybranú budovu v okolí svojho bydliska, tam vybrať alebo vyplniť papierový lístok za plentou a vhodiť ho do urny. Všetky kľúčové úkony pritom volič robí pod dohľadom volebnej komisie, no zároveň skryte za plentou, aby nikto nevidel, ktorú stranu či kandidáta si vybral. V prípade pochybností sa dajú hlasy prepočítať, čím sa overí správnosť výsledkov.

Elektronické voľby by museli zabezpečiť všetky tieto vlastnosti (slobodné, tajné, overiteľné), čo je zatiaľ nevyriešený problém. Napríklad je bez dohľadu volebnej komisie ťažké zaručiť, že voľba prebehla slobodne a tajne, bez nátlaku. Ak totiž volič dáva svoj hlas doma alebo niekde na verejnosti, môže ho niekto iný donútiť zmeniť svoje rozhodnutie.

Bez dohľadu volebnej komisie je tiež ťažko overiteľné, za akých podmienok a v akom stave človek hlasuje. Môže byť napríklad pod vplyvom psychoaktívnych látok. To mu síce nebráni hlasovať, registrácia u volebnej komisie v štandardných voľbách však môže pôsobiť ako psychologická bariéra podobného správania.

Online voľby cez počítače, mobily, tablety tiež negarantujú rovnaký prístup všetkým voličom. Nie každý volič totiž môže vlastniť zariadenie, ktoré má prístup na internet a umožňuje mu použiť volebné systémy.

Problémom môže byť aj dôvera v online volebný systém. Mnoho voličov totiž nerozumie digitálnym systémom a môže preto získať dojem, že ho ovplyvňujú „ítečkári", ktorí volebný systém vytvorili a majú ho na starosti.

Treba si tiež uvedomiť, že bezpečnosť elektronických volieb môžu ohrozovať aj digitálni útočníci. Záujem zmeniť výsledok volieb môžu mať zahraničné tajné služby, rôzni aktéri vo vnútri štátu (oligarchovia, mafia či iné skupiny), ale aj obyčajní kriminálnici. Tí sa môžu zamerať na slabiny hlasovacích zariadení/serverov, na ktorých sa zbierajú a sčítavajú hlasy, a snažiť sa ich buď znefunkčniť, alebo masovo manipulovať tak, aby výsledky boli v prospech vybraného kandidáta/strany. Pri papierových voľbách je tiež riziko ovplyvňovania volieb, no nie je centralizované. Môže byť ľahšie napadnúť fyzicky jeden volebný okrsok ako centrálny IT systém, avšak jedným útokom na centrálny systém dokáže útočník ovplyvniť všetky výsledky.

	Výhody	Nevýhody
Papierové voľby	• transparentnosť volebného úkonu • tajná voľba • slobodná voľba • jednoduché a zrozumiteľné pravidlá • overiteľnosť výsledku	• vysoké náklady • horšia dostupnosť pre voličov s dopravnými či zdravotnými obmedzeniami alebo voličov zo zahraničia • časovo a fyzicky náročné manuálne sčítavanie hlasov s nenulovou chybovosťou
Elektronické voľby	• (pravdepodobne) vyššia účasť voličov • nižšie náklady na organizáciu volieb • lepšia dostupnosť pre voličov • rýchle a bezchybné sčítanie hlasov	• dostupnosť vhodných zariadení a softvéru pre všetky spoločenské vrstvy • potenciálne zásahy do slobody a tajnosti voľby • možné kybernetické útoky na IT systémy • úmyselná manipulácia výsledkov volieb v IT systémoch

Elektronické voľby so všetkými výhodami aj nevýhodami už zaviedlo viacero krajín. Niektoré, ako napríklad India či Brazília, na hlasovanie využívajú špecializované hlasovacie zariadenia pripojené na internet, no stále vyžadujú osobnú prítomnosť voliča vo volebnej miestnosti. Odborníci vo viacerých prípadoch potvrdili, že tieto zariadenia majú zraniteľnosti a problémy so zabezpečením.

O krok ďalej sú v oblasti elektronických volieb Estónci, ktorí ako prví zaviedli hlasovanie na diaľku cez internet. Volič sa pritom musí preukázať svojím elektronickým občianskym preukazom a viacnásobne potvrdiť svoju identitu.

Záujem o elektronické voľby zvýšila aj globálna pandémia koronavírusu, najmä preto, že by umožnila konanie volieb aj napriek prísnym obmedzeniam osobného kontaktu. Federálnu administratívu Spojených štátov to viedlo k verejnému vyhláseniu, v ktorom voľby cez internet označila za vysoko rizikové a odporúča jednotlivým štátom vyhnúť sa tejto forme hlasovania, prípadne ju obmedziť len na občanov, ktorí nemajú inú možnosť, ako odovzdať svoj hlas.

Nie každý je online tým, kým sa zdá

Kľúčové slová:

online identita | overenie identity | falošné účty | falošné profily

Otázky, na ktoré odpovedá táto podkapitola:

Kto je kto na internete? Ako si online overiť cudziu identitu?

Praktické cvičenia k tejto podkapitole:

Animália

Kto je kto na internete?

„Na internete nikto nevie, že si pes." Tento známy komiks Petra Steinera, ktorý vyšiel v americkom týždenníku The New Yorker, veľmi dobre vystihuje jeden z problémov internetu – overovanie identity.

Ak sa totiž s niekým používateľ zoznámi online, často sa musí spoliehať iba na informácie, ktoré mu o sebe poskytne druhá strana sama na niektorom zo svojich profilov alebo pri priamej komunikácii. Overiť si jeho/jej identitu môže byť mimoriadne náročné, ak nie aj nemožné.

Ukážme si to na príklade: Na internete si ma do priateľov pridá Olivia123, ktorá tvrdí, že má 18 rokov, rada číta, jazdí na snouborde a zbožňuje filmy a seriály. V realite si tento profil vytvoril 30-ročný muž, ktorý nemá prácu, knihy takmer nečíta a väčšinu času trávi za počítačom.

V skutočnom svete by používateľ takéto klamstvo odhalil okamžite, no na internete je to komplikovanejšie. Navyše podvodník si môže ľahko vytvoriť nový profil s inou fotografiou z internetu a vymyslieť si ďalšie meno či záľuby. Tento postup môže, samozrejme, opakovať donekonečna. Falošné konto pritom môže používať aj na škodlivé či nelegálne účely.

Ako si online overiť cudziu identitu?

Ak sa niekto snaží s používateľom nadviazať kontakt, môže sa používateľ pokúsiť overiť identitu druhej strany viacerými spôsobmi.

V prvom rade môže použiť dostupné meno a údaje a vyhľadať si ich cez Google. Niektoré z výsledkov môžu poskytnúť informáciu, kde daná osoba býva, chodí do školy a či pracuje v oblasti/regióne, ktorý si uvádza v profile.

Ak Google ponúkne napríklad profily s vyhľadávaným menom na sociálnej sieti, mal by si používateľ pozrieť informácie, ktoré tam vyhľadávaná osoba poskytla. Už niektoré vonkajšie znaky konta pritom môžu byť signálom, že ide o falošný profil – napríklad má málo priateľov, žiadne fotografie, prípadne len selfies, kde nie sú žiadni ďalší ľudia.

Opatrnosť je na mieste aj v prípade, že na profile používateľ nájde obsah, ktorý vyzerá až príliš dobre na to, aby bol skutočný. Fotografie by používateľ mal skúmať podrobne ako vyšetrovateľ so zameraním na detaily v pozadí.

Užitočná pri overovaní je aj e-mailová adresa používateľa, na ktorú sa viažu profily na sociálnych sieťach ako TikTok, SnapChat, Instagram, Facebook, Twitter, Reddit a iné. Ak si podvodník nedá záležať na detailoch, môže na rôznych stránkach uvádzať odlišné či dokonca protichodné údaje.

Niektoré služby vám meno používateľa odhalia, až keď sa s ním stanete priateľmi alebo sa inak skontaktujete. Ak ste už odsúhlasili pridanie nového „priateľa“, podrobne si prejdite jeho/jej stránku. Všimnite si, kedy bola stránka vytvorená, či uvedené údaje súhlasia s tým, čo o sebe daný človek tvrdí a tiež, čo zdieľal v minulosti, aký jazyk používal a ako sa správal k iným používateľom.

Bezpečnosť prehliadača

Kľúčové slová:

cookies | dark web | deep web | história prehliadania | inkognito mód | povrchový web | bezpečné vyhľadávanie | surfovanie | útočník v prehliadači

Otázky, na ktoré odpovedá táto kapitola:

Ako môže používateľ zvýšiť bezpečnosť prehliadača? Čo je história prehliadania? Surfuje používateľ anonymne, keď používa inkognito mód? Ako rozoznať falošné či nebezpečné stránky? Čo má používateľ robiť, ak sa ocitol na nebezpečnom webe? Aké sú najčastejšie formy útoku cez prehliadač? Ktorú časť webu nájde používateľ pomocou vyhľadávača?

Praktické cvičenia k tejto kapitole:

Súboj sociálnych sietí, Nauč svoju babku používať Facebook, Ako vyzerá šifrovaná komunikácia, Inkognito mód, Phishingový útok

Ako môže používateľ zvýšiť bezpečnosť prehliadača?

Jedným z krokov, ktoré používateľ môže urobiť pre svoju bezpečnosť, je používať kvalitný a aktualizovaný prehliadač. Mal by tiež myslieť na to, že na zariadení môže mať nainštalovaných viacero prehliadačov a aktualizáciou by pred použitím mal prejsť každý z nich.

Viaceré populárne prehliadače majú zabudovanú možnosť „Safe Browsing", ktorá používateľa chráni pred phishingovými útokmi (snaha útočníkov ukradnúť prihlasovacie mená, heslá a iné citlivé údaje) a varuje ho v prípade, že sa snaží pripojiť na stránky, ktoré vyzerajú podozrivo alebo sú známe tým, že šíria škodlivý kód. Ak je to možné, používateľ by si mal funkciu Safe Browsing aktivovať v sekcii „Nastavenia".

Čo je história prehliadania?

Prehliadače majú po nainštalovaní automaticky zapnutú funkciu vytvárania histórie. Tá je užitočná najmä vtedy, ak sa chce používateľ vrátiť k niektorej stránke, ktorú v minulosti navštívil, no nevie si presne spomenúť na jej názov. Zároveň je to zdroj informácií o zvykoch používateľa, ktorý má hodnotu ako pre prevádzkovateľa prehliadača, digitálnych gigantov ako Facebook či Google a (v prípade, že sa dostanú do nesprávnych rúk) aj pre útočníkov.

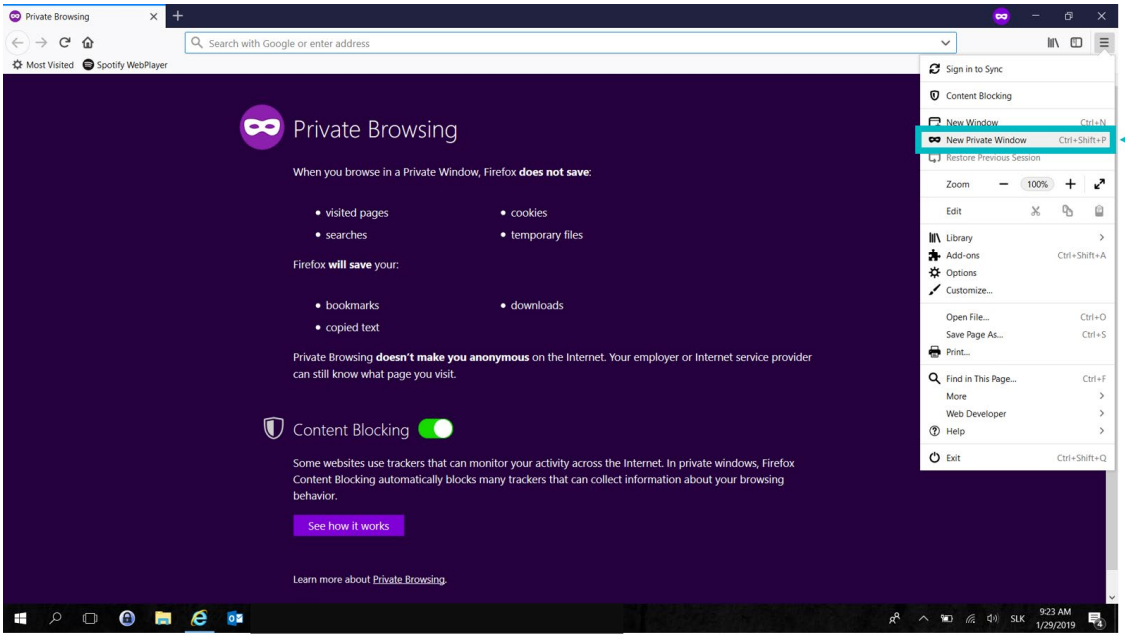
Znamená inkognito mód anonymné surfovanie?

Ak používateľ navštevuje stránky, ktoré obsahujú citlivé údaje (napríklad e-mail, sociálne siete či v dospelosti internetbanking), mal by používať tzv. „inkognito mód". Po jeho zapnutí sa do histórie prehliadania neukladajú a nezbierajú niektoré dáta o správaní používateľa online.

