METIS o.z.

BEZPEČNOSŤ NA INTERNETE

–

METODIKA

Určená pre deti vo veku 10 – 12 rokov

Digitálna koalícia

Obsah

1. ÚVOD

Táto metodika je určená pre učiteľov ako praktická pomôcka pri práci so žiakmi v oblasti jednotlivých tematických okruhov. Jej cieľom je poskytnúť jasné usmernenie, ako viesť vyučovanie, podporiť aktívne zapojenie žiakov a zároveň im pomôcť lepšie porozumieť preberaným témam.

Metodika ponúka návrhy postupov, odporúčania a konkrétne aktivity, ktoré môže učiteľ flexibilne prispôsobiť podľa veku žiakov, ich potrieb a úrovne znalostí. Slúži ako opora pri plánovaní aj realizácii vyučovacích hodín, pričom ponecháva priestor pre vlastnú kreativitu a pedagogický prístup.

Súčasťou metodiky je aj možnosť využitia sprievodnej prezentácie, ktorá môže podporiť vizuálne vnímanie a zrozumiteľnosť učiva. Učitelia ju môžu použiť ako doplnok k výkladu alebo ako nástroj na interaktívnu prácu so žiakmi.

Cieľom metodiky nie je striktne určovať postup, ale ponúknuť rámec a inšpiráciu, vďaka ktorým bude vyučovanie efektívne, zrozumiteľné a pre žiakov podnetné.

2. CIEĽ VZDELÁVANIA

Žiaci budú rozumieť základným pojmom – čo je to osobný údaj, prečo je dôležité ich chrániť, ako bezpečne používať sociálne siete, Wi-Fi, ako si nastaviť heslo, čo je to digitálna stopa, ako bezpečne nakupovať, kedy môže ísť o falošný e-shop, aké rôzne podvody „číhajú na internete“, aký je rozdiel medzi šikanou a kyberšikanou.

3. CHARAKTERISTIKA CIEĽOVEJ SKUPINY

Videá, prezentácia a infografiky sú určené žiakom vo veku 10 – 12 rokov, väčšina detí v tomto veku už má mobilný telefón (smartfón). Aktívne využívajú internet, využívajú rôzne hry, sociálne siete a chaty napr. WhatsApp, YouTube.

Odporúčanie: používať jednoduchý jazyk, krátke aktivity a zapájať žiakov do diskusie.

4. TÉMA - BEZPEČNOSŤ NA INTERNETE - ZÁSADY

OSOBNÉ ÚDAJE (čo sú osobné údaje, aby sme pochopili podstatu, prečo je dôležité ich chrániť).

Cieľ	Žiak rozumie, čo sú osobné údaje a prečo ich treba chrániť.
Priebeh hodiny **Úvod (5 min)**	Otázky: Čo všetko o sebe zdieľaš na internete? Vie niekto cudzí, kde bývaš?
Vysvetlenie (10 min)	Osobný údaj = informácia, podľa ktorej vieme určiť konkrétnu osobu. Príklady: meno, fotografia, adresa, škola
Aktivita (15 min)	“Patrí / Nepatrí na internet” Učiteľ číta situácie, žiaci rozhodujú a vysvetľujú.
Diskusia (10 min)	Prečo je nebezpečné zdieľať adresu? Kto všetko môže vidieť tvoje údaje?
Záver (5 min)	3 pravidlá: nezdieľam citlivé údaje, premýšľam pred zverejnením, keď si nie som istý, opýtam sa

4.1. OSOBNÉ ÚDAJE (čo sú osobné údaje, aby sme pochopili podstatu, prečo je dôležité ich chrániť).

Otázky do publika:

- *Kto z vás má mobil ?*
- *Kto používa internet každý deň ?*
- *Kto má sociálne siete alebo hrá online hry ?*

Cieľ: uvedomenie si, že všetci sú súčasťou online sveta.

Prechodová veta:
„Keď sme online každý deň, musíme vedieť, čo vlastne chránime.“

Vysvetlenie pojmu osobný údaj:

Keďže si chceme hovoriť, o bezpečnosti na internete tak potrebujeme vedieť, čo chceme chrániť, čo sú osobné údaje.

Otázka na deti:
Viete čo sú osobné údaje ?

Osobné údaje sú informácie, na základe ktorých sa dá zistiť kto ste. Predstavte si to ako skladačky, čím viac skladačiek máte tým viac informácií o sebe máte.

4.2. Čo všetko môže byť osobný údaj ?

- meno, priezvisko, adresa, e-mail, fotografia, telefónne číslo ....

