UNIVERZITA PALACKÉHO V OLOMOUCI
PEDAGOGICKÁ FAKULTA
CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE

BEZPEČNÉ CHOVÁNÍ NA INTERNETU PRO KLUKY A PRO HOLKY

NÁMĚTY NA VÝUKOVÉ AKTIVITY

BEZPEČNÉ CHOVÁNÍ NA INTERNETU PRO KLUKY A PRO HOLKY

(náměty na výukové aktivity)

Kamil Kopecký, René Szotkowski, Lukáš Kubala

Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity

1. vydání
Verze 1.0

ISBN: 978-80-244-6197-7 (print)
ISBN: 978-80-244-6198-4 (online: PDF)

Obsah

Úvodní slovo

Vážení a milí čtenáři,

vítáme vás u naší nové publikace, která se zaměřuje na problematiku bezpečného chování v online prostředí, především pak na témata, která se týkají dětských uživatelů internetu. Knížka Bezpečné chování na internetu pro kluky a pro holky je souborem nejrůznějších výukových aktivit (pracovních listů, námětů do výuky apod.) určených především pro žáky základních škol, využít ji však mohou samozřejmě i dospělí. Aktivity jsou rozděleny do několika logicky propojených tematických celků a jsou doplněny o stručné metodiky, které objasňují, jak s daným tématem pracovat (ve škole či mimo školu).

Věříme, že se vám naše aktivity budou líbit!

Za autorský tým

Kamil Kopecký

E-Bezpečí, Pedagogická fakulta

Univerzita Palackého v Olomouci

ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI

Aktivita: Tvoříme bezpečná hesla

? Bezpečné heslo je pro naši bezpečnost v online prostředí velmi důležité, je vlastně klíčem, který nám umožňuje vstupovat do našich uživatelských profilů. Dokázali byste popsat, jak by mělo vypadat bezpečné heslo?

Délka hesla:

Složení hesla:

? Vyzkoušejte si, zda vaše heslo neuniklo na internet. Otevřete si internetové stránky www.haveibeenpwned.com a zadejte vaši e-mailovou adresu. Během chvilky se dozvíte výsledek. Jak jste dopadli?

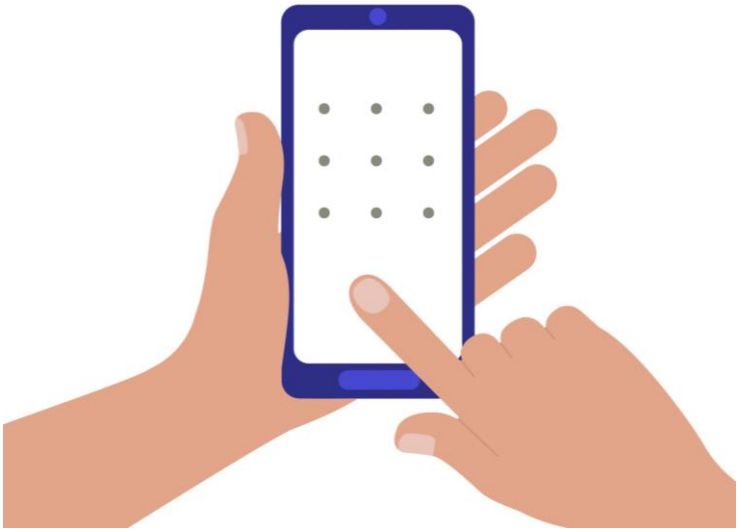
? Policie nás požádala, abychom jí pomohli rozhodnout, které z níže uvedených hesel je nejslabší. Pomůžete?

Ani4ka05	qwerty	Radek2007@
R$obot$201	Chytrej$borec@	MySak999#

Kámoš mi poradil, že dobrou cestou, jak si zabezpečit počítač, může být Dvoufázové zabezpečení účtu. Nevím ale úplně přesně, co to znamená. Poradíš, co bych mohl ke dvoufázovému zabezpečení účtu použít?

Lísteček s tajným kódem přilepený na monitoru	Mobilní telefon	své heslo, které ale napíšu pozpátku
		88PMULEJAPEP

Další možnost, jak si zabezpečit třeba mobilní telefon, představuje využití nějakého speciálního gesta. Dokázali byste vytvořit co nejsilnější gesto? Namalujte jej do šablony mobilního telefonu.



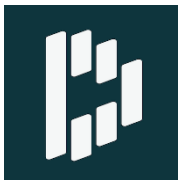
Pozor, zabezpečení mobilního telefonu pomocí gest je docela slabé a dá se prolomit! Daleko lepší je využívat třeba biometrických údajů, které jsou spojeny s lidským tělem (obličejem apod.). Dokázal/a bys uvést, jaké biometrické údaje se dají použít místo běžného hesla?

? K vytvoření silného hesla se dají využít různé Generátory hesel. Vygeneruj si heslo s využitím některého z volně dostupných nástrojů, třeba od firmy Avast nebo Eset. Dokážeš si takové heslo zapamatovat?

www.eset.com/cz/generator-hesel/

www.avast.com/cs-cz/random-password-generator

? Se zajištěním bezpečí ti dokážou pomoci také nejrůznější správci hesel – aplikace, které uchovávají tvoje hesla v bezpečí, takže si je nemusíš pamatovat nebo je mít napsaná třeba někde na lístečku. Určitě si některý z nich vyzkoušej, k oblíbeným patří například Dashlane, Keeper, RoboForm či LastPass.



Dashlane

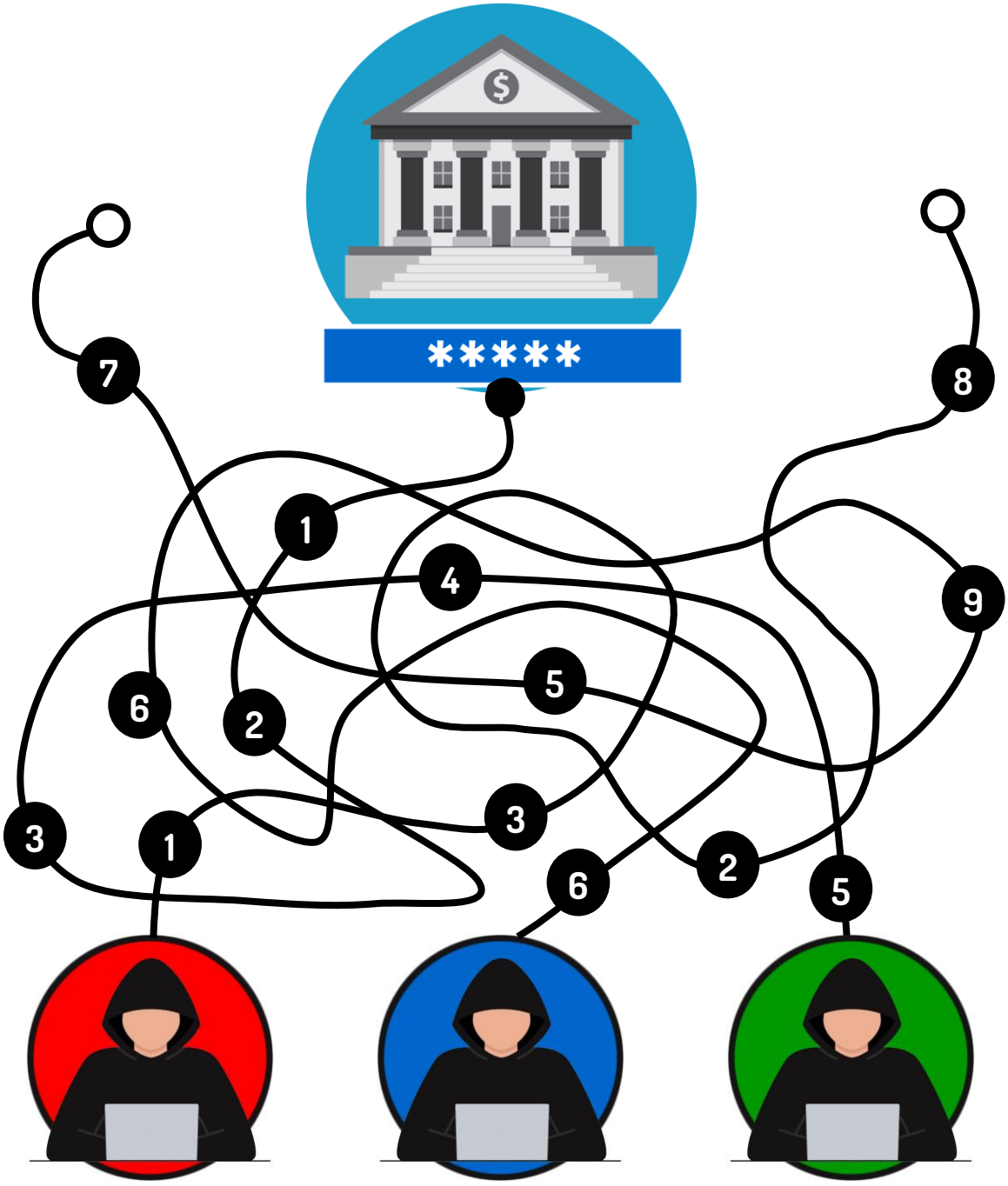
Keeper

RoboForm

LastPass

? Tatínek domů pořídil nový rychlejší router s vestavěným modemem, aby měla celá rodina rychlejší internet. Router vybalil z krabice a připojil ho k internetu. Měl by udělat ještě něco, aby bylo připojení k internetu bezpečné?

Tři Hackeři se rozhodli, že proniknou do počítačové sítě mezinárodní banky a převedou si finanční prostředky na své tajné účty. Banka totiž měla velmi slabé heslo, které se skládalo pouze z 5 číslic. Nakonec se do banky skutečně podařilo jednomu hackerovi proniknout a zadat správné heslo. Poznáte, který z nich to byl? A dokážete určit heslo, které se mu podařilo uhodnout?



Metodika k aktivitě: Tvoříme bezpečná hesla

Bezpečnostní standardy se s rozvojem informačních a komunikačních technologií neustále zvyšují.

Při tvorbě hesla je třeba dodržet několik bezpečnostních standardů:
1. Ideální heslo by mělo být **dlouhé minimálně 15 znaků** (stav v roce 2020).
2. Při tvorbě hesla **používejte číslice, velká i malá písmena abecedy a speciální znaky**. Vhodné je využívat specifické fráze – slovní spojení, obraty, věty, počáteční slabiky slov z konkrétní věty (tzv. metoda Bruce Schneiera).
3. Nikdy **nepoužívejte heslo, které lze najít ve slovníku**! Rovněž nepoužívejte křestní jména ani příjmení.
4. Pro **přístup k různým online službám** (e-mail, sociální sítě) **nepoužívejte stejné heslo**. Heslo musí být unikátní.
5. Po ukončení práce v prostředí internetu se **nezapomeňte odhlásit z účtu**, který právě používáte. Zavření prohlížeče vás z účtu neodhlásí!
6. Heslo **uchovejte v tajnosti**, nikomu jej neprozrazujte, ani svému nejlepšímu kamarádovi.
7. Důležité účty zabezpečte **dvoufázovým (dvouúrovňovým) či víceúrovňovým ověřováním**, které kombinuje heslo a kód (případně specifickou aplikaci) na mobilním telefonu.

Poznámka:

Podle posledních bezpečnostních analýz a matematických výpočtů je bezpečnější dlouhé heslo s méně typy znaků (např. pouze s velkými a malými písmeny abecedy), než heslo krátké s více variantami znaků (písmena, číslice, speciální symboly) – rozdíl je však v zásadě zanedbatelný, oba způsoby tvorby hesla jsou vysoce bezpečné.

Otázky:

1. Jakým způsobem jste vaše heslo vytvořili? (Např. kombinace jména a číslice apod.)
2. Posuďte, zda vaše heslo vyhovuje bezpečnostním standardům. (Tj. porovnáme, zda heslo, které žák vymyslel, odpovídá bodům 1-3 výše uvedených standardů.)
3. Zkuste odhadnout žebříček tří nejčastějších hesel v ČR. (12345, 123456, heslo, na dalších příčkách je heslo123, 123heslo321, aaaaa a qwerty.)
4. Navrhněte způsob, jak vytvořit zapamatovatelné a přitom bezpečné heslo. (Např. zvolíme nějakou známou větu a písmena s diakritikou nahradíme číslicemi, V Českých Budějovicích by chtěl žít každý = v4esk7chbud2jovic9chbycht2l69tka6d7.)

Biometrická hesla (biometrická autentizace)

V posledních letech se stále častěji objevují hesla v podobě biometrických údajů, ať už jde o **otisky prstů** (papilární linie), **biometrický sken obličeje**, **sken oka** (duhovky), **rozpoznávání hlasu** apod. Využívání biometrických údajů nahrazujících klasická hesla se objevuje např. u mobilních telefonů a tabletů. Typickým příkladem je třeba technologie Face ID, kterou s úspěchem využívají zařízení firmy Apple.

Biometrické údaje člověka nejde snadno napodobit a během lidského života se nemění. Biometrika ale zároveň neumožňuje heslo změnit ani si jej svobodně vybrat. Je tedy otázkou, co by se stalo, kdyby tyto údaje unikly a byly nějakým pokročilým způsobem napodobeny. Vytvoření napodobenin by ovšem nebylo vůbec jednoduché – kvalitní biometrické systémy totiž při autentizaci provádí tzv. **test živosti** – při snímání otisku prstu se měří teplota či elektrický odpor, při skenování oka se zase posuzuje, nakolik je posmrtně zakalené, při ověřování podle obličeje se posoudí, zda je předložený obličej trojrozměrný a nejedná se pouze o fotku.

Biometrické údaje v současnosti využíváme např. u prokazování totožnosti (biometrický občanský průkaz, biometrický pas, biometrické brány na letištích – na obrázku vpravo např. na Letišti Praha), nahrazují běžná hesla či PINy při odemykání počítačů, tabletů a mobilních telefonů (otisk, sken obličeje), případně se využívají při vyhledávání důležitých osob na letištích či sportovních utkáních (detekce obličeje). Extrémním příkladem je pak čínský systém kontroly obyvatelstva.

Router

U routeru s modemem je třeba změnit výchozí heslo pro přístup do jeho ovládacího prostředí, které je přednastavené od výrobce. Drtivá většina domácích uživatelů toto nedělá, routery jsou pak snadno napadnutelné.

Tři hackeři

V úkolu o třech hackerech se do banky dostal poslední hacker (zelený), který správně zadal heslo 54321. To se ostatně pravidelně objevuje v žebříčcích nejméně bezpečných a snadno uhodnutelných hesel.

Zdroje:

Biometrie není jen otisk prstu. Dávejte pozor, komu své údaje poskytnete. Svět Chytře. https://www.svetchytre.cz/a/pM8jE/biometrie-neni-jen-otisk-prstu-davejte-pozor-komu-sve-udaje-poskytnete

Generátor náhodných hesel. Avast.
https://www.avast.com/cs-cz/random-password-generator#pc

Aktivita: Bezpečnostní zásady

Pročtěte si následující situace a rozhodněte, co je a co není v online prostředí bezpečné.

1. Roman se ve školní učebně připojil na svůj účet na Instagramu, vkládal na svůj profil fotografie, komentoval a lajkoval příspěvky kamarádů. Poté zavřel prohlížeč a šel do další výuky...

2. Hance přišla na Facebooku zpráva od její kamarádky Jany, která ji požádala o pomoc. Jana zapomněla heslo do svého facebookového účtu a potřebuje si ho obnovit pomocí mobilního telefonu, vybil se jí ale zrovna telefon. Prosí proto Hanku, zda by jí neposlala kód, který jí dorazí na její mobilní telefon. Hanka Janě kód poslala.

3. Honzovi přišel tzv. hoax (nepravdivá, často poplašná zpráva) o tom, že se Bill Gates z Microsoftu rozhodl podělit o své bohatství. A pokud Honza e-mail přepošle dalším lidem, tak mu za každého člověka, který e-mail pošle dál, zaplatí Microsoft 2.43 EUR. Honza e-mail přeposlal všem svým kamarádům.

4. Kláře přišel e-mail: Gratulujeme, vyhrála jsi IPhone X. Každé pondělí vybíráme 10 náhodných výherců. Nyní se štěstí usmálo na tebe. Svou výhru potvrď odesláním SMS ve tvaru GIFT 1133567 na číslo 90399. Klára SMS odeslala.

5. Petr umí skvěle pracovat s počítačem, a proto si vytvořil složité heslo obsahující písmena, číslice i speciální znaky. Aby heslo nezapomněl, napsal si ho na zadní část svého notebooku.

Metodika k aktivitě: bezpečnostní zásady

V rámci aktivity pracujeme s několika běžnými situacemi, se kterými se děti v online prostředí mohou setkat. Situace můžeme doplnit o jakékoli další, v kterých figuruje zabezpečení počítače, mobilního telefonu apod.

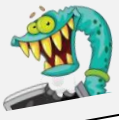
Řešení úkolu:

1. Roman se neodhlásil ze svého účtu na Instagramu, pouze zavřel prohlížeč na počítači v počítačové učebně. Kdokoli, kdo si otevře prohlížeč po Romanovi, bude mít přístup do jeho účtu. Pro zajištění bezpečnosti je tedy třeba **vždy se z daného účtu odhlásit**.
2. Náš příklad je ukázkou **podvodu s tzv. m-platbou** (mobilní platbou) – pokud Hanka Janě odešle kód, který jí dorazil na mobilní telefon, přijde o část kreditu, kód je potvrzením online platby za zboží či službu. Pachatelé tohoto typu podvodu nejdříve zkopírují facebookový profil vašeho přítele či přítelkyně a poté se vás pod falešnou identitou pokusí oslovit a vylákat z vás potvrzující kód.
3. **Přeposílání hoaxů podporuje šíření spamu** a s každým přeposláním se e-mailová adresa Honzy dostala k dalším neznámým lidem. Je pak snadné zařadit adresu do reklamní spamové sítě a zaplavit ji nevyžádanou poštou. Přeposláním totiž Honza potvrdil, že je jeho e-mailová schránka skutečně aktivní a má smysl ji zaplavit reklamou všeho druhu.
4. Jedná se opět o **druh podvodu** – odesláním SMS se na telefonním čísle Kláry aktivovalo předplatné, které jí bude každý týden odečítat z účtu 99 Kč (poslední dvě číslice telefonního čísla). V e-mailu, který jí přišel, budou někde ve spodní části definovány drobným, téměř neviditelným písmem obchodní podmínky, se kterými odesláním SMS souhlasí. Předplatné je nutné zrušit odesláním jiného kódu.
5. **Heslo nepatří ani na zadní stranu notebooku, ani na spodní stranu klávesnice či na lísteček přilepený na monitor**. Heslo si buď pamatujeme, nebo k jeho uložení využijeme specializované aplikace (LastPass, 1Password, KeePass, Sticky Password, Dashlane). Standardem posledních let je také využívání dvoufázového (vícefázového) zabezpečení.

Aktivita: Vyznáte se v počítačových virech?

Na internetu můžeme narazit na velké množství nebezpečných programů, kterým se říká malware (zjednodušeně počítačové viry). Virů existuje celá řada. Pokuste se spojit názvy různých druhů počítačových virů s jejich popisem.

Počítačový červ



Spyware

Trojský kůň

Adware

Ransomware

Na první pohled vypadá jako užitečný program, nicméně umožňuje svému tvůrci otevřít do počítače „zadní vrátka“ a proniknout do něj.

Program, který na počítači bez souhlasu uživatele zobrazuje reklamy (vyskakovací okna v prohlížeči).

Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.

Zablokuje vám počítač a nutí zaplatit částku za odblokování. Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu.

Program, který z počítače tajně odesílá data – třeba vaše soubory.

Metodika k aktivitě: Vyznáte se v počítačových virech?

Řešení:

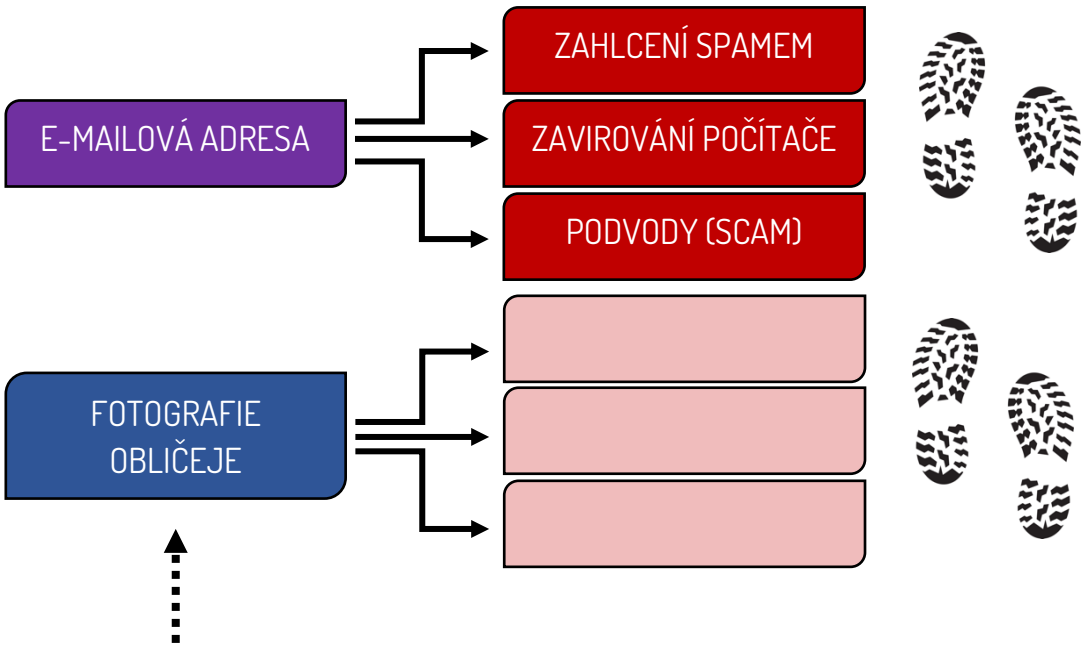
Druh nebezpečného programu	Co dělá
Počítačový červ	Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.
Trojský kůň	Na první pohled vypadá jako užitečný program, nicméně umožňuje svému tvůrci otevřít do počítače „zadní vrátka“ a proniknout do něj.
Spyware	Program, který z počítače tajně odesílá data – třeba vaše soubory.
Adware	Program, který na počítači bez souhlasu uživatele zobrazuje reklamy (vyskakovací okna v prohlížeči).
Ransomware	Zablokuje vám počítač a nutí zaplatit částku za odblokování. Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu. Do této skupiny řadíme tzv. policejní viry.