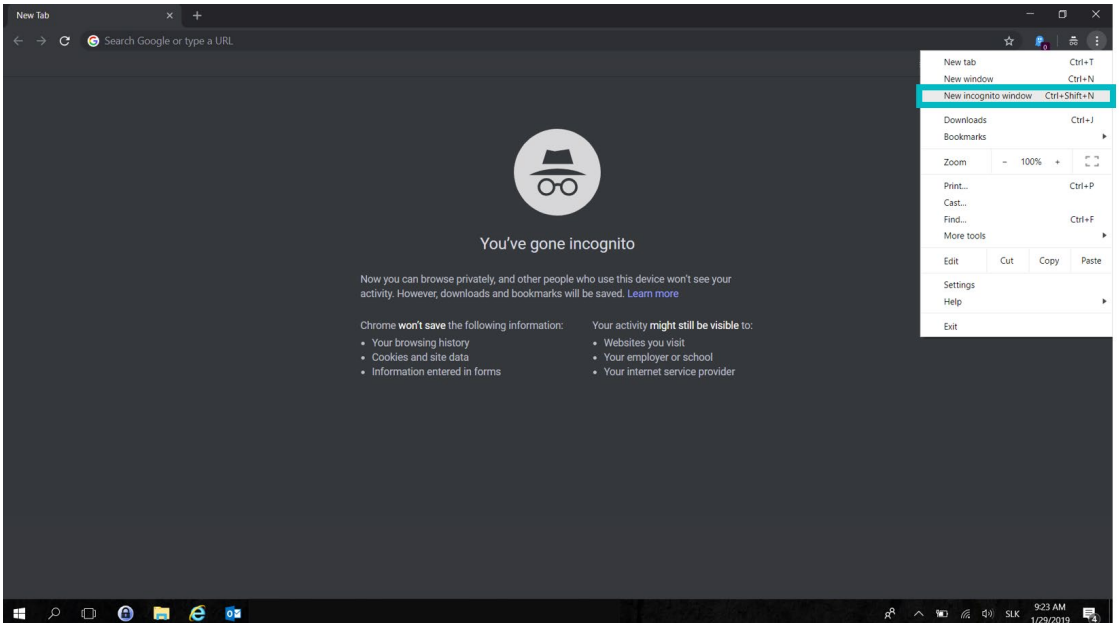
DÔLEŽITÁ POZNÁMKA:

Pozor! Inkognito mód neznamená anonymnú formu surfovania online. Ide len o čiastočné obmedzenie zberu informácií prehliadačom. Informácie o návštevách jednotlivých webov totiž môžu zbierať tvorcovia prehliadača či dodávateľ pripojenia na svojej strane a podľa toho identifikovať zvyky a preferencie používateľa a prispôsobovať im reklamy či obsah, ktorý sa mu/jej neskôr zobrazuje.

Pre zjednodušenie by sme mohli povedať, že inkognito mód skryje používateľom navštívené stránky pred kýmkoľvek, kto použije rovnaké zariadenie po ňom/nej. Údaje sú však stále digitálne zaznamenané a uložené na iných miestach, ako sú napríklad servery prehliadača či online služby (sociálne siete, vyhľadávače atď.), a sú potenciálne dostupné aj pre štátne orgány.



Otvoriť nové súkromné okno



Otvoriť nové inkognito okno

Ako rozoznať ne/bezpečný web?

- **https://**
  V prvom rade by si používateľ mal všímať, či je jeho komunikácia s daným webom zabezpečená šifrovaním. Môže to zistiť pri pohľade na URL adresu, ktorá by sa mala začínať s „https://“. Malé „s“ na konci znamená „secure“, teda zabezpečená verzia http protokolu, ktorú v riadku s adresou stránky potvrdzuje aj malý symbol zámku.

  Ak sa web začína len klasickým „http://“ a URL nezobrazuje zámok, ide o nešifrovanú a nezabezpečenú komunikáciu. Akékoľvek informácie, ktoré používateľ zadá na takejto stránke, odosiela zo zariadenia bez ochrany a umožňuje tak útočníkovi odchytávať ich a čítať.

  Pre pokročilejších: Po kliknutí na zelený zámok si používateľ môže pozrieť aj ďalšie informácie o stránke, ako je napríklad platnosť digitálneho certifikátu, jej vydavateľa či zoznam povolených a zablokovaných cookies.

  Cookies sú malé textové súbory, ktoré si webová stránka ukladá v používateľovom zariadení. Vďaka nim si dočasne uloží vybrané informácie o aktivite a preferenciách používateľa (napr. prihlasovacie meno, jazyk, veľkosť písma atď.) a pri najbližšej návšteve rovnakého používateľa ich automaticky opäť načíta.

- **Jazyk stránky**
  Mnoho gramatických chýb či preklepov na stránke je signálom – aj keď nie jednoznačným – že ide o podozrivý web. Útočníci totiž často obsah stránok len kopírujú a prekladajú zo zahraničných stránok za pomoci verejne dostupných prekladových služieb (napr. Google Translate), čím sa do textov dostávajú nezmysly.

- **Podozrivý obsah**
  Podozrivé je aj to, ak stránka požaduje priveľa citlivých informácií ešte predtým, než je jasné, za aké služby či tovar. Ak narazí používateľ na podobný prípad, je pravdepodobné, že ide o podvod. To platí aj v prípade, že sa autor webu snaží používateľa vystrašiť alebo inak dotlačiť k čo najrýchlejšej registrácii a odovzdaniu osobných údajov. Mladší používatelia (menej ako 13 alebo 16 rokov) by sa tiež pred registrovaním do novej služby mali poradiť s rodičmi, keďže regulácie (General Data Protection Regulation alebo GDPR) neumožňujú, aby odovzdali svoje údaje bez súhlasu rodiča.

Čo robiť, ak sa používateľ dostane na nebezpečnú webovú stránku?

Ak sa už používateľ nechtiac dostane na podozrivú stránku, nemal by klikať na žiadne prvky (tlačidlá, obrázky, linky) a stránku čo najskôr zavrieť. Pre vyššiu bezpečnosť si následne môže svoje zariadenie – počítač alebo androidové mobilné zariadenie – preskenovať spoľahlivým bezpečnostným softvérom, ktorý by mal detegovať, zneškodniť a odstrániť prípadné hrozby, ktoré si používateľ mohol pri návšteve webu stiahnuť.

Aké sú najčastejšie formy útoku cez prehliadač?

Najčastejšie sa používateľ vo svojom prehliadači stretne s pokusmi o phishing, sociálnym inžinierstvom alebo infekciou malvérom.

Sociálne inžinierstvo (v prípade útokov cez prehliadač) je snaha útočníka manipulovať obeť, aby sa dostala na nebezpečnú či falošnú stránku, kde z nej môže útočník vylákať citlivé údaje, vystrašiť ju či prinútiť ju, aby si nainštalovala nechcenú/nebezpečnú aplikáciu alebo iný škodlivý softvér.

Phishing používajú útočníci na zber citlivých údajov, pričom sa vydávajú za dôveryhodnú stránku alebo organizáciu. Útočníkov e-mail (správa) alebo web sa tak môže nápadne podobať napríklad na správy/stránky sociálnej siete, e-mailovej služby alebo internetbankingu, prípadne sa vydávať za e-shop. Príklady a testy, na ktorých si môžu žiaci vyskúšať, či rozoznajú škodlivú stránku od čistej stránky, nájdete v Aktivitách.

Cez prehliadač si môže používateľ stiahnuť aj malvér – v doslovnom preklade do slovenčiny škodlivý kód. Ten sa môže online šíriť rôznymi spôsobmi, ktorým sa podrobnejšie venujeme v jednej z nasledujúcich kapitol. V prípade, že dôjde k infekcii cez prehliadač, najčastejšie sa tak stane cez:

1. **Škodlivé rozšírenia prehliadača**, ktoré si používateľ nainštaluje buď po nátlaku útočníka, alebo z nevedomosti (aplikácia predstiera zaujímavú funkciu, prípadne ju ponúka zadarmo).

2. **Pri návšteve škodlivého webu**. Na infikovanú stránku sa používateľ dostane kliknutím na link v e-maili, dokumente, pri návšteve iného webu či po kliknutí na falošný reklamný baner. Používateľ sa pritom môže nainfikovať aj bez ďalšej aktivity, škodlivý kód sa totiž pri návšteve škodlivého webu sám stiahne a nainštaluje do zariadenia, prípadne ho oskenuje a stiahne doň iný škodlivý kód automaticky.

3. **Tzv. man-in-the-browser (útočník v prehliadači) útok,** pri ktorom je už zariadenie obete nainfikované škodlivým kódom, ktorý umožní útočníkovi prístup do zraniteľného prehliadača. Tam môže následne odchytávať údaje, ktoré používateľ zadáva na webovej stránke alebo ju upraviť, prípadne z nej vyberať citlivé údaje (číslo kreditky, dátum narodenia, prihlasovacie meno, heslo atď.) a posielať ich útočníkovi. Obeť nič netuší, nakoľko prehliadač aj stránky väčšinou reagujú normálne.

Povrchový web, deep web, dark web

Kľúčové slová:

dark web | deep web | povrchový web

Otázky, na ktoré odpovedá táto podkapitola:

Čo je to povrchový web, deep web a dark web? Sú hlbšie časti webu používané iba na nelegálne aktivity? Ako fungujú rôzne vrstvy webu?

Povrchový web

Tvoria ho verejne dostupné webové stránky, ktoré si používatelia dokážu vyhľadať napríklad cez internetové vyhľadávače ako Google, DuckDuckGo alebo Bing. Ide o najmenšiu časť webu, obrazne povedané vrchol ľadovca nad hladinou.

Deep web

Ide o časť internetu „skrytú pod povrchom", ak použijeme metaforu s ľadovcom, tak ide o časť, ktorá sa nachádza pod hladinou mora. Odhaduje sa, že tvorí 96 % celého online obsahu. Názov deep web nesie preto, že ide o stránky a obsah, ktoré nie sú dostupné náhodnému používateľovi. Na ich vyhľadanie či prístup k nim potrebuje používateľ špeciálny softvér, nástroje alebo prístupové práva. Veľká časť deep webu je legálna a legitímna. Patrí sem napríklad elektronická žiacka knižka, vzdelávací obsah určený pre konkrétnu triedu, ale aj platený obsah spravodajských webov, interné systémy firiem a verejných inštitúcií, do ktorých majú prístup len zamestnanci alebo jednotlivci.

Dark web

Je podmnožinou deep webu a časťou ľadovca, ktorá je najhlbšie pod hladinou. Nie je indexovaný (prehľadávaný cez vyhľadávače) a beží na dark nete, teda na infraštruktúre, ktorá poskytuje prevádzkovateľom dark webov a ich používateľom anonymitu. Na pripojenie k dark webu si používateľ potrebuje nainštalovať špeciálny softvér, ako je napríklad TOR alebo služba I2P (Invisible Internet Project).

Keďže dark web je skrytý a anonymný, chráni ľudí, ktorí sú vo svojej krajine či regióne prenasledovaní pre svoju prácu (napr. novinári), náboženské či politické presvedčenie a umožňuje im organizovať sa a bezpečne komunikovať s ďalšími podobne zmýšľajúcimi skupinami a jednotlivcami. Bohužiaľ túto anonymitu zneužívajú aj (kybernetickí) zločinci, napríklad na predaj škodlivého kódu, nelegálne obchody so zbraňami, drogami či službami.

Nelegálne sťahovanie

Kľúčové slová:

autorské práva | peer-to-peer služba | stream | streamovacia stránka | torrent

Otázky, na ktoré odpovedá táto podkapitola:

Čo sa považuje za nelegálne sťahovanie obsahu? Aké hrozby prináša nelegálne sťahovanie obsahu?

Čo sa považuje za nelegálne sťahovanie obsahu?

Ako sme si už spomenuli v kapitole o digitálnej identite, používateľ na internete aktívne a pasívne zanecháva stopy, ktoré opisujú, čo robil. To sa týka aj stiahnutých súborov či pozretých videí, pričom používatelia v súčasnosti veľmi často sťahujú či sledujú nelegálne kópie seriálov či filmov. Najčastejšie na ne môžu používatelia naraziť na streamovacích stránkach[11] plných reklám, stiahnu si ich z bezplatných úložísk alebo ich zdieľajú s inými ľuďmi cez tzv. peer-to-peer služby.

Väčšina z týchto aktivít pritom porušuje autorské práva tvorcov daného diela a tým aj zákony mnohých krajín sveta. Zároveň sa pri sťahovaní či sledovaní používateľ môže vystaviť digitálnym rizikám, ako je útok škodlivého kódu či poškodenie alebo strata osobných dát.

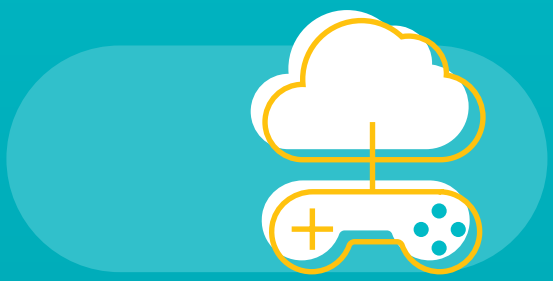
Aké hrozby prináša nelegálne sťahovanie obsahu?

1. Pri sťahovaní filmov/seriálov z úložísk či pri zdieľaní s veľkou skupinou neznámych ľudí (peer-to-peer služby známe tiež ako torrenty) si používateľ môže veľmi ľahko stiahnuť aj niečo, čo pôvodne nechcel. Stačí, keď súbor má názov ako niektorý z populárnych televíznych programov, seriálov, filmov či hier, no namiesto nich obsahuje len škodlivý kód.

