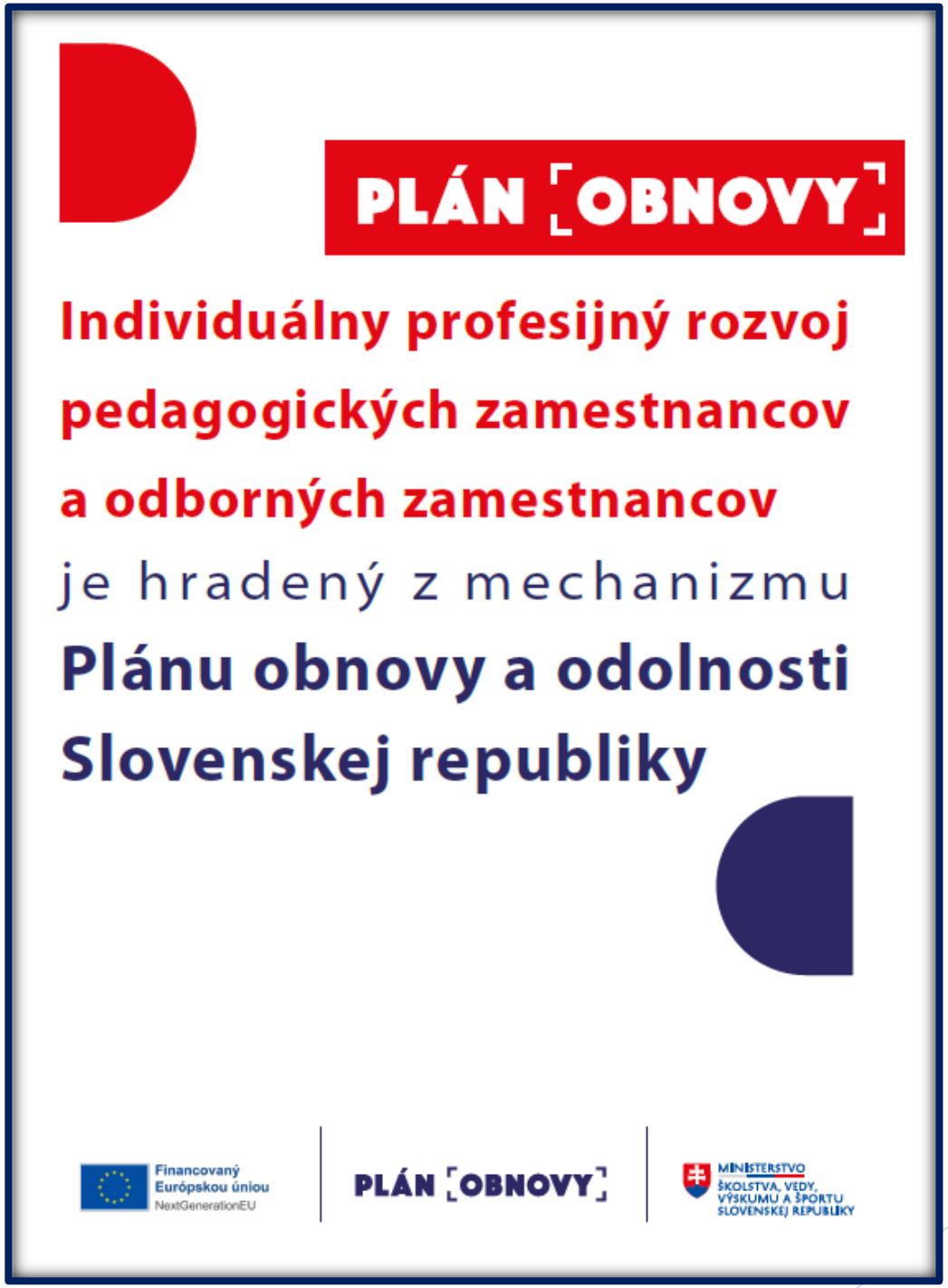

PLÁN OBNOVY
Individuálny profesijný rozvoj
pedagogických zamestnancov
a odborných zamestnancov
je hradený z mechanizmu
Plánu obnovy a odolnosti
Slovenskej republiky
Financovaný Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Program vzdelávania

Cesta za poznaním

Aktualizačné vzdelávanie vytvorené v súlade s § 90d ods. 12 zákona č. 138/2019 Z. z. o pedagogických zamestnancoch a odborných zamestnancoch a o zmene a doplnení niektorých zákonov, obsahové zameranie:

digitálne zručnosti

Vypracovala: Mgr. Lucia Sabopálová

Základné pojmy

- ***Údaj*** - sú správy, ktoré vyjadrujú určité fakty o procesoch, alebo prvkoch reálneho sveta. ***Údajmi môžu byť písmená, čísla, slová, znaky, prípadne ich kombinácie***. Všetky údaje nesú určitý informačný obsah.

- ***Dáta*** **-** sú všetky informácie alebo ich časti v digitálnej forme, ktoré sa dajú spracovať. Dátami sú informácie, ktoré sú nositeľmi významu pre ľudí.

- ***Digitalizácia*** **-** Digitalizácia je proces, pri ktorom sa analógové informácie (alebo údaje) prevádzajú na digitálne. To znamená, že každému údaju sa priradí určitý počet bitov čiže jedinečná kombinácia jednotiek a núl. Toto priradenie musí byť také, aby sa údaj z digitálnej podoby dal jednoznačne pretransformovať späť do analógového tvaru.
- **Digitálne technológie** nám umožňujú pracovať s informáciami prostredníctvom digitálnych prostriedkov ako je počítač, notebook, tablet, mobil, TV, DVD prehrávač... Pomáhajú tvoriť, skúmať, objavovať, vyjadriť či prezentovať myšlienky, názory, postrehy a umožňujú každému byť kreatívnejším, samostatnejším, digitálne zdatnejším.

Informácia *- zahrňuje v sebe správu spolu s jej významom pre príjemcu.* Je to správa, ktorá vyjadruje istý stav, slúži nejakému cieľu alebo vyvoláva nejakú akciu. Správa sa stáva informáciou buď v dôsledku ľudskej interpretácie alebo tým, že ju spracujú algoritmy, alebo že je uložená v súboroch.

- ***Formy informácie môžeme deliť na:***

  - ***Analógové*** – vytvárané, prenášané, spracovávané a uchovávané inak ako za pomoci výpočtovej techniky

  - ***Digitálne*** - vytvárané, prenášané, spracovávané a uchovávané v elektronickej forme.

- ***Každá informácia má tieto vlastnosti:***

  - možno ju merať – jej množstvo (kvantitu), napr. na pošte sa platí za telegram podľa počtu slov (počet slov je vyjadrením množstva informácie)

  - má svojho adresáta – pre ktorého môže, ale nemusí mať význam. Z tohto hľadiska teda môžeme informácie rozdeliť na užitočné a neužitočné.

Uchovávanie (digitálnych údajov) informácií:

- Prvými nosičmi informácií boli steny jaskýň, hlinené tabuľky, papyrus a neskôr papier. Objavom kníhtlače sa stal papier najdôležitejším prostriedkom na uchovávanie a šírenie informácií.