Aktivita: Digitální stopy

Pokaždé, když na internetu něco uděláme, třeba stáhneme písničku nebo film, zapaříme online hru, pokecáme na Discordu nebo zveřejníme něco na Instagramu, zanecháme za sebou tzv. digitální stopu. Na obrázku (níže) vidíš příklady některých digitálních stop. Dokážeš doplnit další?

E-MAILOVÁ ADRESA	PŘEZDÍVKA	FOTKA OBLIČEJE
...	...	...
...	...	...

K digitálním stopám patří také osobní údaje (informace, které jsou spojeny s konkrétní osobou, třeba jméno, fotografie, věk apod.). Které osobní údaje se dají podle tvého názoru zneužít? A jakým způsobem?



Osobní údaje: fotografie obličeje, jméno a příjmení, věk, pohlaví, rodné číslo, e-mailová adresa, adresa bydliště, rodné číslo...

K digitálním stopám patří také tzv. cookies, IP adresa, MAC adresa, geolokace nebo třeba metadata ve fotografiích, které jsme pořídili mobilním telefonem. Dokážeš vysvětlit, co jednotlivé digitální stopy znamenají?

Digitální stopy, které po sobě na internetu zanecháváme, využívají velké firmy – třeba Google či Meta (Facebook) v rámci reklamy. Z digitálních stop, které jsme na internetu zanechali, sestaví náš reklamní profil (Odhalí třeba náš věk, pohlaví, naše zájmy a koníčky apod.), na který potom zaměřují reklamu, která se nám na internetu zobrazuje. Pokud používáte Google či Meta/Facebook, můžete si informace o vás snadno zobrazit. Odpovídá váš reklamní profil realitě?

https://adssettings.google.com/

https://www.facebook.com/ads/preferences

Metodika k aktivitě: Digitální stopy

Digitální stopy představují **vše, co po sobě zanecháváme na internetu**, počínaje osobními údaji a dalšími citlivými údaji přes informace o tom, co na internetu vyhledáváme či nakupujeme. Digitální stopy po sobě zanecháváme vědomě (na internet je vědomě nahráváme), ale také nevědomě (např. informace o naší IP adrese, cookies apod.).

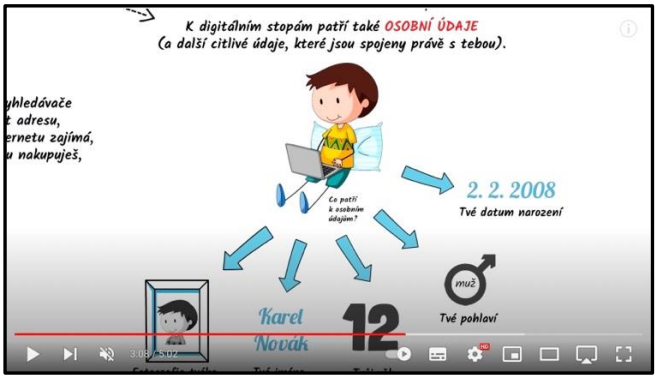
Řešení:

IP adresa	IP adresa (Internet Protocol Address) je jedinečné číslo, které umožňuje identifikovat zařízení připojené do sítě. Je to něco jako adresa našeho počítače či telefonu, který je připojen do sítě. IP adresa je složena ze 4 (či 6) čísel oddělených tečkami (např. 158.194.48.1). Z IP adresy se dá např. poznat, odkud je naše zařízení k internetu připojeno, kdo je poskytovatel našeho internetového připojení apod.
MAC adresa	Jde o tzv. fyzickou adresu zařízení připojeného do počítačové sítě (třeba našeho počítače, notebooku, tabletu či telefonu), která je spojena s konkrétní síťovou kartou. MAC adresa se skládá ze šesti dvojciferných čísel oddělených pomlčkou či dvojtečkou (např. 01:23:45:67:89:ab).
Cookies	Cookies jsou malé textové soubory, které si ukládají webové stránky, které jsme navštívili, do našeho počítače (prohlížeče). Webové stránky si pak umí tyto soubory a data, která obsahují, nahrávat při naší příští návštěvě.
Geolokace	Informace o naší geografické poloze. Pokud např. využíváme sociální sítě z mobilního telefonu, mohou si načíst informace o naší poloze v reálném světě.
Metadata z fotografií	Fotografie, které pořídíme pomocí smartphonu (či digitálního fotoaparátu), obsahují kromě samotné fotografie i další informace (metadata) – třeba o místě a času, kdy byla fotografie pořízena.

Digitálními stopami se zabýváme také v naší online hře Internet Highway, která je zcela zdarma na webu https://www.internethighway.cz.

Videa k aktivitě

Digitální stopy



AKTIVITA: SDÍLET, NEBO NESDÍLET?

Zamysli se, zda by ti po zveřejnění zmíněného obsahu mohlo hrozit nějaké riziko. Rozhodni, jaký obsah je, nebo není vhodný pro veřejné sdílení na sociálních sítích, a vysvětli proč.

1. Fotografie našeho domu.

2. Fotka z párty, na které se spolužáky ze základní školy pijeme pivo.

3. Rodinná fotografie z dovolené, na které právě jsme.

4. Moje fotka ze sportovního utkání, kterého jsem se zúčastnil.

5. Pořídili jsme si nové domácí kino a chci se pochlubit fotkou našeho obýváku.

6. Fotografie našeho psa.

7. Video z auta, na kterém je jasně vidět, že jedeme po dálnici rychlostí 190 km/h.

8. Fotografie mě a mladší sestry v plavkách na dovolené u moře.

9. Tajně jsem na mobilní telefon natočil našeho učitele a video nahrál na YouTube.

10. Chci se pochlubit místem, kam v létě s rodinou poletíme, tak dám na Instagram fotku svého pasu a letenky.

- Jaký typ fotografií bychom nikdy neměli veřejně sdílet?
- Proč bychom se neměli chlubit na internetu, že s rodinou odjíždíme na dovolenou nebo že se právě nacházíme v zahraničí?
- Hrozí mi nějaké riziko, přestože fotografii sdílím pouze jako dočasný příspěvek (např. přes Snapchat nebo jako Instagram stories)?
- Jak s našimi fotografiemi zachází sociální sítě?

Metodika k aktivitě: Sdílet, nebo nesdílet?

Prostřednictvím aktivity učíme žáky rozlišovat, jaký obsah je, nebo není vhodné veřejně sdílet na sociálních sítích.

Žáci se nejprve zamyslí, zda chování v popsaných situacích může představovat nějaká rizika. Poté se rozhodnou, zda by popsaný snímek či video sdíleli veřejně, a vysvětlí, proč se tak rozhodli a proč jsou vybrané situace problematické či nikoliv.

Aktivitu můžeme realizovat jako skupinovou práci. Žákům vytiskneme připravené kartičky a necháme je rozhodnout o tom, jak potencionálně moc rizikové situace to podle nich jsou. Rizikové situace mohou na stole přemístit doleva. Ty bezproblémové doprava. Pokud některé příhody vyhodnotí jako neutrální nebo pokud si nebudou jistí, nechají je ležet uprostřed stolu.

Žáci se také mohou podělit o své osobní zkušenosti se sociálními sítěmi, na jejichž základě můžeme vytvořit další kartičky.

Snažíme se, aby žáci pochopili rozdíl mezi soukromým a veřejným sdílením. Můžeme se doptávat na další otázky.

Otázky učitele (průvodce):

1. Proč bychom měli obsah, který sdílíme, rozlišovat podle toho, zda je určen pro přátele/rodinu, nebo pro širokou veřejnost?
2. Jaké fotografie či videa bychom neměli sdílet veřejně?
3. Jaké nám hrozí nebezpečí?
4. Jak sociální sítě a platformy, které používáme, zachází s našimi soubory?

Shrnutí:

Žákům bychom měli vysvětlit všechny důsledky a rizika spojená s veřejným sdílením osobních informací a měli bychom je upozornit, že obnažené fotografie nebo fotografie obsahující citlivé informace jsou problematické vždy.

Žáci by neměli zapomínat ani na to, že mnohdy pouhým užíváním online platformy dávají soukromým společnostem, které platformu vlastní, automaticky souhlas k libovolnému nakládání s obsahem, jenž nahráli nebo sdíleli prostřednictvím dané služby. To se týká i tzv. dočasných příspěvků (např. fotografie na Instagram Stories), jejichž kopii si za pomoci screenshotu (snímek obrazovky) může vytvořit i potencionální útočník a následně si ji uložit třeba do počítače, nahrát na cloudové úložiště, vytisknout nebo rovnou veřejně rozšiřovat na dalších online platformách.

Řešení:

1. **Fotografie našeho domu.**

Snímek může obsahovat číslo popisné nebo název ulice. Kdokoliv na internetu tak může zjistit, kde dítě bydlí. Z fotografie lze vyčíst i další informace, např. majetkové poměry rodiny nebo jaké další vybavení je součástí pozemku.

2. **Fotka z párty, na které se spolužáky ze základní školy pijeme pivo.**

Dítě vědomě vytváří digitální stopu, která může mít v budoucnu negativní dopad na jeho soukromý či pracovní život. Fotografie mohou posloužit i jako důkazní prostředek pro Policii ČR v případě porušení zákona.

3. **Rodinná fotografie z dovolené, na které právě jsme.**

Děti i dospělé bychom měli poučit, že v žádném případě nesmí na internet veřejně sdílet informace o tom, že jsou s celou rodinou na dovolené, a upozorňovat tak na fakt, že jejich byt či dům je prázdný a nikdo není doma. Taková informace je svým způsobem pozvánkou pro potencionálního zloděje.

4. **Moje fotka ze sportovního utkání, kterého jsem se zúčastnil.**

Jde o běžnou fotografii, která pro dítě nepředstavuje žádné riziko. Výjimkou mohou být např. fotografie z plaveckého závodu, viz bod č. 8.

5. **Pořídili jsme si nové domácí kino a chci se pochlubit fotkou našeho obýváku.**

Z této fotografie můžeme vyčíst majetkové poměry rodiny, což jako příspěvek na veřejném profilu dítěte může být lákadlem pro potencionálního zloděje. Především pak v kombinaci se situací popsanou v bodě 3, kdy se rodina nachází na dovolené a byt či dům je opuštěný.

6. **Fotografie našeho psa.**

Snímek našeho domácího mazlíčka bez dalších osobních informací nepředstavuje žádné riziko.

7. **Video z auta, na kterém je jasně vidět, že jedeme po dálnici rychlostí 190 km/h.**

Pokud by dítě zveřejnilo na internetu záznam z jízdy autem, na kterém rodič nebo kdokoliv jiný zřetelně překračuje maximální povolenou rychlost pro motorová vozidla, mohl by takový materiál posloužit jako důkazní prostředek pro Policii ČR.

8. **Fotografie mě a mladší sestry v plavkách na dovolené u moře.**

Na dovolené chceme všechny zážitky pečlivě zdokumentovat pomocí smartphonu či fotoaparátu, abychom se s nimi mohli pochlubit rodině nebo známým. Ovšem buďme obezřetní v tom, jaké fotografie budeme v době dovolených pořizovat a sdílet. Obzvláště pokud jde o fotografie našich dětí. V této souvislosti je totiž důležité upozornit na fenomén zvaný **sharenting**. Tím označujeme nadměrné používání sociálních médií (a obecně internetových služeb) rodiči, kteří v nich aktivně sdílejí obsah, v němž figurují jejich děti.

Podrobnější informace o fenoménu sharenting najdete v našem videu.

9. **Tajně jsem na mobilní telefon natočil našeho učitele a video nahrál na YouTube.**

Žáci mohou fotit a natáčet jiné osoby pouze s jejich souhlasem. Přestože existuje několik výjimek uvedených v § 88-89 zákona č. 89/2012 Sb., podle kterých můžeme zachytit a šířit podobu člověka i bez jeho souhlasu, učitelé nejsou úřední osoby a nevztahuje se na ně tedy výjimka spojená se statutem úředního činitele.

Podrobněji se tomuto tématu věnujeme v kapitole **Autorské právo a pirátství**, konkrétně v metodice k aktivitě **Fotíme a sdílíme**.

Nezapomeňme, že veřejný příspěvek v podobě fotografie nebo videa může obsahovat další osobní údaje, např. adresu školy, kterou žák navštěvuje a kde konkrétní učitel pracuje.

10. **Chci se pochlubit místem, kam v létě s rodinou poletíme, tak dám na Instagram fotku svého pasu a letenky.**

Veřejně dostupné fotografie našeho pasu a letenky představují opravdu bezpečnostní riziko. Nejenže opět zveřejňujeme informaci o tom, že v určité datum bude náš byt či dům opuštěn, ale navíc poskytujeme i důležité informace z letenek, jako jsou číslo rezervace (booking reference) a čárový kód.

Díky číslu rezervace v kombinaci s jménem pasažéra se může kdokoliv přihlásit do online check-inu (proces odbavení) a zjistit si naše datum narození nebo číslo pasu. Po přihlášení je možné zadané údaje i změnit, což by mohlo výrazně zkomplikovat náš odlet. V případě čárového kódu může kdokoliv zjistit nejen naše číslo rezervace, ale i číslo letu a naše místo v letadle. Nezapomínejme ani na další dokumenty, u kterých lze čárový kód zneužít, příkladem může být vstupenka na koncert.

AKTIVITA: OZNAČOVÁNÍ UŽIVATELŮ

Uživatelé internetu se často nechávají dobrovolně či nedobrovolně označit na fotografiích, které sdílí se svými přáteli na sociálních sítích.

Zdroj: Picworld, IZiSpicy, Sport.Onet

Prohlédni si přiložené fotografie. Jaká rizika mohou být spojena se sdílením takového materiálu na internetu? Jak by nám takové fotografie mohly uškodit? Vymysli 5 příkladů (situací v běžném životě).

.....

.....

.....

.....

.....

Metodika k aktivitě: Označování uživatelů

Cílem aktivity je upozornit žáky na fakt, že nad čímkoliv, co sdílíme na internetu, prakticky ihned ztrácíme kontrolu.

Veškerý nevhodný materiál, jako jsou např. snímky z večírků, kde se objevuje alkohol nebo jiné návykové látky, případně nahota, se může nekontrolovaně šířit internetem a my máme jen velmi omezené možnosti, jak tomu zabránit.

Žáci by si měli uvědomit, že pozdější smazání nevhodné fotografie ještě není zárukou toho, že snímek opravdu zmizí z internetu. Např. útočník, který by chtěl kompromitující materiály využít ke kyberšikaně, si je může včas uložit do počítače, nahrát na cloudové úložiště, vytisknout nebo rovnou veřejně rozšiřovat na dalších online platformách.

S materiálem podobnému tomu z aktivity se pojí i několik dalších rizik. **Dítě vědomě vytváří digitální stopu, která může mít v budoucnu negativní dopad na jeho soukromý či pracovní život**. Fotografie mohou posloužit i jako důkazní prostředek pro Policii ČR v případě porušení zákona.

Žáci by neměli zapomínat ani na to, že mnohdy pouhým užíváním online platformy dávají soukromým společnostem, které platformu vlastní, automaticky souhlas k libovolnému nakládání s obsahem, jenž nahráli nebo sdíleli prostřednictvím dané služby.

Nejlepší způsob, jak zamezit šíření nevhodné fotografie či videa, je takový materiál vůbec nevytvářet.

AKTIVITA: MOBILNÍ TELEFON A JEHO BEZPEČNOST

- MOBILNÍ TELEFON JE SUPER NÁSTROJ, KTERÝ VĚTŠINA Z NÁS POUŽÍVÁ KAŽDÝ DEN. MÁTE SVŮJ MOBILNÍ TELEFON ZABEZPEČEN, ABY SE DO NĚJ NEMOHL DOSTAT NĚKDO JINÝ? A JAKÝM ZPŮSOBEM?

MOBIL NEMÁM NIJAK ZABEZPEČEN

ČÍSELNÝ PIN NA SIM KARTĚ

ČÍSELNÝ PIN PŘÍMO DO MOBILU

ZABEZPEČENÍ GESTEM (KŘIVKA)

BIOMETRICKÉ ZABEZPEČENÍ (OTISK PRSTU, TVÁŘ)

ODEMYKÁNÍ CHYTRÝMI HODINKAMI

HESLO (KOMBINACE ZNAKŮ)

JINÝ ZPŮSOB

- MÁTE VE SVÉM MOBILNÍM TELEFONU ULOŽENO <u>NĚCO, CO NESMÍ VIDĚT NIKDO JINÝ NEŽ VY</u> (PŘÍPADNĚ TI, KTERÝM TO POVOLÍTE)?

- DOKÁZALI BYSTE VÁŠ ODBLOKOVANÝ A ODEMČENÝ MOBILNÍ TELEFON NA POUHÝCH 10 MINUT PŮJČIT TŘEBA VAŠEMU SPOLUŽÁKOVI?

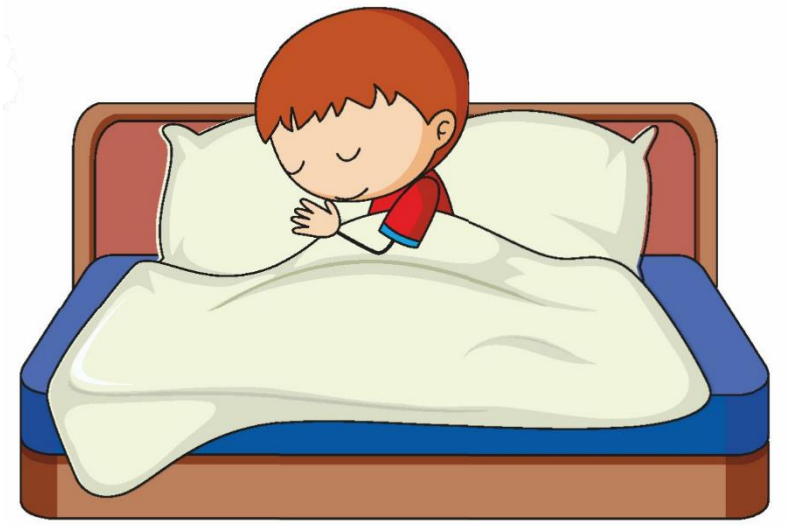
- JAK BYSTE SE CÍTILI, KDYBY VÁŠ SPOLUŽÁK Z VAŠEHO TELEFONU VEŘEJNĚ ČETL VAŠE POSLEDNÍ SOUKROMÉ ZPRÁVY – TŘEBA SMS, KONVERZACE Z DISCORDU, WHATSAPPU, SNAPCHATU ČI MESSENGERU? NEBO KDYBY TŘEBA VEŘEJNĚ NASDÍLEL VAŠE FOTOGRAFIE A VIDEA? CO BYSTE V OBOU PŘÍPADECH DĚLALI?

- Co byste dělali, kdybyste váš mobilní telefon ztratili? Existují nějaké možnosti, jak mobilní telefon zase najít?

- Instalujete si do svého mobilního telefonu aplikace a hry? Hrozí při instalaci aplikací či her z internetu nějaká rizika?

- Máte ve svém mobilním telefonu aktivní cloud (Google, Apple apod.)? Tedy vaše fotografie a videa se automaticky nahrávají na vaše úložiště na internetu – mimo váš mobilní telefon? Je automatické zálohování obsahu nějak rizikové?

- Říká se, že bychom mobilní telefon neměli používat těsně před spaním. Dokázali byste vysvětlit, proč?



Přečtěte si následující článek, který se týká populárního obchodu s aplikacemi Google Play. Poté odpovězte na otázky.

Tyto aplikace z Google Play umí vysát účet. Zbavte se jich.

Čističe systému, foto editory, audio rekordéry... to jsou typy aplikací dostupných přes klasický obchod Google Play, u nichž je obecně velmi pravděpodobné, že vám možná splní daný požadavek, ale také obsahují malware a namísto užitku způsobují hlavně trápení. Společnost Trend Micro upozorňuje na několik aplikací, které Google ze svého obchodu vyhodil právě proto, že obsahovaly **zákeřný bankovní malware**. Aplikace shromažďovaly přihlašovací údaje oběti do bankovnictví, jejich PINy, hesla a další informace, **malware také umožňoval zachytávat textové zprávy (SMS) a ovládat infikované telefony**. **Zdroj: Světandroida.cz**

Věděli jste o tom, že i z oficiálních online obchodů si můžeme stáhnout do svého mobilu zavirovanou aplikaci?

V čem jsou nebezpečné aplikace, které umí zachytávat naše SMSky?

Dá se mobilní telefon chránit nějakým antivirovým programem? A máte nějaký takový nainstalován? A existují vůbec antivirové programy pro mobilní telefony? Využijte internetový vyhledávač a zkuste najít nějaké příklady programů, které by pomohly ochránit váš mobil.

Metodika k aktivitě: Mobilní telefon a jeho bezpečnost

První mobilní telefon dostává dítě zpravidla s nástupem na základní školu, v první či druhé třídě, využívá jej tedy již od útlého věku. Proto je nutné, aby bylo seznámeno se základy jeho bezpečného používání. Otázky z aktivity jsou tedy voleny tak, aby se dotkly klíčových oblastí:

1. **Základní zabezpečení mobilního telefonu** – nejvíce bezpečná hesla jsou hesla biometrická v kombinaci s PINem, málo bezpečné je zabezpečení pomocí gest.
2. **Využívání automatického zálohování do cloudu** – drtivá většina smartphonů automaticky zálohuje veškeré fotografie či videa přímo do cloudu (vzdáleného úložiště na internetu) – zde je důležité, aby byl přístup do cloudu také zabezpečen, především pomocí dvoufázového či vícefázového ověřování. Pokud by cloud nebyl dostatečně zabezpečen (např. by využíval univerzální heslo), hrozí riziko, že veškeré materiály (fotografie, videa) mohou uniknout. Vždy je tedy nutné mít zabezpečen i cloud.
3. **Instalace různých aplikací a her** – aplikace je zapotřebí stahovat z ověřených zdrojů (např. AppStore, Google Play, Microsoft Store) a vždy je nutno také zvážit, jaká práva aplikaci povolíme. Žáky bychom měli upozornit na to, že i v oficiálních obchodech mohou být nebezpečné aplikace, které obsahují nejrůznější druhy malware.