2. Nainfikovať sa škodlivým kódom alebo skončiť na nebezpečnej stránke môže používateľ aj pri sledovaní seriálov a filmov na bezplatných streamovacích službách. Tie sú totiž známe obrovským počtom reklám, z ktorých niektoré môžu viesť k škodlivému webu či kódu. Na stiahnutie do zariadenia používateľa pritom stačí jediný nesprávny klik.

3. Sťahovanie nelegálneho obsahu má aj právne riziká, teda ak používateľa úrady prichytia s pirátskou kópiou, môže byť potrestaný. Trest sa líši od krajiny ku krajine, ale v niektorých prípadoch ide o mimoriadne vysoké pokuty a niekde dokonca aj roky vo väzení.

11 Pozor, nemýliť si s platenými streamovacími službami, ako je Netflix či HBO GO.



Online hry

Kľúčové slová:

falošná aplikácia | herný klient | netiketa

Otázky, na ktoré odpovedá táto kapitola:

Aké sú základy digitálnej bezpečnosti pri hraní online hier? Čo majú spoločné hry pre viacerých hráčov a sociálne siete? Potrebuje používateľ pri hraní hier antivírus? Ako spoznať falošné hry? Prečo sa im vyhnúť? Čo by mal používateľ robiť, ak narazí na nevhodné správanie v (online) hre pre viacerých hráčov? Čo by mal používateľ urobiť pred predajom hernej konzoly/počítača či iného zariadenia?

Aké sú základy digitálnej bezpečnosti pri hraní online hier?

Hráč/používateľ by pri hraní hier mal dodržiavať pravidlá kybernetickej bezpečnosti. Na hru by preto mal používať len **overené a zabezpečené zariadenia**, ako je napríklad domáci počítač či vlastný telefón. Zariadenie by malo byť pripojené na dôveryhodnú sieť (najlepšie domácu) a používať aktualizovaný a výrobcom podporovaný[12] operačný systém a aplikácie. Zariadenie by malo tiež používať spoľahlivé a aktualizované bezpečnostné riešenie (antivírus).

Ak hráč používa na spúšťanie hier herných klientov, mal by dbať na ich dobré zabezpečenie pomocou silného hesla, a ak je to možné, tak aj používať dvojfaktorovú autentifikáciu[13]. Herný klient je program, v ktorom sa hry dajú kúpiť, nainštalovať, spúšťať. Poskytuje priestor aj na hru viacerých hráčov a ich komunikáciu. Populárnymi príkladmi takýchto služieb sú Steam či Origin. Herný klient tiež obsahuje platobné informácie (napr. kreditnú kartu, ktorou hráč platí za nové hry), ktoré sú cennou korisťou pre útočníka. Podobné pravidlá platia aj pre zabezpečenie hernej konzoly (napr. Xbox, Nintendo alebo PlayStation).

Čo majú spoločné hry pre viacerých hráčov a sociálne siete?

Vďaka rýchlemu internetovému pripojeniu a rozmachu hier pre viacerých hráčov sa z herných svetov stali v podstate sociálne siete. V nich si hráči namiesto profilu so svojimi fotografiami vytvárajú fiktívne postavy, ktoré plnia rôzne úlohy či zbierajú predmety.

Ak to robia v režime viacerých hráčov (multiplayer), tak sa pri plnení úloh môžu spájať s ďalšími používateľmi, ktorých v skutočnom živote nepoznajú a nikdy ich nestretli. V takých prípadoch by najmä mladší hráči mali byť rovnako opatrní ako pri sociálnych sieťach a dodržiavať tie isté pravidlá bezpečnosti. Vyhnúť by sa preto mali zdieľaniu citlivých údajov vo svojom hráčskom profile či pripodobňovaniu hernej postavy k ich skutočnému ja. Rovnako by sa hráči mali vyhýbať kontaktu s ľuďmi, ktorí ich oslovujú v rámci hry a snažia sa o osobné stretnutie alebo od nich žiadajú osobné údaje.

Potrebuje používateľ pri hraní hier antivírus?

Hráčom vždy odporúčame mať pri hraní spustený bezpečnostný softvér, ktorý ich dokáže chrániť pred škodlivým obsahom. Ten sa k nim môže dostať aj priamo v hre. Príkladom môžu byť škodlivé odkazy, ktoré hráčom – vedome alebo nevedome – zašle niekto zo spoluhráčov.

Útočníci tiež často predstierajú, že zaslaný odkaz navedie hráča k bonusovému predmetu či inej výhode v rámci hry (napr. k novému rozšíreniu). Často sa však len snažia obeť donútiť, aby si otvorila stránku, ktorá ju zmanipuluje, aby si vypla ochranné prvky (ako je aj antivírus) a následne infikuje jej zariadenie škodlivým kódom.

12 Výrobca udržiava danú verziu systému/programu a vydáva preň záplaty a aktualizácie.
13 Detailnejšie sa tejto forme zabezpečenia venujeme v kapitole Heslá.

Ako spoznať falošné hry? Prečo sa im vyhnúť?

Hráči by si hry mali vždy kupovať z oficiálnych a overených obchodov. Dôvodom je, že útočníci radi zneužívajú popularitu hier, aby zasiahli čo najviac obetí. Často využívajú niektorú z nasledujúcich techník:

1. **Vytvorenie falošnej verzie hry**, ktorá napodobňuje populárne tituly, ako sú Minecraft či Fortnite, no má namiesto nich škodlivý obsah. Spoľahlivý antivírus dokáže takéto riziko odhaliť. S podobnými falošnými aplikáciami sa pritom používatelia/hráči môžu stretnúť aj v niektorých oficiálnych obchodoch (napr. Google Play). Všimnúť si ich môžu aj vďaka hodnoteniam predchádzajúcich používateľov. Tí si pravdepodobne hru nainštalovali a odhalili, že je škodlivá, na čo upozorňujú vo svojich komentároch.
2. **Infikovaním skutočnej hry škodlivým kódom**, ktorým ju zmenia na tzv. „trójskeho koňa". Takéto hry sa najčastejšie vyskytujú v neoficiálnych obchodoch či online fórach, odkiaľ si ich hráči môžu stiahnuť „zadarmo". Cenou za takúto hru je infekcia, ktorá môže mať ďalekosiahle následky, najmä ak ukradne dáta alebo poškodí zariadenie obete.

Čo by mal používateľ robiť, ak narazí na nevhodné správanie v (online) hre pre viacerých hráčov?

Podobne ako v akejkoľvek komunite, tak aj medzi hráčmi sa človek môže stretnúť s rôznymi prejavmi skupinového správania. Hra umožňuje priechod rôznych emócií pod vplyvom adrenalínu a plného hráčskeho nasadenia. Hráč sa tak môže stretnúť s agresívnymi komentármi, nadávkami, osočovaním a pod. Aj v ňom/nej pritom môžu vrieť emócie a tiež ich možno vyjadrí v hernom čete. Ak dá emociám voľný priebeh jednorazovo, je to v poriadku, hráč však nemusí strpieť pravidelné osočovanie.

- Používateľ najlepšie urobí, ak na jednorazový prejav agresie nereaguje a berie ho „s rezervou" a nenechá sa vťahovať do nekorektnej komunikácie.
- Ak sa nevhodné správanie v skupine opakuje, je namieste zvážiť, či v hre pokračovať, či nie je lepšie vybrať si inú skupinu hráčov.
- Aj v hráčskom prostredí, tak ako v akýchkoľvek skupinách, sa totiž môže diať šikanovanie alebo nenávistné prejavy, a nie je vhodné sa tomu vystavovať. Taktiež môže ísť o používateľa, ktorý je agresorom a hráčske prostredie len využíva na to, aby mohol niekomu ubližovať.
- Mnohé hry – podobne ako sociálne siete – umožňujú hráčom nahlásiť nevhodné správanie či problematických spoluhráčov a podvodníkov. Zodpovedné nahlásenie zlepšuje bezpečnosť nielen pre hráča, ktorý problém nahlásil, ale aj pre všetkých ostatných v hre.
- Ak sa v hre alebo hráčskej komunite dejú veci, ktoré používateľa znepokojujú, je dobre, aby to povedal niekomu, komu dôveruje.
- Rovnaký meter platí na všetkých hráčov, a preto je dobré, keď používateľ nezabúda, že aj jeho správanie a komentáre môže niekomu padnúť zle. „Netiketa" platí aj pri hraní.

Čo by mal používateľ urobiť pred predajom hernej konzoly/počítača či iného zariadenia?

Ak sa hráč rozhodne predať alebo vymeniť svoju hernú konzolu, počítač alebo iné (mobilné) zariadenie, mal by z nej predtým vymazať nielen všetky svoje údaje a hry, ale ideálne ju vrátiť späť do výrobných nastavení. Táto možnosť je obvykle dostupná v nastaveniach hernej konzoly alebo v nastaveniach operačného systému počítača. Dôvodom je, že sa tak odstráni nielen uložený obsah, ale aj prepojenia na rôzne online kontá a služby, ktoré by inak používateľ dal spolu so zariadením do rúk kupujúcemu.

Malvér a iné škodlivé aktivity

Kľúčové slová:

advér (adware) | backdoor | botnet | bankový malvér | červ | coinminer | cryptominer | Distributed Denial of Service (DDoS) útok | downloader | dropper | exploit kit | hybridná vojna | keylogger | kryptomena | kryptopeňaženka | kybernetická zbraň | kyberšpionážny malvér (malware) | panel nástrojov (toolbar) | password stealer | phishing | potenciálne nechcené aplikácie (potentially unwanted applications, PUA) | ransomvér | scam | skimming | sociálne inžinierstvo | spam | spyvér | trójsky kôň | vírus | vyspelá pokročilá hrozba (advanced persistent threat, APT) | zero-day zraniteľnosť

Otázky, na ktoré odpovedá táto kapitola:

Čo je malvér? Čo všetko dokáže malvér? Aké kategórie a druhy malvéru poznáme? Čo motivuje útočníkov k škodlivej činnosti? Ako vyzerajú potenciálne nechcené aplikácie tzv. PUA/PUP? Ako vyzerajú útoky bežného malvéru? Čo dokáže vyspelý malvér určený na cielené útoky (APT)? Prečo sa už nehovorí o počítačových vírusoch a červoch? Čo okrem škodlivého kódu útočníci ešte používajú? Aké ďalšie formy útokov poznáme?

Praktické cvičenia k tejto kapitole:

Posielanie falošných e-mailov z dôveryhodnej adresy, Rozpoznávanie phishingu a spamu, Phishingový útok, Inkognito mód

Čo je malvér?

Toto slovo pochádza z anglického slova malware, ktoré sa skladá z malicious (škodlivý) a software (softvér). V doslovnom preklade ide o škodlivý softvér alebo škodlivý kód. Ide o presnejší názov na označenie (počítačového) vírusu, ktorý je len jedným z možných typov malvéru.

Čo všetko dokáže malvér?

Malvér môžeme rozdeliť do rôznych kategórií. Ak by sme ich zaradili do skupín podľa rizika, ktoré predstavujú, išlo by o:

1. **Potenciálne nechcené aplikácie (označované tiež ako PUA)**
   Tieto aplikácie sa radia do šedej zóny a majú len niektoré nevhodné vlastnosti. Nie sú totiž priamo škodlivé pre používateľa, no často ho otravujú, zavádzajú, zbytočne zaťažujú jeho zariadenie a môžu byť prvým krokom k skutočne škodlivým kódom či miestam na internete. Používateľ si takéto aplikácie často nainštaluje ako súčasť „balíčka" s iným softvérom alebo sa s ich aktivitou stretne na podozrivých weboch.

2. **Malvér**
   Malvér zahŕňa škodlivý kód, ktorého jasným cieľom je poškodiť používateľa. Môže napríklad kradnúť dáta, prístupové údaje alebo sledovať používateľa a jeho aktivitu online, prípadne vydierať či kradnúť peniaze. Cieľom väčšiny malvéru je zarobiť peniaze útočníkom, ktorí ho šíria a riadia. Malvér obsahuje mnoho podkategórií ako ransomvér, spyvér, trójske kone, downloader, keylogger, backdoor, advér (adware) a mnohé ďalšie.

3. **Vyspelý malvér určený na cielené útoky (skrátene APT[14])**
   V angličtine sa pre túto kategóriu používa pojem pokročilá vyspelá hrozba alebo advanced persistent threat (APT). Ako už názov naznačuje, ide o mimoriadne prepracované typy škodlivého kódu vytvorené skúsenými útočníkmi, ktorí do ich tvorby investovali veľa času, energie a peňazí. Väčšinou sa zameriavajú na citlivé oblasti, ako sú dodávky elektriny, vládne alebo medzinárodné inštitúcie či dopravné systémy. Môže spôsobiť vážne škody a ohroziť ľudské životy. Viaceré z nich sa označujú aj ako kybernetické zbrane či kyberšpionážne nástroje. Bežný človek sa s útokmi APT pravdepodobne nestretne, môže však pocítiť ich dôsledky v prípade, že obmedzia dodávky elektriny či znefunkčnia niektorý zo štátnych úradov.

Čo motivuje útočníkov k škodlivej činnosti?