- Objav a vývoj písacieho stroja predstavuje prvý krok k mechanizácii zápisu a rozmnožovania textov na papieri.

Uchovávanie (digitálnych údajov) informácií:

- Rastúci objem informácií ukázal, že papier nie je dostatočným médiom. Preto sa začali používať platne, magnetofónové pásky a dnes už používame CD, DVD, USB kľúče... Majú oproti papieru väčšiu kapacitu a dovoľujú dokumenty, texty a údaje opravovať, kopírovať, posielať e-mailom, vkladať do iného dokumentu alebo na webové stránky a spracúvať ich rôznymi spôsobmi.
- Informácie na začiatku 3. tisícročia sú ľahko dostupné, ale je ich tak veľa, že potrebujeme pomôcky na ich vyhľadávanie (indexy, katalógy alebo vyhľadávacie webové stránky) a spracúvanie (počítače). Musíme sa tiež naučiť, *ako sa vzdelávať, ako informácie vyhľadávať a spracúvať a ako ich zverejňovať*.

Vyhľadávanie informácií

- Na vyhľadávanie digitálnych údajov a informácií používame bežné vyhľadávače (ako napr. Google, Books, Bing atď.). Môžeme využiť viaceré postupy a triky vyhľadávania.
- Relevantnejšie výsledky vyhľadávania môžeme dosiahnuť pri použití správne formulovaného vyhľadávacieho dotazu.
- Formulácia vyhľadávacieho dotazu - väčšina databáz nerozumie prirodzenému jazyku, ktorý požíva človek. Na formuláciu vyhľadávacieho dotazu môžeme využiť:

  - kombináciu kľúčových slov (autor, názov, predmet, rok vydania a pod.)

  - blízkosť a pozíciu vyhľadávaných termínov

  - spresnenie vyhľadávacieho dotazu (vyhľadávanie presnej frázy – použijeme úvodzovky).

Vyhodnocovanie a spravovanie digitálnych údajov

- Na internete nájdeme veľké množstvo informácií. Je na našom uvážení, ktoré informácie považujeme za relevantné. Ale taktiež tu platí pravidlo, aby sme si každú informáciu overili z viacerých zdrojov, aby nedochádzalo k šíreniu poplašných správ či nepravdivých informácií. Taktiež na sociálnych sieťach, aby sme nezdieľali, neuverejňovali a zbytočne nezahlcovali nepravdivými, nepresnými či falošnými informáciami.


06.11.2022 18:00 | Správy | Zaujímavosti

Kedy príde koniec sveta? Tieto šialené apokalyptické predpovede vydesili ľudstvo: Máte obľúbenú?

Zdieľanie prostredníctvom digitálnych technológií

- **Zdieľanie** je spoločné využívanie zdroja alebo priestoru. Je to tiež proces delenia a distribúcie.
- Zdieľať v digitálnom svete môžeme v podstate čokoľvek (súbory, texty, obrázky, videá...).
- Existujú služby, ktoré dočasne podržia váš obsah na svojich serveroch, odkiaľ si ich môže adresát stiahnuť. A potom sú tu weby, kde si môžete kúpiť priestor, na ktorom zálohujete svoj obsah a zároveň ho môžete zdieľať s vybranými ľuďmi.
- Na internete nájdeme mnoho stránok práve pre tieto účely: ulozto.sk, uschovna.sk, iCloud, GoogleDisk, BOX, MediaFire...
- Zdieľať môžeme aj prostredníctvom sociálnych sietí, e-mailov, SMS a rôznych aplikácií...

Interakcia, komunikácia a spolupráca prostredníctvom digitálnych technológií

Komunikácia – je prenos zmyslami vnímateľných informácií. Pri komunikácii si vzájomne vymieňame textové, zvukové, obrazové a iné informácie.

- Má dve formy: - verbálnu (jazykové prostriedky reči) – ústne a písomné,
  - neverbálnu (mimojazykové prostriedky)
- ***Verbálna komunikácia:***
  - ***ústna*** - *hlasová*
  - ***písomná*** – tlačená a elektronická

Existujú rôzne spôsoby elektronickej komunikácie:

- tie, ktoré ***nedávajú*** veľa ***času na rozmyslenie*** (videokonferencia, videohovor...)
- tie, kde si svoju ***odpoveď môžeme*** dôkladnejšie ***premyslieť*** (e-mail, sms...)

Netiketa

- Súbor pravidiel, ktoré by mal používateľ internetu dodržiavať, pokiaľ chce byť považovaný za slušného človeka.

- The Computer Ethics Institute: „Nenič prácu iných, nepoužívaj počítač k škode iných ľudí, nepouži a nevytvor kópiu softvéru, ktorý si nezaplatil, neprivlastni si intelektuálne dielo niekoho iného...“

- Neposielaj zbytočné informácie, dodržiavaj gramatiku, píš s diakritikou, nepublikuj nepravdivé informácie, zdrž sa vulgarizmov, uvádzaj predmet e-mailu...

Pravidlá netikety:

1. Nikdy nezabúdajte, že na druhom konci sú ľudia a nie počítač. To, čo anonymne napíšete stroju, by ste možno nikdy nepovedali dotyčnému do očí.
2. Dodržiavajte všetky pravidlá slušnosti z normálneho života. Čo je zlé v bežnom živote, bude určite nevhodné aj na internete.
3. Politika, náboženstvo a iné rozporuplné témy by mali byť diskutované s maximálnou ohľaduplnosťou a taktom.
4. Majte ohľad k druhým. Nie každý má rýchle internetové pripojenie ako vy. Mnohí sa pripájajú z domu cez pomalý modem, za ktorý platia! Neposielajte teda zbytočné a zbytočne veľké e-mailové správy.

5. Publikovať nepravdivé informácie, alebo niekoho ohovárať tiež nie je vhodné.

6. Nevydávajte prácu niekoho iného za svoju. Ak využijete prácu (obrázok, text, súbor...) iných, mali by ste spomenúť ich autorstvo.

7. Pomôžte, ak viete. Niekto z diskusnej skupiny má konkrétny problém. Ak viete odpoveď, pomôžte. Nabudúce pomôže niekto vám. V diskusnej skupine platí zásada „Najprv počúvaj, až potom píš.“

8. Rešpektujte súkromie iných.

9. Nezneužívajte svoju moc a vedomosti. Používatelia so špeciálnymi privilégiami, napr. správcovia serverov, administrátori ktorí majú prístup ku všetkému, musia mať dôveru iných používateľov.

10. Odpúšťajte druhým ich chyby. Každý začínal, každý sa učil... Netreba hneď reagovať výsmešne alebo so zlosťou.

11. Nerozosielajte reťazové listy, spam či poplašné správy. Upozornite aj ostatných, že takéto správanie na internete nie je vhodné.

Digitálna identita a súkromie

- 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 hracích serveroch (Fortnite), skrytý za vymyslenou prezývkou.

- Niektoré identity dokonca používateľ môže vytvoriť zámerne odlišné, aby nebolo možné vystopovať ich originálneho majiteľa – falošný e-mail, konto, pod ktorým sa používateľ prihlási na odoberanie napríklad reklamných letákov.