Velmi důležité je uvědomit si, jak **citlivé informace ve svém mobilu děti (a samozřejmě i dospělí) mají** – k tomu slouží aktivity, které jsou spojeny s půjčováním mobilního telefonu spolužákům a zveřejňováním jeho obsahu. Prožitek spjatý právě s pocitem, že může být obsah našeho mobilu zneužit, umocní dopad celé aktivity. Realizaci prožitkových aktivit spojených se zapůjčováním mobilního telefonu je třeba zvážit v závislosti na klimatu v dané skupině dětí.

Proč by se děti neměly na mobilní telefon (či jiný displej) dívat před spaním? Protože displeje vyzařují světlo s převažující **„modrou složkou", která blokuje produkci lidského hormonu melatoninu** (tzv. spánkový hormon). Ten se začne vylučovat s příchodem večera, v průběhu noci pak pročišťuje naše tělo a umožňuje nám zdravě spát. Pokud ale před spaním sledujeme modrou část světelného spektra, blokuje se produkce tohoto hormonu, hůře se nám usíná a tělo se nestihne „pročistit". Více naleznete v animaci za touto kapitolou.

V další části žáci mohou pracovat s článkem, který upozorňuje na výskyt infikovaných aplikací v oficiálních internetových obchodech. Zde je důležité zejména to, že aplikace může ovládnout naše SMSky. To znamená, že **podvodníci, kteří aplikaci ovládají, mohou z našich SMS zpráv odchytnout potvrzovací kódy našich plateb a ovládnout tak zcela náš účet**.

Videa k aktivitě

Mobilní telefon a modré světlo

KYBERNETICKÁ ŠIKANA – KYBERŠIKANA

Aktivita: Co víme o kyberšikaně?

Přečtěte si následujících 10 situací a zkuste rozhodnout, které z nich se dají považovat za kyberšikanu a které naopak ne.

1. Kamarád ti pošle ošklivou SMS zprávu, ve které tě urazí, a pak už to nikdy neudělá.

2. Někdo tě vyfotí svým mobilním telefonem a fotku upraví tak, aby tě zesměšňovala. Pak ji začne rozesílat tvým spolužákům.

3. Někdo ti vytvoří falešný profil na Instagramu a jeho prostřednictvím uráží, pomlouvá a napadá další uživatele internetu.

4. Někdo tě pomocí mobilního telefonu natočí, jak sedíš na záchodě. Video nahraje na YouTube.

5. Maminka ti zakázala internet, protože jsi zlobil/a.

6. Někdo ti napsal na tvoji zeď na sociální síti, že tě nemá rád (nepoužil nadávky).

7. Spolužáci o tobě na internetu vytvořili veřejnou diskusní skupinu, ve které o tobě rozšiřují lži a pomluvy.

8. Spolužák tě vydírá – pokud mu nebudeš odevzdávat kapesné, rozšíří o tobě na internetu, že jsi homosexuál (gay/lesba).

9. Tvůj nejlepší kamarád ti na profil napíše: „Ty jsi ale dobytek!“ a doprovodí svůj vzkaz několika smajlíky.

10. Kamarád tě ve škole urazil, a proto jsi se rozhodl/a pomstít. Tajně jsi ho ve škole vyfotil/a a začal/a jsi jeho fotografii rozšiřovat na internetu s doprovodným komentářem, že je zloděj.

? Je podle vašeho názoru kyberšikana trestný čin?

? Dokázali byste najít několik rozdílů mezi kyberšikanou, která probíhá v online prostředí, a běžnou tradiční šikanou, která probíhá např. ve škole? Pokuste se doplnit následující tabulku:

	Tradiční šikana	kyberšikana
Kde probíhá?		
Kdy probíhá?		
Jak probíhá?		
Jaký má dopad?		
Kolik lidí se do ní zapojuje?		
Jak se dá zastavit?		
Víme, kdo je útočník?		

Metodika k aktivitě: Co víme o kyberšikaně?

Cílem aktivity je především **vymezení hranic kyberšikany a vysvětlení rozdílů mezi kyberšikanou a prostým škádlením.** Využíváme především metody brainstormingu, samotné pojmy vysvětlují žáci, učitel slouží jako průvodce. Jednotlivá zjištění zapisuje do podoby pojmových či mentálních map.

U kyberšikany musí platit, že **je intenzivní, má na oběť dopad a je to opakovaný jev** (zpravidla dlouhodobější). Není to tedy jednorázový akt, který dále nepokračuje. U kyberšikany rovněž neexistuje rovnováha sil (u přátelského pošťuchování a škádlení jsou síly vyrovnány).

Kyberšikana není z pohledu trestního zákoníku trestným činem, ovšem některé její vážné formy trestné jsou – např. vydírání, vyhrožování apod.

Další otázky učitele (průvodce):

1. Zkuste říct vlastními slovy, co je kyberšikana.
   (Učitel roztřídí zjištění do logických oblastí – pojmové mapy.)
2. Znáte někoho, kdo zažil kyberšikanu na vlastní kůži? Můžete popsat, co se mu stalo?
3. Zkus popsat, co cítí oběť.
   (Fyzické projevy, psychické projevy.)
4. Proč vlastně lidé páchají kyberšikanu?
   (Např. z pomsty, upevnění pozice ve skupině, nebo přeženou vtip apod.)
5. Páchají kyberšikanu pouze chlapci, nebo i dívky?
   (Samozřejmě obě pohlaví.)
6. Na koho se obrátit, když mám s kyberšikanou problém?

Řešení úkolů:

1. Nejde o kyberšikanu – je to jednorázová agrese.
2. Jde o kyberšikanu.
3. Jde o kyberšikanu, tzv. krádež identity.
4. Jde o kyberšikanu.
5. Nejde o kyberšikanu, přestože žáci rádi vykřikují, že je to šikana.
6. Nejde o kyberšikanu – lidé mají právo vyjadřovat i negativní názory.
7. Jde o kyberšikanu.
8. Jde o kyberšikanu – i vydírání je kyberšikanou, přestože ještě nedochází k šíření.
9. Nejde o kyberšikanu, ale o škádlení. Kamarádi mohou použít i vulgární výrazy, přesto je nevnímají jako ponižující a ubližující, síly jsou vyrovnány.
10. Jde o kyberšikanu.

Videa k aktivitě

Pro podporu této aktivity můžete využít celou řadu videí, které naleznete na YouTube kanálu E-Bezpečí: http://youtube.com/ebezpeci.

Kyberšikana

Kyberšikana – proč vzniká?

Aktivita: Agresivní kluci

Přečtěte si příběh Marie, který se skutečně stal v jednom českém městě. Poté se pokuste zodpovědět otázky pod textem příběhu.

Čtyři žáci 7. třídy nesnášeli svoji spolužačku Marii. Založili si proto diskusní skupinu na sociální síti Facebook s názvem „Nesnášíme Marii Novákovou“. Ve skupině Marii uráželi, nadávali jí, zveřejňovali její fotografie. Postupně do skupiny přidali celou třídu a nakonec skupinu zveřejnili. Čím více dětí se do komunikace zapojilo, tím horší příspěvky se ve skupině objevovaly, kluci si nakonec psali o tom, že Marii zavraždí, že jí rozřežou na kusy, že její tělo spálí apod.

Myslíte si, že své výhrůžky mysleli kluci vážně?

URČITĚ NE — **ASI NE** — **ASI ANO** — **URČITĚ ANO**

- Mohou nadávky a výhrůžky v online světě lidem ublížit? Pokud ano, jak?

- Jak byste se cítili, kdybyste byli Marií? Co byste prožívali?

- Jak byste situaci řešili? Co by mohla Marie udělat? Navrhněte vhodná řešení.

- Zažili jste někdy i vy sami podobnou situaci jako Marie? A jak jste ji řešili?

Metodika k aktivitě: Agresivní kluci

Cílem aktivity je zamyslet se nad rozdíly mezi online světem a světem reálným, navrhnout případná řešení situace z pohledu oběti, ale také rodiče a učitele. Zároveň navrhnout vhodná opatření, jak v budoucnu zamezit opakování této situace.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie dítěte, která je důležitá k podpoře emočního prožitku u dětí a k jejich identifikaci se s obětí. Následně je necháme zodpovědět na položené otázky a rozvedeme diskusi na téma, zda může verbální agrese v online prostředí člověku ublížit.

Otázky učitele (průvodce):

1. Myslíte si, že své výhrůžky mysleli kluci vážně?
   (Ve skutečnosti samozřejmě kluci nechtěli Marii fyzicky ublížit.)
2. Jak byste se cítili, kdybyste byli Marií? Co byste prožívali?
   (Žáci mohou navrhnout mnoho různých emocí: vztek, strach, frustrace, nenávist, touha po pomstě.)
3. Mohou nadávky a výhrůžky v online světě lidem ublížit? Jak?
4. Jak byste situaci řešili z pohledu Marie?
   (Diskusi můžeme navést třeba k technickým řešením – blokace uživatele, blokace obsahu na internetu, oslovení dospělého – učitele, rodiče, kontaktování pachatelů atd. Pozor, bubliny obsahují i řešení, která vhodná nejsou! Nechte žáky vybrat! Případně doplnit možnosti.)
5. Představte si, že byste byli učitelem, kterému se Marie svěřila. Jak byste danou situaci řešili?
6. Představte si, že byste byli rodiči, kteří na internetu narazili na diskusní skupinu o svém dítěti. Co byste dělali?
7. Myslíte si, že by bylo dobré v této situaci kontaktovat policii? Jak byste to provedli? Co byste policii sdělili?
8. Existují nějaké instituce, poradny apod., které vám mohou pomoci?

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že **i na internetu můžeme lidem vážně ublížit a že oběť často nedokáže rozlišit, zda své výhrůžky myslíme nebo nemyslíme vážně**. Stejně tak je nutné upozornit na důsledky, které můžeme svým chováním způsobit.

Navazující aktivity (v návaznosti na další disciplíny):

1. Tvorba plakátu, který upozorňuje na nebezpečí kybernetické šikany.
2. Tvorba letáčku, který obsahuje kontakty (odkazy, telefonní čísla) na organizace, které nám mohou pomoci kyberšikanu vyřešit.
3. Zpracování „vlastní přednášky" pro spolužáky o tom, co je kyberšikana.
4. Zpracování krizového postupu, co má oběť udělat, pokud zažívá kyberšikanu.

Dokončení příběhu:
Uvedený příběh vychází ze skutečného příběhu kyberšikany a vyvíjel se následovně ve dvou liniích:

1. Ředitel školy se o existenci diskusní skupiny dozvěděl, nechal ji zablokovat a potrestal žáky, kteří skupinu založili, sníženou známkou z chování.

2. Nezávisle na postupu ředitele se na Facebook podívala maminka Marie (vyhledávala jméno a příjmení své dcery, protože chtěla vědět, zda nemá na Facebooku profil). Nalezla diskusní skupinu, navštívila ji, vytiskla komunikaci mezi žáky a oznámila věc policii. Ta zahájila vyšetřování – podezření ze spáchání trestného činu (vražda ve stádiu plánování). Výslechy žáků odhalily, že o tento skutek nejde – věc byla vyhodnocena jako přestupek.

Aktivita: Youtuberka Katka

Přečtěte si příběh Katky, která se chtěla stát úspěšnou youtuberkou. Poté se pokuste zodpovědět otázky pod textem příběhu.

13letá Katka milovala youtubery a také se chtěla youtuberkou stát. Na YouTube si vytvořila svůj vlastní kanál, do kterého pravidelně nahrávala videa zaměřená na módu (oblast fashion – líčení, česání, vzhled…). Některým dětem z její třídy se líbila a snažily se jí napodobovat. Několik spolužaček a spolužáků ji však začalo urážet, nadávat jí, jak je ohavná, jak je odpudivá, jak jí to nesluší.

Na Instagramu si proto vytvořili vlastní profil, do kterého nahrávali různé fotografie Kateřiny, které vulgárně komentovali. Do profilu začalo přispívat stále více spolužáků a spolužaček.

Jak byste reagovali, kdybyste byli na místě Katky?

Kdo z vás sleduje pravidelně YouTube? Jaká videa na YouTube sledujete?

Sledujete také youtubery? Chtěli byste být jako youtuberi? Proč?

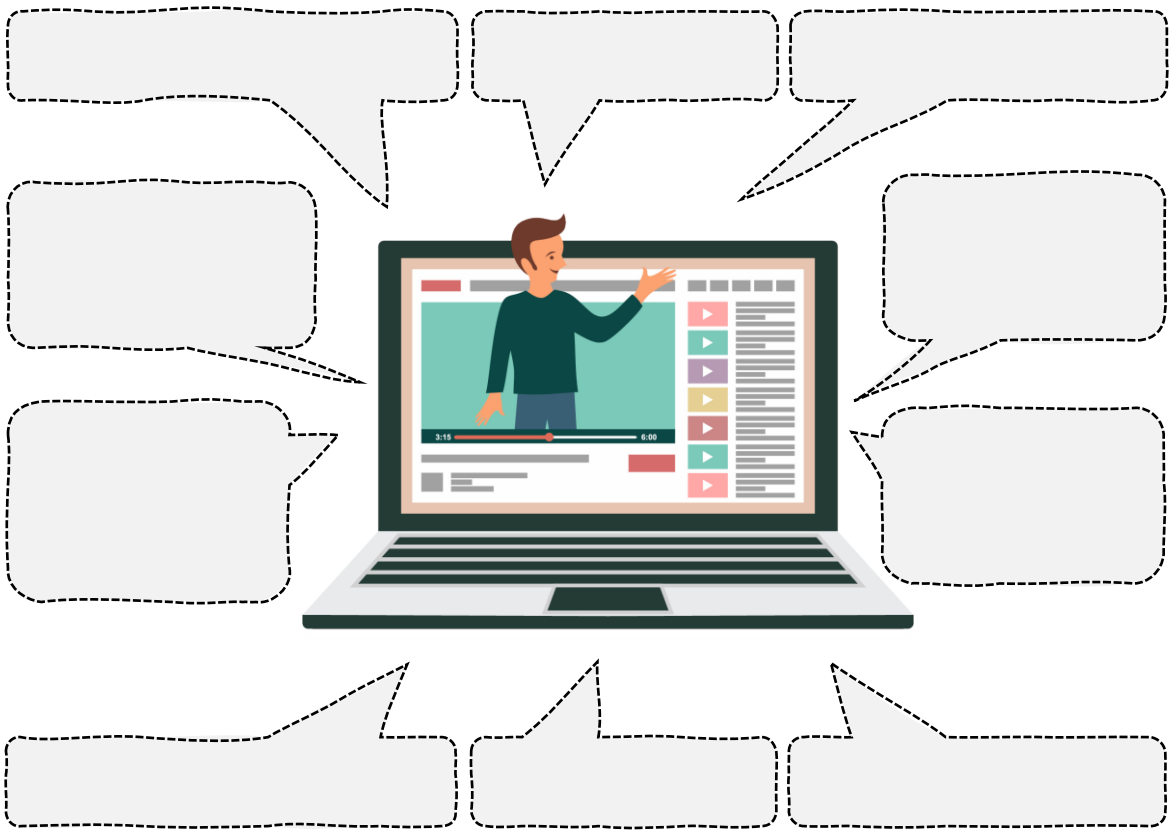
Myslíte si, že má youtuberství nějaká pozitiva? Uveďte alespoň 5 příkladů.

.....	.....	.....
.....	.....	.....

Myslíte si, že má youtuberství nějaká negativa? Uveďte alespoň 5 příkladů.

.....	.....	.....
.....	.....	.....

Mnoho youtuberů a youtuberek se dokáže natáčením a streamováním videí docela dobře uživit. Co všechno ale musí skutečně úspěšný youtuber zvládnout? Jaké znalosti a dovednosti potřebuje? Vymyslete alespoň 10 znalostí a dovedností, které jsou pro práci youtubera důležité, a dopište je do jednotlivých bublin.



Metodika k aktivitě: Youtuberka Katka

Aktivita se zaměřuje na kyberšikanu ve spojení s fenoménem youtuberství – děti jsou v kontaktu s prostředím YouTube již od malička. Obsah na YouTube sledují podle výzkumů realizovaných v ČR od cca 9 let, přičemž kolem 13. roku věku přecházejí na další sociální platformy, jako jsou Instagram či TikTok. Aktivitu proto věnujeme právě činnostem spojeným s YouTube.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie dítěte, která je důležitá k podpoře emočního prožitku u dětí a k jejich identifikaci se s obětí. Následně je necháme zodpovědět na položené otázky a rozvedeme diskusi na téma, zda může verbální agrese v online prostředí člověku ublížit.

Otázky učitele (průvodce):

1. Jak byste reagovali, kdybyste byli na místě Katky?
   (Otázka otevírá prostor pro konfrontaci různých názorů a přístupů k této situaci. Existuje celá řada reakcí, např. snaha zablokovat nepřátelský profil, vypnout komentáře na vlastním profilu, zrušit vlastní profil, různé druhy konfrontací (třeba pomocí reakčního videa), ignorace problému apod.)
2. Kdo z vás sleduje YouTube? Jaká videa na YouTube sledujete?
3. Sledujete youtubery? Chtěli byste být jako youtubeři? Proč?
4. Myslíte si, že má youtuberství nějaká pozitiva?
5. Myslíte si, že má youtuberství také nějaká negativa?
6. Jak byste reagovali, kdybyste byli Katkou? Co byste dělali na jejím místě?
7. Když je někdo na internetu slavný, má pouze své fanoušky, nebo i tzv. hatery?
8. Jaké technické dovednosti potřebujete mít, abyste se mohli stát youtubery?
9. Jaké další vlastnosti, dovednosti či znalosti potřebujete pro práci youtubera?

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že sláva v prostředí internetu má svá pozitiva i negativa a že v podstatě každý úspěšný youtuber/streamer/influencer má své nepřátele – hatery. A že také existuje jen hrstka úspěšných, kteří vyrostli na ohromném množství neúspěšných. Současně pokračujeme v poselství, že i na internetu můžeme lidem vážně ublížit a že oběť často nedokáže rozlišit, zda své výhrůžky myslíme nebo nemyslíme vážně. Stejně tak je nutné upozornit na důsledky, které můžeme svým chováním způsobit.

Práce youtubera

V současnosti může být youtuberství zajímavým zdrojem výdělku, pro řadu influencerů se dokonce stalo jejich hlavním zdrojem příjmu. Ovšem jako každá jiná lidská činnost vyžaduje celou řadu znalostí a dovedností. Zde najdete některé z nich:

1. **Komunikační dovednosti**

   Musí umět mluvit srozumitelně, jasně, plynule, mít dostatečnou slovní zásobu atd.

2. **Všeobecný přehled, systematické vyhledávání nových témat**

   Měl by mít všeobecný přehled a umět systematicky vyhledávat nová a zajímavá témata, která dokáže zpracovat a která se budou líbit publiku.

3. **Tvorba scénářů**

   Musí umět vytvořit srozumitelný a přehledný scénář svého videa, který upoutá pozornost.

4. **Technické dovednosti – hardware**

   Musí umět pracovat s technikou – kamera, mikrofon, světla apod.

5. **Technické dovednosti – software**

   Musí umět sestříhat video apod.

6. **Základy práva**

   Musí vědět, jaký obsah smí a nesmí ve videích používat, aby video nebylo zablokováno či omezeno jeho zpeněžení (monetizace).

7. **Práce s komunitou**

   Musí umět pracovat se svými fanoušky, naučit se reagovat na jejich ohlas, komentáře, vytvořit si strategii pro práci s hejtry apod.

8. **Time management**

   Musí si umět plánovat čas – kdy bude tvořit, kdy sbírat materiál, kdy zveřejňovat, v jaké frekvenci, kdy bude odpočívat apod.

9. **Znalosti cizího jazyka**

   Cizí jazyk, především angličtina, se hodí nejenom na internetu.

10. Schopnost vyjednávat podmínky (např. spolupráce)

Youtubeři běžně komunikují s firmami, které jim nabízejí různé druhy reklamní spolupráce. Proto je důležité umět vyjednat ideální finanční či nefinanční podmínky. K tomu je např. zapotřebí umění sebeprezentace, schopnost argumentovat atd.

Další možnosti práce s tématem:

Natáčení videí lze s úspěchem využít na podporu rozvoje mluveného projevu u žáků a může být zajímavou alternativou referátu prezentovaného před třídou, která je vhodná např. pro žáky více ostýchavé, introvertní apod.

K umocnění tématu lze využít také různé druhy audiovizuálního obsahu, který se na kyberšikanu v prostředí sociálních sítí zaměřuje. Můžeme vyjít např. z refrénu klipu Cizí zeď: „Rádi píšem na cizí zeď a další jed plodí další jed. A to, že každý může mít svůj hlas, neznamená, že musí soudit nás."

Klip Cizí zeď (Kazma, kampaň 1/10)

https://www.stream.cz/onemanshow/10027737-pisen-ktera-se-pres-noc-stala-hitem-onemanshow-foundation-cizi-zed

Aktivita: Petr z Minecraftu

Přečtěte si příběh Petra, který má rád Minecraft. Poté se pokuste zodpovědět otázky pod textem příběhu.

Zdroj obrázku: Microsoft

11letý Petr byl vášnivým hráčem online hry Minecraft, se svými kamarády hrál tuto hru na serveru, který denně navštívilo a do hry se připojilo více než 2 000 uživatelů. Jednotliví hráči společně komunikovali za pomoci běžného textového chatu, řada z nich však také využívala instant messenger s VoIP – Skype. Při objevování světa Minecraftu se Petr seznámil s 13letým Jakubem. Z obou chlapců se stali herní přátelé a večer spolu pravidelně hráli a komunikovali přes Skype, stejně tak si nahrávali své herní pokroky a sdíleli je na YouTube. Ke komunikaci využívali taky webkameru. V rámci komunikace prostřednictvím videochatu pro vzájemné pobavení předváděli různé směšné a komické kreace, kterými doprovázeli hraní, řada z nich byla rovněž intimního charakteru (např. částečně vysvlečení předváděli různé fiktivní praktiky).