Motivácie dnešných kyberzločincov sa pritom výrazne líšia od ich predchodcov v 80. a 90. rokoch, keď sa objavili prvé kybernetické útoky. V minulosti bolo ich hlavným cieľom ukázať svetu svoje vlastné schopnosti, prípadne vybudovať si imidž v rámci „hackerskej" komunity.

Hlavnou motiváciou dnešných útočníkov sú peniaze. Škodlivý kód sa vyrába tak, aby mal čo najširšie použitie, dal sa predávať a opakovane používať rôznymi útočníkmi výmenou za nemalé sumy. Predaj vopred vytvoreného malvéru ako služby zjednodušuje prístup k škodlivému kódu aj pre neskúsených zločincov, ktorí nedokážu malvér sami napísať, no dokážu ho účinne šíriť a využívať vo svoj prospech.

14 Advanced Persistent Threat, teda pokročilá pretrvávajúca hrozba.

Existuje aj úzka skupina mimoriadne vyspelých útočníkov (APT), ktorí vytvárajú škodlivý kód s cieľom poškodiť vybraný cieľ. Zisk v ich prípade nie je dôležitý, keďže peniaze im poskytuje zadávateľ úlohy – s najväčšou pravdepodobnosťou štát, ktorý na to má financie a dôvod napríklad v rámci hybridnej vojny. Keďže dôsledky tejto aktivity majú presah aj do skutočného sveta a dokážu poškodiť napríklad priemyselné zariadenia či životne dôležité systémy, hovoríme o kybernetických zbraniach.

Ako vyzerajú potenciálne nechcené aplikácie tzv. PUA[15]?

Najčastejšie sa používateľ dnes stretne s tzv. **coinminermi** (alebo cryptominermi), ktorých úlohou je využívať počítač obete na ťažbu kryptomien, ako je Bitcoin či Monero. Existujú pritom nechcené programy, ktoré sa za týmto cieľom nainštalujú do zariadenia, niektoré tú istú činnosť dokážu robiť aj priamo v prehliadači, keď si obeť otvorí stránku s takýmto kódom[16]. Do menej nebezpečnej kategórie PUA sa radí najmä preto, že používateľovi stačí zavrieť okno prehliadača, prípadne celý prehliadač, aby jeho aktivitu ukončil.

V minulosti boli rozšírené aj **tzv. lišty nástrojov (toolbar)**, ktoré si obeť vedome alebo nevedome nainštalovala do svojho prehliadača. Tieto lišty však väčšinou neslúžili svojmu účelu a používateľovi spomaľovali prehliadač a komplikovali prácu v programe.

Medzi PUA sa radia aj rôzne **aplikácie a rozšírenia prehliadača**, ktoré sľubujú, že po nainštalovaní odstránia chyby a nadbytočnú záťaž či dokonca „poupratujú" zariadenie a zvýšia jeho výkon. V drvivej väčšine prípadov ide o fiktívne sľuby bez skutočných výsledkov. Ich cieľom je najčastejšie zobrazovanie reklamy alebo zber dát o správaní používateľa.

Ako vyzerajú útoky bežného malvéru?

Malvér môže mať rôzne podoby. Do tejto skupiny sa radia vírusy, červy, ale aj trójske kone, či ďalšie typy škodlivého kódu. Nižšie si povieme viac o niektorých skupinách malvéru, s ktorými sa dnešný používateľ stretne asi najčastejšie:

- **Trójsky kôň (alebo Trojan)**
  Funguje na podobnom princípe ako pôvodný trójsky kôň. Navonok predstiera legitímnu funkciu (napríklad prehrávač videa, četovacia aplikácia) alebo sa vydáva za neškodný súbor (dokument, aktualizácia), no v skutočnosti má za cieľ škodiť. Niektoré trójske kone pritom naozaj poskytujú používateľovi časť sľúbených funkcií či služieb, no ich hlavným cieľom je najmä zbierať dáta, škodiť, okradnúť a pod.
- **Ransomvér**
  Po infekcii buď zablokuje obrazovku zariadenia, alebo zašifruje jeho dáta. Za odblokovanie/odšifrovanie od obete následne žiada výkupné. Najznámejšie príklady boli WannaCry (2017) alebo CryptoLocker (2013). Ransomvér (Not)Petya (2017) bol aj súčasťou najničivejšieho kyberútoku v histórii, ktorý napáchal škody za minimálne 10 miliárd dolárov.

15 Potentially unwanted applications

16 Pozor! Niektorí používatelia sa môžu do ťažby kryptomien zapájať vedome a úmyselne si do zariadenia alebo na svoje webové stránky nainštalovať podobný kód s cieľom zarobiť peniaze.

- **Spyvér**
  Škodlivý kód, ktorý špehuje infikované zariadenie obete. Cieľom je zozbierať čo najviac informácií o jej správaní, ale tiež hesiel, prístupových kódov či iných citlivých dát, ktoré sa následne odosielajú na server útočníkov. Tí zozbierané údaje speňažia prostredníctvom „dark webu“[17] alebo využijú na ďalšiu škodlivú činnosť. Touto cestou sa citlivé dáta používateľa môžu dostať do rúk zločincov, ktorí ich dokážu zneužiť na poškodenie obetí, napríklad ďalšou krádežou dát, peňazí či krádež ich identity.

- **Bankový malvér**
  Zameriava sa výhradne na krádež finančných informácií obete, ako sú čísla kreditných kariet, prístupy do bankových účtov, kryptopeňaženiek či iných služieb spojených s peniazmi alebo kryptomenami.

- **Downloader/Dropper**
  Tento škodlivý kód sa po inštalácii pripojí na vybranú webovú stránku či server a stiahne do zariadenia obete ďalší škodlivý kód podľa výberu útočníka.

- **Password Stealer**
  Password stealer je typovo veľmi podobný spyvéru a bankovému malvéru, no zameriava sa na súbory či programy, ktoré by mohli obsahovať heslá. Mnohé sa napríklad snažia kradnúť heslá uložené v prehliadačoch či zraniteľných manažéroch hesiel.

- **Keylogger**
  Tento kód sleduje naozaj každý krok používateľa alebo presnejšie každé jeho „ťuknutie“ do klávesnice alebo pohyb myši. Týmto spôsobom dokáže detailne zachytávať (mapovať) činnosť obete a môže ukradnúť aj dáta, ktoré obeť nemá nikde uložené a len ich príležitostne zadáva do niektorej služby či programu.

- **Backdoor**
  Aj tento názov je veľmi výstižný. Backdoor predstavuje „zadné vrátka“, ktoré útočník dokáže zneužiť na prístup do systému obete, jej sledovanie či inštalovanie ďalšieho malvéru. Backdoor je často základným nástrojom a východiskom vyspelých útočníkov (APT), o ktorých podrobnejšie píšeme nižšie.

- **Advér (adware)**
  Ak je zariadenie infikované advérom, zobrazuje sa mu neprimerané množstvo reklám a to aj v čase, keď by to neočakával – napríklad keď má vypnutý prehliadač. Ak sa vám advér nezdá príliš nebezpečný, môžete sa mýliť. Okrem toho, že obťažuje používateľa, používa aj niektoré agresívne techniky, ktoré sú charakteristické pre malvér. Môže tak bez vedomia obete napríklad manipulovať nastavenia zariadenia či inštalovať alebo odinštalovať ďalší softvér. Práve tieto kroky pritom môžu znamenať riziko ďalšej, oveľa vážnejšej infekcie.

Samozrejme, funkcie škodlivého kódu môžu byť rôzne a môžu sa zameriavať napríklad aj na sieťovú komunikáciu, zbierať citlivé dáta z pamäte zariadenia, či dokonca útočiť ešte predtým, než sa vôbec naštartuje operačný systém. Výnimkou nie sú ani rôzne kombinácie už uvedených funkcií alebo malvér, ktorý má viacero úrovní či modulov s podobnou funkciou (downloader + ransomvér, downloader + bankový malvér + keylogger atď.)

17 Bližšie sa tejto téme venujeme v časti Povrchový web, deep web, dark web na str. 68.

Čo dokáže vyspelý malvér určený na cielené útoky (APT[18])?

Zločinci, ktorí stoja za týmto malvérom, sú vo väčšine prípadov mimoriadne skúsení vývojári, ktorí majú za sebou roky práce so škodlivým kódom. Ich „produkty" sú väčšinou modulárne – teda skladajú sa z viacerých častí, ktoré sa dajú ľahko pridať alebo ubrať – využívajú verejne neznáme zraniteľnosti v softvéri či veľmi prepracované manipulačné techniky, aby sa dostali do systémov obete. Je pravdepodobné, že na vývoj malvéru majú dostatok času a peňazí, takže zisk nie je ich hlavnou motiváciou a zameriavajú sa skôr na špionáž či výsledný ničivý efekt svojej práce.

Príkladom cieleného útoku bol útok na firmy, ktoré distribuujú elektrinu na Ukrajine, pri ktorom útočníci cielili na priemyselné „vypínače" a počítače, ktoré ich ovládajú. Celkovo išlo len o niekoľko desiatok zariadení. Dostali sa k nim cez infikované prílohy mailov, na ktoré klikli zamestnanci distribučnej firmy a otvorili tým dvere nebezpečnému malvéru BlackEnergy a neskôr Industroyer. Obom sa nakoniec podarilo odpojiť bežných ľudí od elektriny na niekoľko hodín. Prepracovaný škodlivý kód bol aj zdrojom zatiaľ najničivejšieho útoku v histórii známeho ako Petya or NotPetya. Ten odstavil viaceré globálne firmy a spôsobil škody za vyše 10 miliárd USD, a to napriek tomu, že jeho pôvodným cieľom boli len ukrajinské spoločnosti.

Prečo sa už nehovorí o vírusoch a červoch?

Obe tieto kategórie škodlivého kódu boli rozšírené v minulosti – presnejšie v 80. a 90. rokoch. Dnes je škála malvéru oveľa širšia a vírusy ani červy nepatria k najdominantnejším typom, najmä ak sa porovnajú s PUA, trójskymi koňmi, advérom či ransomvérom.

- **Vírusy** fungovali podobne ako chrípka či iné vírusové ochorenie. Potrebovali hostiteľa, teda zraniteľné programy a aplikácie, ktoré mohli nainfikovať, a prostredníctvom ktorých sa ďalej šírili.
- **Červy** na šírenie nepotrebovali ďalší program ako vírusy. Dokázali sa replikovať (množiť) samotné a šíriť sa prostredníctvom siete, e-mailov, četových aplikácií či prenosných médií (napr. USB kľúčov). Takéto správanie sa objavuje aj v súčasnosti v spojitosti s trójskymi koňmi, tie však na tento účel využívajú rôzne – často aj legitímne – nástroje či aplikácie.

Čo okrem škodlivého kódu útočníci ešte používajú?

Na to, aby útočník mohol niečo získať, potrebuje, aby obeť aspoň čiastočne spolupracovala. Keby totiž vytvoril sledovací škodlivý kód, ktorý nemá prístup k disku s dokumentmi, fotoaparátu, mikrofónu či iným častiam systému, veľa by nezískal.

Útočníci preto často používajú tzv. **sociálne inžinierstvo**, teda prepracované techniky, ktorými manipulujú používateľa, aby im nevedome dal súhlas na zásahy do zariadenia. Viac o tejto forme útoku nájdete nižšie.

Vyspelejší útočníci majú aj ďalšie nástroje, ako sa môžu dostať do zariadenia. Niektorí hľadajú a využívajú doposiaľ neznáme **zero-day zraniteľnosti** v softvéri[19], prípadne majú špecializované nástroje na ich hľadanie (tzv. **exploit kity**). V iných prípadoch si zase útočníci vytipujú legitímny softvér, ktorý „nakazia" (niektorú z jeho verzií) škodlivým kódom. Pôvodní tvorcovia legitímneho softvéru o tom však nevedia a používateľ, ktorý si infikovanú verziu nainštaluje, sa nevedome nainfikuje škodlivým kódom.

18 Advanced Persistent Threat, teda pokročilá pretrvávajúca hrozba.

19 Zero-day zraniteľnosť je zraniteľnosť, o ktorej tvorca softvéru nevie a útočník ju zneužíva bez toho, aby o nej niekto vedel. Najčastejšie sa útočníci sústredia na známe a zdokumentované zraniteľnosti, ktoré už boli zverejnené online, nakoľko ide o lacnejšiu a ľahšiu alternatívu.

Ktoré ďalšie formy útokov poznáme?