Digitálna identita a súkromie

- Ak sa používateľ s niekým zoznámi online, často sa musí spoliehať iba na informácie, ktoré mu o sebe poskytne druhá strana. Overiť si jeho/jej identitu je mimoriadne náročné, ak nie aj nemožné.

- Kľúčovou pri digitálnej identite je **reputácia.** Tú si človek buduje svojím správaním a interakciami s inými používateľmi. Ak má používateľ dobrú reputáciu, umožňuje mu to pôsobiť dôveryhodnejšie, spoľahlivejšie.

Ako si 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.

- Už niektoré vonkajšie znaky konta môžu byť signálom, že ide o falošný profil – napríklad málo priateľov, žiadne fotografie, prípadne len selfies, kde nie sú žiadni ďalší ľudia.

Ako si overiť cudziu identitu?

- Opatrnosť je na mieste aj v prípade, že na profile používateľ nájde obsah, ktorý vyzerá až príliš dobre na to, aby bol skutočný.

- Užitočná pri overovaní je aj e-mailová adresa, na ktorú sa viažu profily na sociálnych sieťach ako TikTok, SnapChat, Instagram, Facebook, Twitter a iné.

- Ak si podvodník nedá záležať na detailoch, môže na rôznych stránkach uvádzať odlišné či dokonca protichodné údaje.

Digitálna stopa

- Ak má používateľ e-mailový účet, je prihlásený na sociálnej sieti, hráva online hry alebo len tak surfuje po rôznych zábavných, spravodajských či iných stránkach, vytvára pritom **digitálne stopy.**

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

- **aktívna digitálna stopa** – zahŕňa všetky vedome poskytnuté a zverejnené údaje na internete. Ak používateľ pošle e-mail, zverejní blog, dá lajk, zdieľa video alebo text na sociálnej sieti, alebo si píše cez čet, všetky tieto a im podobné informácie sa stávajú *aktívnou digitálnou stopou*.

- **pasívna digitálna stopa** – tvoria ju 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.

Digitálna stopa

- 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.
- **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, 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 napriek vymazaniu môže opätovne objaviť na internete a v budúcnosti skomplikovať používateľovi napríklad prijímací pohovor či iné príležitosti.

Aktivita – zverejňovanie fotografií





- Úlohou je spoločne v skupine rozhodnúť, ktoré fotografie by boli pre Lukáša v poriadku a ktoré by mu vadili, keby boli zverejnené.

General Data Protection Regulation

- **GDPR** alebo všeobecné nariadenie na ochranu osobných údajov. Ide o nariadenie Európskej únie, ktoré upravuje a nahrádza doterajší zákon o ochrane osobných údajov.
- Ochrana fyzických osôb v súvislosti so spracovávaním osobných údajov patrí medzi základné ľudské práva. Najdôležitejší je rešpekt súkromného a rodinného života či uchovávanie citlivých informácií o ostatných.
- Súbor ucelených pravidiel na ochranu dát **je účinná od 25.5.2018**. V roku 2016 bolo GDPR schválené. **Do 25. 5. 2018 museli všetci zrevidovať a zjednotiť informačné systémy a postupy pri práci s údajmi**. Nariadenie zaručuje vysokú ochranu pred zneužitím citlivých informácií.
- Určuje nielen spôsob, akým majú byť dáta zbierané, uchovávané a chránené, ale aj vysoké pokuty v prípade ich úniku či krádeže.

Ochrana osobných údajov a súkromia v školstve

- Školské zariadenia pri poskytovaní výchovy a vzdelávania spracúvajú osobné údaje rôzneho druhu a rozsahu. Od základných osobných údajov (napríklad meno, priezvisko, dátum narodenia, bydlisko, kontaktné údaje) môže v niektorých prípadoch dochádzať k spracúvaniu osobitnej kategórie osobných údajov – napríklad údaje týkajúce sa zdravia žiaka. Práve z týchto dôvodov sa na školy a škôlky vzťahuje nariadenie GDPR, ktoré sa uplatňuje v praxi od 25. mája 2018.
- Medzi údaje, ktorým nariadenie GDPR poskytuje ochranu nepatria len osobné údaje žiakov ale aj ich rodičov, prípadne zákonných zástupcov a ďalších blízkych osôb, ďalej tiež osobné údaje pedagógov a uchádzačov o zamestnanie, či študentov na praxi. Medzi kategórie osobných údajov, ktoré sa v školskom prostredí spracúvajú môžeme radiť nielen základné údaje, ale aj informácie o prospechu žiaka, či dokonca aj údaje týkajúce sa jeho mentálnej úrovne (vrátane výsledkov psychologickej diagnostiky).

Ochrana zariadení a dát

- V dnešnej dobe sú údaje (a predovšetkým osobné údaje) hlavnou komoditou. To znamená, že všetci musíme urobiť, čo je v našich silách, aby sme si svoje osobné údaje chránili pred každým, kto by mohol počúvať a zneužiť tieto údaje nesprávnym spôsobom.

- Každá oprávnená osoba je povinná zachovať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Preto by sme mali mať zariadenia a v nich dôležité a citlivé informácie chránené heslom.

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

Čo by malo spĺňať dobré heslo?

- **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** – minimálne 8 znakov, ideálne 16 a viac. Dobrou možnosťou sú bezpečnostné frázy.

- **Obsahuje čísla, veľké a malé písmená a špeciálne znaky** – v hesle použiť aj špeciálne znaky napr. €, %, *, #, @. Avšak nemali by nahrádzať znaky, na ktoré sa tradične podobajú (teda nahrádzať „a“ za „@“; „e“ za „3“ a pod.).

Čo by malo spĺňať dobré heslo?

- **Je tajné** – pozná ho len samotný používateľ.

- **Nedá sa ľahko uhádnuť** - nemalo by ísť o číselné rady „123456“ alebo jednoduché slová ako „heslo“. Útočníci, ktorí používateľa poznajú, dokážu ľahko uhádnuť kombináciu údajov o používateľovi (menopriezvisko19XX, mená detí, obľúbená postava či fráza z filmu...).

- **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 (napr. „To čo zješ, t8 ti už ni%to nevezme“ – je dostatočne dlhá, obsahuje veľké aj malé písmená, medzery, čísla, špeciálny znak a je ľahko zapamätateľná).

Zálohy a aktualizácie

Prečo treba zálohovať dáta?

- Odpoveď je jasná. Všetko sa kazí a tak sa aj médium na ktorom máte svoje dáta môže pokaziť. Pri poruche je stále riziko straty údajov, nech už sú uložené na pevnom disku, USB kľúči alebo na CD/DVD.

- Zálohovať treba, aby ste nenávratne neprišli o jedinečné dáta, napríklad fotky detí ako rástli, zábery zo svadby, spomienky na dovolenku, dôležité dokumenty, tabuľky, pesničky, filmy...

Zálohy a aktualizácie

Prečo sú aktualizácie dôležité?

- Nové funkcie, zlepšenie výkonu, príjemnejší vzhľad, jednoduchšie ovládanie.

- Okrem toho aktualizácie plnia ešte jednu veľmi dôležitú úlohu. **Opravujú chyby** v operačných systémoch, softvéroch a aplikáciách, **ktoré by mohli hekeri zneužiť**.