4.3. Prečo sú dôležité tieto osobné údaje ?

- sú len tvoje a identifikujú ťa, na základe týchto informácií o tebe, ťa vedia ostatní identifikovať,
- týmito údajmi sa vieš prihlásiť do hier, do svojho počítača, telefónu, preto je potrebné ich chrániť.

4.4. Kde sa osobné údaje objavujú ?

- v súčasnej dobe ti stačí internet a tam nájdeš veľa informácií o rôznych ľuďoch, osobné údaje sú všade, preto je potrebné ich chrániť aby neboli zneužité.

4.5. Aké osobné údaje na internet nepatria ?

- na internet nepatria osobné údaje intímneho charakteru, dehonestujúce fotografie, sú to napr. fotky, za ktoré by som sa hanbil, adresa a presné miesto bývania, školy, krúžkov, telefónne číslo, heslá, informácie o rodine, priateľoch čokoľvek čo nechcem aby videli cudzí ľudia

4.6. Ak, si nie som istý či tieto informácie patria na internet, položím si tieto otázky:

- **Hanbil by som za tieto informácie ?**
- **Ukázal by som ich naozaj každému ?**

HESLÁ

- Prečo ich používať.
- Ako si vytvoriť dobré heslo.
- Využívanie 2 faktoru.
- Chcem používať heslá, neviem si ich zapamätať – password manager, výhody.
- Ako si overím či bolo moje heslo prelomené alebo hacknuté.

Cieľ	Žiak chápe význam silného hesla a vie, ako ho vytvoriť.
Priebeh **Úvod**	Otázka: Používa niekto rovnaké heslo všade?
Vysvetlenie	Silné heslo: • má viac znakov • obsahuje písmená, čísla • nie je jednoduché (12345, meno)
Aktivita	Žiaci vytvoria "najlepšie heslo" (bez zdieľania reálneho hesla).
Záver	• heslo nikomu nehovorím • nepoužívam jedno heslo všade

4.7. HESLÁ

Otázky pre deti:
Zdvihnite ruku, kto z vás používa telefón (smartfón), kto má svoj počítač, tablet ?

Deti reagujú. Prihlási sa cca 80% - 90% detí v triede.

Máte mobil/počítač/tablet voľne dostupný alebo ho máte chránený ?

Deti reagujú. Hlásia sa či majú tieto zariadenia.
Ak deti povedia, že majú svoje zariadenia zaheslované, resp., ak používajú heslo poďme sa pozrieť ako by malo bezpečné heslo vyzerať.

4.8. Ako si vytvoriť dobré heslo ?

Heslo by malo mať 12 - 15 znakov, malo by obsahovať malé a veľké písmená, číslice a aj špeciálne znaky.

Poďme si spolu vytvoriť bezpečné heslo, resp. máme tu niekoľko hesiel, povedzme si, ktoré je podľa vás najbezpečnejšie.

4.9. Využívanie 2 faktorovej autentifikácie (ďalej ako „2FA“). Čo to je a prečo je to dobrý nápad ?

Mať heslo je super, je to ako mať dvere od domu zamknuté a 2FA je ako keby ste mali ešte bezpečnostný zámok. Aplikácie, ktoré využívate napríklad na chatovanie, alebo e-maily, ktoré máte tam je to možné nastaviť. Tak isto si viete nastaviť aj iné ochrany súkromia.

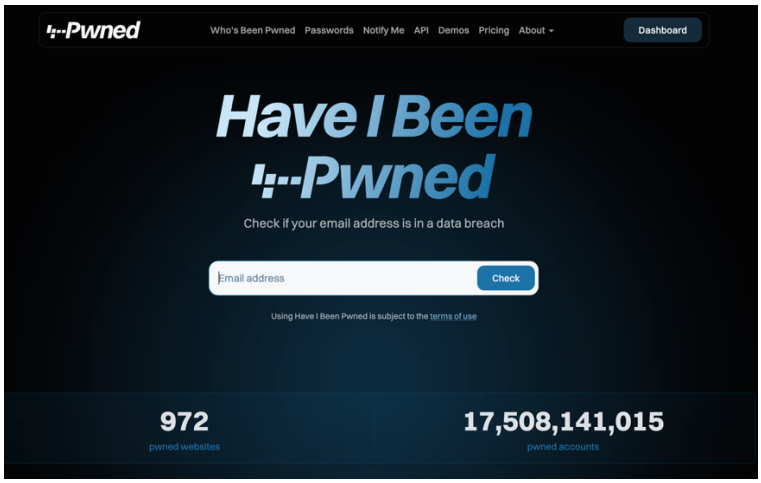
4.10. Chcem používať heslá, neviem si ich zapamätať.