Kybernetické útoky majú rôzne podoby a škodlivý kód nemusí byť jediným alebo výsledným nástrojom, ktorý útočníci využívajú. Ďalšími príkladmi sú:

- **Botnet** je sieť infikovaných zariadení („botov"), ktorú na diaľku ovláda útočník prostredníctvom servera alebo príkazmi, ktoré si zariadenia odovzdávajú medzi sebou. Botnet môže šíriť spam alebo škodlivý kód, slúžiť ako krytie pre útočníka, dá sa používať na DDoS útoky (definícia nižšie). Existujúci botnet môže útočník dokonca aj prenajímať prostredníctvom dark webu ďalším útočníkom na iné účely. Botnet môžu tvoriť aj milióny zariadení, aktuálne sa útočníci sústredia najmä na internet vecí (smart zariadenia alebo IoT), ktorý je známy horším zabezpečením.
- **Distributed Denial of Service (DDoS)** útok má za cieľ znefunkčniť stránku alebo online službu, pričom na to využíva sieťovú prevádzku (traffic) vytvorenú botnetom. Veľká sieť infikovaných zariadení totiž dokáže robiť obrovské množstvo prístupov na určenú stránku, čím preťaží servery, na ktorých beží.
- **Exploit** je anglické slovo, ktorého význam („využiť niečo vo svoj prospech") sa v negatívnom zmysle preniesol aj do oblasti digitálnej bezpečnosti. Ide totiž o program, kus kódu alebo postup, ktorý útočníci vytvorili tak, aby zneužíval zraniteľnosti a chyby v softvéri alebo hardvéri obete s cieľom ich ovládnuť.
- **Phishing** je snaha útočníkov zbierať citlivé údaje a dáta o obeti, pričom útočníci sa vydávajú za dôveryhodnú organizáciu, službu alebo osobu. Zaslaný falošný odkaz používateľa zavedie na stránku, ktorá sa nápadne podobá napríklad na stránky sociálnej siete, e-mailovej služby, internetbankingu. Na phishingové linky môže používateľ často naraziť v spamových e-mailoch, šíria sa však aj cez čet, sociálne siete či SMS. Mnohé z nich dokáže odchytiť bezpečnostný softvér, stále však platí používateľské pravidlo dvakrát meraj a raz klikaj.
- **Sociálne inžinierstvo** je snaha útočníka zmanipulovať obeť, aby navštívila nebezpečnú či falošnú stránku, kde z nej môže útočník vylákať citlivé údaje. Ide tiež o techniky, ktoré sa snažia obeť vystrašiť či iným spôsobom prinútiť, aby vykonala aktivitu, ktorú požaduje útočník, napríklad si nainštalovala nechcenú/nebezpečnú aplikáciu alebo škodlivý softvér. Príkladmi takýchto postupov je phishing či scam.
- **Spam** je akákoľvek nevyžiadaná elektronická pošta, ktorá môže mať podobu e-mailu, SMS správy alebo správy v četovej aplikácii.
- **Scam** je typ sociálneho inžinierstva, v ktorom ide o snahu útočníka oklamať obeť alebo skupinu obetí a získať ich dôveru, ktorú následne môže útočník využiť vo svoj prospech. Tieto premyslené klamstvá najčastejšie zneužívajú ľudské vlastnosti, ako sú naivita, súcit, nezodpovednosť či chamtivosť. Príkladmi scamu sú falošné e-shopy s lacnými značkovými okuliarmi či súťaže, pri ktorých útočníci sľubujú napríklad nový iPhone zadarmo. Obete však nakoniec len pripravia o dáta alebo peniaze.
- **Skimming** patrí do kategórie útokov spojených s bankovníctvom. Skimmer je nenápadné hardvérové zariadenie, ktoré útočníci nainštalujú na bankomat, aby skenovalo údaje o vložených kartách. Tieto cenné údaje sa následne uložia na disk alebo odošlú útočníkovi, ktorý ich môže ďalej speňažiť alebo využiť na nákupy v mene obete. Podobné útoky sa pritom dejú aj v digitálnom prostredí, kde útočníci kusom škodlivého kódu nainfikujú platobnú bránu legitímneho e-shopu.

Bezpečnostné riešenie (antivírus)

Kľúčové slová:

antivírus | bezpečnostné riešenie | malvér | falošný antivírus | strojové učenie (machine learning)

Otázky, na ktoré odpovedá táto kapitola:

Čo robí antivírus? Prečo potrebuje používateľ antivírus? Čo si má používateľ všímať pri výbere antivírusu? Aký je rozdiel medzi plateným a neplateným antivírusom? Chránia dva antivírusy lepšie ako jeden? Prečo je pomenovanie antivírus nepresné a čo by ho malo nahradiť?

Čo robí antivírus?

Antivírus, alebo presnejšie bezpečnostné riešenie, je softvér, ktorý chráni používateľa pred hrozbami a rizikami v digitálnom prostredí. V prípade, že bezpečnostné riešenie narazí na škodlivý kód, správanie alebo aktivitu útočníkov, upozorní používateľa cez notifikáciu.

Prečo potrebujem antivírus?

Informácie majú v dnešnom svete obrovskú hodnotu. To si uvedomujú aj útočníci a zneužívajú preto mnohé technické aj psychologické nástroje, aby sa k nim dostali a mohli ich výhodne predať, prípadne využiť na vlastné obohatenie. Mnohí používatelia si myslia, že nemajú žiadne cenné informácie, no opak je často pravdou. Infikované zariadenie používateľa navyše môže byť cenným zdrojom alebo prostredníkom na ďalšie šírenie škodlivého kódu.

Technicky zdatnejší útočníci, ktorých cieľom je zarobiť na obeti alebo jej dátach, píšu vlastný škodlivý kód a neustále sa ho snažia vylepšovať, predávať a šíriť. Menej šikovní si už dnes škodlivý kód môžu aj kúpiť, prípadne sa sústredia na vytváranie rafinovaných klamstiev, cez ktoré obeť zmanipulujú a následne od nej vymámia citlivé informácie ako napríklad prístup k jej bankovému účtu.

Samozrejme, existuje aj pomerne veľká šedá zóna, v ktorej sa oba prístupy kombinujú. Viac informácií o tom, ako môže vyzerať škodlivý kód, si môžete prečítať v kapitole „Malvér".

Veľkej časti týchto hrozieb môže používateľ predísť používaním kvalitného a spoľahlivého bezpečnostného softvéru (bežne označovaného ako antivírus). Antivírus by mal hrozby odhaľovať použitím rôznych technológií a poskytovať viacero vrstiev ochrany. Hrozby sa totiž dajú detegovať na rôznych miestach, napríklad na sieťovej úrovni, pri vstupe do zariadenia, po spustení, ale aj v prípade, ak sa škodlivý kód vydáva za prílohu e-mailu.

Čo si všímať pri výbere antivírusu?

Dobrou praxou pri výbere antivírusu je sledovanie jeho výsledkov v nezávislých testoch. Príkladom organizácií, ktoré robia podobné testy, sú VirusBulletin, AV Comparatives alebo AV-Test.

V ich testoch si používateľ môže pozrieť rôzne vlastnosti bezpečnostného softvéru – napríklad akú záťaž pre zariadenie daný antivírus predstavuje, aké percento škodlivých kódov dokáže zachytiť a zablokovať či koľko falošných poplachov pri svojej činnosti vyvolá.

Kľúčovým pri výbere by mal byť aj fakt, že daný bezpečnostný softvér používa mix viacerých technológií, ktoré dokážu používateľa chrániť na viacerých úrovniach. Antivírusy, ktoré majú jednu dominantnú technológiu alebo sa zameriavajú len na jeden typ detekcie, môžu útočníci ľahšie obísť.

Môžeme to prirovnať k bezpečnostným prvkom auta. Vozidlo, ktoré má asistenčné systémy, dokáže vyrovnať šmyk, má bezpečnostné pásy a množstvo airbagov, je určite bezpečnejšie ako starší model, ktorý chráni posádku len jedným z týchto prvkov.

Dôležité je tiež sledovať, či bezpečnostný softvér, ktorý si používateľ vybral, požiada o súhlas so spracovaním dát, tak ako to vyžadujú zákony EÚ a jednotlivých štátov. Používateľ by mal byť ešte pred inštaláciou informovaný, aké dáta bude antivírus zbierať a na aký účel.

Aký je rozdiel medzi plateným a neplateným antivírusom?

Akýkoľvek overený bezpečnostný softvér je lepší ako žiadny. Vo všeobecnosti existujú dve hlavné kategórie antivírusov – platené a neplatené.

Neplatený antivírus poskytuje určitú úroveň ochrany, no firma, ktorá ho vytvára, si musí na svoju prevádzku zarobiť iným spôsobom. Môže tak robiť buď zberom a predajom dát o správaní svojich používateľov, predajom funkcií za príplatok priamo v aplikácii alebo zobrazovaním reklamy.

Platený antivírus používateľa stojí v priemere niekoľko desiatok eur ročne. Za túto sumu však môžu jeho tvorcovia pracovať na jeho prevádzke a na ďalšom rozvoji technológie, pričom používateľa nezaťažujú reklamou a stačí im na tieto účely zbierať len dáta o škodlivom kóde. Niektoré bezpečnostné programy pritom ponúkajú takzvané skúšobné lehoty, pričom si ich používateľ môže nainštalovať a používať ich niekoľko týždňov či mesiacov bezplatne.

Pozor na softvér, ktorý sa na antivírus iba chce podobať, no neposkytuje žiadnu ochranu – tzv. **falošný antivírus**. Ide o podvod, ktorý môže obeť stáť nemalé peniaze a navyše môže ohroziť aj jeho bezpečnosť. Pri výbere je tak kľúčové overiť si, či daný antivírus je spoľahlivý a overený.

Chránia ma dva antivírusy lepšie ako jeden?

Ak na zariadení bežia dva alebo viaceré bezpečnostné softvéry s podobným zameraním, zhorší sa nielen ich výkon a používateľská skúsenosť, ale tiež úroveň zabezpečenia. Dôvodom je, že bezpečnostné riešenia pri ochrane kontrolujú prichádzajúce a odchádzajúce dáta, sieťovú komunikáciu a pod., aby včas identifikovali a odstránili škodlivú aktivitu. Ak má tieto práva viacero antivírusov v jednom zariadení, prekážajú si navzájom, čím znižujú svoju efektivitu. Môže to tiež spôsobiť aj komplikácie používateľovi, ktorému sa podobné kolízie zobrazia v podobe množstva falošných poplachov.

Prečo je pomenovanie antivírus nepresné a čo by ho malo nahradiť?

Antivírus a bezpečnostné riešenie sa v súčasnosti často používajú ako synonymá. Z pohľadu výrobcov došlo k výrazným zmenám, ktoré pojem „antivírus“ napriek svojej popularite nedokáže obsiahnuť. Oveľa vhodnejším je preto výraz bezpečnostný softvér alebo bezpečnostné riešenie.

V prvom rade moderné bezpečnostné riešenia sa nezameriavajú len na ochranu pred vírusmi, ale aj pred obrovským množstvom iných škodlivých kódov a aktivít, ktoré neexistovali v čase prvých antivírusov. Na to, aby to dokázali, museli sa klasické antivírusy rozvíjať a pridávať nové technológie a vrstvy ochrany vrátane takých, ako je strojové učenie (machine learning) – teda schopnosť programu analyzovať dáta, hľadať v nich podobnosti či anomálie a učiť sa z predchádzajúcich skúseností. Okrem ochrany pred škodlivým kódom moderný bezpečnostný softvér má aj ďalšie prémiové funkcie a dokáže napríklad šifrovať dáta, bezpečne ukladať a spravovať heslá či pomôcť pri hľadaní strateného alebo ukradnutého zariadenia.

Bezpečnosť internetového pripojenia

Kľúčové slová:

hotspot | internetový prehliadač (browser) | internet vecí (Internet of Things, IoT) | smart domácnosť (smart home) | smart zariadenie | Virtual Private Network (VPN) | webkamera | Wi-Fi so zabezpečeným prístupom (WPA)

Otázky, na ktoré odpovedá táto podkapitola:

Ktoré druhy siete alebo sieťového pripojenia sú bezpečnejšie? Ako spoznať ne/bezpečnú sieť? Ako sa vyhnúť nebezpečnej sieti? Čo je to Virtual Private Network (VPN)? Čo je „internet vecí" (angl. Internet of Things alebo IoT)? Ako IoT súvisí s online bezpečnosťou používateľa? Potrebuje si používateľ zakrývať webkameru?

Praktické cvičenia k tejto podkapitole:

Posielanie falošných e-mailov z dôveryhodnej adresy

Ktoré druhy internetového pripojenia (siete) mávajú vyššiu bezpečnosť?

Najlepšie zabezpečené sú obvykle firemné siete, no postupne sa zlepšuje aj bezpečnosť domácich sietí. Najhoršie sú zabezpečené verejné Wi-Fi siete bez hesla, dostupné na námestiach, v kaviarňach, v dopravných prostriedkoch, hoteloch a na verejných priestranstvách.

Čím sa bezpečná sieť často líši od menej bezpečnej, je použitie lepšieho bezpečnostného protokolu (WPA2 alebo aktuálne ešte len pripravovaného WPA3) a hesla, ktoré si pri pripojení od používateľa vyžiada. Ani tieto znaky však nie sú 100 % garanciou toho, že sieť, na ktorú sa pripájam, nebola zneužitá alebo dokonca vytvorená útočníkom.

Ako spoznať ne/bezpečnú sieť? Čo si všímať?

- **Výber lokality, kde sa pripájam na internet**
  - Pokiaľ je to možné, používateľ by sa mal pripájať na siete, ktorých správcu pozná alebo vie niečo o ich bezpečnostnom nastavení. Bežne do tejto kategórie spadajú školské, domáce (doma či u známych alebo kamarátov) či firemné siete. Pokiaľ je to možné, používateľ by sa mal vyhýbať verejným sieťam.

- **Názov Wi-Fi siete**
  - Keď si používateľ vyberá Wi-Fi sieť, mal by si podrobne preštudovať jej názov. Jedným z rozšírených spôsobov útoku je totiž vytváranie hotspotu/siete, ktorá má **takmer** identický názov ako legitímna sieť na danom mieste. Týmto spôsobom útočníci zvýšia šancu, že sa obeť na internet pripojí cez ich Wi-Fi a budú môcť sledovať, aké údaje obeť odosiela.