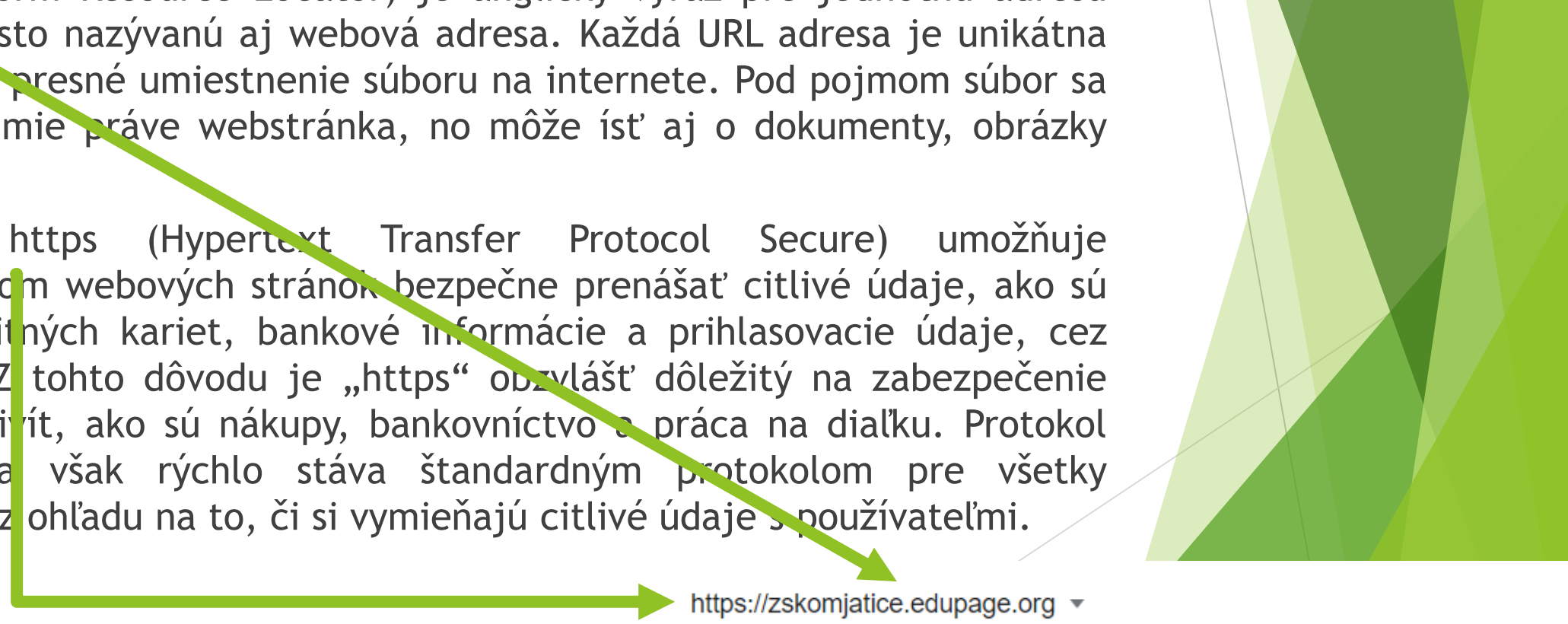
- Množstvo kyberútokov sa deje práve vďaka „dieram“ v softvéroch, cez ktoré hekeri do počítača či iného zariadenia „prepašujú“ malware.

Bezpečnosť internetového 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 mal prejsť každý z nich.
- Viaceré populárne prehliadače majú zabudovanú možnosť „Safe Browsing“, ktorá používateľa chráni pred phishingovými útokmi (snaha útočníkov ukradnúť prehlasovacie mená, heslá a 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 túto funkciu aktivovať v sekcii „nastavenia“.

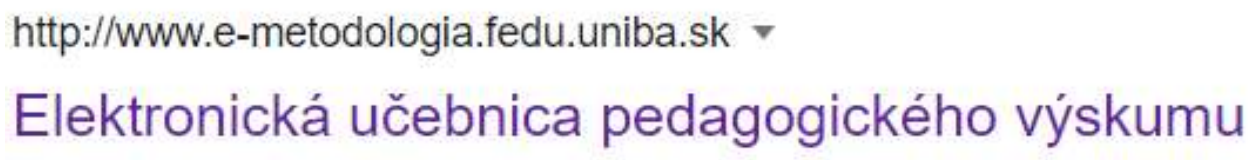
Ako rozoznať ne/bezpečný web?

- V prvom rade by si používateľ mal všímať, či je jeho komunikácia s daným webom zabezpečená šifrovaním. Môžeme to zistiť pri pohľade na URL adresu, ktorá by sa mala začínať „https://“.
- **URL** (Uniform Resource Locator) je anglický výraz pre jednotnú adresu zdroja, často nazývanú aj webová adresa. Každá URL adresa je unikátna a popisuje presné umiestnenie súboru na internete. Pod pojmom súbor sa často rozumie práve webstránka, no môže ísť aj o dokumenty, obrázky či videá.
- Protokol https (Hypertext Transfer Protocol Secure) umožňuje používateľom webových stránok bezpečne prenášať citlivé údaje, ako sú čísla kreditných kariet, bankové informácie a prihlasovacie údaje, cez internet. Z tohto dôvodu je „https“ obzvlášť dôležitý na zabezpečenie online aktivít, ako sú nákupy, bankovníctvo a práca na diaľku. Protokol „https“ sa však rýchlo stáva štandardným protokolom pre všetky servery bez ohľadu na to, či si vymieňajú citlivé údaje s používateľmi.

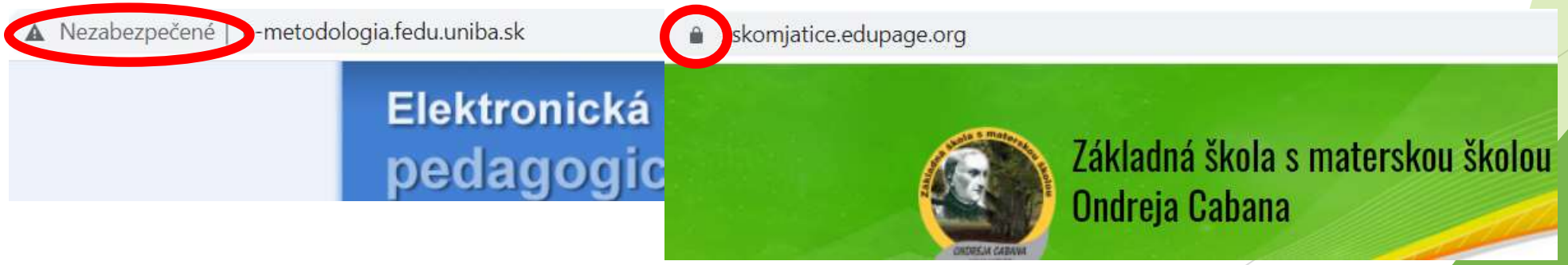


„http://“ vs. „https://“

- 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, umožňuje tak útočníkovi odchytávať ich a čítať.



- Ľahko po spoznáme a spozorujeme na akejkoľvek stránke, hneď po jej zobrazení a načítaní v hornom riadku, kde URL adresu píšeme.