Zdroj obrázku: PlanetMinecraft.com

Jejich přátelství trvalo od 6. ledna do 11. června – tehdy mezi nimi došlo k hádce. Hádka byla spojena se samotnou hrou a v rámci návalu vzteku Petr zničil velké množství staveb, které společně ve hře vytvořili. Jakub se na Petra naštval a na YouTube nahrál videozáznamy intimních kreací Petra. Na YouTube také uveřejnil jméno a příjmení Petra, společně s jeho e-mailem. Videa se začala velmi rychle šířit internetem a brzy si získala pozornost velkého množství uživatelů, kteří záznamy posměšně komentovali, vytvářeli parodie a videa dále rozesílali prostřednictvím sociálních sítí Facebook a Instagram.

? Hrajete online hry? A znáte nebo hrajete hru Minecraft?

? Přečtěte si výše uvedený příběh a rozhodněte, jak byste jej vyřešili z pohledu Petra a z pohledu Jakuba.

Metodika k aktivitě: Petr z Minecraftu

Aktivita se věnuje **kyberšikaně spojené s hraním online her** (v našem případě Minecraftu, lze zde však dosadit libovolnou oblíbenou online hru) a je cílena především na chlapce. Aktivita je zaměřena na důležitost ochrany osobních údajů v online prostředí a na riziko jejich zveřejnění a zneužití ke kybernetické šikaně.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie. Následně je necháme zodpovědět na položené otázky a rozvedeme diskusi na téma, zda může verbální agrese v online prostředí člověku ublížit.

Otázky učitele (průvodce):

1. Hrajete online hry? A znáte nebo hrajete hru Minecraft?
2. Přečtěte si uvedený příběh a rozhodněte, jak byste jej vyřešili z pohledu Petra a z pohledu Jakuba.
3. V našem příběhu došlo k úniku osobních údajů. Zkuste uvést, které osobní údaje jsou na internetu nejvíce zneužitelné a proč. Které osobní údaje máte na internetu vy sami?
4. Jakým způsobem je možné chránit si své osobní údaje? Jakým způsobem je máte chráněny?
   (Heslo, anonymizace v prohlížeči, využívání různých anonymizačních aplikací – Tellonym apod.)
5. Co byste dělali v situaci, kdy byste zjistili, že na internet uniklo video (třeba z webkamery), které je pro vás ponižující – jste na něm zachyceni ve směšné situaci?
6. Kdybyste na YouTube narazili na video, které ponižuje někoho jiného, jak byste se zachovali?
   (Ignorování, nahlášení videa, oznámení rodičům s radou o pomoc apod.)
7. Který osobní údaj je podle vás v online prostředí nejvíce zneužitelný?
   (Otázku lze pojmout jako brainstorming, výsledkem by měl být osobní údaj, který umožňuje naši jednoznačnou identifikaci – fotografie obličeje, případně intimní fotografie, na které je rozpoznatelný náš obličej.)

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že je v prostředí internetu nutné chránit si své osobní údaje, protože mohou být zneužity pro kybernetickou šikanu. V našem příkladu pracujeme s prostředím online her, ale k úniku osobních údajů může dojít např. i v prostředí sociálních sítí – je třeba uvědomit si, že osobní údaje (jméno a příjmení, kontaktní údaje, fotografie a video) mají svou hodnotu a je nutné si je chránit.

Aktivita: Hranice kyberšikany

Přečtěte si následující tvrzení a zkuste rozhodnout, zda s nimi souhlasíte.

1. Každý máme právo na svobodu slova, proto můžeme na internetu psát o komkoli cokoli.

2. Pokud na mě na internetu někdo zaútočí – třeba mi nadává, vyhrožuje mi a uráží mě – mám právo mu toto oplatit stejným způsobem.

3. Na internetu si můžeme dělat všechno, co chceme, protože nejde o reálný svět, ale o svět virtuální, ve kterém neplatí to, co ve světě skutečném.

4. Na internetu jsou si všichni rovni, a proto zde neplatí žádná pravidla slušného chování.

5. Pokud mě na sociálních sítích někdo uráží, mám právo ho zablokovat (vzájemně se na sítích nevidíme).

Metodika k aktivitě: Hranice kyberšikany

Aktivita Hranice kyberšikany využívá metody „andělé a démoni" a je zaměřena na rozvoj argumentačních dovedností žáků. Třída je rozdělena do dvou skupin, ze kterých vždy jedna obhajuje daný výrok a druhá je v opozici. Po zadání tématu mají žáci prostor na sestavení svých argumentů a protiargumentů, které poté prezentují. Učitel jako mediátor zapisuje výsledné argumenty v bodech do dvou sloupců na tabuli.

Výrok 1 se zaměřuje na svobodu slova (projevu) na internetu – ta však není neomezená. Svoboda projevu je jedním ze základních lidských práv, které je definováno v řadě dokumentů – ve Všeobecné deklaraci lidských práv, Mezinárodním paktu o občanských a politických právech a v ČR především v Listině základních lidských práv a svobod (článek 17).

(1) Svoboda projevu a právo na informace jsou zaručeny.
(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.
(3) Cenzura je nepřípustná.
(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.
(5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.

Při argumentaci využíváme především kombinace odstavce 2 a odstavce 4 – **tedy máme sice právo vyjadřovat své názory, ale nesmíme zasahovat do práv a svobod druhých lidí** (např. nesmíme podněcovat k násilí či nenávisti, pomlouvat, diskriminovat atd.). Na internetu jednoduše komunikujeme slušně (netiketa).

Výrok 2 se zaměřuje na obranu svých práv na internetu. **Pokud nás někdo napadne na internetu, musíme volit adekvátní reakci** – např. pokud nám někdo vyhrožuje, neznamená to, že mu budeme vyhrožovat také. Máme celou řadu nástrojů, jak svá práva bránit – od nahlášení příspěvku administrátorům, oznámení útoku rodičům, učiteli, blokování až po ochranu práv soudní cestou (policie, občanskoprávní spor). V případě, že reagujeme stejně, jako agresor, dopouštíme se stejného jednání – které sice lze argumenty ospravedlnit, ale není v souladu s netiketou (role se přepnuly – z oběti je útočník). Jednoduše se nesnižujeme na úroveň agresora a snažíme se o nadhled.

Výrok 3 cílí na vnímání internetu jako něčeho, co je čistě virtuální. Ale i na internetu jsme odpovědní za vše, co děláme. Jako příklad lze využít kauzu nenávistných komentářů fotografie prvňáčků z teplické základní školy. Policie ČR začala stíhat hned několik osob, které fotografii

komentovaly, některé z osob již byly za své jednání odsouzeny (podmíněný trest, pokuta 20 000 Kč). Podobně lze využít příkladu online verbálních útoků na zpěváka Radka Bangu. I zde někteří autoři neunikli svému trestu. Výsledkem argumentačního souboje by tedy mělo být, že i **na internetu jsme odpovědní za vše, co děláme**.

Výrok 4: Samozřejmě i na internetu existují pravidla slušného chování, kterým se říká **netiketa**.

Poslední výrok se zaměřuje na to, zda máme právo zablokovat si komunikaci s člověkem, který nám na internetu ubližuje – třeba nás pomlouvá, uráží či jinak dehonestuje. Ano, na to **máme právo** a k tomu ostatně slouží také blokační tlačítka – máme právo chránit si náš online prostor (např. profil) a máme právo rozhodovat o tom, kdo se k našemu obsahu dostane. Je to podobné, jako když si uzamkneme svůj byt či když si zablokujeme obtěžující telefonní číslo.

Zdroje:

Za nenávistné komentáře pod fotkou prvňáků dostala žena podmínku a pokutu. iDnes.cz. https://www.idnes.cz/plzen/zpravy/soud-zakladni-skola-teplice-komentar-nenavist-prvnaci-rozhodnuti-pokuta-podminka.A180914_161810_plzen-zpravy_vb

Rasistický útok na Radka Bangu alias Gipsyho: Padly tresty! Blesk.cz. https://www.blesk.cz/clanek/celebrity-ceske-celebrity/510607/rasisticky-utok-na-radka-bangu-alias-gipsyho-padly-tresty.html

Mladík na Bangově Facebooku hrozil Židům, musí odpracovat sto hodin. iDnes.cz. https://www.idnes.cz/zpravy/cerna-kronika/radek-banga-soud-vyhruzky.A170823_223741_domaci_lre

SEXTING A JEHO RIZIKA

Aktivita: Nezvládnutý rozchod

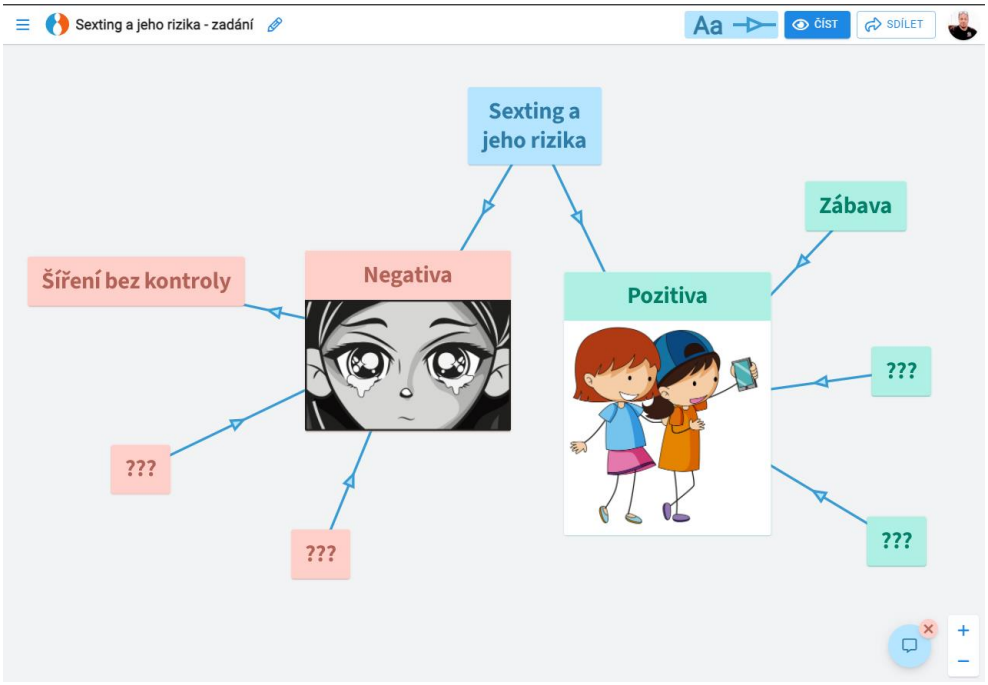
Přečtěte si následující příběh a pokuste se zodpovědět otázky pod textem.

15letá Zuzana chodila s Petrem již několik let, milovala ho, zbožňovala ho, měla s ním sex. Sex si společně natáčeli videokamerou a fotili. Po dvou letech se však spolu rozešli. Petr vytvořil falešnou webovou stránku Zuzany, na kterou umístil její osobní údaje (jméno, příjmení, telefonní číslo, e-mail, intimní fotografie a videa), a rozšířil odkaz na tuto stránku mezi spolužáky Zuzany, učitele, rodiče Zuzany i rodiče spolužáků a další uživatele sociálních sítí. Zuzana se o stránce dozvěděla po několika dnech – podle počítadla stránku navštívilo více než 5 000 uživatelů.

Co byste dělali být na místě Zuzany? Co se vlastně dá v takové situaci dělat?

? V našem případě spolu Petr a Zuzana provozovali sexting, tj. pořídili a vzájemně sdíleli intimní materiály (fotografie, videa). Mohli sexting ale skutečně legálně realizovat?

? S využitím některého z online nástrojů určeného pro tvorbu pojmových a myšlenkových map (např. OrgPad) vytvořte mapu, která zobrazuje pozitiva a negativa sextingu. Inspiraci můžete hledat níže.



(Rozpracovaná pojmová mapa zaměřená na sexting a jeho rizika, OrgPad)

Metodika k aktivitě: Nezvládnutý rozchod

Cílem aktivity je uvědomit si, jakou hodnotu mají naše osobní údaje a jak je snadné je zneužít. A zejména pak upozornit na riziko tzv. **sextingu** – tj. dobrovolného sdílení osobních údajů s jinými uživateli (přáteli, partnery). Na příběhu demonstrujeme, jak je rizikové sdílet intimní materiály v rámci partnerského vztahu.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie partnerského páru, která je důležitá k podpoře emočního prožitku u žáků a k jejich identifikaci se s obětí. Následně je necháme zodpovědět na položené otázky a rozvedeme diskusi na téma, zda může být sexting rizikový.

Otázky učitele (průvodce):

1. Co byste dělali být na místě Zuzany? Co se vlastně dá v takové situaci dělat?
2. V našem případě spolu Petr a Zuzana provozovali sexting, tj. pořídili a vzájemně sdíleli intimní materiály (fotografie, videa). Mohli sexting ale skutečně legálně realizovat? (Ne, nebylo jim 18 let, mohli sice mít sex, ale nesměli se u něj fotit.)
3. Poškodilo nějakým způsobem chování Petra Zuzanu? (Ano, dopad na psychický stav, ale pravděpodobně i na stav fyzický – psychosomatické projevy.)
4. Myslíte si, že Petr porušil zákon? (Ano, na jedné straně vyráběl a šířil tzv. dětskou pornografii, dále se dopustil trestného činu pomluvy apod.)
5. Jak si myslíte, že příběh dopadl? Zkuste jej dokončit.

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že **sexting může člověku vážně ublížit a že není dobré spoléhat ani na důvěryhodnost partnera** (nikdy nevíme, jak dlouho nám vztah vydrží, a pokud dojde k nezvládnutému rozchodu, může se stát útočníkem i náš vlastní partner).

Dokončení příběhu:

Uvedený příběh vychází ze skutečného příběhu kyberšikany využívající sexting. Jména osob byla změněna.

Zuzana kontaktovala online poradnu projektu E-Bezpečí a také Policii ČR, která vyhodnotila jednání Petra jako závažné. Petr byl nakonec potrestán podmíněným trestem a finanční náhradou vzniklé újmy.

Aktivita: Michael z Gifyo

Přečtěte si následující příběh a pokuste se zodpovědět na otázky pod textem.

Zdroj: Facebook, případ E-Bezpečí

Gifyo je název sociální sítě, která se orientovala na výměnu animovaných obrázků, gifů. 15letá Žaneta se rozhodla, že si vyzkouší, jak Gifyo funguje. Žaneta byla jazykově zdatná a angličtina jí nečinila žádné potíže, zaregistrovala se a stala se aktivní uživatelkou. Jednoho dne se seznámila s Michaelem. Michael byl krásný, štíhlý, černovlasý 16letý vyznavač stylu emo. Michael pocházel z Francie a stejně jako Žaneta sítě Gifyo aktivně využíval, svůj profil zásoboval různými fotografiemi, na některých byl od pasu nahoru nahý. Žanetě rovněž odeslal odkaz na svůj profil na Facebooku a ona si jej přidala do přátel.

Michael začal se Žanetou konverzovat, začali si společně vyměňovat stále odvážnější fota a jednoho dne mu Žaneta poslala svou vlastní fotografii „nahoře bez", přičemž na ní byl zřetelně a jasně zachycen Žanetin obličej.

Michael začal Žanetě psát o další fotografie. Žaneta však odmítla. Způsob jejich komunikace se pak ze dne na den radikálně změnil. Michael oznámil Žanetě, že navštívil její facebookový účet a získal kontakty na její přátele a rodiče s tím, že pokud mu nezašle další intimní materiály, zveřejní její fotografie na erotických portálech a informuje o jejich existenci její přátele. Žaneta mu nevěřila, načež Michael zveřejnil první 3 fotografie na veřejném úložišti fotografií, zatím s omezeným přístupem (veřejnost neměla do galerie fotografií přístup, fotografie mohl zobrazit pouze Michael a Žaneta). Vydírání pokračovalo stále intenzivněji a v tuto chvíli Žaneta kontaktovala poradnu E-Bezpečí...

? Co udělala Žaneta špatně a jak byste se zachovali vy?

? Jak si myslíte, že se bude příběh vyvíjet dál?

? Má smysl v této situaci kontaktovat policii?

? Existují nějaké další organizace, na které se můžete v krizové situaci v online světě obrátit? Znáte jejich názvy, webovky či telefonní čísla?

Metodika k aktivitě: Michael z Gifyo

Cílem aktivity je uvědomit si, jak **snadno mohou být naše intimní materiály v online prostředí zneužity – např. v rámci intenzivního vydírání**. Výsledkem by mělo být ovlivnění postoje žáků směrem ke sdílení intimních materiálů s neznámými lidmi bez ověřené identity.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie partnerského páru, která je důležitá k podpoře emočního prožitku u žáků a k jejich identifikaci se s obětí. Následně je necháme zodpovědět na položené otázky a rozvedeme diskusi na téma, zda může být sexting rizikový.

V rámci aktivity využíváme skutečný případ, který byl řešen online poradnou projektu E-Bezpečí a který je podrobně zpracován zde:

http://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sexting/522-gifyo

Otázky učitele (průvodce):

1. Co udělala Žaneta špatně a jak byste se zachovali vy?
2. Komu všemu mohl Michael poslat fotografie Žanety?
   (V příběhu je popsáno, že si Žaneta přidala Michaela mezi své facebookové přátele, tím pádem mohl vidět její přátele a poslat jim intimní fotografie Žanety.)
3. Jak si myslíte, že se bude příběh vyvíjet dál? Zkuste navrhnout řešení.
4. Má smysl kontaktovat policii?
   (Určitě ano! Policie může pomoci usvědčit pachatele, zajistit bezpečnost oběti atd.)
5. Existují organizace, na které byste se mohli v tomto případě obrátit o pomoc?
   (Organizací je celá řada – Linka bezpečí, Safer Internet Centrum, NIC.cz, Dětské krizové centrum a samozřejmě E-Bezpečí apod.)

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že sexting může člověku vážně ublížit a že není dobré nechat se nachytat na fotografie v profilech, které mohou být podvrženy. A že to, co z počátku vypadá jako dokonalá virtuální láska, se může rychle změnit v temnou noční můru.

Dokončení příběhu:

Uvedený příběh vychází ze skutečného příběhu kyberšikany využívající sexting. Jména osob byla změněna.

Poté, co Žaneta situaci nahlásila týmu projektu E-Bezpečí, bylo zahájeno policejní vyšetřování. Během něj se zjistilo, že Michael ve skutečnosti vůbec neexistoval. Fotografie Michaela

pocházela ze zahraniční fotogalerie, za profilem se ve skutečnosti skrýval 33letý muž z Prahy, který podobným způsobem vydíral několik dívek. Policie muže zadržela a bylo proti němu zahájeno trestní řízení (trestný čin sexuální nátlak a další TČ).

Navazující otázky:

1. Lze si někde na internetu ověřit, jaký je původ fotografie, tj. kde všude na internetu je daná fotografie uložena?

Ano, existuje funkce **reverzní vyhledávání podle fotografie**, která je součástí vyhledávače Google (část Google Obrázky). Můžeme také využít specializovaný server TinEye.

S žáky si můžeme vyhledávání vyzkoušet, například stáhnout z internetu libovolnou fotografii celebrity a zkusit vyhledat její výskyt – třeba pomocí služby **Google Obrázky** (https://www.google.cz/imghp?hl=cs).

2. Dá se z fotografie zjistit, kdy a kde byla pořízena?

Ano, **do originální fotografie se ukládá celá řada informací** (tzv. metadat či Exif), např. o tom, kdy a kde přesně byla fotografie vytvořena. Tyto informace je také možné z fotografií přečíst pomocí různých programů a aplikací. Pozor, jakmile začneme fotografie upravovat a nahrávat na sociální sítě, informace z fotografií může zmizet. Sociální sítě si také umí tyto informace z fotografie načíst.

3. Týká se vydírání pomocí intimních materiálů pouze dívek, nebo také chlapců? A jde chlapce vůbec zneužít?

Vydírání se týká jak dívek, tak i chlapců. V České republice najdeme mnoho případů, kdy došlo k intenzivnímu vydírání, které skončilo sexuálním zneužitím chlapce (či skupiny chlapců). Dávejme si tedy pozor i na situace, kdy od chlapce intimní materiály vyžaduje dívka.

Typickým příkladem může být případ „Piškot a Meluzín“, ve kterém došlo k sexuálnímu zneužití více než 39 dětí, převážně chlapců. Pachatelé za své skutky dostali trest odnětí svobody ve výši 10 let.

Aktivita: Chatování s kámoškou

Na lístečcích je zachycena skutečná komunikace dvou 13letých dívek, které se seznámily na internetu. Jedna se jmenuje Hanka a druhá Pavla. Pořadí jednotlivých zpráv je však přeházeno. Pokuste se seřadit lístečky tak, jak komunikace ve skutečnosti probíhala.

Moc se mi nechce, spíš mi nějakou pošli ty, ano?

Nemusíš se stydět, vždyť tu nikdo není, jsme tu jen my dvě kámošky...

Díky, ty jsi úplné zlatíčko. Pošleš mi taky nějakou svojí v podprsence?

Udělala jsem ti něco? Promiň, nechtěla jsem tě otravovat... Ty mi nevěříš? Ale já ti fotku poslala, já ti věřím...

Nevadí, klidně mi ji pošli.

Tak dobře, posílám svou fotku v podprsence...

Nechci... stydím se...

Taky ti to sluší, jsi hezká

- Co myslíš, probíhá komunikace skutečně mezi dvěma dívkami? Nebo je to pravděpodobně jinak?

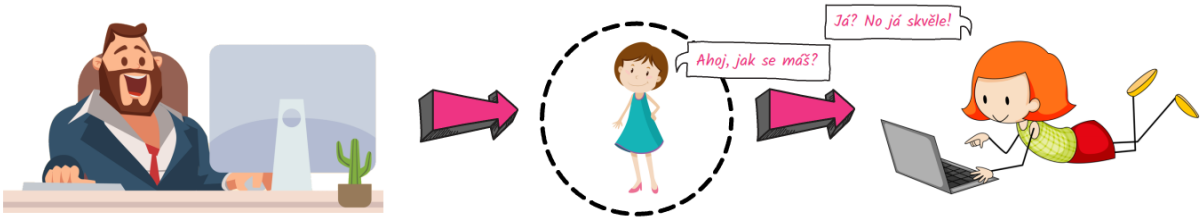
- O čem by ses bavil/a s člověkem, kterého znáš pouze ze sítě? Napadají tě nějaká témata?