KONKRÉTNY PRÍKLAD: Kaviareň má vytvorenú vlastnú sieť *Kaviaren_wifi*, útočník preto vytvorí inú s podobným názvom *Kaviaren_wifi_free*, *Kaviaren_wifi1*. Pokiaľ si používateľ názov neoverí u personálu, podvod pravdepodobne neodhalí.

- **Bezpečnostný protokol/heslo**
  - Momentálne najvyššiu úroveň ochrany poskytuje protokol WPA2 (Wi-Fi Protected Access 2, čo v preklade znamená Wi-Fi so zabezpečeným prístupom 2). Dáta, ktoré používateľ odosiela na sieti zabezpečenej týmto protokolom, sa šifrujú, čo útočníkom bráni v ich čítaní. Výskumníci však našli aj v tomto protokole slabiny a pracuje sa na novšej verzii protokolu WPA3.
  - Protokoly WEP (Wired Equivalent Privacy) alebo WPA (Wi-Fi Protected Access verzia 1) sú dnes zastarané a nedostatočne chránia komunikáciu používateľa pred útokmi zvonka. Ak ich používa niektorá dostupná Wi-Fi sieť, je lepšie sa jej vyhnúť.
- **Hľadajte https://**
  - Ak sa používateľ pripája cez verejnú Wi-Fi a nemôže si byť istý jej bezpečnosťou, mal by navštevovať len stránky, ktorých URL adresa sa začína s **https://**. Znamená to totiž, že komunikácia so stránkou je šifrovaná a útočníkovi, ktorý je na tej istej sieti, bráni v čítaní dát, ktoré chce používateľ odosielať.

Ako sa vyhnúť nebezpečnej sieti?

Dnes má takmer každý používateľ mobilný telefón s dátovým balíkom. Pokiaľ je dostatočne veľký, môže si používateľ vytvoriť vlastnú Wi-Fi sieť tzv. „hotspot", ktorý si sám vytvorí, vrátane úrovne bezpečnosti (ideálne WPA2 alebo WPA3) a hesla. Ten môže následne použiť na pripojenie ďalších zariadení, ako sú notebook, tablet či ďalšie telefóny. Pre útočníka je nabúranie sa do takejto siete výrazne náročnejšie.

Čo je to Virtual Private Network (VPN)?

Ak používateľ nemá možnosť vytvoriť si vlastnú sieť, môže ako alternatívu využiť VPN službu (Virtual Private Network), ktorá dokáže vytvoriť šifrovaný tunel medzi zariadením používateľa a cieľovou stránkou. Tento tunel je pre útočníka takmer neprelomiteľný. Nevýhodou je, že spoľahlivé a kvalitné VPN služby nie sú dostupné zadarmo. Niektoré prehliadače takúto možnosť majú zabudovanú – napr. Opera alebo EPIC. VPN predstavuje vyššiu formu zabezpečenia, ktorá má význam najmä v prípade, že si používateľ potrebuje zachovať anonymitu alebo potrebuje obísť obmedzenia v pripojení na internet. Príkladmi takýchto situácií sú novinári, ale napríklad aj občianski aktivisti, ktorých prenasleduje či obmedzuje autoritársky režim v ich krajine.

Čo je „internet vecí“ (angl. Internet of Things alebo IoT)?

Pod pojmom internet vecí sa rozumejú všetky zariadenia, ktoré označujeme ako „smart“ alebo „inteligentné“. Označenie smart zariadenia znamená okrem splnenia ďalších podmienok najmä fakt, že je pripojené na internet. Kým v minulosti išlo najmä o počítače a neskôr k nim pribudli mobilné telefóny a tablety, dnes už do tejto kategórie spadajú mnohé televízory, kamery, hodinky, chladničky či dokonca automobily. Pripojenie na internet umožňuje rozšíriť funkcie týchto zariadení, no zároveň vytvára cestu, cez ktorú sa do nich môžu dostať útočníci.

Ako IoT súvisí s online bezpečnosťou používateľa?

Internet vecí stále viac a viac dotvára naše domácnosti a odhaduje sa, že v najbližších desaťročiach budú po celom svete k internetu pripojené celé domáce siete tzv. „smart homes“. Tie pritom budú o obyvateľoch domu zbierať obrovské množstvo citlivých informácií a dát. Ide o cennú komoditu najmä pre kybernetických zločincov, ktorí podobné údaje dokážu nielen ukradnúť a predať, ale ich aj zneužiť na sledovanie obete. V najhoršom prípade sa im dokonca môže podariť takúto smart domácnosť ovládnuť.

Nejde o žiadne sci-fi – zraniteľnosti tohto druhu sa zatiaľ našli takmer v každom zariadení, ktoré experti na kybernetickú bezpečnosť testovali. Niektoré koncové zariadenia trpia závažnejšími problémami – sú napríklad zabezpečené len slabým alebo žiadnym heslom, nechránia uložené údaje šifrovaním – iné sú centrálami smart domácností a v prípade úniku dát alebo objavenej zraniteľnosti predstavujú veľké riziko pre súkromie svojich majiteľov.

DOBROU UKÁŽKOU, kam až podobné zraniteľnosti môžu viesť, je úvodná scéna z populárneho seriálu Mr. Robot (séria 2, epizóda 1).

Potrebujem si zakrývať webkameru?

Laptopy, smartfóny aj tablety majú dnes už bežne zabudované fotoaparáty alebo webkamery. Táto technológia rozširuje možnosti pri telefonovaní o video, ale zjednodušuje aj vytváranie nových fotografií na sociálne siete, čety či do osobnej zbierky.

Neprináša to však iba výhody, ale aj riziko, že tieto technológie niekto zneužije proti majiteľovi zariadenia. Útočníci už vo viacerých prípadoch ukázali, že práve webkamera môže byť užitočným nástrojom pri sledovaní obete. Tento efekt ešte znásobuje fakt, že smartfóny už používatelia takmer neodkladajú a majú ich takmer stále na dosah.

O bezpečnosť svojej kamery sa starajú aj mnohé vedúce osobnosti z technologického sveta, pričom asi najznámejším je zakladateľ a šéf Facebooku Mark Zuckerberg. Práve on si na svoj profil ešte v roku 2016 pridal fotografiu, kde v pozadí vidieť jeho počítač s prelepenou kamerou a mikrofónom.

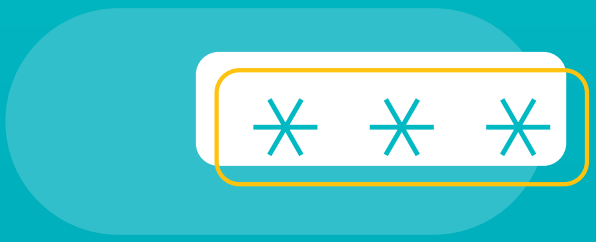
Aj keď nie každý má také cenné informácie ako šéf Facebooku, aj súkromné či intímne fotografie môžu byť cennou korisťou útočníka. Ten svoju obeť môže vydierať ich zverejnením alebo môže takýto citlivý obsah predať na dark webe.

Zaútočiť týmto spôsobom si však vyžaduje spoluprácu obete. Útočník ju totiž musí presvedčiť alebo oklamať, aby si do zariadenia nainštalovala škodlivú aplikáciu. Tá potom dokáže aktivovať kameru či zozbierať staršie zábery a poslať ich útočníkovi. Vo veľkej časti prípadov, ktoré sa dostali až do médií, útočník dokonca mal fyzický prístup k zariadeniu a špionážnu aplikáciu sám ručne nainštaloval.

Na to, aby tento scenár nenastal, mal by (si) používateľ:

- Zakrývať fotoaparát, resp. zabudovanú kameru na svojom zariadení. Niektoré počítače už majú takúto vlastnosť od výroby, no ak nie, je dobré kameru aspoň prelepiť nepriehľadnou páskou, prípadne na ňu použiť špeciálnu krytku.
- Používať spoľahlivý bezpečnostný softvér, ktorý dokáže bezpečnosť kamery chrániť aj softvérovo a blokovať pokusy o jej zneužitie.
- Uistiť sa, že kamera je bežne vypnutá a nesníma svet okolo seba. Pravidelne tiež kontrolujte, ktorá aplikácia či program na zariadení má prístup k fotografiám a fotoaparátu.
- Odkladať zariadenia so zabudovanou webkamerou tak, aby v ich zábere neboli citlivé miesta v izbe či byte. Fotoaparát by nemal mieriť napríklad na posteľ, kúpeľňu či iné oblasti, kde by mohli vzniknúť nechcené intímne zábery.
- Vyhnúť sa tvorbe fotografií s intímnym obsahom, ktoré by mohli skončiť v nesprávnych rukách. Tínedžeri by tiež mali myslieť na to, že takéto zábery je lepšie nezdieľať ani s aktuálnym partnerom/aktuálnou partnerkou, nakoľko v prípade, že vzťah nevyjde, môžu zábery skončiť v nesprávnych rukách či na internete.

Učitelia a rodičia by pri webkamerách (rovnako ako pri iných pravidlách kybernetickej bezpečnosti) mali ísť príkladom a dodržiavať uvedené zásady rovnako ako ich žiaci či deti.



Heslá

Kľúčové slová:

bezpečnostná fráza | dvojfaktorová autentifikácia | heslo | manažér hesiel (password manager) | útok hrubou silou (brute force útok) | viacfaktorová autentifikácia

Otázky, na ktoré odpovedá táto kapitola:

Čo je to heslo? Ako sa najčastejšie kradnú heslá? Čo by malo spĺňať dobré heslo? Čo môže používateľ robiť, ak má priveľa hesiel? Čím môže používateľ nahradiť heslo? Čo je to dvoj/viacfaktorová autentifikácia? Ako útočníci kradnú heslá?

Praktické cvičenia k tejto kapitole:

Crackovanie hesiel, Diskusia o heslách, Plagát o bezpečných heslách, Školská Wi-Fi sieť, Ako vyzerá šifrovaná komunikácia?

Čo je to heslo?

Heslo je slovo, slovné spojenie, bezpečnostná fráza, veta alebo séria znakov, ktoré by mal poznať len používateľ a zväčša v kombinácii s prihlasovacím menom slúži na jeho identifikáciu pri prístupe do digitálnych zariadení, systémov či služieb.

Čo by malo spĺňať dobré heslo?

Dobré heslo by malo spĺňať viacero pravidiel. Vlastnosti dobrého hesla:

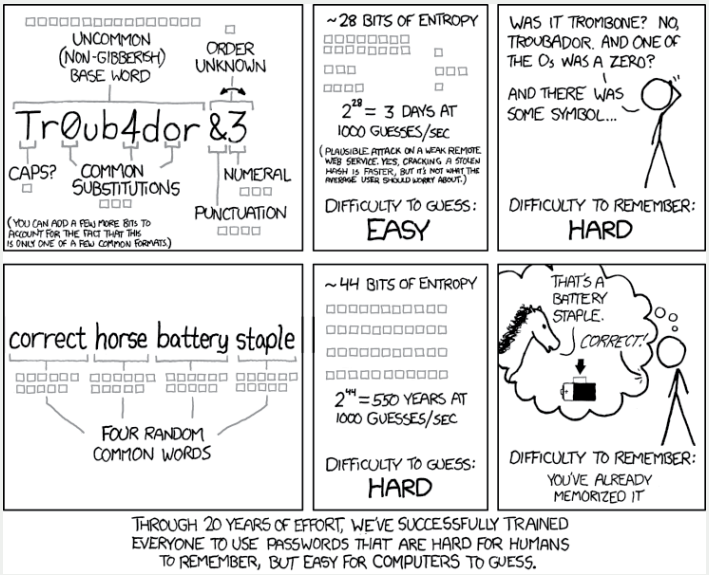
- **Je tajné** – Pozná ho len samotný používateľ.[20]
- **Je unikátne** – Každá služba či zariadenie by malo byť chránené rôznym heslom, aby v prípade, že používateľovi niekto heslo ukradne, nezískal prístup do viacerých jeho účtov/zariadení naraz.
- **Je dlhé** – Má minimálne 8 znakov, ideálne 16 a viac. Dobrou možnosťou sú bezpečnostné frázy, ktoré opisujeme v jednom z nasledujúcich bodov.
- **Obsahuje čísla, veľké a malé písmená a špeciálne znaky (@, #, $, %)** – Mnohé systémy vyhodnocujú heslá veľmi komplexne a rozoznajú aj rozdiel medzi veľkým a malým písmenom. Špeciálne znaky a čísla by nemali nahrádzať znaky, na ktoré sa tradične podobajú (teda „a“ nenahrádzať „@“; „e“ za „3“ a pod.).
- **Nedá sa ľahko uhádnuť** – nemalo by ísť o jednoduché číselné rady ako „123456“ alebo jednoduché slová ako „heslo“. Útočníci dokážu uhádnuť aj populárne citácie z filmov a kníh, slová zo slovníkov či kombináciu údajov o používateľovi napr. „menopriezvisko19xx“. Údaje, z ktorých sa skladá heslo, si mnohí používatelia dávajú aj na sociálne siete, odkiaľ ich útočníci v prípade zlého nastavenia jednoducho pozbierajú a použijú pri hádaní.
- **Tvorí ho bezpečnostná fráza** – Veta alebo fráza (vrátane medzier), ktorú si používateľ ľahko zapamätá, a ktorá je zároveň dostatočne dlhá a zložitá, aby sa nedala uhádnuť. Príklad dobrej bezpečnostnej frázy je „To čo zješ, t8 ti už ni#to nevezme“, pretože sa skladá z 34 znakov, obsahuje medzery, malé, veľké písmená, čísla, špeciálny znak a je ľahko zapamätateľná[21].