Najčastejšie formy útoku cez prehliadač

Najčastejšie sa používateľ vo svojom prehliadači stretne s týmito formami útoku:

- pokusmi o phishing,
- sociálnym inžinierstvom,
- infekciou malvérom.

Phising

Používajú ho útočníci na zber citlivých údajov, pričom sa vydávajú za dôveryhodnú stránku, organizáciu, službu či osobu. Útočníkov e-mail alebo web sa môže nápadne podobať napríklad na stránky sociálnej siete, e-mailovej služby alebo internetbankingu, prípadne sa vydávať za e-shop.

Najčastejšie riziká phisingu:

- krádež peňazí z bankového účtu,
- krádež účtov na sociálnych sieťach,
- krádež identity na podvod,
- poškodenie reputácie,
- únik osobných údajov,
- obmedzenie prístupu k dátam.

Sociálne inžinierstvo

Je to snaha útočníka manipulovať obeť, aby sa dostala na nebezpečnú či falošnú stránku, kde z nej môže útočník vylákať citlivé údaje, či prinútiť ju, aby si nainštalovala nechcenú/nebezpečnú aplikáciu alebo iný škodlivý softvér.

Ako funguje sociálne inžinierstvo:

- útočník zhromažďuje informácie,
- buduje vzťah a dôveru s obeťou,
- využije dôveru,
- využije informácie vo svoj prospech.

Malvér

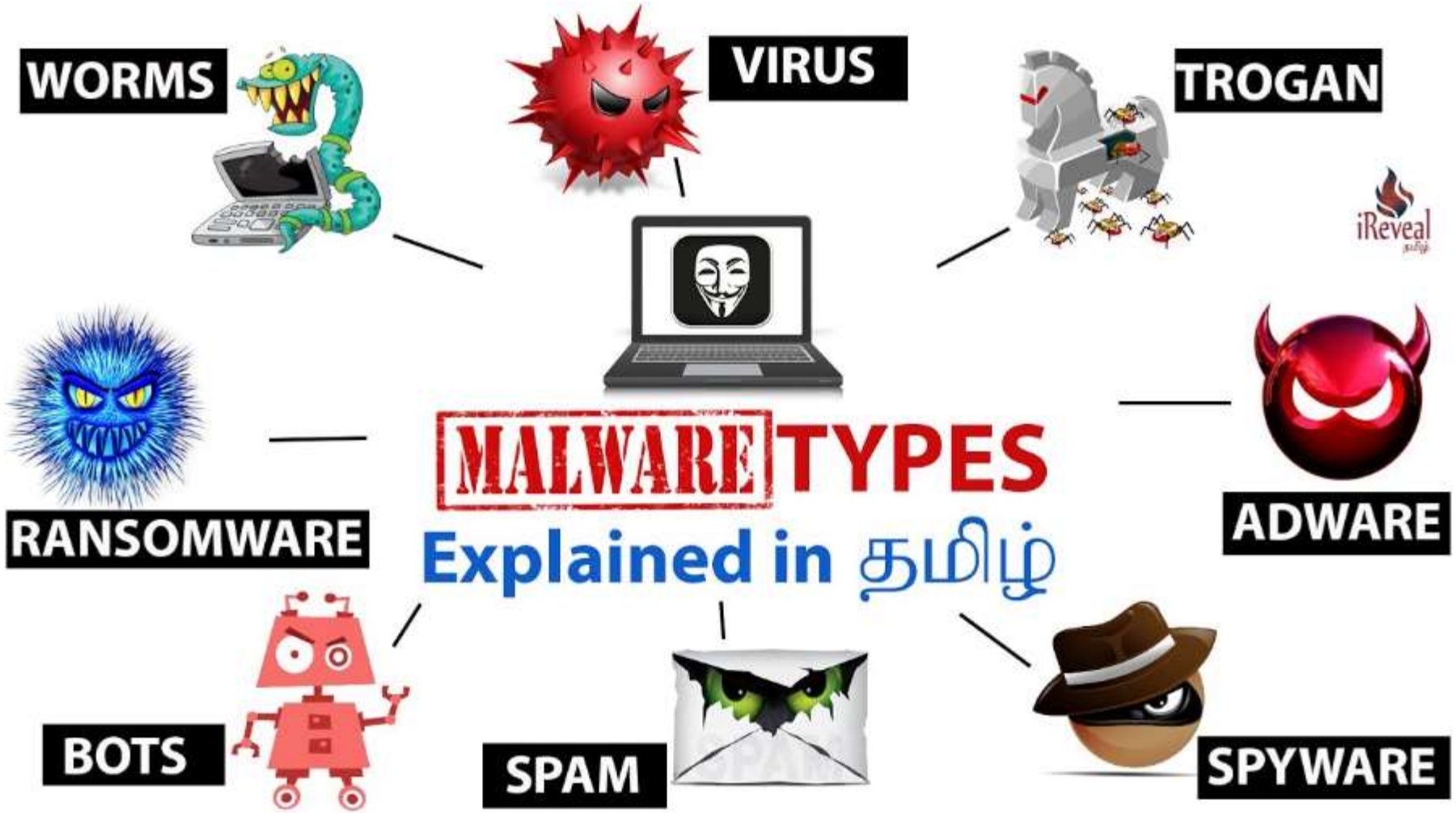
V doslovnom preklade do slovenčiny znamená „škodlivý softvér“.

Malvér zahŕňa všetky druhy škodlivého softvéru vrátane najznámejších foriem, ako sú:

- **trójske kone**,
- **ransomware**,
- **adware**,
- **vírusy**,
- **červy** a
- **bankový malvér**.

Spoločným menovateľom všetkého, čo spadá pod termín malvér, je nekalý úmysel jeho autorov alebo prevádzkovateľov.

Typy malvérov



Jazyk stránky a podozrivý obsah

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

- Podozrivé je aj to, keď stránka požaduje priveľa citlivých informácií ešte predtým, než je jasné, o aký tovar či službu máme záujem. Ak narazí používateľ na podobný prípad, je pravdepodobné, že ide o podvod.

Digitálne občianstvo

- Podstatou digitálneho občianstva je bezpečné a vedomé používanie technológií a internetu.
- V strede záujmu je človek a jeho digitálne zručnosti.
- Vďaka technologickým inováciam sa v posledných rokoch mnohé oblasti presunuli do digitálneho priestoru.
- Digitálne občianstvo zahŕňa širokú škálu aktivít, od vytvárania obsahu online, cez jeho prijímanie, zdieľanie, hranie, socializáciu, učenie či prácu.

Digitálne občianstvo

- Rovnako ako sme občanmi krajiny vo fyzickom svete, postupne sa nimi stávame aj v tom digitálnom. Prináša to mnohé výhody, ako je nonstop dostupnosť služieb, ušetrený čas, ktorý by sme inak strávili čakaním na úradoch, ušetrené zdroje, ktoré by štát vynaložil na úradníkov, ale aj nižšia chybovosť a neúnavnosť automatizovaných systémov.