- O čem by ses určitě nebavil/a s člověkem, kterého znáš pouze ze sítě? Napadají tě nějaká témata?

Metodika k aktivitě: Chatování s kámoškou

Aktivita navazuje na příběh Michaela a Žanety a upozorňuje na to, jak snadno může do online prostředí uniknout intimní materiál, a to v rámci komunikace dvou „dětí“. Ve skutečnosti je jedno z dětí agresor – dospělý člověk (modrá část).

Aktivita vychází z modelu vydírání dětí v kyberprostoru, který je podrobně zpracován např. zde: https://www.pediatriepropraxi.cz/pdfs/ped/2014/06/07.pdf a zde: https://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/687-vydiranideti. Na lístečcích jsou zachyceny skutečné záznamy komunikace mezi pachatelem, který se v online prostředí vydává za dítě, a dítětem.



Správné pořadí lístečků (žáci samozřejmě mohou vymyslet vlastní variace):

1. Ahoj, promiň, něco jsem na internetu hledala a omylem jsem si tě přidala do přátel. Já jsem Pavla. Můžeme si spolu třeba psát, chceš? 😊
2. Tak dobře. A o čem si chceš psát?
3. Ty jsi tak strašně hodná, že sis mě přidala. Můžeme být skvělé kámošky, ano? Můžeme si psát o čemkoli. A třeba si i vyměnit nějaké hezké fotečky, chceš?
4. Dobře, začneš? 😊
5. Jasně, pošlu ti svou vlastní fotku, ať víš, jak vypadám, ano? A ty mi pak pošleš svou vlastní, souhlasíš? 😊
6. Dobře, tak mi ji pošli, ano?
7. Poslal jsem ti fotku... už k tobě letí. A ty mi na oplátku taky pošli, jak vypadáš 😊
8. Díky za fotku, na oplátku posílám svou.
9. Jéé, ty jsi na té fotce nádherná. Moc ti to sluší. Jsi překrásná. Pošleš mi další? 😊
10. 😊 Moc se mi nechce, spíš mi nějakou pošli ty, ano?
11. Tak dobře, mám jednu malinko... odvážnější, takovou trošku intimnější v podprsence... můžu ti ji poslat? 😊 Nevadí ti to?
12. Nevadí, klidně mi ji pošli.
13. Tak dobře, posílám... ale jak říkám, je trošku intimnější, jsem tam v podprsence. 😊
14. Taky ti to sluší, jsi hezká. 😊
15. Díky, ty jsi úplné zlatíčko. 😊 Pošleš mi taky nějakou svojí v podprsence?

16. Nechci... stydím se...
17. Nemusíš se stydět, vždyť tu nikdo není, jsme tu jen my dvě kámošky... 😊
18. Já ti fakt nic takového posílat nechci...
19. Udělala jsem ti něco? ☹ Promiň, nechtěla jsem tě otravovat... Ty mi nevěříš? ☹ Ale já ti fotku poslala, já ti věřím...
20. Tak dobře, posílám svou fotku v podprsence...

Otázky učitele (průvodce):

1. Zkuste popsat, jak by mohla komunikace probíhat dál.
2. Mohla by být fotografie, kterou Hanka odeslala neznámé Pavle, nějakým způsobem zneužita?
3. Všimli jste si, jakým způsobem byla zahájena komunikace?
   (Jakoby náhodou, ale toto je právě strategie útočníka.)
4. Pro komunikaci agresora a dítěte je typická manipulace lichotkami, všimněte si, jak často jedna dívka chválí tu druhou.
5. Kdo spolu skutečně komunikuje? Jedná se o dvě dívky, nebo jste si všimli něčeho jiného?
   (V internetové komunikaci je třeba sledovat i detaily. Pokud se podíváme na lísteček č. 7, zjistíme, že najednou dívka komunikuje v mužském rodě – tj. pachatel se spletl!)

Dokončení příběhu:

Náš příběh vychází ze skutečných příběhů komunikace dětí a dospělých osob (maskovaných za děti), ve kterých došlo k úniku intimních materiálů a jejich zneužití pro vydírání.

V našem příběhu se z Pavly vyklubal muž, který z dětí lákal intimní materiály a vydíral je tím, že pokud nepošlou další fotografie, zveřejní vše na internetu a děti budou mít ostudu. Z obavy proto pachatele zásobovaly těmito materiály – často spadajícími do oblasti dětské pornografie. Muž takto vydíral více než 100 dětí ve věku 11-15 let.

Aktivita: Super pokec na videochatu

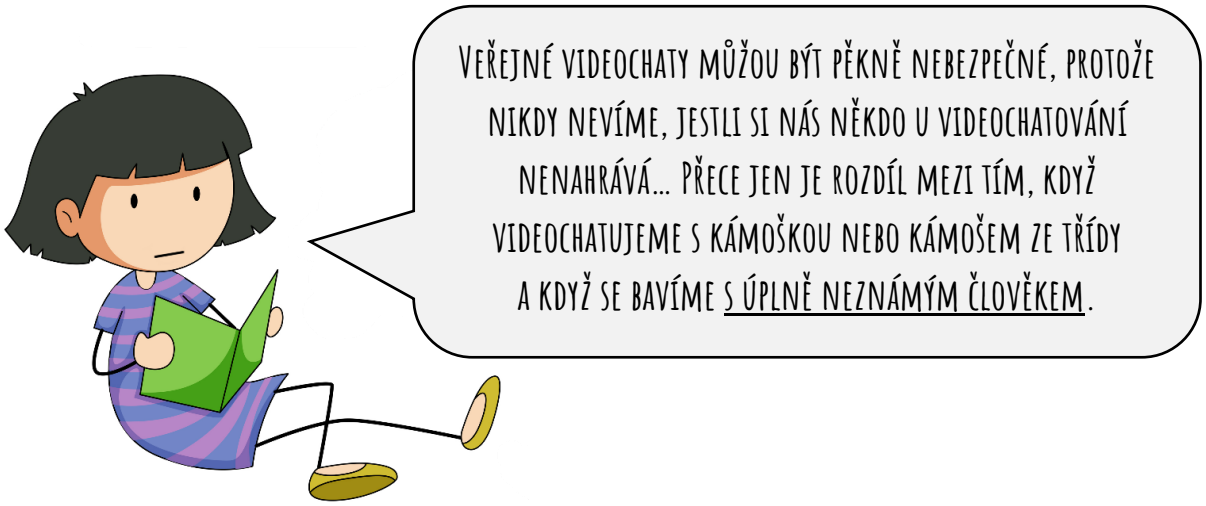
? Přečtěte si následující příběh, který se skutečně stal, a pokuste se zodpovědět otázky pod textem.

Vendy s oblibou navštěvovala nejrůznější sociální sítě a služby a byla na nich hodně aktivní – ráda sdílela zážitky ze svého života a ráda poznávala nové lidi. S některými z nich si i dlouho psala. Psaní ji však časem čím dál více obtěžovalo. Přestalo ji totiž bavit pořád někomu zdlouhavě odepisovat. Jednoho dne však objevila kouzlo videochatu, kde si mohla prostřednictvím webkamery povídat s různými lidmi z celého světa bez otravného psaní. Na jednom velmi oblíbeném videochatu potkala úžasného kluka, který se zdál jako jediný normální a který se jí velmi líbil.

Videochatovali spolu přes 5 hodin, rozuměla si s ním. V jednu chvíli se dostali do momentu, kdy Vendy měla na webce „něco" ukázat a on se na to díval. Byla v tílku a měla tanga a ukazovala svůj zadek. Kluk byl nadšený, Vendy říkal, jak je krásná a jak jí to sluší. Pak přešli na Instagram, kde si pro změnu chvíli psali, ale pak to nějak pominulo. Vendy to chvilku mrzelo, ale pak si řekla, že takových „pokecůˮ bude ještě spousta a příště se seznámí na videochatu s možná ještě úžasnějším klukem. Na bezva pokec zapomněla a dál chodila na videochat, kde potkávala další nové lidi. Tady by mohl náš příběh skončit. Opravdu?

Asi po měsíci od super pokecu s klukem z videochatu zažila Vendy šok. Překvapená kamarádka jí napsala, jestli se náhodou nezbláznila. Vendy zprávě od kamarádky nerozuměla, proto jí kamarádka poslala odkaz na video na velmi známých stránkách s pornografií, kde byla Vendy natočená, jak se ukazuje před webkamerou. Na videu byla jen Vendy, kluk, se kterým si povídala, tam natočený nebyl. Video mělo za měsíc sdílení 25 tisíc zhlédnutí a navíc bylo Vendy vidět do obličeje.

- Udělala Vendy něco špatně? Pokud ano, co?
- Jak se asi příběh vyvíjel dál?
- Myslíte si, že může být problém, když je na videu vidět náš obličej?
- Napadá vás nějaký způsob, jak by se Vendy dalo pomoci?
- Má smysl v této situaci kontaktovat policii?



Metodika k aktivitě: Super pokec na videochatu

Cílem aktivity je popsat rizika spojená s videochatem, dále upozornit na citlivost zveřejňování osobních údajů, uvědomit si, jak **snadno mohou být naše osobní údaje včetně intimních materiálů v online prostředí zneužity – např. k dehonestování v podobě zveřejňování intimních videí apod**. Aktivita by měla přispět k ovlivnění afektivní stránky žáků směrem k uvědomění si rizik sdílení intimních materiálů s neznámými lidmi.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům příběh vytiskneme, a to včetně fotografie dívky, která je důležitá k podpoře emočního prožitku u žáků a k identifikaci se s obětí. Následně žáky necháme zodpovědět položené otázky a rozvedeme diskusi na téma rizikovosti sextingu.

V rámci aktivity využíváme skutečný případ, který byl řešen online poradnou projektu E-Bezpečí.

Otázky učitele (průvodce):

1. Co udělala Vendy špatně a jak byste na žádost o obnažování před webkamerou reagovali vy?
2. Proč je nebezpečné, když je na takovémto videu vidět náš obličej?
3. Mohlo být video Vendy rozšířeno i na jiné pornografické stránky?
4. Jak si myslíte, že se příběh vyvíjel dál?
5. Zkuste navrhnout možná řešení, jak dál postupovat.

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že **sexting prostřednictvím webkamery může člověku vážně ublížit** a že není dobré nechat se nachytat na lichotky, kterými nás náš komunikační partner zahrnuje. Na počátku většiny komunikací na internetu je chování účastníků velmi příjemné, protože protistrana často za vše chválí, je milá a empatická.

Dokončení příběhu:

Uvedený příběh vychází ze skutečného příběhu sextingu. Jména osob byla změněna.

Poté, co Vendy svůj případ zaslala prostřednictvím elektronického formuláře do poradny projektu E-Bezpečí (www.napisnam.cz), byla věc předána k prošetření Policii ČR. Během vyšetřování nebyla zjištěna totožnost pachatele, který pořídil záznam videochatu s Vendy. Velmi problematické bylo odstranění videozáznamu z pornografických stránek. Po dlouhém vyjednávání a intervenci ze strany Policie ČR bylo video odstraněno, ovšem mezitím se stalo tzv. virálním – začalo se nekontrolovaně a hromadně šířit na internetu, tudíž není možné dané video definitivně z internetu odstranit.

Aktivita: Co víme o sextingu?

Dokázal/a bys vysvětlit, co je to vlastně sexting? Využít můžeš následující lístečky… Ale pozor, nenech se zmást!

Je to jiný název pro sex!

Součást seznamování.

Sdílení intimních fotek a videí.

Týká se to jen holek.

Posílání nudesek.

Do níže uvedených vět doplň správný věk. Věděl/a by sis se vším rady?

1. Od __ let můžu mít sex!
2. Od __ let můžu fotit své vlastní intimní fotografie (fotky, na kterých jsem obnažený/á).
3. Od __ let můžu mít účet na sociální síti bez souhlasu rodičů.

Komu byste dali svou intimní fotografii („nudesku")? Vyberte či doplňte další možnosti…

Kámoška nebo kámoš	Učitel nebo učitelka z naší školy	Můj přítel nebo přítelkyně	Trenér nebo trenérka
Mamka nebo taťka	Kámoš nebo kámoška z online hry	Spolužák nebo spolužačka	Oblíbený youtuber či youtuberka

Metodika k aktivitě: Co víme o sextingu?

Cílem aktivity je především vymezení hranic sextingu. Využíváme hlavně metody řízené diskuse a brainstormingu, samotné otázky zodpovídají žáci, učitel slouží jako průvodce či korektor v případě, že děti zodpoví otázku nesprávně. Jednotlivá zjištění učitel zapisuje na tabuli (např. do podoby pojmových či mentálních map).

Aktivitu realizujeme v situaci, kdy mají žáci povědomí o tom, co je sex (např. absolvovali sexuální výchovu apod.). Aktivita je tedy vhodná pro žáky 13+, nicméně sexting se objevuje i u dětí mladších.

Jen pro připomenutí – **sexting je odesílání či jiné sdílení vlastních intimních materiálů s jinými uživateli internetu**. Sexting může být realizován dobrovolně, ale také nedobrovolně – pod nátlakem.

Odpovědi na úkoly:

1. Sexting je sdílení (odesílání, ale i přijímání) vlastních intimních materiálů. Je velmi často součástí seznamování. Slovo „nudesky" je název právě pro intimní materiály, které se v rámci sextingu využívají. Sexting se týká dívek i chlapců.
2. Věkové limity:
   Od 15 let mohu mít sex.
   Od 18 let mohu fotit vlastní intimní fotografie.
   Od 15 let mohu mít účet na sociálních sítích bez souhlasu rodičů.
   Dříve 13 let, od 2019 v ČR sjednoceno v souvislosti s opatřením GDPR na 15 let.

Otázky učitele (průvodce):

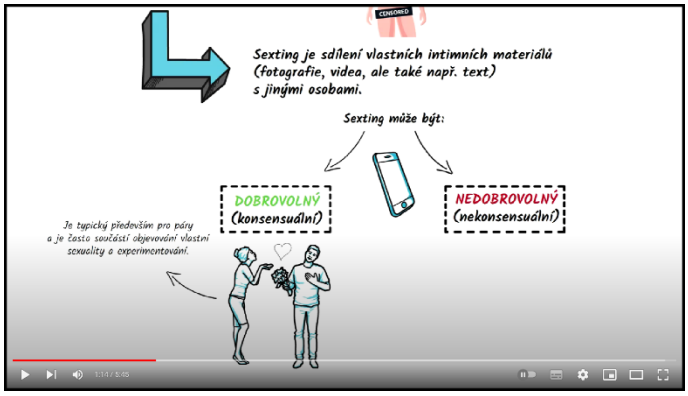
1. Sex je mezi lidmi normální, víte ale, od kolika let může mít člověk sex? A můžete se u sexu fotit?
   (Je důležité rozlišit, že sex mohou mít děti od 15 let, ale až do 18 let nesmí sexuální akt zachycovat – ani fotografií či videem.)
2. Slyšeli jste někdy slovo sexting? Zkuste vlastními slovy říct, co to je sexting.
   (Pokud termín neznají, vysvětlí jej učitel.)
3. Dali byste svému partnerovi (příteli, přítelkyni) svojí fotografii? A co svoji obnaženou fotografii? A dali byste mu fotografii papírovou, nebo digitální?
4. Představte si, že byste svou intimní fotografii poskytli svému partnerovi či partnerce. Co všechno by s ní mohl udělat? Mohl by ji třeba i nějakým způsobem zneužít?
5. Představte si situaci, že by vaše fotografie unikla do prostředí internetu – je možné ji odstranit? Jakým způsobem?

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že sexting může být rizikový, protože **pokud někomu poskytneme svou vlastní fotografii, může ji zneužít proti nám** (což si popíšeme v dalších aktivitách) – například ji použít k našemu vydírání, vyhrožování, může ji rozšířit po internetu apod. Pokud se intimní fotografie dostane na internet, je velmi obtížné – téměř nemožné – se jí zcela zbavit.

Videa k aktivitě

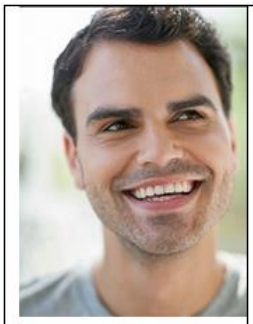
Sexting



ONLINE SEZNAMOVÁNÍ

Aktivita: Poznáš sexuálního útočníka?

? Prohlédni si pozorně fotografie pěti osob a zkus rozhodnout, která z nich je sexuální útočník. Svůj výběr zdůvodni.



1

2

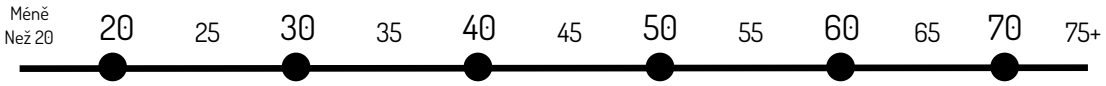
3

4

5

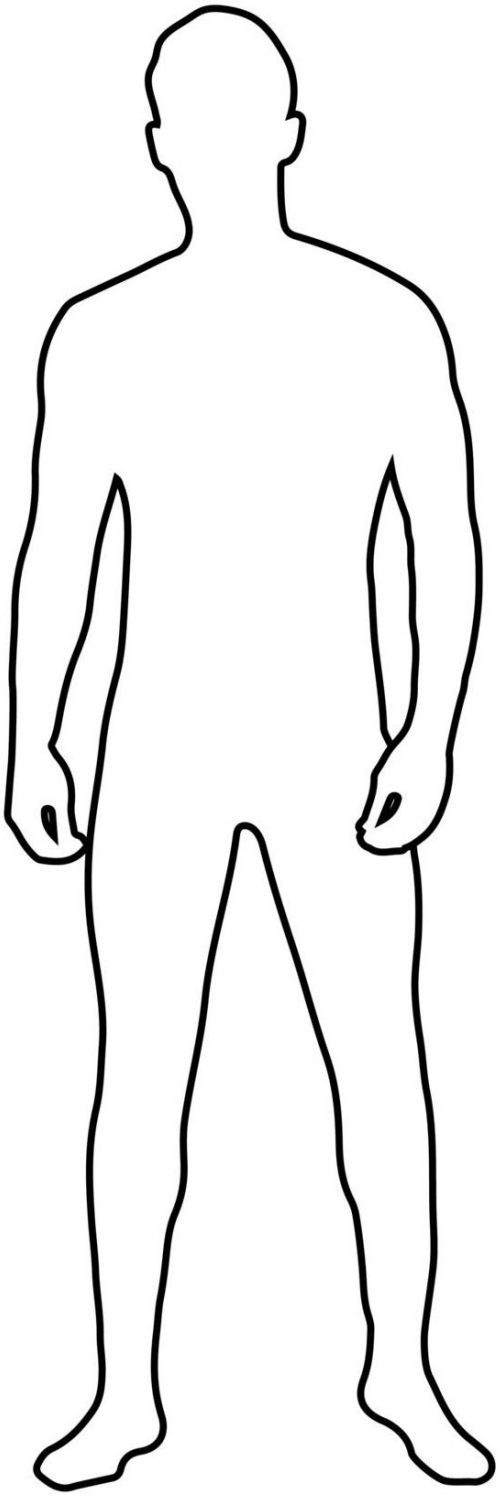
? Dokázal/a bys vymyslet nějaký způsob, jak si ověřit, s kým na internetu skutečně komunikuješ?

? Jak staří jsou podle tebe sexuální útočníci? Svůj výběr zakroužkuj na časové ose.



? Jsou podle tebe sexuální útočníci na internetu spíše muži, nebo ženy?

Jak podle tebe vypadá sexuální útočník? Je hubený, nebo tlustý? Má dlouhé vlasy, nebo je plešatý? Je to vůbec muž, nebo to je žena? Má nějaký typický rys nebo poznávací znamení? Zapoj svou fantazii a nakresli ho! Můžeš využít připravenou siluetu, nebo si celého pachatele nakresli sám.



Metodika k aktivitě: Poznáš sexuálního útočníka?

Cílem aktivity je **uvědomit si, že podle fotografie nelze sexuálního útočníka odhalit**. Jednotlivé fotografie jsou vybrány tak, abychom dětem cíleně nabídli široké množství charakterů – typického usměvavého extroverta, uzavřeného zasmušilého introverta, prototyp „silného muže" (bez vlasů, zato s bradkou), seniora či představitele tzv. umělce.

Mezi fotografiemi je ale skutečně skryt sexuální útočník, jedná se o muže s číslem 2. Jde o Stephena Walkera, 22letého sexuálního útočníka z Oxfordu, který byl v roce 2011 odsouzen k trestu odnětí svobody na 3,5 roku za sexuální aktivity s dívkami mladšími 13 let. Podrobnosti o celém případu naleznete zde: https://www.oxfordmail.co.uk/news/9054270.sex-attacker-stole-girls-childhood/.

Stephen Walker, 22letý sexuální útočník

Co se týče **způsobů ověření skutečné identity člověka**, se kterým komunikujeme, můžeme využít např. možnosti ověření na webové kameře – stačí svého online kamaráda vyzvat, ať například právě teď napíše něco konkrétního na papír a ukáže to na webkameru.

K otázce **stáří pachatelů sexuálních útoků** na děti v online prostředí bychom uvedli, že se ve veřejném prostoru objevuje mnoho zkreslených informací o tom, jak staří pachatelé sexuálních útoků jsou. **K četným mýtům např. patří, že pachatel je staršího věku.** Ve skutečnosti však najdeme pachatele ve všech věkových kategoriích. Podrobnosti k problematice lze nalézt např. zde: https://www.e-bezpeci.cz/index.php/pohledem-vedy/1819-jaky-je-vlastne-vek-pachatelu-sexualne-motivovane-trestne-cinnosti-pachane-na-detech-dle-193b.

V drtivé většině případů jsou pachateli těchto útoků muži.