V tomto prípade odporúčam mať tzv. password managera, kde si uložíte svoje heslá a pamätáte si iba jedno silné heslo. Pri password managerovi odporúčam nastaviť 2FA.

4.11. Ako si overím či bolo moje heslo prelomené alebo hacknuté ?

Sú určité obdobia kedy je viac únikov osobných údajov z rôznych mailingových služieb, alebo iných spoločností, ktoré poskytujú rôzne služby napr. sociálne siete. Či bolo vaše heslo prelomené si viete overiť na tejto webovej stránke:

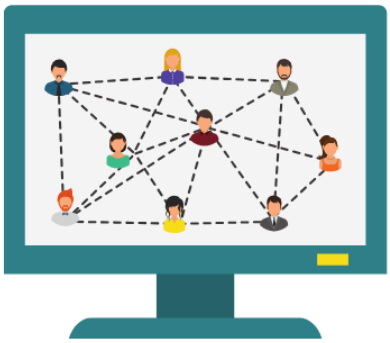
https://haveibeenpwned.com/



WIFI

Cieľ	Žiak rozumie rizikám verejných sietí.
Vysvetlenie	Nie každá Wi-Fi je bezpečná.
Aktivita	Situácia: "Som v obchodnom centre a pripojím sa na voľnú Wi-Fi." Otázky: • Je to bezpečné ? • Čo by som nemal robiť ?
Záver	• neprihlasujem sa do účtov na verejnej Wi-Fi • používam len dôveryhodné siete

- Vieme, aké sú dáta pre deti dôležité, nikdy ich nie je dosť.
- Využívanie dát prostredníctvom Wi-Fi.
- Prihlasovanie sa do verejnej Wi-Fi.
- Chcem sa prihlásiť do verejnej Wi-Fi, ako to urobiť správne.



4.12. WI-FI

Úprimne rozumiem ako je pre vás dôležité pripojenie. Ale ak si vyčerpáte dáta a chcete sa pripájať na rôzne „free Wi-Fi“ má to aj svoje ALE ....

Prihlasovanie do siete, ktorá je verejná nie je bezpečné, nakoľko môže v danom priestore sedieť útočník, ktorý by chcel vaše osobné údaje. Ako prirovnanie si predstavte, že ste v miestnosti plnej ľudí chcete niečo povedať svojmu kamarátovi a je to ako keby ste mu to hovorili cez mikrofón a všetci to počujú.

4.13. Ak, sa chcete prihlásiť do verejnej Wi-Fi, ukážme si ako to urobiť správne.

Ak sa predsa len chcete pripojiť na verejnú Wi-Fi napr. na dovolenke odporúčam Vám aspoň, aby ste používali VPN (virtuálna privátna sieť). VPN je tajný tunel, pre tvoje osobné

údaje. Ale poďme si to vysvetliť pre lepšie pochopenie. Predstavte si, že používanie VPN je ako keď posielate list v obálke. Keď sa však pripájate bez VPN je to ako keby ste posielali pohľadnicu, ktorú si môžu prečítať všetci.

DIGITÁLNA STOPA

Cieľ	Žiak chápe, že jeho správanie na internete zanecháva stopu.
Vysvetlenie	Digitálna stopa = všetko, čo na internete urobíme.
Aktivita	Otázky: Čo sa stane, keď zverejním fotku ? Dá sa vždy vymazať ? Kto ju môže vidieť ? Môže sa to použiť proti mne ?
Záver	Premýšľam pred zverejnením lebo internet si „pamätá".

4.14. DIGITÁLNA STOPA

Čo je to digitálna stopa ? Počuli ste už o niečom takom ?
Digitálne stopy predstavujú všetko, čo po sebe zanechávame online. Od osobných údajov a iných citlivých informácií až po informácie o tom, čo vyhľadávame alebo nakupujeme online. Predstav si, že je to ako stopa v snehu.

4.15. Aké poznáme druhy ?

Digitálne stopy po sebe zanechávame nie len vedome (vedome nahrávame), ale aj nevedome (napr. informácie o našej IP adrese, súbory cookie atď.). Teda dá sa povedať, že digitálne stopy o nás môžu vytvárať aj naši kamaráti/rodičia a to v prípadoch, keď o nás napríklad zverejnia informácie, napr. fotku.