- Občania vďaka elektronizácii nemusia úradom opakovane poskytovať svoje údaje, nakoľko sú dostupné v centralizovaných systémoch štátu. Digitalizované služby úradov tiež zjednodušujú administratívne úkony (napr. prepis vozidla, zmena adresy...). Občania tak z domu môžu vyplniť online formulár, podpísať ho vďaka čipu v občianskom preukaze a kliknutím ho zaslať úradníkom.

Digitálne občianstvo

- Centralizácia a automatizácia majú aj tienistú stránku. Aj pri IT systémoch môžu nastať výpadky, či obdobia, kedy budú systémy preťažené, čo môže obmedzovať služby.

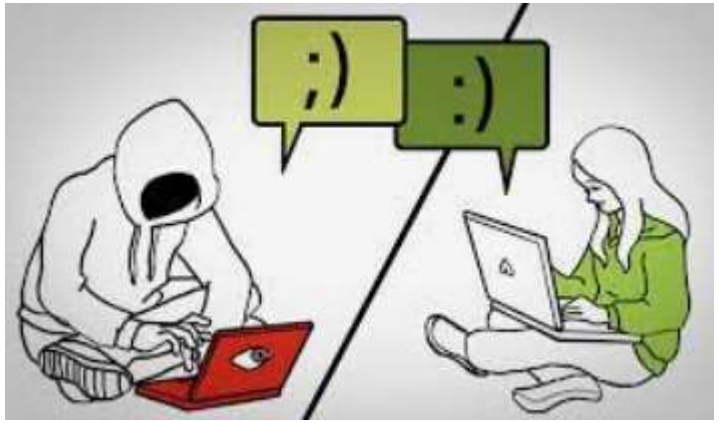
- Ďalším rizikom je, že systémy nebudú dostatočne chránené a zabezpečené pred útokmi zvonka, čo môže umožniť únik citlivých dát.

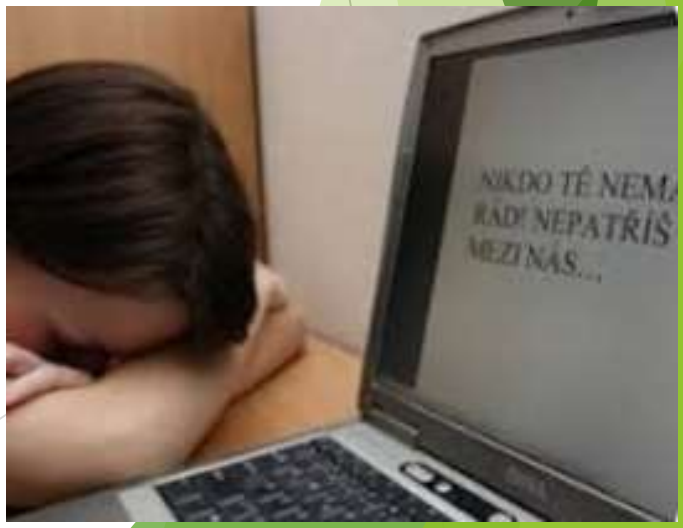
Na internete zodpovedne

Aj pri používaní internetu platí zlaté dobré pravidlo „Internet je dobrý sluha, ale zlý pán“. Využívajme digitálne prostriedky s mierou, správajme sa na internete zdvorilo, vyjadrujme sa slušne a hlavne zodpovedne!

- http://sk.sheeplive.eu/fairytales/zodpovedne
- http://sk.sheeplive.eu/fairytales/korunka-krasy

Kyberšikanovanie





Kyberšikanovanie

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

- Ak dochádza ku kynberšikanovaniu, obeť je často zároveň šikanovaná aj v offline prostredí. Kyberšikanovanie teda nie je odtrhnuté od reality zažívanej tvárou v tvár, útočníci majú v digitálnych nástrojoch len ďalšie možnosti, ako ublížiť obeti.

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

Základné znaky kyberšikanovania

- **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.

- **Opakované ubližovanie.** Jednorazový agresívny čin tvárou v tvár sa väčšinou nepovažuje za šikanovanie. Pri kyberšikanovaní je to zložitejšie, nakoľko napr. na sociálnej sieti môže byť zdieľaný aj jeden zosmiešňujúci príspevok, ktorý môže byť podporený „lajkmi“, zosmiešňujúcimi komentármi, či následným rozposielaním ďalším používateľom.

Základné znaky kyberšikanovania

- Agresor môže byť **jedno dieťa,** ale aj **skupina detí.**
- Ide o **zámer** dnému alebo viacerým osobám.
- Vzniká **v dyn** hre je nielen obeť a útočník, ale liadajúci, ktorí sú pre útočníka zdr (obdiv, povzbudenie, odmietnutie, obeť sú svedkami zahanbenia.
- Kyberšikanova iné fyzické či psychické týranie **porušovaním práv dieťaťa.**

Formy kyberšikanovania

- ***SMS správy, rýchle 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 a urážlivé komentáre*** – vyjadrenie súhlasu so škodlivým a ubližujúcim obsahom, čiže pridanie sa na stranu agresora.

- ***Happy slapping***, tiež známe ako „fackovanie pre zábavu“. Ide o nový typ ubližovania, ktorý spája šikanovaie tvárou v tvár s kyberšikanovaním. Agresor fyzicky napadne obeť a celé to nahráva na mobilný telefón. Následne nahrávku zverejní na internete a rozpošle rovesníkom. Agresormi býva často skupina. Efekt tejto formy agresie je pre psychiku obete devastujúca.

Spôsoby kyberšikanovania

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 a/alebo vulgárny text. Prevaha a obsah týchto správ púta pozornosť obete, ktorá s nimi nesúhlasí a nevie ich brať na ľahkú váhu.
- **Zastrašuje a vydiera obeť,** napríklad tak, že sa nabúra do jej profilu na sociálnej sieti, zmení heslo a profil následne zneužije. Môže tak zmeniť pôvodné správy, zverejňovať nevhodné príspevky, komunikovať s kontaktmi v mene obete... Takýto „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.

Spôsoby kyberšikanovania

- **Očierňuje či ohovára obeť -** šíri klebety a poškodzujúce klamstvá s cieľom poškodiť dobré meno obete.
- **Zámerne vylučuje obeť z online komunity**, či už na sociálnych sieťach, v četových miestnostiach alebo v diskusiách. Takéto vylúčenie 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 (spamovaním, posielaním fotografií, správami, „lajkmi“, prezváňaním...) 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.

Kyberšikanovanie vs. ubližovanie tvárou v tvár

- **Pocit anonymity u agresorov uvoľňuje zábrany a spôsobuje väčšiu krutosť**. V prostredí internetu sa človek cíti anonymný, akoby sa mohol vydávať za inú osobu a bol nepostihnuteľný.

- **Kyberšikanovanie zastihne obeť kdekoľvek.** Kým ubližovanie tvárou v tvár je viac-menej viazané na určité miesta, a teda aj viac predvídateľné, pri kyberšikanovaní sa cez digitálne nástroje dá ublížiť hocikde, hocikedy a mnohonásobne viac.

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

Kyberšikanovanie vs. ubližovanie tvárou v tvár

- **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 ho videl... Rozmery publika kyberšikanovania je nemožné odhadnúť, keďže obsah je možné ukladať do digitálneho sveta a znovu preposielať.

- **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.