Aktivita: Kamarád ze sítě

Šárka (16 let) se na sociální síti seznámila se zajímavým a milým klukem z Velké Británie. Pojďme se společně podívat na jeho profil na sociální síti.

Jak byste DJ Peta popsali? Dokázali byste uvést jeho 3 charakterové vlastnosti?

A jak byste ho zhodnotili celkově?

POZITIVNĚ — **SPÍŠE POZITIVNĚ** — **SPÍŠE NEGATIVNĚ** — **NEGATIVNĚ**

Metodika k aktivitě: Kamarád ze sítě

Aktivita se zaměřuje na problematiku podvodných profilů, které jsou online útočníky využívány v rámci tzv. **kybergroomingu**. **Kybergrooming je riziková forma komunikace, ve které dospělá osoba manipuluje dítětem s cílem přimět je k osobní schůzce v reálném světě**. Komunikace velmi často probíhá v prostředí sociálních sítí, případně s využitím dalších komunikačních nástrojů (instant messengerů). Pachatelé obvykle s dítětem komunikují prostřednictvím falešných profilů.

V naší aktivitě prezentujeme ukázku falešného profilu Petera Chapmana, který jej využíval v rámci komunikace s dospívajícími dívkami. Na svém profilu uváděl falešný věk (ve skutečnosti mu v době útoků bylo 33 let) a podvržené fotografie.

Ve skutečnosti Peter Chapman vypadá takto:

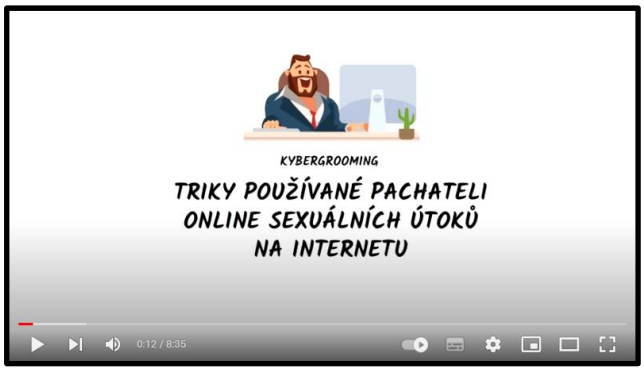
Aktivity pro žáky:

1. Prohlédněte si s žáky profil Petera Chapmana (alias DJPETA) a poté se podívejte, jak vypadá ve skutečnosti. Liší se jeho reálná podoba od podoby, kterou zveřejnil na sociálních sítích?
2. Přečtěte si společně případ Peter Chapman vs. Ashleigh Hallová, který naleznete na webu E-Bezpečí: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1429-peter-chapman-vs-ashleigh-hall-velka-britanie-2010. Co Chapman udělal a jak byl potrestán?
3. Setkali jste se někdy s tím, že by nějaký váš kamarád na svém profilu využíval jako profilovou fotografii fotografii někoho jiného?

Videa k aktivitě

Kybergrooming I

Kybergrooming II



Aktivita: Nenápadné otázky

Sexuální útočník se většinou snaží zjistit co nejvíce informací o své oběti. Mnohdy se ptá na obyčejné otázky, které mu ale o tobě prozradí spoustu důležitých informací. <u>Napiš, proč si myslíš, že by se tě útočník ptal právě na tyto věci</u>:

Mám rozbitý telefon, tak musím používat bráchův počítač, protože já svůj nemám. Co ty, píšeš mi z mobilu, nebo máte doma taky společný počítač?

_____

_____

_____

Taky mě štve, že máme s bráchou společný pokoj. Ale naštěstí chodí často ven s kamarády a já mám při chatování chvilku soukromí. Máš to stejně jako já, nebo máš svůj vlastní pokoj?

_____

_____

_____

Občas bráchovi závidím, že má tolik kámošů. Se mnou se nikdo moc bavit nechce. Chtěl bych alespoň jednoho nej kámoše, kterému bych se mohl se vším svěřovat… Ty máš někoho takového?

_____

_____

_____

Někdy mám chuť zajít za svým taťkou a říct mu, co mě trápí. Ale bojím se, co by si pak o mně myslel. Jaký máš vztah s rodiči ty? Svěřuješ se jim často, nebo se taky bojíš?

_____

_____

_____

Sexuální útočník se během komunikace snaží navázat s obětí co nejužší vztah a budovat důvěru. Využívá proto různé formy úplatků a dárečků, které mu mohou pomoci ověřit osobní údaje, které už od oběti získal. Napiš, co by od tebe útočník získal kromě důvěry, kdyby ti napsal toto:

_____

_____

_____

_____

_____

_____

Obvykle za tyto služby chtějí sexuální útočníci něco na oplátku. Co to bude?

Metodika k aktivitě: Nenápadné otázky

V rámci tzv. **kybergroomingu** (forma komunikace, při které se útočník snaží ve vyhlédnuté oběti vyvolat falešnou důvěru a přimět ji k osobnímu setkání) využívá útočník velké množství technik a postupů.

Sexuální útočník se během procesu manipulace snaží zjistit co nejvíce informací o své oběti. Pracuje tak na vybudování a prohloubení jejich virtuálního vztahu. Nejčastěji se můžeme setkat s technikou **mirroring**, tzv. efekt zrcadlení (pachatel napodobuje oběť ve snaze prolomit její zábrany), **vábení a uplácení oběti** (luring) nebo **phishing** (snaha získat co nejvíce osobních informací o oběti).

První část:

V první části této aktivity se zaměřujeme na techniku **phishing**. Náš fiktivní pachatel se v chatu ptá na čtyři zdánlivě obyčejné otázky, které mu však mohou o oběti prozradit spoustu důležitých informací.

Přečtěte si s žáky útržky online komunikace a nechte je zamyslet se nad tím, proč by se útočník ptal zrovna na tyto otázky a zda by pravdivé odpovědi mohly pro potencionální oběť znamenat riziko.

Otázka č. 1:

Mám rozbitý telefon, tak musím používat bráchův počítač, protože já svůj nemám. Co ty, píšeš mi z mobilu, nebo máte doma taky společný počítač?

- Součástí všech otázek je historka, kterou si pachatel vymyslel a která má v dítěti vyvolat pocit, že komunikuje s vrstevníkem. Ovšem podstatou první otázky je zjistit, zda má oběť vlastní telefon či počítač, nebo zda používá zařízení, ke kterému mají přístup i ostatní členové rodiny. Pokud by tomu tak bylo, existuje vysoké riziko, že někdo z rodiny odhalí závadnou komunikaci. Jestliže oběť používá vlastní zařízení, ke kterému nikdo jiný nemá přístup, riziko odhalení je pro pachatele minimální.

Otázka č. 2:

Taky mě štve, že máme s bráchou společný pokoj. Ale naštěstí chodí často ven s kamarády a já mám při chatování chvilku soukromí. Máš to stejně jako já, nebo máš svůj vlastní pokoj?

- Ve druhé otázce pachatel rozvíjí vymyšlený příběh o svém rodinném soužití a zjišťuje, zda má oběť soukromý pokoj, nebo zda svůj pokoj sdílí s ostatními členy rodiny, kteří by mohli online konverzaci zahlédnout a pachatele tak náhodou odhalit. Případně se útočník dozví, jaký vztah má oběť se svými sourozenci. Taková informace je pro něj důležitá. Jestliže má dítě se sourozenci dobrý vztah, pravděpodobně se jim běžně svěřuje, což by mohlo opět vést k odhalení pachatele.

Otázka č. 3:

Občas bráchovi závidím, že má tolik kámošů. Se mnou se nikdo moc bavit nechce. Chtěl bych alespoň jednoho nej kámoše, kterému bych se mohl se vším svěřovat… Ty máš někoho takového?

- Náš fiktivní pachatel se snaží v oběti vzbudit empatii. Cílem je zjistit, zda má ve svém životě člověka (kamarád, rodič, sourozenec apod.), kterému se pravidelně svěřuje. Pokud ano, je vysoká pravděpodobnost, že takovému člověku o svém novém online kamarádovi řekne. Proto se pachatel během celého procesu manipulace snaží oběť izolovat od okolí, nejčastěji pomocí citového vydírání a zastrašování. Ideální obětí jsou tak děti s emocionálními problémy, děti s nízkou sebeúctou či nedostatkem sebedůvěry nebo naivní a přehnaně důvěřiví jedinci.

Otázka č. 4:

Někdy mám chuť zajít za svým taťkou a říct mu, co mě trápí. Ale bojím se, co by si pak o mně myslel. Jaký máš vztah s rodiči ty? Svěřuješ se jim často, nebo se taky bojíš?

- Poslední otázka je variací na otázku č. 3, ovšem tentokrát se pachatel zaměřuje přímo na vztah dítě-rodič.

U poslední otázky se můžeme se žáky zamyslet i nad kontextem celé zprávy. Proč by pachatel psal, že se bojí se svými problémy svěřit rodině? O jaké naše obavy by se mohl zajímat? Kam dál by mohl např. s adolescentem/teenagerem rozvíjet konverzaci?

Žákům nezapomeňme zdůraznit, že podobný styl komunikace neslouží jen k získávání informací, ale jde i o snahu útočníka navázat s obětí blízký vztah a získat tak její plnou důvěru.

Druhá část:

Ve druhé části aktivity se podíváme blíže na techniku **vábení a uplácení oběti**, tzv. luring. Jde o formy dárečků, mezi které patří např. peníze, značkové oblečení a elektronika, kredit do mobilního telefonu nebo počítačové hry. Tyto úplatky pomohou útočníkovi prohloubit vztah s obětí, zvýšit jeho důvěryhodnost a především pak ověřit osobní údaje, které již získal.

Přečtěte si s žáky zprávy od našeho fiktivního pachatele a nechte je zamyslet se nad tím, proč by nám nabízel právě tyto dárečky.

Zpráva č. 1:

Moji rodiče pracují pro Apple. Nebudeš mi věřit, ale máme doma už alespoň deset iPhonů! Pořád je dostávají jako reklamní předměty zdarma. Dáváme je celé rodině… Jestli chceš, můžu ti taky jeden poslat!

- Jednoduchý trik, jak získat adresu nebo si ověřit bydliště vyhlédnuté oběti. Vzhledem k ceně nabízeného zařízení jde o lákavou nabídku, kterou dítě většinou přijme.

Zpráva č. 2:

Včera jsem měl štěstí! Byl jsem na Twitchi a u jednoho streamera jsem vyhrál dvakrát CD-key pro náhodou hru! Jeden jsem už aktivoval a dostal jsem super strategii. Můžu ti aktivovat ten druhý klíč. Stačí, když mi dáš tvůj e-mail a na Steamu si mě přidáš do přátel.

- S minimální investicí se pachateli dostane do rukou kontakt na oběť v podobě e-mailové adresy. Pokud si navíc dítě přidá útočníka do přátel na platformě **Steam** (služba určená k distribuci her a softwaru), získá přístup k jeho online profilu, kde nalezne další osobní informace. Může se také dozvědět, které hry dítě nejčastěji hraje. Pokud půjde o multiplayer hru (videohra pro více hráčů), stačí si ji nainstalovat a oslovit oběť i ve hře. To opět ještě prohloubí vztah mezi útočníkem a obětí.

Zpráva č. 3:

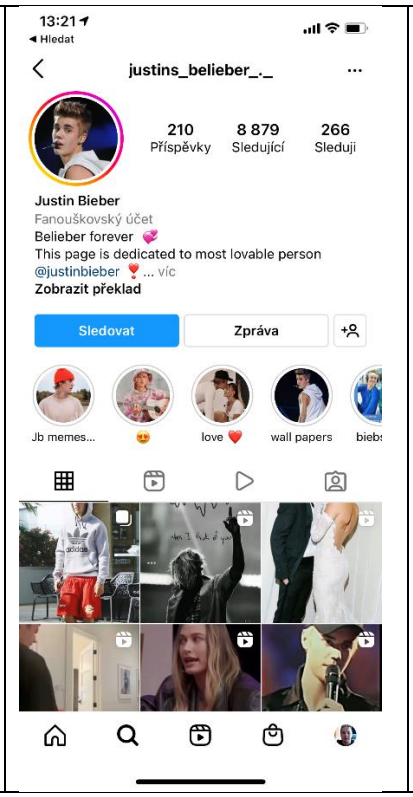
Ty nemáš mobilní tarif? Jen kredit? To je náhoda, já používám taky jenom kredit! Dobíjím si ho přes kupóny, které mamka dostává v práci zdarma. Stačí, když mi pošleš svoje telefonní číslo a taky ti ho dobiju!

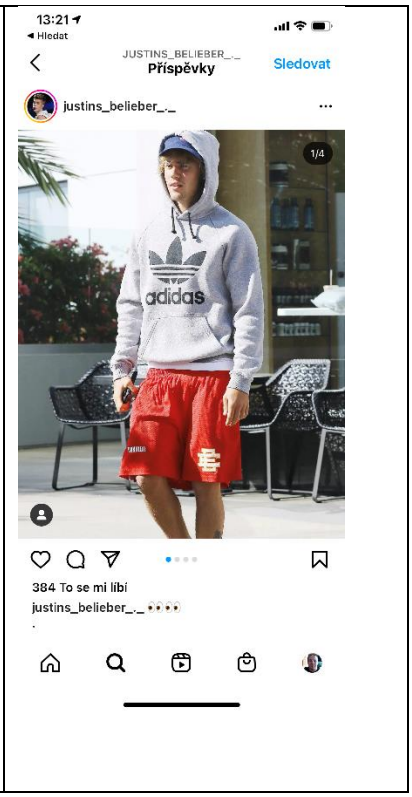
- S minimálním úsilím útočník získává další cenný údaj – telefonní číslo.

Díky úplatkům může pachatel získat i ten nejcitlivější údaj, kterým je fotografie obličeje dítěte.

Aktivita: Justin Bieber

Kamarádka Káťa se svěřila spolužačce Romaně s tím, že si po večerech píše se zpěvákem Justinem Bieberem. Romaně to ale přišlo docela podezřelé, proto Káťu poprosila o pár screenů profilu, se kterým si píše. Prohlédněte si pozorně následující screeny a rozhodněte, jestli jde skutečně o profily Justina Biebera.





Dokázali byste ze screenu zjistit, o jaký typ profilu se ve skutečnosti jedná?

Jak se dá na sociálních sítích rozpoznat, že si skutečně píšete s celebritou (nebo minimálně se správcem jejího opravdového profilu)?

Metodika k aktivitě: Justin Bieber

Aktivita pracuje s tématem falešných profilů v online prostředí a s problematikou seznamování v online prostředí. V našem příkladu pak cílí také na to, zda dokážeme rozpoznat oficiální profil celebrity od profilů jiných – např. fanouškovských či přímo podvodných.

Pomoci může např. speciální modrá ikona – tzv. verified check mark.

Verified check mark („ověřená kontrolní značka") nebo také **verified badge** („ověřovací odznak") je speciální ikona umístěná u názvu profilu, která znamená, že daný profil byl ověřen a skutečně patří dané osobnosti (třeba influencerovi), firmě, instituci apod.

Tento štítek využívají např. sociální sítě Facebook, Twitter, Instagram apod. Nezískáváte jej však automaticky, musíte o něj požádat a splnit různá kritéria – váš profil např. musí být unikátní, musí obsahovat všechny informace, musí být ale také třeba zajímavý.

V našem případě profil tuto speciální značku NEOBSAHUJE, nejde tedy o oficiální profil Justina Biebera, ale o tzv. fanouškovský profil. Káťa si tak po večerech se skutečným Justinem Bieberem opravdu nedopisuje a měla by proto být obezřetná.

K navazujícím aktivitám pak může patřit rozpoznávání „oficiálních" a „neoficiálních" profilů nejrůznějších veřejně známých osobností.

Aktivita: Seznamka

Přečtěte si následující příběh a pokuste se zodpovědět otázky pod textem.

David se už dlouhou dobu snažil seznámit s nějakou super holkou. Spolužačky se mu nelíbily, mezi kamarádkami to taky nebylo ono, proto se rozhodl, že štěstí zkusí na seznamkách. Holek tam bylo spoustu, ale dlouho na žádnou super holku nenarazil. Až jednou…

Na seznamce ho oslovila velmi příjemná slečna ze Slovenska jménem Agáta. Byl nadšený. Velmi si rozuměli, psali si o různých společných zájmech a zálibách. Agáta Davidovi psala, jak je úžasný, že konečně našla někoho „normálního“, komu může svěřit i svá tajemství.

Jednoho večera, když už si dopisovali přes měsíc, Agáta Davidovi navrhla, že by se mohli vidět na webkameře. Řekla Davidovi, že by ale to první setkání na webce mělo být něčím

originální, ne jen, že se jeden na druhého bude koukat. Navrhla mu, že si na webce zahrají jednoduchou hru na úkoly. Pravidla byla taková, že si Agáta na chvilku zapne webku, něco předvede, webku vypne a David to zopakuje. David byl nadšený a samozřejmě souhlasil. Agáta byla taky nadšená, že se konečně uvidí. Agáta postupně zapínala webkameru, nejdříve do kamery jen zamávala, pak chvilku tančila, ale nakonec se začala svlékat a obnažovat. David vše bez problému zopakoval… tedy se i svlékal a obnažoval.

Agáta pak hru ukončila a přestala Davidovi psát…

- Zamyslete se, jak se asi příběh vyvíjel dál?

- Mohl se David bavit přes kameru s někým úplně jiným, než byla Agáta?

- Jakým způsobem se dá ověřit osoba, se kterou se bavíte přes webkameru?

- Mohla si Agáta pořizovat záznam konverzace před webkamerou (nahrávat si obraz z webkamery)? Dokázali byste si vy sami nahrát obraz, který vidíte na webkameře?

Metodika k aktivitě: Seznamka

Cílem aktivity je popsat rizika spojená s videochatem a problematikou s názvem **webcam trolling**. Aktivita by měla přispět k ovlivnění afektivní stránky žáků směrem k uvědomění si rizik spojených s komunikací s neznámým (neověřeným) člověkem prostřednictvím webkamery a rizik spojených s obnažováním před lidmi, které známe pouze z internetu.

Co je Webcam trolling?

Webcam trolling je sofistikovaný způsob, jak vylákat z vyhlédnuté oběti intimní až pornografické, sextingové materiály, jež bývají posléze využity k vydírání.

Podstatou webcam trollingu je využití **specializovaného programu** (virtuální webkamery) a předtočených krátkých videí, tzv. **videosmyček** (stažených z internetu), zachycujících reálné osoby z videochatů, které lze do programu nahrávat a následně prezentovat protistraně.

Webcam blackmailing je zneužití webkamery k vydírání skrze webovou kameru.

Aktivitu je vhodné realizovat jako skupinovou práci. Žákům příběh vytiskneme, a to včetně ilustračního obrázku, který je důležitý k podpoře emočního prožitku u žáků a pro identifikaci se s obětí. Následně žáky necháme zodpovědět položené otázky a rozvedeme diskusi na téma rizikovosti webcam trollingu.

V rámci aktivity využíváme upravený skutečný případ, který byl řešen online poradnou projektu E-Bezpečí.

Otázky učitele (průvodce):

1. Zamyslete se, jak se asi příběh vyvíjel dál?
2. Mohla Agáta pořizovat záznam konverzace před webkamerou?
3. Mohl se David bavit přes webkameru s někým úplně jiným, než byla Agáta?
4. Mohl si David ověřit, s kým se před webkamerou baví? Pokud ano, jak to mohl udělat? (Ověření se dá provést tak, že osobu na webkameře požádáme, aby právě teď něco konkrétního napsala na lísteček a ukázala ho na kameru. Podrobněji viz další aktivity.)

Shrnutí diskusní části:

Závěrem diskuse by mělo být sdělení, že webcam trolling může člověku vážně ublížit a že není dobré nechat se nachytat na libá slova protistrany v komunikaci. Není vhodné žákům zakazovat komunikaci a seznamování prostřednictvím webkamer, ale je nutno upozornit je na důležitost ověřit si protistranu v komunikaci. Jednou z indicií, že na druhé straně není ten, kdo se prezentuje na webkameře, je **výmluva na nefunkční mikrofon**.

Dokončení příběhu:

Uvedený příběh vychází ze skutečné kauzy, ve které došlo k webcam trollingu. Jména osob byla změněna.

Poté, co Agáta přestala Davidovi psát, přestala reagovat i na jeho prosby o další kontakt. David nechápal, co se děje, dokonce se začal obávat, že se Agátě něco zlého stalo. Asi po 4 hodinách, kdy se Agáta neozývala, byl Davidovi doručen e-mail, kde mu někdo napsal, že vše, co s Agátou dělali na webkameře, bylo natáčeno a video je již zavěšeno na YouTube, zatím v neveřejné části. E-mail dále pokračoval podmínkou, za které nebude video zveřejněno, případně odesláno rodině, kamarádům apod. Podmínkou bylo zaplacení **400 Eur** prostřednictvím PayPal peněženky. V tento moment David odeslal svůj případ přes elektronický formulář do poradny projektu E-Bezpečí (www.napisnam.cz). Případ byl následně předán k prošetření Policii ČR. Během vyšetřování nebyla zjištěna totožnost pachatele, který pořídil záznam videochatu s Agátou. Stopy pachatele (pachatelů) vedly až do Ghany.

Jednání, kterého se David stal účastníkem, se odborně nazývá **sextortion**, což je online vydírání prostřednictvím intimních materiálů pořízených nejčastěji za pomoci webcam trollingu. Tento fenomén se začal objevovat v poslední době, zejména na zahraničních seznamkách.

Doporučení pro případné oběti:

Pokud již dojde k úniku intimních materiálů, je důležité dané osobě (osobám) **NIC dalšího NEZASÍLAT, případně NEPLATIT (nezasílat žádné peníze), zálohovat veškerou online komunikaci, nic nemazat a pachatele neblokovat.**

Dále je doporučováno s danou osobou již nekomunikovat! Obvykle pachatelé od dalšího vydírání upustí. Pachatelům jde především o další intimní materiály, peníze apod., intimní materiály proti obětem ve většině případů nepoužijí. Pokud by pachatel od vydírání neustoupil, je doporučeno vše ohlásit na příslušném oddělení Policie ČR.