4.16. Prečo je dôležité rozmýšľať čo robím na internete ?

Lebo vytváram takéto snehové stopy v online priestore. Internet si veľa pamätá. Tak isto nie všetko sa dá vymazať, a zároveň, ak nahrám nejakú fotku, môže si ju niekto stiahnuť alebo urobiť screenshot. Tak je to aj s komunikáciou v rôznych aplikáciách. Položte si otázku už pred zverejnením, či tak o 5 rokov ste s tým v poriadku, že je táto fotka na internete.

4.17. Hovorí Ti niečo právo na zabudnutie ?

Ide o právo na výmaz podľa článku 17 GDPR, môžeš napr. GOOGLE požiadať, ak tam nájdeš o sebe nejakú informáciu, ktorá už nie je aktuálna alebo ťa môže poškodiť o jej výmaz.

5. TÉMA - SOCIÁLNE SIETE

Cieľ	Žiak chápe, ako sa bezpečne správať online.
Aktivita	Situácie: - neznámy človek píše správu - niekto chce fotku Otázky: - odpísať alebo ignorovať ? - je to bezpečné ?
Záver	- nepridávam si cudzích ľudí - nezdieľam osobné informácie

Grafický prehľad (Timeline)

Rok	Sieť	Kľúčová vlastnosť
1997	SixDegrees	Prvé profily a zoznamy priateľov
2002	Friendster	Online networking
2003	LinkedIn	Profesijné prepojenie
2003	MySpace	Hudba, profily, prvá masová sieť
2004	Facebook	Globálne prepojenie, novinky (Feed)
2005	YouTube	Zdieľanie videí
2006	Twitter	Real-time správy, hashtagy
2010	Instagram	Mobilné foto/video
2011	Snapchat	Miznúce správy, Stories
2016	TikTok	Krátke video, AI algoritmus

5.1. AKÉ SOCIÁLNE SIETE POZNÁTE ?

Deti odpovedajú:

- Facebook,
- Instagram,
- TikTok,
- Whatsapp,
- Snapchat,
- YOUTUBE

5.2. Čo sú sociálne siete ?

- sú to nové médiá, konkurujú súčasným médiám (tlač, televízia), umožňujú nám ako užívateľom tzv. digitálnu interakciu (lajky, komentovanie, hodnotiť (emotikony) a zdieľať,
- my sami však môžeme byť aktívni tvorcovia šíriť svoj obsah. Je dôležité však povedať, že za to čo šírime sme zodpovední a mali by sme si overovať informácie tzv. fackcheking.

5.3. Akým spôsobom môžeme využívať sociálne siete ?

- aktívne - aktívne tvoríme nejaký obsah
- pasívne – iba sledujeme

5.4. PREČO POUŽÍVAME sociálne siete ?

Pozitívne vymedzenie
- sebaprezentácia,
- slobodné vyjadrovanie názorov a myšlienok,
- jednoduché a efektívne zdieľanie informácií,
- rýchla a jednoduchá komunikácia s ostatnými používateľmi,
- nástroj na štúdium a podnikanie,
- voľný čas - zábava.

Negatívne vymedzenie
- online podvody,
- kyberšikana,
- kyberšikanovanie, kybergrooming (nebezpečné online zoznamovanie),
- návykové správanie (netolizmus),
- šírenie hoaxov a dezinformácií,
- narušenie súkromia.

5.5. PREČO TRÁVÍME TAKÝ DLHÝ ČAS NA SOCIÁLNYCH SIEŤACH ? Prečo nás to baví, prečo je každému ponúkaný iný obsah ?

Sociálne siete prispôsobujú každému svoj obsah na mieru – tzv. personalizovaný obsah. To znamená, že každý z nás vidí niečo iné, iné sa mu zobrazuje. O tom, aký obsah sa nám zobrazí a ktorý bude skrytý, ktorý neuvidíme, rozhodujú algoritmy.

5.6. Čo sú to tie algoritmy ?

Algoritmy sú matematické vzorce a iné systémy ktoré určujú, aký obsah sa nám zobrazí na základe nášho správania, našich lajkov a iných faktorov na sociálnej sieti. Tieto algortimy využívajú umelú inteligenciu, napr. pri analýze obsahu a odporúčajú nám obsah.

Algoritmus sociálnych sietí ako sme si povedali analyzuje naše správanie v online prostredí. Aby ste vedeli, čo to znamená, povieme si to na príkladoch.
Tento algoritmus sleduje

- naše interakcie (správanie) – na čo najviac reagujme, čo sa nám páči (napr. to môžu byť príspevky o športe, módnych trendoch ...)
- naše preferencie, čo sledujeme, čo sme sledovali predtým
- popularitu obsahu – ak niektorí príspevok má veľa lajkov, zdieľaní stáva sa populárnym a algoritmus to môže vyhodnotiť, že by sa nám mohol páčiť
- časové faktory – ako dlho strávime na danom príspevku, napr. keď scrollujeme tak už ten okamih kedy sa zastavíme nad príspevkom sa zarátava ...