DOPLNKOVÝ MATERIÁL:
Zoznam 100 najhorších hesiel, ktoré unikli na internet, je dostupný každý rok, zverejňuje ho spoločnosť TeamID.

20 V prípade menších detí sa odporúča zdieľať heslá s rodičmi, prípadne ich vytvárať s ich pomocou.

21 Bohužiaľ, po zverejnení tohto materiálu už nie je dostatočne bezpečná, pretože ju pozná príliš veľa ľudí a dá sa ľahko uhádnuť.

Na ukážku vhodných postupov môže poslúžiť aj tento komiks:



Čo môže používateľ robiť, ak má priveľa hesiel a nedokáže si ich zapamätať?

Odporúčame používať aplikáciu, ktorá dokáže používateľovi uložiť celé zoznamy hesiel a takýto zoznam chráni nielen ďalším heslom, ale aj šifrovaním. Takáto aplikácia sa nazýva manažér hesiel (v angličtine password manager). Pri ich výbere si treba dať pozor na podvody a hľadať nezávisle overené značky, ktoré majú dobrú povesť a overenú bezpečnosť – príkladmi sú Sticky Password, KeePass či LastPass. Niektoré operačné systémy majú password manažér už v sebe zabudovaný – Keychain na MacOS.

Čím môže používateľ nahradiť heslo?

Čiastočné náhrady hesiel dnes predstavujú čítačky odtlačkov prstov či sken tváre. Aj tie však pre prípad, že odtlačok ani tvár nefunguje, využívajú ako zálohu číselný PIN kód.

Vo všeobecnosti sa heslá zabezpečujú pridaním ďalšieho overenia/kroku, ktorý má zaručiť, že heslo zadala správna osoba. Ide o takzvanú **dvojfaktorovú alebo viacfaktorovú autentifikáciu**. Táto forma overenia môže prebiehať viacerými spôsobmi:

- **Využitím inej komunikačnej cesty** – napr. zaslaním overujúcej SMS na mobil používateľa.
- **Využitím iných, vopred dohodnutých kódov** – napr. GRID karta obsahujúca tabuľku kódov, z ktorej sa vyžaduje jeden náhodne vybraný kód; elektronická čítačka – hardvérové zariadenie, ktoré používateľovi hesla vytvorí unikátny kód, pričom druhá strana ho vie overiť.

- **Využitím špeciálnej aplikácie, ktorá vytvára časovo obmedzené kódy** – Kód obvykle platný po obmedzenú dobu, napr. 30 sekúnd. Pokiaľ tento časový limit vyprší, kód sa zmení a stratí platnosť. To výrazne skracuje čas na útok, čo ešte viac zlepšuje bezpečnosť hesla. Tieto aplikácie dokážu spolupracovať len s niektorými online službami. Príkladom pomerne univerzálnych riešení sú Google Authenticator alebo Microsoft Authenticator.

Odstrašujúce príklady, ktoré môže učiteľ uviesť (na základe reálnych prípadov):

Dievča používalo na Facebooku slabé heslo, ktoré sa dalo ľahko uhádnuť. Pri ceste do zahraničia sa navyše prihlásilo na nezabezpečenú Wi-Fi sieť, kde útočník heslo odchytil. Vďaka týmto informáciám sa mu podarilo nabúrať sa jej do účtu, z ktorého jej ukradol súkromné fotografie, ktoré si posielala s priateľom. Následne sa jej vyhrážal ich zverejnením, pokiaľ nezaplatí. Keď to odmietla, fotografie rozposlal do všetkých skupín, ktoré mala vytvorené v Messengeri.

Obeť mala v rámci svojej firmy vytvorený mailový server, no používala jednoduché heslo. Keďže išlo o verejne dostupný systém, útočník ho našiel na internete a heslo prelomil. Následne posielal všetkým kontaktom v zozname škodlivé e-maily a nevhodné reklamy.

Ako sa najčastejšie kradnú heslá?

Existuje niekoľko možností, ako útočník môže získať heslo svojej obete:

1. **Sledovaním** – Znie to absurdne, ale útočníci aj dnes často získajú heslo nazeraním cez rameno svojej obete, prípadne jej nahrávaním na video. Platí to pre prístup do zariadenia, rovnako ako pre prihlasovanie do online služieb.

Ilustračné video ukazuje, že ani dlhý a zložitý kód nemusí používateľa spoľahlivo ochrániť.

2. **Sociálnym inžinierstvom** – Útočník zmanipuluje alebo oklame obeť, aby mu údaje sama poskytla. Môže na to využiť falošnú stránku, špeciálne pripravený e-mail či správu na sociálnych sieťach, kde sa vydáva za dôveryhodnú osobu/inštitúciu alebo predstiera, že ide o požiadavku banky/sociálnej siete/online služby.

3. **Škodlivým kódom** – Útočník nainfikuje zariadenie obeti škodlivou aplikáciou alebo kódom (napr. cez zraniteľnosť v softvéri, použitím sociálneho inžinierstva, cez infikovanú stránku atď.), ktoré sú špeciálne vytvorené tak, aby vyhľadávali, sledovali a kradli heslá a posielali ich útočníkovi.

4. **Útokom na sieťovú komunikáciu** – Útočník môže odchytávať údaje obete na sieťovej úrovni. Ak sa útočník rozhodne dáta odchytávať na verejnej Wi-Fi, vo väčšine prípadov musí byť v bezprostrednom okolí obete[22]. Podobný útok sa dá urobiť aj za pomoci škodlivého kódu, ktorý nevyžaduje fyzickú prítomnosť.

5. **Hádaním (tzv. brute force útok, resp. útok hrubou silou)** – Jedna z najčastejšie využívaných taktík. Útočník háda bežne používané alebo prednastavené prihlasovacie heslá, používa slovníky či známe frázy. Na tento účel má útočník vytvorený špeciálny kód, prípadne celé zariadenia, ktoré dokážu hádať tisíce hesiel v rádoch sekúnd. To mu umožňuje jednoducho a rýchlo prelomiť konto so slabým či krátkym heslom. Na ilustráciu stačí povedať, že štvormiestny kód zložený z písmen a číselných znakov dokáže útočník uhádnuť takmer okamžite.

    a. Príklady kalkulačiek na výpočty sily hesiel:

Online Password Calculator

Brute Force Calculator

22 Útočníkovi stačí dostať sa do blízkosti domu či bytu obete. Dnešné Wi-Fi prístupové body totiž často majú dosah aj niekoľko desiatok metrov za hranicou bytu/domu. Navyše útočník vybavený anténou dokáže vzdialenosť, v ktorej zachytí signál, ešte zväčšiť.

Aktualizácie

Kľúčové slová:

aktualizácia (update) | firmvér | operačný systém | záplata (patch)

Otázky, na ktoré odpovedá táto kapitola:

Čo sú to aktualizácie a ako sa používateľ dozvie, že je potrebné softvér aktualizovať? Prečo sú aktualizácie dôležité? Prečo neodkladať aktualizácie? Mal by si používateľ zapnúť automatické aktualizácie? Ktoré programy a časti zariadenia je potrebné pravidelne aktualizovať?

Čo sú to aktualizácie a ako sa používateľ dozvie, že je potrebné softvér aktualizovať?

Aktualizácie sú nové verzie softvéru alebo ich častí. Často sa pomocou nich opravujú chyby v softvéri a zvyšujú bezpečnosť aplikácií.

S aktualizáciami sa skôr alebo neskôr určite stretne každý používateľ digitálnych zariadení. Operačný systém alebo aplikácia ho upozorní na potrebu aktualizácie najčastejšie pomocou vyskakovacieho okna. Po vykonaní aktualizácie môže byť požadovaný aj následný reštart zariadenia.

Niektoré aktualizácie sa v slovenčine nazývajú aj záplatami, keďže opravujú „diery". Iné (ako napríklad aktualizácie bezpečnostného softvéru) len aktualizujú vybrané databázy či pridávajú nové funkcie. V angličtine ide najčastejšie o slová „update" či „patch".

Prečo sú aktualizácie dôležité?

Aktualizácie môžu mať viaceré úlohy. Z pohľadu bezpečnosti opravujú zraniteľné či slabé miesta a zvyšujú bezpečnosť programu, používateľa aj jeho zariadenia. Ďalšou úlohou aktualizácií je odstraňovať problémy, na ktoré upozorňujú používatelia – napríklad nefunkčné tlačidlá, chýbajúce funkcie a podobne – a tým zlepšovať svoj výkon a užitočnosť pre používateľov.

Väčšie aktualizácie aplikácií či operačného systému, ktoré sa označujú ako prechod na novšiu verziu, často prinášajú aj ďalšie výhody v podobe nových funkcií a možností, čím sú pre používateľa lákavé.

Prečo neodkladať aktualizácie?

Vyskakovacie okná upozorňujúce na aktualizácie väčšinou obsahujú možnosť odsunúť aktualizáciu o niekoľko minút, hodín či dní. Bohužiaľ práve táto možnosť je lákavá, keďže v danej chvíli používateľovi ušetrí čakanie a neobmedzí ďalšie používanie zariadenia. Aktualizácia však môže riešiť významnú bezpečnostnú či inú chybu v programe alebo zariadení a je preto dôležité ju neodkladať.

Kvôli útočníkom treba softvér aktualizovať najskôr, ako je to možné. Práve oni totiž často využívajú známe zraniteľnosti, aby sa dostali do zariadenia obete. Čím dlhšie používateľ odkladá aktualizáciu, tým väčšie je riziko, že zraniteľnosti môže zneužiť útočník.

Mal by si používateľ zapnúť automatické aktualizácie?

Dobrou možnosťou, ako udržovať svoje zariadenia na čo najvyššej bezpečnostnej úrovni, je aktivovať si automatické aktualizácie. Tie sa pritom môžu nainštalovať aj na konci dňa, v noci či tesne pred vypnutím zariadenia. Automatické aktualizácie sa väčšinou dajú zapnúť priamo vo vyskakovacom okne, ktoré sa používateľovi samo objaví, prípadne v nastaveniach zariadenia.

Ktoré programy a časti zariadenia je potrebné pravidelne aktualizovať?

Aktualizácie sú potrebné pre všetky operačné systémy. Medzi najpopulárnejšie patria Windows, MacOS, Linux, iOS, Android, Windows Phone. Aktualizácie sú potrebné aj pre všetky aplikácie a programy, ktoré v zariadení bežia vrátane internetového prehliadača, prehrávača hudby, grafických programov či hier. Vo výnimočných situáciách je potrebné aktualizovať aj tzv. firmvér – teda softvér pod úrovňou operačného systému, vďaka ktorému funguje celý hardvér.

Slovník

Táto príručka obsahuje niektoré pojmy a výrazy, ktoré sú špecifické pre oblasť IT bezpečnosti. Pre lepšiu orientáciu a pochopenie materiálu by sme preto odporúčali, aby sa s nimi čitateľ aspoň v rýchlosti oboznámil predtým, než použije príručku. V nasledujúcom slovníku dopĺňame aj vysvetlenia niektorých pojmov, ktoré nadmerným používaním v médiách stratili časť svojho významu, ktorá je z nášho pohľadu kľúčová.

Aplikácia

Aplikácia je všeobecne definovaná ako akýkoľvek program alebo počet programov určených pre koncových používateľov.

Bot

Cieľový počítač, ktorý je infikovaný malvérom a je súčasťou botnetu.

Botnet

Slovo botnet sa skladá z dvoch výrazov: bot a net. Bot je skratka pre „robot" a net je skratka pre network (sieť). Botnety teda pomenúvajú skupiny systémov, ktoré sú vzájomne prepojené. Útočníci, ktorí vytvárajú malvér, nie sú v praxi schopní sa manuálne prihlásiť do každého infikovaného počítača. Namiesto toho na správu veľkého počtu infikovaných systémov používajú práve botnety, ktoré to robia automaticky.

Cielené útoky

Cielené útoky sú formou personalizovaného útoku. Ten môže byť zameraný na jednotlivca, spoločnosť alebo softvér. Tvorcovia malvéru pri tejto forme útoku bývajú zväčša skúsení a na vývoj malvéru majú dostatok času a peňazí.

Firewall

Výraz „firewall" sa pôvodne vzťahoval na konštrukciu, ktorá má okolo požiaru vytvoriť zábranu, aby sa zamedzilo šíreniu ohňa a narastaniu jeho ničivých následkov na ľudí a majetok.

Hacker

Na rozdiel od populárneho použitia komunita zameraná na IT bezpečnosť nevníma hackerov len v negatívnom kontexte. Toto slovo totiž opisuje jednotlivca, ktorý sa snaží nájsť nové či originálne využitie pre systém alebo jeho časť, ktorého pôvodné využitie bolo úplne odlišné. Dali by sa vo všeobecnosti rozdeliť do troch kategórií: etických hackerov (white hat), tých, ktorí sa pohybujú v šedej zóne (grey hat) a na hackerov, ktorí majú jednoznačne zlý úmysel (black hat).