Zdroje:

Co je sextortion? E-Bezpečí.
https://e-bezpeci.cz/index.php/71-trivium/2421-co-je-sextortion

Co dělat, když tě někdo vydírá? E-Bezpečí.
https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1873-co-delat-kdyz-te-nekdo-vydira

Další užitečné informace lze nalézt i na http://youtube.com/ebezpeci.

Aktivita: Hnusák z Minecraftu

Nejprve si přečtěte text, který informuje o případu, který se odehrál v prostředí populární hry Minecraft. Potom zodpovězte na otázky pod textem.

Adam Isaac zneužíval chlapce v prostředí hry Minecraft.

20. ledna 2017

Adam Isaac, 23letý pedofil z Walesu (Velká Británie) v prostředí Minecraftu obtěžoval chlapce ve věku 12 a 14 let. Chlapcům nabízel virtuální dárečky, komunikoval s nimi prostřednictvím Skype a Snapchatu, začal si s chlapci vyměňovat různé intimní fotografie a videa, která používal k vlastnímu sexuálnímu uspokojení. S chlapci rovněž komunikoval prostřednictvím webkamery a nutil je k sexuálním aktivitám. **Byl odsouzen k trestu odnětí svobody na 2 roky.**

Zdroj: BBC News

Dokázali byste nějakým způsobem rozpoznat, s kým se v prostředí Minecraftu skutečně bavíte? Napadají vás nějaké způsoby, jak si ověřit identitu vašeho online kamaráda?

Co všechno se dá z článku o Adamu Isaacovi zjistit? Doplňte vaše zjištění do bublin u jeho fotografie. Odpovídá Adam Isaac vaší představě o tom, jak vypadá online útočník?

Zdroj fotografie:
Policie Jižní Wales

Pokud hrajete Minecraft či jinou online hru, znáte skutečnou identitu vašich spoluhráčů? Kolik z nich jste jich viděli prostřednictvím webkamery? Kolik z nich jste viděli osobně v reálném světě?

Metodika k aktivitě: Hnusák z Minecraftu

Aktivita se zaměřuje na problematiku rizikového seznamování v prostředí oblíbené online hry, v našem případě Minecraftu. Výchozí situací je text o pachateli sexuálních útoků na děti v kyberprostoru – Adamu Isaacovi.

Případ je velmi dobře zmapován např. zde:

Minecraft paedophile Adam Isaac groomed boys online. BBC News.
Online: https://www.bbc.co.uk/news/uk-wales-south-east-wales-38691882

V češtině pak např. zde:

Kopecký, K. Počet případů kybergroomingu spojených s Minecraftem roste. Rodiče, pozor! E-Bezpečí. Online: https://www.e-bezpeci.cz/index.php/temata/kybergrooming/1222-minecraft-kybergrooming

V úvodu aktivity pracujeme s textem, který dále využíváme u dalších, navazujících úkolů. Využíváme **čtení s porozuměním**, přičemž žáka vedeme k uvědomění si několika klíčových informací:

1. Pachatelé mohou být „schováni" mezi online kamarády, se kterými hrajeme online hry.
2. Pachatelé mohou být mladí. Nemusí jít o starce.
3. Pachatelé se mohou zaměřovat na chlapce (ne jen na dívky).
4. Je důležité naučit se ověřovat si, s kým se v online světě bavíme (ověřování identity).

Jak ověřit identitu neznámého člověka? Využijme webkamery!

Jednou z možností, jak si ověřit identitu člověka, se kterým komunikujeme, je **požádat ho, aby se ukázal na webkameře, promluvil a aby udělal něco unikátního** – ideálně napsal na papír vzkaz, který mu nadiktujeme, a to právě teď, v reálném čase!

Pozor, i komunikace prostřednictvím webové kamery se dá podvrhnout – existuje druh manipulace, která se nazývá **webcam trolling**! Tento podvod funguje tak, že si pachatel do svého počítače nainstaluje speciální aplikaci (virtuální kameru), která mu umožní nahradit skutečný obraz z webkamery předtočeným videozáznamem.

ONLINE PODVODY

Aktivita: Podvodníci a podvodnice

Petru Novákovi přišel do e-mailové schránky následující e-mail. Pozorně si jej přečtěte a zkuste Petrovi poradit, co by měl udělat.

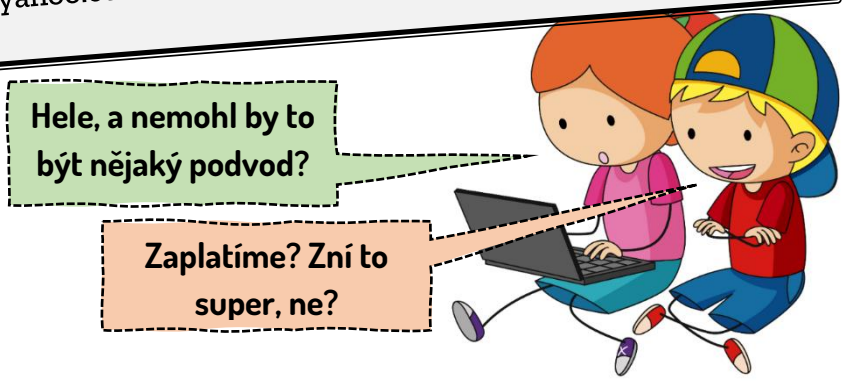
Od: gsmith77@yahoo.com

Předmět: Gratulujeme!!!

Milý příteli,

jsem advokát George Smith, který vyřizuje pozůstalost po Janu Novákovi, který před měsícem zemřel v Nigérii a který po sobě zanechal **3 000 000** $ (USD). Pátráním v rodokmenu se mi podařilo zjistit, že jsi jediný žijící příbuzný, který má nárok na celé dědictví! Gratuluji! Jediné, co musíte nyní udělat, je do 7 dnů potvrdit zájem o dědictví na e-mail na konci tohoto dopisu a uhradit úřední poplatek ve výši 300 $ (USD). Poté budou finance převedeny na tvůj bankovní účet.

Se srdečným pozdravem,
George Smith, advokát
gsmith77@yahoo.com



Dokážete spočítat, kolik českých korun je 3 000 000 $ (USD)? A kolik je 300 $? Zaplatili byste 300 $, abyste měli šanci získat 3 miliony $?

3 000 000 USD	=	Kč
300 USD	=	Kč

Hedvice přišla na Messenger zpráva od kámošky Romany, která potřebuje pomoc. Přečtěte si zprávu a zodpovězte otázky.

Poslali byste Romaně kód, který po vás požaduje?
Jsou s posíláním podobných kódů spojena nějaká rizika?
Slyšeli jste někdy slovo M-platba? Víte, co to znamená?

? Možná i vy na internetu nakupujete a možná také někteří z vás (ti starší) používají kreditní kartu – třeba od mamky či taťky. Přečtěte si pozorně následující článek a zodpovězte na navazující otázky.

Muž z Prahy prodával šaty za 390 korun. Přišel o dva miliony.

Novinky.cz

Muž chtěl prodat na inzertním portálu šaty. Přes internet se mu ozvala žena, která projevila o šaty zájem. Poté mu poslala odkaz, který obsahoval potvrzení přijetí částky a jméno kupující, muž vše potvrdil a byl přesměrován na obrazovku, kam doplnil informace o své bance a také údaje o své platební kartě, včetně CVV kódu. Poté už jen čekal na peníze za zboží. Když ale peníze nepřicházely, rozhodl se muž zkontrolovat svůj účet. V bance zjistil, že karta byla zneužita a z účtu mu zmizely prostřednictvím 20 plateb 2 miliony korun.

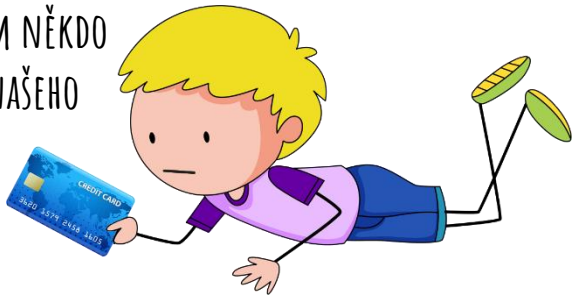
Zdroj: Novinky.cz

? Dokážete vysvětlit, co udělal muž z příběhu špatně?

? Jaké informace můžeme poslat člověku, který si od nás chce něco koupit, abychom měli jistotu, že nám nemůže vykrást náš účet?

? V článku se píše o tzv. CVV kódu. Co to ale vlastně je a k čemu tento kód slouží?

? Představme si, že bychom zjistili, že nám někdo neznámý bez našeho vědomí převedl z našeho účtu peníze. Je nějaký způsob, jak dostat své peníze zpět?



Lukáš brouzdal internetem a najednou mu na obrazovce vyskočilo hlášení, že se stal miliontým návštěvníkem webových stránek a za odměnu může získat nový mobilní telefon – stačí pouze kliknout na odkaz a potvrdit výhru. Lukáš klikl na odkaz a objevila se níže uvedená webová stránka. Prohlédněte si ji a zodpovězte na otázky.

Měl by Lukáš zadat číslo svého telefonu do formuláře a potvrdit svou výhru pomocí SMSky? Co se vlastně stane, když SMS odešle?

Vyhrál Lukáš skutečně mobilní telefon? Nebo se stalo něco jiného?

V které části těchto webových stránek jsou ukryty ty nejdůležitější informace?

Přečtěte si následující příběh a poté zodpovězte na otázky pod textem.

Hedvika byla na prázdninách u babičky, která má nový počítač s připojením na internet. Babička je nadšená uživatelka internetu, ráda si zde hledá informace, píše a videotelefonuje si se svou rodinou a také se zde seznamuje s novými lidmi. Hedvice se pak svěřuje, s kým zajímavým se v online prostředí zase seznámila. Dnes třeba přišla s tím, že si začala dopisovat s americkým vojákem Henrym, který je zrovna na vojenské misi. Voják jí napsal, že by se po misi rád přestěhoval do Evropy – do České republiky – a to dokonce za babičkou. Dále psal, že se mu babička líbí, že by se rád usadil, že má na účtu hodně peněz a že by se o babičku dobře postaral... Jenom potřebuje, aby mu babička trošku finančně vypomohla, protože se nyní nemůže ke svým penězům na účtu ze zahraničí dostat...

Hedvika si myslí, že komunikace babičky s americkým vojákem není v pořádku. Co myslíte vy, mohlo by skutečně jít o nějaký podvod? A jak by mohl tento podvod fungovat?

Prohledejte internet a zkuste zjistit informace o případech, kdy starší ženy komunikovaly na internetu s „americkými vojáky" či jinými podezřelými uživateli internetu a byly podvedeny. O jak velké částky přišly? A má tento druh podvodu nějaký název?

Jak byste babičku přesvědčili, že jde pravděpodobně o podvod? A co byste jí poradili, když už peníze do zahraničí odeslala?

Metodika k aktivitě: Podvodníci a podvodnice

V této kapitole se věnujeme různým druhům online podvodů, které označujeme souhrnným názvem SCAM. Se scamem se běžně setkávají jak děti, tak i dospělí uživatelé internetových služeb, scam se šíří internetem, především prostřednictvím spamu, případně – v omezené míře – za pomoci sociálních sítí.

Typickým zástupcem scamu je tzv. **scam419** – tj. dopisy, které nám nabízejí závratné zbohatnutí. Jediné, co musíme udělat, je zaplatit nejrůznější druhy poplatků, daní, pojištění apod. Ve skutečnosti samozřejmě nezbohatneme, podstata podvodu je právě v ochotě platit menší částky ve vidině získání milionů. V našem případě pracujeme s historkou o „dědictví", která je však vymyšlená.

K typickým podvodům, na které narazíme v online prostředí, patří **podvody s tzv. m-platbami** (platbami prostřednictvím mobilního telefonu). S těmito podvody jsme se krátce seznámili již v úvodních aktivitách našeho materiálu, nyní se na tento typ podvodu podíváme podrobněji. Pachatel nejprve naklonuje profil našeho kamaráda (tj. vytvoří duplicitní profil, do kterého zkopíruje fotografie, jméno a příjmení a další informace z původního profilu) a potom nás osloví s prosbou o pomoc. Jeho cílem je získat kód, který nechal poslat do našeho mobilního telefonu. Tento **kód však slouží k autorizaci finanční transakce** – např. platby v e-shopu apod. Pokud bychom tedy našemu „kamarádovi" kód poslali, s vysokou pravděpodobností dojde k odečtení financí z našeho účtu. Tento typ podvodu simulujeme právě v aktivitě komunikace Hedviky a Romany.

V současnosti je populárním typem podvodu také **podvod spojený s nákupem a prodejem zboží především na inzertních portálech** (Sbazar apod.). Podvodník předstírá, že chce koupit zboží, které nabízíme, pošle nám však odkaz, který vede na falešnou platební bránu, jež požaduje zadání detailních údajů o naší platební kartě a našem účtu. Pokud tyto údaje vyplníme, hrozí riziko, že přijdeme o finance na našem účtu (viz příklad z aktivity).

Velmi kritickou informací, která je spojena s platbou pomocí platební karty, je především tzv. **CVV (card verification value) či CVC (card verification code) kód**. Jde o číslo, které je uvedeno na zadní straně kreditní karty a které slouží k autorizaci transakce. Tento kód je vyžadován u všech plateb, kde platební karta není fyzicky přítomna a kde nelze vyžadovat osobní PIN platební karty (ten vyžadují třeba bankomaty). **Dávejme si proto velký pozor, kam tento kód zadáváme!**

Dětem, které např. využívají pro online nákupy platební karty rodičů, je velmi důležité vysvětlit, jak rizikové je zadávání těchto údajů na internet a že je nutné, aby každou transakci probrali s rodičem. To platí i v případě mikroplateb. Velmi dobré je také mít nastaveno potvrzování online plateb za pomoci mobilního telefonu.

Otázka: Představme si, že bychom zjistili, že nám někdo neznámý bez našeho vědomí převedl z našeho účtu peníze. Je nějaký způsob, jak dostat své peníze zpět?

Odpověď: V tomto případě je nutné podat **co nejrychleji reklamaci na platbu u své banky**, buďto osobně nebo cestou zákaznické linky. Došlo-li k odčerpání finančních prostředků prostřednictvím Vaší platební karty, okamžitě provést blokaci karty. Další asi nejdůležitější možností je **oznámit neoprávněnou transakci na Policii ČR**. Policie ČR má zákonné prostředky, jak zablokovat peníze na protiúčtu a sledovat neoprávněný finanční tok.

Další úkol je věnován problematice **podvodných výher** – v našem případě výhře mobilního telefonu na internetu. Zde je třeba upozornit na několik věcí:

1. Lukáš z příběhu **nic nevyhrál, pouze „má fiktivní šanci" něco vyhrát**.

2. Pokud Lukáš zadá do formuláře své telefonní číslo a pokud potvrdí zprávu, která mu přijde do mobilního telefonu SMSkou, **přihlásí se ve skutečnosti k předplatnému (tzv. subscription)**. Tzn., že mu v pravidelných intervalech budou chodit na telefon zpoplatněné SMS zprávy za 99 Kč / týden. Tyto informace jsou totiž ukryty v drobném, často nečitelném textu na spodním okraji stránky.

Pozor, důležitá informace (na kterou je třeba upozornit žáky) – **předplatné lze zrušit tak, že na telefonní číslo daného předplatného odešlete opět SMS zprávu ve speciálním tvaru**, v našem případě **STOP ANO na číslo 90466**.

3. Pokud jde o různé typy soutěží, výher a služeb – **důležité informace bývají často skryty ve spodní části webových stránek – tak, abychom je snadno přehlédli**.

Další aktivity a otázky se zaměřují na tzv. **romance scam** (romantický scam). Jeho základem je zneužití oběti (zpravidla seniora) prostřednictvím nabídnutí romantického vztahu (který je zpravidla zakončen nabídkou k sňatku), přičemž v průběhu komunikace pachatel/pachatelka od oběti vylákává finance. Oběť tak neustále platí, zatímco pachatel vymýšlí stále nové výmluvy, proč potřebuje peníze. Přestože se tento podvod netýká přímo dětí, děti mohou aktivně upozornit své prarodiče na to, že se zřejmě stali terčem podvodu.

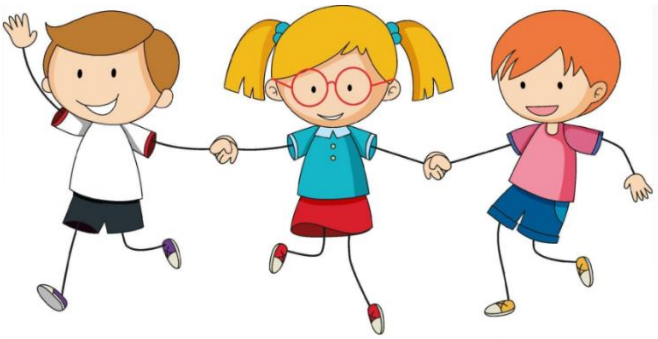
Pokud jsme peníze zaslali a zjistili, že jde pravděpodobně o podvod, okamžitě kontaktujeme policii a svou bankovní instituci, ze které jsme peníze převedli.

Na romance scam je zaměřeno video, jež naleznete na další straně.

Online podvodům se podrobně věnujeme v našem seriálu **Prevíti na síti** na https://youtube.com/ebezpeci.

V našich videích se seznámíte s tím, jak funguje phishing, scam, podvodná reklama, podvody spojené s m-platbami či sextortion.

Když budeme vědět, jak internetové podvody fungují, tak nás na internetu nikdo nenapálí!



Videa k aktivitě

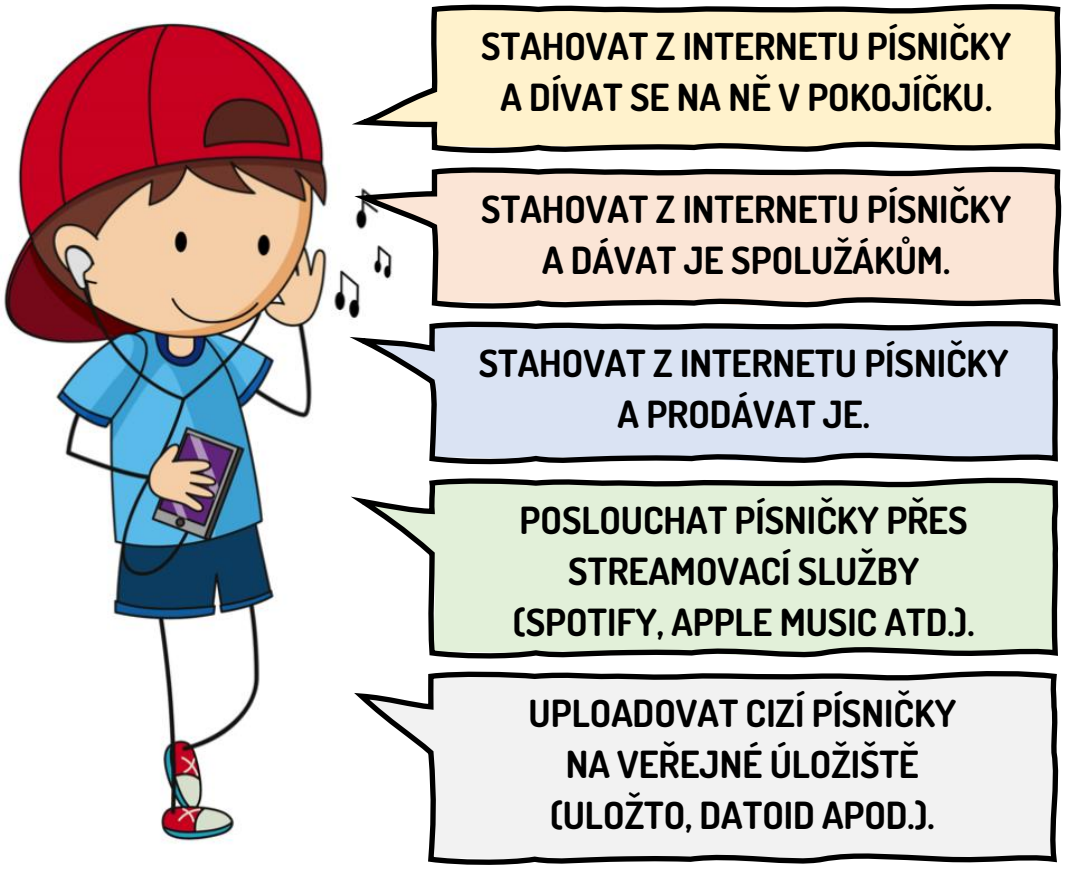
Online podvody

Romance scam

AUTORSKÉ PRÁVO A PIRÁTSTVÍ

Aktivita: Stahujeme ze sítě

Většina z nás si určitě z internetu stáhla nějaký ten film, seriál, hudbu nebo třeba počítačovou hru. Víte ale, co je a co není legální? Rozhodněte, které aktivity jsou na internetu legální a které ne.