5.7. Prečo to takto funguje ?

Cieľom týchto algoritmov je zaistiť, aby sme strávili na sociálnych sieťach viac času a je to preto aby sa nám zobrazovalo viac reklám.

A tu sa dostávame k otázke, či sú sociálne siete zadarmo ? Často sa stretávam, že deti si radi stiahnu rôzne aplikácie, lebo sú zadarmo ...

Lenže toto je mylná predstava. Používanie sociálnych sietí nie je zadarmo. Platíme svojimi osobnými údajmi, svojím správaním, svojou interakciou. Tým, že sociálne siete majú tieto informácie vedia nám ponúkať rôzne reklamy.

Aby ste si to vedeli predstaviť, pokiaľ sa mne páči oblečenie a kozmetika tak sa mi nebudú zobrazovať informácie o autách.

Každá naša interakcia (zdieľanie, lajk, komentovanie alebo zastavenie na nejakom príspevku) je analyzované a ukladané. A tieto informácie sú použité pre reklamu.

5.8. A teraz sa poďme pozrieť na hrozby, ktoré na nás číhajú na sociálnych sieťach a na čo si je treba dávať pozor.

Tu ma zaujíma, či ste naozaj s niekedy takouto hrozbou stretli. Ak áno, skúste mi popísať, čo sa stalo, prípadne či ste to riešili s nejakou blízkou osobou (rodičom, v škole atď..)

6. TÉMA HROZBY – SOCIÁLNE SIETE

Cieľ	Žiak rozumie rizikám spojeným so sociálnymi sieťami a vie sa bezpečne správať.
Aktivita	Situácie: "Niekto, koho nepoznám, si ma chce pridať". "Niekto ma žiada o fotku". "Vidím, že všetci majú lepší život". Otázky: Čo by si urobil/a? Je to bezpečné?
Záver	- nepridávam si cudzích ľudí - nezdieľam osobné údaje - premýšľam pred zverejnením - ak mám problém, poviem to dospelému

6.1. Hrozby sú:

- **rôzne riziká spojené s únikom osobných údajov, kyberšikanou, nenávistné prejavy, nebezpečné výzvy, kybergrooming, nebezpečné zoznamovanie a iné.**

6.2. Únik osobných údajov – osobné údaje sú všetky informácie, ktoré o sebe poskytujeme pri tvorení svojho profilu, zároveň všetky informácie, ktoré o sebe poskytujem ako napr. pri rôznych príspevkoch napr. fotky z dovolenky. Čo je však nebezpečné je ak zdieľate nejaké citlivé údaje napr. nejaké intímne fotografie. Preto je dôležité aby ste rozmýšľali aké informácie poskytujete, zdieľate.

6.3. Hate-speech – alebo nenávistné prejavy. Každý z nás by si mal uvedomiť, že sociálne siete nie sú anonymné a mali by sme k sebe navzájom pri online komunikácií k sebe navzájom správať s rešpektom a úctou. Tieto prejavy môžu byť jednorazové alebo môžu vyústiť až do kyberšikany.

6.4. Nebezpečné výzvy – bývajú súčasťou naozaj rôznych sociálnych sietí, autor týchto výziev nabáda užívateľov aby plnili nejakú výzvu, avšak tieto výzvy

bývajú extrémne a môžu dokonca spôsobiť smrť. To, že ste výzvu splnili si máte natočiť na video.

6.5. Nebezpečné zoznamovanie

Tým, že sociálne siete slúžia aj ako komunikačný kanál, veľa krát nás môžu požiadať o priateľstvo alebo s nami sa budú snažiť nadviazať kontakt osoby, ktoré nepoznáme. Ak nepoznáme ich identitu, tak s nimi nenadväzujte kontakt. V skutočnosti neviete, či tieto osoby sú skutočne osoby, za ktoré sa vydávajú. Neviete si overiť ich identitu.
Ak sa Vám niečo také stalo a poskytli ste nejaký nevhodný obsah takejto osobe a nemáte z toho dobrý pocit, tak sa to nebojte povedať blízkej osobe.

7. TÉMA - PODVODY, TRIKY

Cieľ	Žiak vie rozpoznať základné podvody a manipulatívne správanie na internete.
Aktivita	Situácie: "Pošli mi tvoje heslo, som admin hry". "Klikni na tento link a vyhraj mobil". Otázky: Je to pravda alebo podvod ? Čo by si urobil/a ?
Záver	- neverím neznámym správam - neklikám na podozrivé odkazy - neposielam údaje - poviem dospelému

A teraz sa poďme pozrieť na hrozby, ktoré na nás číhajú na sociálnych sieťach a na čo si je treba dávať pozor.