Strata zábran v prostredí internetu

- **Často prebieha s pocitom anonymity a nepostihnuteľnosti.**

- **Sťažuje empatiu.** Pokiaľ ide 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, 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 ponechá voľný priechod emóciám, túžbam a správaniu, ktoré by inak bežne tlmilo jeho/jej svedomie.

Dizinhibičný efekt

„prílišná online uvoľnenosť“

Ide o ***znižovanie zábran a opatrnosti*** ľudí na internete z dôvodu pociťovania anonymity.

Práve táto uvoľnenosť je dôvodom, pre ktorý sú ľudia v komunikácii online ***odvážnejší ale 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** - trolling, nenávistné prejavy online (cyberhate)
- **Systematickou formou ubližovania** – kyberšikanovanie (cyberbullying) či prenasledovanie online (cyberstalking)

Aktivita - Džin

- Na internete komunikujeme s ľuďmi odlišne, už len preto, že sa na človeka nepozeráme tvárou v tvár, ale len cez displej, kde vidíme len jeho meno či fotografiu. To že reálne človeka nevidíme, uvoľňuje naše zábrany. Človek sa ľahko odviaže a neraz povie aj to, čo by sa inému do očí nikdy neodvážil povedať. Táto strata zábran má svoje prínosy aj riziká.

- https://www.kybersikanovanie.sk/index.php/filmy/kybersikanovanie-zatocme-s-nim-spolocne

- Teraz zapojte trochu svojej fantázie a v skupinách nakreslite stratu zábran na internete ako postavu - superhrdinu/superzloducha – ako džina, ktorý sa dostal z fľaše von.

Trolling

- Pojem **trolling** alebo **trolovanie** bol do internetovo-informatického slangu prevzatý nie náhodne. Zákernosť, snaha škodiť, ubližovať boli typickými povahovými vlastnosťami pripisovanými trollom, že sa stali úplne logicky symbolom tohto fenoménu.
- 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.**
- **Pre trolla je cieľom získanie pozornosti a pocitu moci.** Pre používateľa je preto najlepšie, ak ju trollovi neposkytne.

Trolling

Troll je označenie škodlivého používateľa, ktorý:

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

Trolling

V prípade kontaktu s trollom platí hlavná **základná zásada:**

NEREAGOVAŤ v rámci diskusie, nekomentovať, nevysvetľovať, nezapájať sa...

- Nezapájajte sa do podobných diskusných fór – uvedomte si, že ich zakladateľom resp. pisateľom poburujúcich reakcií je obvykle človek, ktorý presne tento efekt chce dosiahnuť – chce vyvolať čo najbúrlivejšie reakcie.
- Každý prejav oprávneného pobúrenia, vyslovenie nesúhlasu vyvoláva okamžité a obvykle neadekvátne reakcie druhej strany.
- Nikdy sa nesnažte vnášať do takejto diskusie kvalifikovaný názor – aj keď akokoľvek rozumiete problematike obvykle sa to obráti proti Vám.

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 diskriminuje, hanobí alebo sa snaží vylúčiť iných pre ich príslušnosť k rase, etniku, jazyku, národu, národnosti, farbe pleti, náboženskej viere, pohlaviu, rodovej identite, sexuálnej orientácii, politickému presvedčeniu, veku, mentálnemu či fyzickému zdraviu.

- **Nenávistné prejavy sú nekorektné**, ale v porovnaní s trollingom sú vážnejšie tým, že **porušujú ľudské práva a slobody, diksriminujú** a preto môžu byť kvalifikované ako **priestupok** alebo **trestný čin**.

Cyberhate

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.

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,
- ako byť aktívnym používateľom internetu a správne reagovať na cyberhate.

Aktivita – veselo, smutno

Na lístočky napíšte čo najviac situácií, zážitkov, udalostí, ktoré kamaráta/kamarátku potešia, alebo rozsmútia, nahnevajú na internete.

- Z akých zážitkov na internete môžu byť ľudia smutní/nahnevaní?
- Z akých zážitkov sa ľudia na internete tešia?
- Je viac dobrých či zlých zážitkov na internete?
- Ako môžeme zabrániť tomu aby mal niekto na internete zlý zažitok?
- Ako pomôcť tomu, aby mali deti na internete viac dobrých ako zlých zážitkov?

Ako rozpoznať, že je dieťa šikanované

Kyberšikanovanie je pre dieťa výrazným stresom, spôsobuje úzkosť, depresívne emočné ladenie, strach, pocit 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, vyhýbanie sa spoločnosti...
- ***V správaní dieťaťa niečo ubudne*** **-** obmedzenie kontaktu s rovesníkmi, záujmov, činností, uzatváranie sa do seba, horší prospech a správanie...
- ***V správaní dieťaťa niečo pribudne*** **-** riskantné aktivity, užívanie návykových látok, sebapoškodzovanie, záškoláctvo...
- ***Stresové reakcie pri používaní počítača, smartfónu***

Ako zakročiť proti kyberšikanovaniu

- **Naučiť deti, čo je šikanovanie a kyberšikanovanie**
  - Naučiť deti rozpoznať hranice medzi zábavou a šikanovaním.
  - Naučiť deti, ako znížiť riziko šikanovania a kyberšikanovania.
- **Naučiť deti, ako postupovať, keď sa stretnú so šikanovaním a kyberšikanovaním**
  - Deťom odporučiť konkrétne osoby, na ktoré sa môžu obrátiť v prípade problémov, ako sú rodičia, súrodenci, rovesníci pre emocionálnu podporu, alebo učitelia informatiky pre technickú podporu.
- **Aktivizovať deti k pomoci slabšiemu**
  - Deťom pomáhať rozvíjať schopnosť aktívne brániť seba a iných pri ubližovaní.

Ako zakročiť proti kyberšikanovaniu

- **Zlepšiť sociálne zručnosti detí, podporiť ich sebaobraz a empatiu**
  - Deťom môžeme pomôcť tým, že ich naučíme rozoznávať vlastné pocity, aby vedeli byť citlivé voči vlastnému prežívaniu aj prežívaniu iných.
  - Pomôcť deťom zlepšiť ich sebaoobraz a sociálne zručnosti, aby si vedeli vytvárať a udržiavať zdravé vzťahy.
  - V triede podporiť hodnoty kamarátstva , prijatia a spolupatričnosti.
- **Podporiť u detí zručnosti bezpečného používania internetu**
  - Vysvetliť deťom, ako sa lepšie chrániť pomocou technických prostriedkov.
- **Uistiť deti o tom, že je dobrým krokom zdôveriť sa**
  - Vysvetliť deťom, že o probléme sa môžu zveriť dospelým, ktorý vedia v danej situácii pomôcť.

Aktivita – čo deti vidia, to opakujú

- https://www.kybersikanovanie.sk/index.php/filmy/co-deti-vidia-to-deti-opakuju

- Neznamená to, že všetko, čo sa niekedy naučili, je len zlé. Aj schopnosť kričať, brániť sa pred útokmi alebo prejaviť hnev je dôležitá – slúži nám na to, aby sme prežili v ťažkých situáciách a ubránili si svoje hranice.
- Čo ste sa naučili od rodičov, čo od kamarátov?
- Od koho iného ste sa ešte učili?
- Kedy je ktoré správanie užitočné a pomáha vám?
- Čo si myslia, že sa niekto učí od vás?