Vo všeobecnosti tak hackerom je aj človek, ktorý rozoberie rádio a namiesto prijímania signálu a počúvania hudby ho upraví, aby slúžilo ako vysielač či rušička signálu. Etickí hackeri sa zase snažia hľadať slabiny v systéme organizácie s cieľom informovať ju o nich a pomôcť pri ich odstraňovaní. Tento proces sa tiež nazýva ***penetračné testovanie****.*

Hackovanie

Kybernetickým útočníkom vo filmoch často stačí mať pripojenie na internet a v priebehu niekoľkých minút (či dokonca sekúnd) sa dostanú do akéhokoľvek systému, či už je to elektronický zámok od dverí, interná sieť vybranej tajnej služby alebo policajné či dopravné kamery. Zložitosť dnešných systémov je na takej úrovni, že podobná akcia by zločincom trvala týždne či možno mesiace, už len preto, že by sa museli zorientovať, ako jeho prvky fungujú. Hackovanie je často dlhodobá a cieľavedomá aktivita, pri ktorej hacker (etický hacker alebo útočník) hľadá zraniteľnosti vo vybranom systéme a snaží sa ich využiť.

Kryptomena

Digitálne aktívum, ktoré využíva kryptografiu na zabezpečenie transakcií, kontrolu vytvárania ďalších menových jednotiek a overovanie prevodu aktív. Populárnym príkladom kryptomeny je Bitcoin.

Malvér/škodlivý kód

Názov malvér vznikol spojením dvoch anglických slov: „malicious“ a „software“. V doslovnom preklade znamená škodlivý softvér alebo škodlivý kód. Ide o presnejší názov (počítačových) vírusov, ktoré sú len malou podskupinou malvéru.

Sociálne inžinierstvo

Ide o kategóriu útokov, ktoré nevyžadujú takmer žiadne technické znalosti. Útočníci sa ich prostredníctvom snažia oklamať alebo manipulovať obete tak, aby porušili pravidlá bezpečnosti. Cieľom môže byť presmerovanie obete na nebezpečnú či falošnú stránku, vylákanie citlivých údajov, prípadne snaha vystrašiť obeť, aby si nainštalovala nechcenú/nebezpečnú aplikáciu alebo iný škodlivý softvér. Tento typ útoku zneužíva ľudskú nevedomosť a slabosti.

Spam a Phishing

Spam je akákoľvek nevyžiadaná elektronická pošta, napríklad e-mail, SMS alebo správa v četovej aplikácii. **Phishing** je snaha útočníkov vylákať citlivé údaje a dáta od obete, pričom útočníci sa vydávajú za dôveryhodnú organizáciu, službu alebo osobu. Phishingový útok môže mať podobu e-mailu, na ktorý má obeť odpovedať, alebo odkazu na stránku, ktorá sa nápadne podobá napríklad na web sociálnej siete, e-mailovej služby, internetbankingu. Odkazy na phishingové stránky sa bežne šíria v spamových e-mailoch, cez čet, sociálne siete či SMS. Pre učiteľov a žiakov sú dostupné online phishingové testy. Odkazy na tieto cvičenia nájdete v druhej časti príručky s názvom Aktivity.

Umelá inteligencia

Umelá inteligencia (AI) zatiaľ predstavuje nedosiahnuteľný ideál. Pojem existuje už viac ako 60 rokov a vzťahuje sa na inteligentný a sebestačný počítač, ktorý sa dokáže samostatne učiť výlučne na základe vstupných informácií z prostredia a bez zapojenia človeka.

Útočník

Keďže hackeri so zlými úmyslami sú len jednou podmnožinou, pojmy útočník, kyberzločinec či kybernetický kriminálnik sú oveľa výstižnejšie a používame ich naprieč touto príručkou.

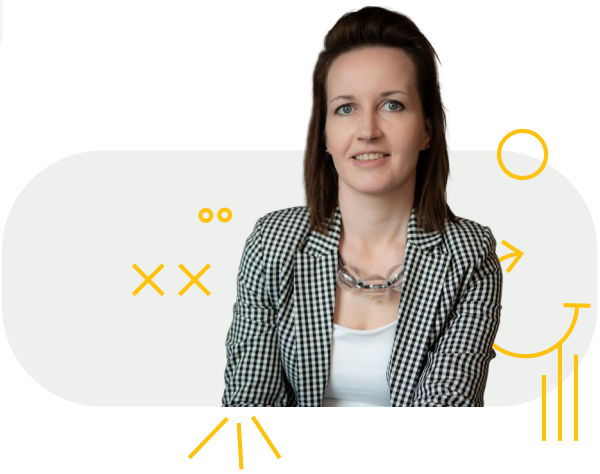
Zraniteľnosť

Chyba v softvéri, ktorá predstavuje bezpečnostné riziko zneužiteľné útočníkom.

Autori príručky

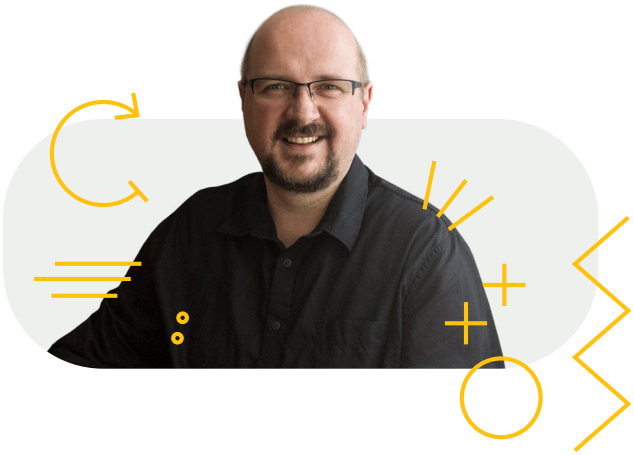
Ondrej Kubovič — špecialista na digitálnu bezpečnosť

Ondrej pracuje v spoločnosti ESET ako špecialista na digitálnu bezpečnosť už viac ako päť rokov. Jeho náplňou práce je zvyšovanie povedomia o najnovších kybernetických hrozbách u širokej verejnosti. Na túto tému je odborníkom a na mnohé riziká sa pozerá aj očami svojich dvoch neterí, ktoré sú už súčasťou digitálneho sveta prostredníctvom účtov svojich rodičov na sociálnych sieťach. Je členom tímu tvorcov materiálov pre projekt Digital Skills, ktorý ponúka školenia a informácie o kybernetickej bezpečnosti pre slovenské školy. Ondrej dúfa, že aj napriek všetkej škodlivej aktivite, ktorú ESET Vírus Lab na internete odhalí, budeme môcť vytvárať zábavné detské on-line zážitky a čo je najdôležitejšie, hlavne bezpečne.



Jarmila Tomková – psychologička

Jarmila je uznávanou slovenskou psychologičkou. Pracovala vo Výskumnom ústave detskej psychológie a patopsychológie, kde viedla výskumné tímy skúmajúce možnosti a riziká používania internetu deťmi. Koordinovala slovenský tím nadnárodnej výskumnej siete EU Kids Online. Pracovala tiež ako školská psychologička, kde navrhla a implementovala niekoľko rozvojových a preventívnych programov, napríklad Študenti proti šikanovaniu. Jarmila naďalej pracuje ako konzultantka pre organizácie a školy pri prevencii a intervencii negatívneho správania, ako je šikanovanie a nenávistné prejavy. Taktiež založila a vedie občianske združenie ViaSua, ktoré sa venuje podpore duševného zdravia a osobného rastu jednotlivcov, rodín a spoločnosti všeobecne. Tá sa dosahuje poradenstvom, zvyšovaním povedomia a destigmatizáciou problémov duševného zdravia. Jazyk a diskurz považuje za rozhodujúci a vždy uprednostňuje participatívny a rovnocenný prístup.



Peter Kučera – Učiteľ informatiky

Peter je učiteľ informatiky na 1. súkromnom gymnáziu v Bratislave (1. súkromná stredná škola v Bratislave) a autor niekoľkých učebníc. Záleží mu na kvalite výučby tohto predmetu nielen na škole, kde učí, ale vo všetkých častiach spoločnosti. Poskytuje aj praktické hodiny pre študentov študijného odboru Výučba počítačov na Fakulte matematiky, fyziky a informatiky Univerzity Komenského v Bratislave.

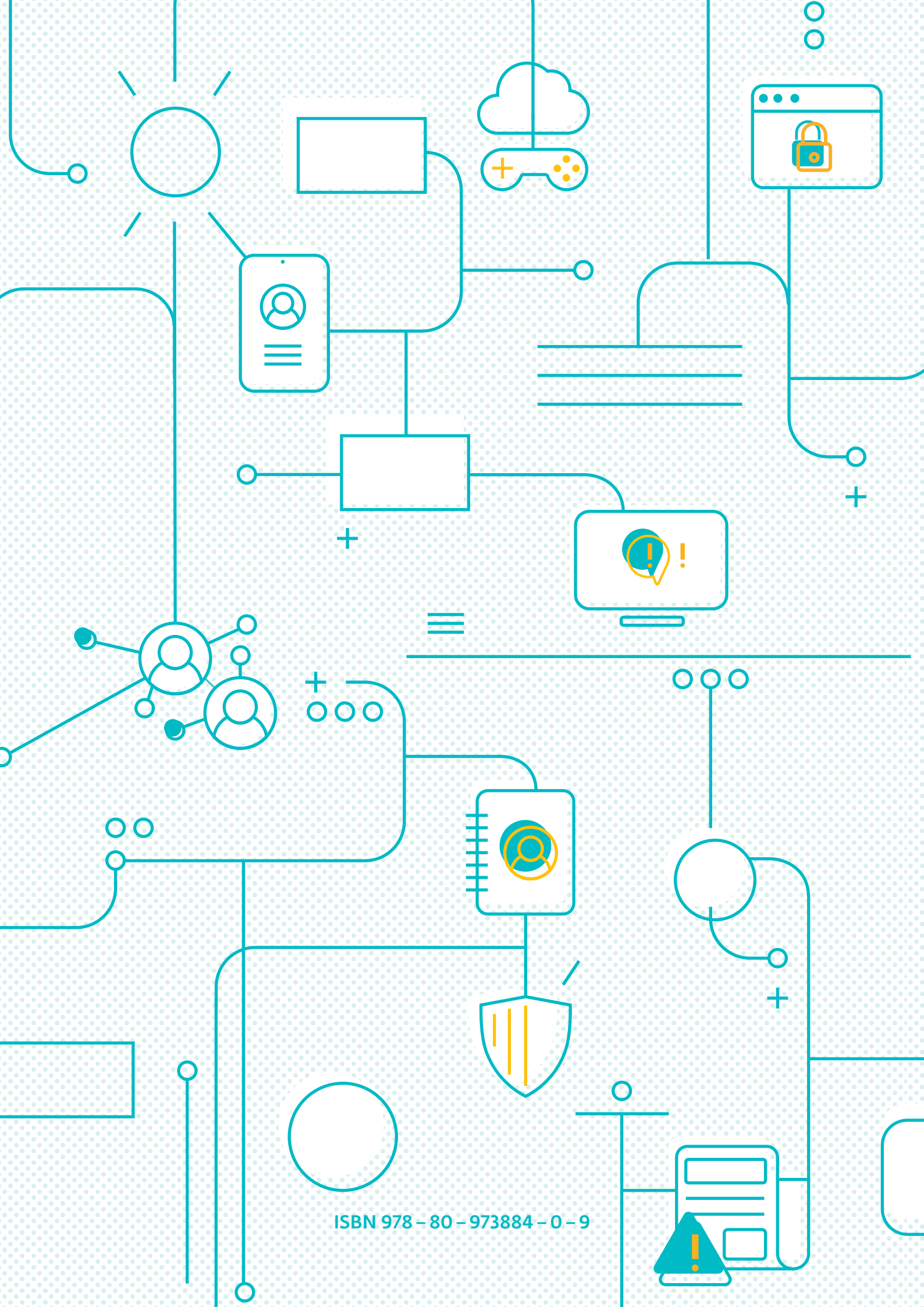
Vytvoril sériu učebníc s názvom Tvorba v Pythone, ktoré obsahujú príručky pre učiteľov, a implementuje výcvikové kurzy jazyku Python pre učiteľov. Peter založil a vedie Klub učiteľov informatiky, ktorý funguje ako platforma na zdieľanie skúseností a zavádzanie nových tém. Komunita učiteľov v klube spoločne reaguje na aktuálny vývoj v oblasti digitálnych technológií a prináša nové témy a návrhy odborníkov pre učiteľov a študentov.

Digitálnu bezpečnosť považuje za kľúčovú tému dnešnej online doby. Pri rýchlom vývoji technológií je ťažké sledovať zmeny a reagovať na ne s dostatočnou flexibilitou. Preto je dôležité pomáhať učiteľom a študentom pri vzdelávaní a odbornej príprave v tejto oblasti.

Jakub Daubner – Vedúci interných systémov v spoločnosti ESET

Jakuba bavili prírodné vedy od detstva, preto sa rozhodol študovať teoretickú informatiku a aplikovanú informatiku. Paralelne so štúdiom sa stal členom ESET Vírus Labu, kde sa mu v priebehu 10 rokov podarilo vybudovať oddelenie 45 vývojárov. Jeho tím sa zameriava najmä na vývoj interných nástrojov a automatických systémov. Vytvoril tiež detekčný modul založený na strojovom učení a umelej inteligencii. Jakub okrem toho vedie žiacku programátorskú skupinu na základnej škole a tiež spolupracuje s Ondrejom Kubovičom na projekte Digital Skills, v rámci ktorého pripravujú vzdelávacie materiály a školia učiteľov.

ISBN 978 – 80 – 973884 – 0 – 9



ISBN 978-80-973884-0-9