Lektor otázka:
Tu ma zaujíma, či ste sa naozaj s niekedy s takouto hrozbou stretli. Ak áno, skúste popísať, čo sa stalo, prípadne, či ste to riešili s nejakou blízkou osobou (rodičom, v škole atď..)

Hrozby sú:

- **môžu to byť rôzne riziká spojené s únikom osobných údajov, kyberšikanou, nenávistné prejavy, nebezpečné výzvy, kybergrooming, nebezpečné zoznamovanie a iné.**

7.1. Internetové podvody

Čím sa stal internet populárnejší, tak ho aj zločinci začali využívať ako prostriedok a tým môžeme hovoriť o náraste kybernetickej kriminality. Cieľom týchto podvodov je vylákať od užívateľov rôznymi technikami finančné prostriedky a to napríklad:

- romance scam, ide o podvod spojený so zoznamovaním,

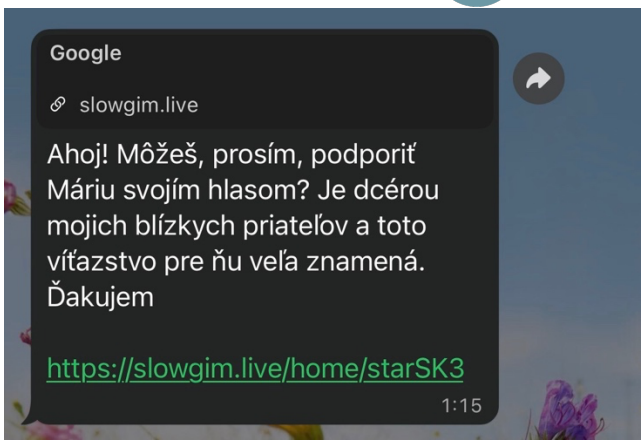
- automatizovaný sextortoin, kedy sa hacker vyhráža, že zverejní nejaké intímne fotografie, tým, že prenikol do vášho počítača,
- rôzne podvody s kryptomenami, kedy často prichádza k tzv. spoofingu, kedy si útočník zakryje svoje telefónne číslo iným telefónnym číslo a pod týmto číslom telefonuje a predáva napr. kryptomeny ...

7.2. PODVODY NA WhatsAppe

Hovorí lektor: Nedá mi nespomenúť aj časté podvody prostredníctvom online platformy WhatsApp. WhatsApp je veľmi obľúbená online platforma u detí, najmä vo veku 10 rokov a viac. Deti si prostredníctvom nej vytvárajú rôzne skupiny. Rôzne kanály kde predstavujú svoj životný štýl a nabádajú na sledovanie tohto kanála.
Aj tu platia rovnaké pravidlá ako pri sociálnych sieťach. Musíte si uvedomiť, čo všetko o sebe poskytujete, že všetky informácie, ktoré zdieľate, môžu byť osobnými údajmi.

Prostredníctvom WhatsApp však prebiehajú aj rôzne podvody, ktoré by sme mali spomenúť. *Stretol sa niekto z Vás v poslednej dobe s takouto správou ?*

- ide o typy správy, od ľudí, ktorých máte v kontaktoch, avšak kontakt, ktorý vám túto správu poslal ani o tom v skutočnosti ani nevie. Ide o napr. o typ správy – podporte na súťaži kamarátkinu dcéru ..., náhodou som našiel tvoju fotku, si toto ty ?, príde vám prihlásenie do sociálnej siete facebook prostredníctvom WhatsAppu, môže vám prísť ponuka práce s linkom, ďalej to môže byť podvod s rozbitým telefónom a informáciou kontaktuj ma cez WhatsApp.



7.3. QR – kódy a podvody

Sú veľmi obľúbené avšak aj v tomto smere sú útočníci veľmi kreatívny a zneužívajú ich na rôzne podvody. Tieto podvody sa nazývajú Quishing (QR phishing) je to podvod, pri ktorom útočníci nahrádzajú legitímne QR kódy falošnými, čím vás presmerujú na podvodné stránky.

Skenujete QR kódy ? Vedeli ste o tomto ?
Pred skenovaním odporúčam, aby ste si overili, či daný QR kód nie je nalepený. Často krát sa stáva, že podvodný QR – kód býva nalepený na existujúcom Q-kóde. Po naskenovaní takéto podvodného QR – kódu vás útočníci presmerujú na podvodnú webovú stránku.
Tam sa môžu pokúsiť: získať vaše prihlasovacie údaje, infikovať váš telefón alebo počítač malvérom, prinútiť vás zadať údaje z platobnej karty.