Aktivita – dokonči príbeh

- Na pracovnom liste sú dva príbehy kyberšikanovania, jeden z pohľadu obete, jeden z pohľadu agresora.
- Vašou úlohou je napísať spoločne, ako sa príbeh bude ďalej rozvíjať a ako skončí.

- Bolo ťažké vymyslieť, ako by príbeh pokračoval ďalej?
- Aký koniec príbehu ste vymysleli – dobrý alebo zlý a prečo? Chceli ste, aby to skončilo dobre alebo nie?
- Poznáte podobné príbehy zo skutočného života?
- Viete si predstaviť, že by ste sa dostali do podobnej situácie? Ako by ste sa zachovali?
- Čo by ste spravili, ak by postava z príbehu bol/a váš kamarát/ka?

Digitálna bezpečnosť

Bezpečné vyhľadávanie a surfovaie na internete

- **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.**

Bezpečnostné riešenie - antivírus

- Moderné bezpečnostné riešenia sa nezameriavajú len na ochranu pred vírusmi, ale aj pred obrovským množstvom iných škodlivých kódov a aktivít.

- 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.

Ako si vybrať správne bezpečnostné riešenie?

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.

Ako si vybrať správne bezpečnostné riešenie?

- **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. Niektoré bezpečnostné programy pritom ponúkajú takzvané skúšobné lehoty, pričom si ich používateľ môže nainštalovať a používať ich niekoľko týždňov či mesiacov bezplatne.

Bezpečné internetové pripojenie (internetová sieť)

- 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.

- Pokiaľ je to možné, používateľ by sa mal pripájať na siete, ktorých správcu pozná, alebo vie niečo o ich bezpečnostnom nastavení.

Bezpečné internetové pripojenie (internetová sieť)

- 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.

- 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 ***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.

Infikovaný prehliadač

Cez prehliadač si môže používateľ stiahnuť aj **malvér.** Ten sa môže online šíriť rôznymi spôsobmi.

K infekcii cez prehliadač, dôjde najčastejšie cez:

- **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.

- **Tzv. man-in-the-browser útok** (útočník v prehliadači), 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.

Internet je voľne rozdelený do 3 oblastí podľa toho, ako dostupné sú informácie:

- Povrchový web
- Deep web
- Dark web

Povrchový web

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

- Je to oblasť internetu, ktorú väčšina z nás pozná, ide o verejne prístupné webové stránky.

Deep web – hlboký web

- Sú to oblasti internetu, ktoré sú skryté pred verejnosťou, ale nie sú určené na zákernú činnosť.
- Ide o časť internetu „skrytú pod povrchom“, ak použijeme metaforu s ľa ra. O
- N sú d im 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 – temný web

- J… pod h…
- P… itu.
- N… ovať špeciálny softvér.

- 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.

Nelegálna činnosť na internete

- Ako sme si už spomenuli v časti 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 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.

Nelegálne sťahovanie obsahu

- ***Pri sťahovaní*** filmov/seriálov z úložísk či pri zdieľaní s veľkou skupinou neznámych ľudí 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***.

- ***Nainfikovať*** sa škodlivým kódom alebo skončiť na nebezpečnej stránke môže používateľ aj ***pri sledovaní seriálov a filmov na bezplatných streamovacích službách***. Tie sú známe obrovským počtom reklám, z ktorých niektoré môžu viesť k škodlivému webu či kódu.

- ***Sťahovanie*** nelegálneho obsahu má aj ***právne riziká***. Ak používateľa úrady prichytia s pirátskou kópiou, môže byť potrestaný. V niektorých prípadoch ide o mimoriadne ***vysoké pokuty***.

Stream

- je doručovanie audio a video súborov klientovi zo servera cez internet.
- je technológia, ktorá nepretržite prenáša audiovizuálny obsah medzi zdrojom a koncovým užívateľom. Dáta sú streamované (prenášané, vysielané) prostredníctvom elektronickej siete.

Autorské práva

- chráni výsledky tvorivej duševnej činnosti autorov (fyzických osôb) - **diela**, ktoré sú z umeleckej alebo vedeckej oblasti, ako napr. slovesné diela, diela výtvarného umenia, fotografické diela, hudobné diela, audiovizuálne diela, divadelné diela, architektonické diela. Chránené sú aj počítačové programy.
- Na označenie diela, ktoré je chránené autorským právom je možné použiť znak „©"(používa sa najčastejšie v spojení s menom autora a rokom vytvorenia diela). Toto označenie má však len informatívny význam (nevyplýva zo zákona, nie je povinnosť ho používať) a dielo je plne chránené aj bez tohto označenia. Treba mať preto na pamäti, že označenie diela týmto znakom ochranu autorským právom **nezakladá**.

Film – Cyberbully (2015)

https://film.kukaj.io/cyberbully

Zoznam zdrojov a použitej literatúry:

- https://www.statpedu.sk/files/sk/o-organizacii/projekty/projekt-dvui/publikacie/zakladna_digitalna_gramotnost.pdf
- http://www.zssosbs.edu.sk/zaloha/Informa/zaklpoj.htm
- http://skola.dvp.sk/co-je-informacia/
- https://uniba.sk/fileadmin/ruk/ak/ig-vyhladavanie.pdf
- https://slideplayer.cz/slide/14571050/
- https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_sk.htm
- https://www.osobnyudaj.sk/sluzba/12-gdpr-pre-skoly-a-skolky
- https://www.ssl.com/sk/Naj%C4%8Dastej%C5%A1ie-ot%C3%A1zky/%C4%8Do-je-https/

Zoznam zdrojov a použitej literatúry:

- https://www.cas.sk/clanok/2733911/kedy-pride-koniec-sveta-tieto-sialene-apokalypticke-predpovede-vydesili-ludstvo-mate-oblubenu/
- https://www.eset.com/sk/malver/
- https://gdpr-slovensko.sk/co-je-gdpr/
- https://www.websupport.sk/blog/2017/08/najpopularnejsie-stranky-na-zdielanie-suborov/
- https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html
- https://support.microsoft.com/sk-sk/topic/%C4%8Do-je-kybernetick%C3%A1-bezpe%C4%8Dnos%C5%A5-8b6efd59-41ff-4743-87c8-0850a352a390
- https://digiq.sk/temy/digitalne-obcianstvo/
- http://pcsluzba.sk/ako-zalohovat-subory.html
- https://preventista.sk/info/nekrmte-trollov/

Zoznam zdrojov a použitej literatúry:

- https://sk.wikipedia.org/wiki/Aktualiz%C3%A1cia
- https://www.lexika.sk/blog/bezpecne-online-pravidelne-aktualizacie/
- https://bezpecnenanete.eset.com/sk/
- https://sk.martech.zone/types-clear-deep-dark-web/
- https://www.dusevnevlastnictvo.gov.sk/web/guest/autorske-pravo
- https://www.kybersikanovanie.sk/index.php/filmy/kybersikanovanie-zatocme-s-nim-spolocne
- https://zskomjatice.edupage.org/
- http://www.e-metodologia.fedu.uniba.sk/