Prečo sú QR kódy tak nebezpečné?
Na rozdiel od bežných odkazov pri QR kóde nevidíte hneď, kam vedie, takže sa ťažšie odhaľuje, že ide o podvod.

8. TÉMA - ONLINE NÁKUPY

Cieľ	Žiak vie, ako si dať pozor na nakupovanie online.
Aktivita	Príklad: Otázky: rôzne situácie, kde si žiaci vyskúšajú či pôjde o e-shop falošný alebo skutočný
Záver	Praktické príklady. Žiaci budú vedieť ako nakupovať.

Lektor - otázka

8.1. Online nákupy sú veľmi pohodlné a rozšírené. Kto z vás už nakupuje na internete a má vlastnú platobnú kartu ? Tým, že nakupovanie prostredníctvom internetu je také jednoduché, tak to čoraz viac využívajú aj podvodníci.

Deti odpovedajú.

Lektor – poďme si povedať niekoľko informácií, ktoré nám pomôžu, aby sme nenaleteli podvodníkom. Nájdeme niekoľko spoločných znakov, ktoré tieto podvodné e-shopy majú.

8.2. Falošné e-shopy

- obvykle majú podozrivo nízke ceny,
- chýbajú kontaktné údaje,
- e-shop nemá sídlo v Slovenskej republike,
- zlá slovenčina, strojový preklad ako s translátorom,
- je možnosť platiť iba kartou.

8.3. Falošné bazárové ponuky

- predávajúci vám pošle link na „platobnú bránu“ alebo link na „prepravnú spoločnosť“ - je to podvod ich cieľom je získať údaje z platobnej karty.

8.4. Časová tieseň

- máme posledné kusy,
- musíte si teraz kúpiť, taká zľava už nebude,
- vysoká zľava,
- neoverené recenzie.

8.5. HRA, OVERENIE E-SHOPU

Lektor – Ako predchádzať aby sme sa nenachytali, ako si overiť e-shop skôr ako si niečo objednám ?

- cena, ak je príliš nízka je potrebné si ju overiť,
- pozrieť si v pätičke informácie o e-shope ako napríklad: kontaktné údaje, či je tam IČO, či je e-shop slovenskou spoločnosťou, či sa riadi slovenskou legislatívou,
- recenzie, zistiť si recenzie na daný e-shop aj prostredníctvom prehliadača,
- má stránka bezpečné zabezpečenie napr. (https)
- možnosti platby, aké sú (platobná brána, dobierka ...)

Ak som naletel, čo mám robiť ?

- povedať to rodičom, zavolať do banky aby zablokovali kartu,
- kontaktovať políciu s informáciou o tomto type podvodu.

Poďme sa zahrať hru odhaľ falošný e-shop ?

Situácia 1

„Značkové tenisky, bežná cena 120 €, dnes len za 19,99 €. Stránka nemá kontaktné údaje, iba formulár. Platba možná iba prevodom vopred.“

Je to bezpečné ?
Aké sú varovné signály ?

Očakávané odpovede:
- príliš nízka cena, chýba kontakt, iba platba vopred

Situácia 2

Na bazári niekto predáva hernú konzolu lacnejšie.

Kupujúci pošle link na „kuriéra“, kde treba zadať údaje z karty.

Je to bezpečné ?
Prečo nie ?

Pointa: Kuriér nikdy nepotrebuje údaje z tvojej karty.

Situácia 3 (bezpečný príklad)

E-shop má:
IČO, obchodné podmienky, recenzie, platbu kartou cez bankovú bránu

Je toto bezpečnejší nákup ? Prečo ?

Na tieto úlohy si môžu pripraviť dve kartičky, jedna pravda/nepravda, alebo jedna červená/zelená.

9. TÉMA - KYBERŠIKANA

Cieľ	Žiak vie rozpoznať kyberšikanu a reagovať.
Aktivita	Príklad: “Niekto sa vysmieva spolužiakovi v chate”. Otázky: Je to v poriadku ? Čo by si urobil ?
Záver	- neubližujem online - pomôžem spolužiakovi - poviem dospelému

Lektor otázka:
Zaujíma ma, či ste naozaj s niekedy takouto hrozbou stretli. Ak áno, skúste mi popísať, čo sa stalo, prípadne, či ste to riešili s nejakou blízkou osobou (rodičom, v škole atď..). Či sa o tom rozprávate ?

Deti reagujú ....majú už nejaké znalosti.

Lektor, vysvetľuje:
Kyberšikana - je najčastejšia forma agresie s ktorou sa môžete stretávať v online priestore.

9.1. Čo to je kyberšikana ?

- je to forma opakovaných intenzívnych agresívnych útokov, môže ísť o jednotlivca alebo o skupinu žiakov, pri ktorom sa využívajú moderné komunikačné zariadenia napr. mobilný telefón, tablet, PC ...,
- nie vždy je úmyselná,
- páchateľmi kyberšikany bývajú častokrát spolužiaci alebo vrstevníci,
- motívom býva často pomsta, že si ju zaslúžite, skupinový tlak v triede, z nudy.

Páchatelia si myslia, že ich nie je možné vystopovať, ale zanechávajú digitálne stopy. Táto anonymita je iba zdanlivá. Kyberšikana však môže vzniknúť ako nevhodný vtip napríklad ak by ste odfotili spolužiaka v nejakej nevhodnej situácií a táto fotografia by sa šírila prostredníctvom sociálnych sietí. Môže ísť o nevhodnú fotografiu, napr. oblial sa na obede.

9.2. Čo všetko napr. môže patriť do kyberšikany ?

- ponižovanie, nadávanie a urážanie v online prostredí,
- vyhrážanie a zastrašovanie v online prostredí,
- vydieranie v online prostrední,
- šírení ponižujúcich, zahanbujúcich videí a fotografií,

- vytváranie falošných profilov.

9.3. Zahráme sa hru, kde si vysvetlíme a uvidíme rozdiely, kedy ide o kyberšikanu alebo iba o nepríjemnú sms/správu od spolužiaka:

Otázka na žiakov	Ide o kyberšikanu ?
Kamarátka zo školy Ti pošle nepríjemnú správu/smsku. Túto smsku poslala iba jeden krát.	Nie
Niekto si ťa v škole vyfotí , upraví fotku prostredníctvom aplikácie/umelej inteligencie. Táto fotka ťa ale zosmiešňuje. Fotku si nenechá pre seba ale pošle ju tvojim spolužiakom.	Áno
Máš svoj profil na sociálnej sieti a niekto Ti okomentoval tvoj príspevok a nepáči sa Ti jeho komentár. Komentár nie je hanlivý, vyjadruje iba nesúhlas s príspevkom.	Nie
Stala sa Ti na obede nepríjemná vec, pošmykol si sa vylial na seba obed. Túto	Áno

tvoju nepríjemnú vec niekto natočil a nahral na YouTube.	

9.4. Ako postupovať v prípade, ak si myslíte, že ste obeťou kyberšikany ?

Určite o tom povedzte dospelému, napríklad učiteľovi, výchovnej poradkyni alebo rodičom. Ukáže im celú komunikáciu, ktorú vám agresor píše, resp. aké správy dostávaš. Ak vieš urob si screenshoty, ak nevieš, popros rodiča alebo učiteľa.

Ak je to možné obmedz komunikáciu s agresorom, prestať mu odpisovať. Ak už budeš mať všetky dôkazy, alebo ich zabezpečenia tvoji rodičia, môžeš si agresora zablokovať.

10. ZÁVER

Táto metodika poskytuje učiteľom praktický nástroj na vedenie žiakov k bezpečnému, zodpovednému a uvedomelému správaniu v online prostredí. Vzhľadom na to, že digitálny svet je už prirodzenou súčasťou života detí, je dôležité, aby vedeli rozpoznávať riziká, správne reagovať na problémové situácie a chrániť tak svoje súkromie.

Úlohou učiteľa nie je len odovzdávať informácie, ale najmä viesť žiakov k premýšľaniu, diskusii a zodpovednému rozhodovaniu. Prostredníctvom konkrétnych príkladov, otázok a aktivít majú žiaci možnosť lepšie pochopiť dôsledky svojho správania a osvojiť si zásady bezpečného pohybu na internete.

Metodika zároveň ponecháva priestor pre flexibilitu a prispôsobenie podľa potrieb konkrétnej triedy. Jej cieľom je podporiť učiteľa v tom, aby vytváral bezpečné a otvorené prostredie, v ktorom sa žiaci neboja pýtať, zdieľať svoje skúsenosti a učiť sa z nich.

Dôležitým výsledkom by nemali byť len vedomosti, ale aj postoje – schopnosť kriticky myslieť, chrániť seba aj ostatných a vedieť vyhľadať pomoc v prípade potreby.

11. ZDROJE

https://www.e-bezpeci.cz/