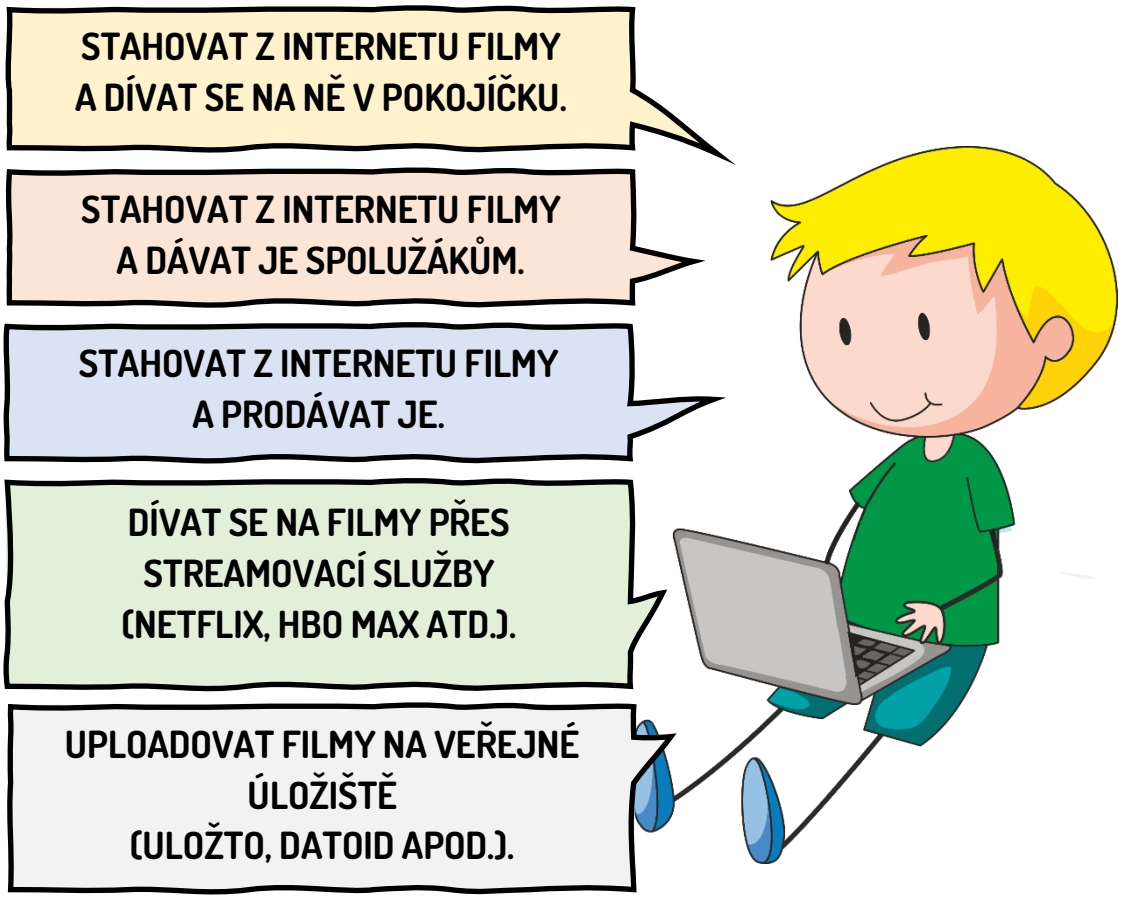


Posloucháte streamovanou hudbu či mluvené slovo? Jakou službu používáte? A platíte za poslech, nebo ne?

Spotify YouTube Music TIDAL

deezer music Music

Teď se podíváme na to, jestli víte, jak je to se stahováním filmů a seriálů z internetu. Rozhodněte, které aktivity jsou LEGÁLNÍ a které ne.



Sledujete filmy a seriály prostřednictvím streamovacích služeb (VOD)? Jakou službu používáte? A platíte za sledování, nebo ne?

NETFLIX HBO max prime video

Disney+ tv+ VOYO

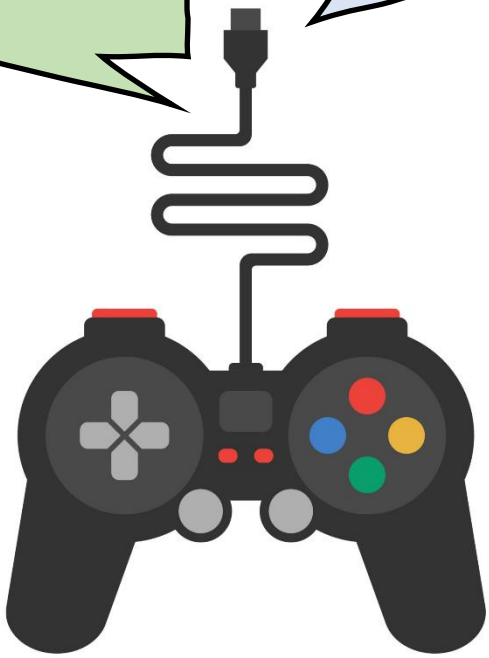
Je na čase podívat se na problematiku software, tedy počítačových programů – her, aplikací apod. Rozhodněte, které aktivity jsou legální a které ne.

STAHOVAT A HRÁT POČÍTAČOVÉ HRY PROSTŘEDNICTVÍM OFICIÁLNÍCH HERNÍCH PLATFOREM (STEAM, ORIGIN, UPLAY, EPIC GAMES APOD.).

STAHOVAT Z RŮZNÝCH VEŘEJNÝCH ÚLOŽIŠŤ POČÍTAČOVÉ HRY, KTERÉ JSOU BĚŽNĚ ZA PENÍZE.

KOPÍROVAT PRO KAMARÁDY RŮZNÉ CD, DVD ČI USB FLASH DISKY S POČÍTAČOVÝMI HRAMI, KTERÉ MÁM LEGÁLNĚ ZAKOUPENY.

SDÍLET S KAMARÁDY INSTALAČNÍ SOUBORY HER PROSTŘEDNICTVÍM CLOUDU.



Hrajete hry také na svém mobilním telefonu? A jakým způsobem je do mobilního telefonu instalujete? Hrozí při instalaci nějaká rizika?

Aktivita: The Pirate Bay

Přečtěte si následující text o jednom z největších případů počítačového pirátství a zodpovězte na otázky.

Kauza The Pirate Bay

V roce 2009 proběhl soud s provozovateli **BitTorrent trackeru The Pirate Bay**. Odsouzena byla čtveřice jeho zakladatelů: Peter Sunde, Fredrik Neij, Gottfrid Svartsholm a Carl Lundström, každý **k jednomu roku trestu odnětí svobody** (trest jim byl později zmírněn) **za napomáhání umožnění porušování autorských práv**. Zároveň jim byla vyměřena **pokuta**, která byla v průběhu soudních řízení postupně zvyšována až na **46 000 000 SEK** (švédských korun).

Soudní dvůr Evropské unie vydal v této kauze rozhodnutí, ve kterém uznal, že provozování platformy pro sdílení obsahu je tzv. sdělováním veřejnosti **a je nesporné, že Pirate Bay zprostředkovává uživatelům prostřednictvím protokolu BitTorrent autorsky chráněná díla**. Zároveň uznal, že pirátské kopie na internet neukládá provozovatel, ale uživatelé. Provozovatel ale podle soudu hraje při zpřístupňování těchto děl nepominutelnou roli. S torrenty totiž pracuje: Torrentové soubory indexuje, aby se díla, na které odkazují, dala dobře vyhledávat a stahovat, kategorizuje je podle typu, žánru nebo jejich popularity, nefunkční či zastaralé torrenty promazává a část obsahu aktivně filtruje.

(Převzato a upraveno ze serverů Lupa.cz a CNews.cz)

Víte, co jsou to tzv. torrenty, o kterých se v textu hovoří? Jak vlastně torrenty fungují? A stahujete i vy sami z internetu obsah prostřednictvím torrentů?

Jakou pokutu dostali provozovatelé The Pirate Bay? Dokázali byste zjistit, jaká by byla výše pokuty v Kč? Jak dlouho by vám trvalo vydělat si na tuto pokutu, kdybyste např. brali průměrný plat? Využijte internetu a doplňte tabulku.

Pokuta v SEK (švédská koruna)	Pokuta v CZK (česká koruna)	Průměrná měsíční mzda v ČR v CZK	Doba splácení

Metodika k aktivitám: Stahujeme ze sítě a Pirate Bay

Vše, co je na internetu, někomu patří – na veškerý obsah, který najdeme na internetu, se vztahuje zákon číslo 121/200 sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, který chrání veškerá literární, vědecká a umělecká díla, jako je hudba, filmy, obrazy, ale i nákresy, výkresy. Tento zákon se samozřejmě vztahuje na počítačové programy – hry, aplikace apod.

Podle české legislativy **můžete bezplatně stahovat pro osobní potřebu i komerční obsah (filmy, hry, hudbu), tj. nedopouštíte se ničeho nezákonného,** nicméně **nesmíte tento obsah rozmnožovat, šířit** nebo např. **realizovat projekce díla veřejnosti či většímu publiku (promítání).** V žádném případě také **nesmíte za nelegální obsah požadovat peníze. Dílo můžete využívat výhradně pro osobní potřebu (= offline).**

Pozor, toto neplatí pro počítačové programy (tedy i počítačové hry), ty nesmíte stahovat ani pro osobní potřebu. Výjimku tvoří programy, které se označují jako freeware, shareware, trial či jiné druhy programů, jež jsou zdarma (například tzv. svobodný software).

Pozor, pokud stahujeme obsah pomocí tzv. BitTorrentů, současně stahovaný obsah šíříme, tj. porušujeme zákon a můžeme být potrestáni.

Typ obsahu	**Stahovat zdarma** (pro osobní potřebu)	**Šířit** (kopírovat, dělat projekce)
Hudba	**ANO**	**NE**
Filmy, seriály	**ANO**	**NE**
Komerční software (hry, programy…)	**NE**	**NE**
Software pro volné užití (freeware, shareware…)	**ANO**	**ANO**

BitTorrent je nástroj, který je určený především ke stahování větších souborů. Stahované soubory se nejdříve rozdělí na menší části (bloky), jež se začnou stahovat a současně sdílet s dalšími uživateli, který daný soubor stahují. Ti, kteří soubory stahují, se označují termínem **leech** (pijavice), a ti, kteří již soubor či jeho část stáhli a sdílí jej, se nazývají **seed** (seed je semínko, tedy něco jako rozsévači). Termínem **peer** se pak označují všichni, ať již stahují, nebo sdílí. **Torrent** je soubor, který obsahuje informace (metadata) o tom, kdo jej sdílí, jak je rozdělen, jaká je jeho velikost atd.

Problémem stahování prostřednictvím torrentů je tedy to, že v průběhu stahování soubor současně sdílíme, tedy jej aktivně šíříme.

Řešení výpočtu:

Pokuta v SEK (švédská koruna)	Pokuta v CZK (česká koruna)	Průměrná měsíční mzda v ČR v CZK	Doba splácení
46 000 000	**108 100 000***	**37 839***	**238 let (1 osoby)** **59,5 let (4 osoby)**

* Využit kurz 1 SEK = 2,35 CZK (Kč), průměrná mzda v ČR 37 839 Kč (2021)

Doba splácení = 108 100 000 / 37 839 / 12 = 238 let. Pokud by tedy pokutu splácela jedna osoba, strávila by splácením 238 let (za předpokladu, že by odevzdala celou svou výplatu na splácení dluhu). Pokud by se na splácení dluhu podílely 4 osoby a každá splácela čtvrtinu, strávily by splácením téměř 60 let.

Zdroje:

Jak na internet: Autorský zákon na Internetu.
https://www.jaknainternet.cz/page/1771/autorsky-zakon-na-internetu/

Přelomový rozsudek: Pirate Bay porušuje autorská práva a smí se blokovat. Lupa.cz.
https://www.lupa.cz/clanky/prelomovy-rozsudek-pirate-bay-porusuje-autorska-prava-a-smi-se-blokovat/

Zakladatelé The Pirate Bay prohráli další soud. Cnews.cz.
https://www.cnews.cz/zakladatele-the-pirate-bay-prohrali-dalsi-soud/

Webová stránka www.thepiratebay.org.

Aktivita: Fotíme a sdílíme

Téměř každý z nás má k dispozici mobilní telefon, který umožňuje fotit a natáčet videa. Natáčení a focení mobilním telefonem má ale svoje omezení! Rozhodni, jaká omezení má tvorba fotografií a jejich zveřejňování.

MOBILNÍM TELEFONEM SI MŮŽU VYFOTIT, KOHO CHCI, NEMUSÍM HO ŽÁDAT O SOUHLAS.

MOBILNÍM TELEFONEM SI MŮŽU VYFOTIT PANÍ UČITELKU, NEMUSÍM MÍT JEJÍ SOUHLAS.

MOBILNÍM TELEFONEM SI MŮŽU VYFOTIT KAMARÁDY, NEMUSÍM MÍT JEJICH SOUHLAS.

MOBILNÍM TELEFONEM SI MOHU FOTIT OSOBY POUZE S JEJICH SOUHLASEM.

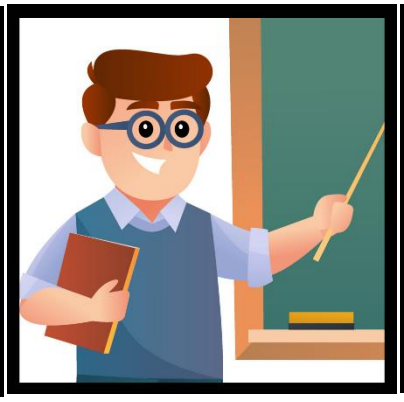
MOBILNÍM TELEFONEM SI MŮŽU FOTIT SKUPINY LIDÍ, TŘEBA NA ULICI.

VŠE, CO MOBILNÍM TELEFONEM VYFOTÍM, MOHU NAHRÁT NA INTERNET.

MOBILNÍM TELEFONEM SI MOHU FOTIT SÁM SEBE (SELFÍČKO).

Nyní se podíváme na složitější situace. Rozhodni, co všechno ti zákon umožňuje. A co naopak nesmíš.

MOBILNÍM TELEFONEM MŮŽEŠ VYFOTIT ZLODĚJE PRCHAJÍCÍHO Z BANKY I BEZ JEHO SOUHLASU.



MOBILNÍM TELEFONEM MŮŽEŠ NATOČIT UČITELE V HODINĚ I BEZ JEHO SOUHLASU.

MOBILNÍM TELEFONEM MŮŽEŠ VYFOTIT POLICISTU, KTERÝ TI UDĚLUJE POKUTU, I BEZ JEHO SOUHLASU.

MOBILNÍM TELEFONEM MŮŽEŠ NATÁČET FILMY, KTERÉ SE PROMÍTAJÍ V KINĚ. NEPOTŘEBUJEŠ K TOMU SOUHLAS.

MOBILNÍM TELEFONEM MŮŽEŠ V NOCI FOTIT A NATÁČET OSOBY V JEJICH BYTECH I BEZ JEJICH SOUHLASU.

MOBILNÍM TELEFONEM MŮŽEŠ NATÁČET ČI FOTIT SOUSEDA ZA PLOTEM I BEZ JEHO SOUHLASU.

Napadají vás další situace, kdy si nejste jisti, jak je to se souhlasem s fotografováním či natáčením?

Metodika k aktivitě: Fotíme a sdílíme

Pořizování fotografií a videí je omezeno zákonem, konkrétně zákonem 89/2012 Sb., který se nazývá občanský zákoník. V tomto zákoně nalezneme řadu práv, která jsou spojena s ochranou osobnosti člověka – např. práva spojená s ochranou podoby a soukromí člověka. Pro naše potřeby je nejdůležitější § 84, který říká, že „**zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením**“. Následující § 85 potom říká, že **rozšiřovat podobu člověka je možné jen s jeho svolením**.

V našem případě tedy žáci mohou fotit a natáčet jiné osoby pouze s jejich souhlasem. Výjimkou by mohly být fotografie/videa, která zachycují osoby zezadu (není jim vidět do obličeje), případně zachycují skupinu osob bez detailní identifikace. Samozřejmě fotit můžeme i sami sebe – ovšem pozor, s výjimkou případů tvorby tzv. dětské pornografie (do 18 let věku).

Existuje několik výjimek uvedených v § 88-89, kdy můžeme zachytit a šířit podobu člověka i bez jeho souhlasu:

1. Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí **k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob**.

Např. Bezpečnostní kamera, která chrání majetek na prodejně, zaznamená zloděje.

2. Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí **na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu**.

Např. Natočíme kamerou autonehodu, natočíme vloupání, předávání drog, zaznamenáme důkazy korupce (= veřejný zájem) apod.

3. Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít **přiměřeným způsobem** též **k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství**.

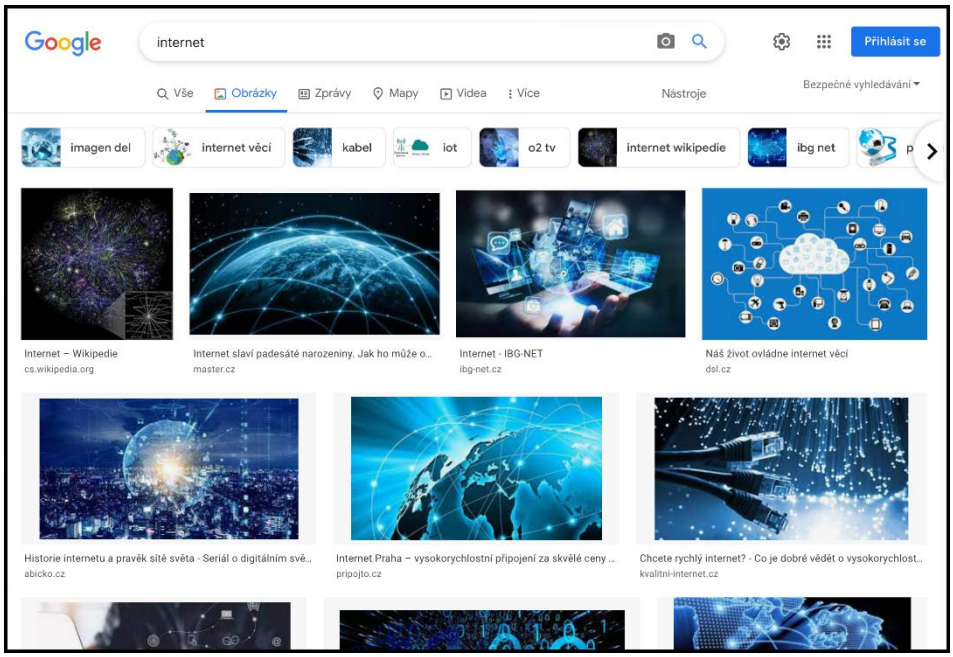
Např. Vyfotíme fotografii z koncertu a poté ji publikujeme v novinách. Vyfotíme skupinovou fotografii ze závodů a zavěsíme ji na webovou stránku školy.

Řešení složitějších situací:

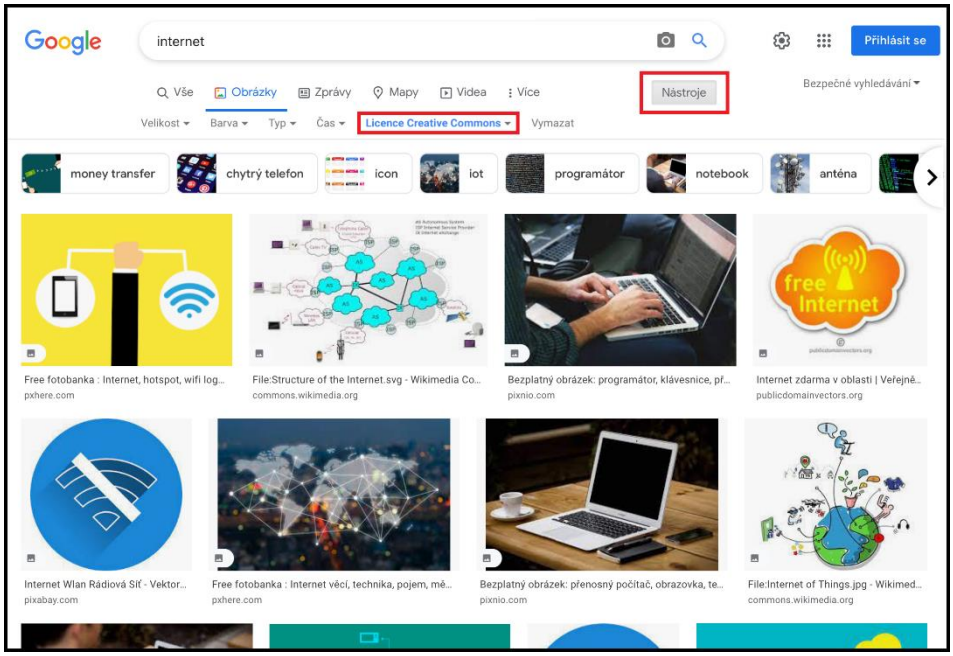
1. Podezřelého (pravděpodobně lupiče), který prchá z banky, natočit či vyfotit můžeš i bez jeho souhlasu, tvé jednání lze považovat za jednání ve „veřejném zájmu". Neměl/a bys ale jeho foto nikde zveřejňovat. Ideálně fotografii předej např. policii.
2. **Učitele ve výuce fotit či natáčet bez jeho souhlasu nesmíš**. V posledních letech se hodně diskutuje o tom, zda je možné natáčet učitele z důvodu „veřejného zájmu" – např. v souvislosti s aktivním šířením dezinformací, každopádně neodůvodněné „preventivní" či jiné neodůvodněné nahrávání pedagogů ve výuce bez jejich souhlasu je neakceptovatelné. Učitelé nejsou úřední osoby, nevztahuje se na ně tedy výjimka spojená se statutem úředního činitele.
3. **Policistu si při výkonu činnosti nahrávat a fotit můžeš**. Záznam (video, fotografii) však nesmíš využít nepřiměřeným způsobem a nesmíš jej volně zveřejňovat a rozšiřovat.
4. **Nahrávání filmů v kině je zakázáno.**
5. **Fotografování a natáčení lidí v jejich domácnostech bez jejich souhlasu je zakázáno**, jde o vážný zásah do jejich soukromí.
6. **Souseda, který je na svém pozemku za plotem, bez jeho souhlasu natáčet nesmíš.** Výjimku by mohly tvořit situace, kdy nahráváš ve „veřejném zájmu", tj. dopouští se na svém pozemku např. nezákonného jednání.

Další aktivity

1. Na internetu najdeme velké množství fotografií, které můžeme lehce stáhnout a použít např. v naší prezentaci, na našem webu apod. Vyzkoušejte s žáky vyhledat libovolnou fotografii pomocí nástroje **Google Obrázky**. Mohou takto vyhledané fotografie žáci skutečně použít? Jaká jsou pravidla využití fotografie např. v prezentaci, videu či na webu? Co je a co není legální?
2. Vyzkoušejte s žáky vyhledat fotografie, které jsou volně k použití (např. pomocí nástroje Google Obrázky).



Výsledky hledání pomocí nástroje Google Obrázky po zadání hesla „internet“.



Výsledky hledání pomocí nástroje Google Obrázky po zadání hesla „internet“ s filtrem Licence Creative Commons.

Zdroje:

Zákon 89/2012 Sb. (občanský zákoník).
https://www.zakonyprolidi.cz/cs/2012-89

Pořízení důkazu a ochrana osobnosti. Právní prostor.
https://www.pravniprostor.cz/clanky/procesni-pravo/porizeni-dukazu-ochrana-osobnosti

RIZIKA SOCIÁLNÍCH SÍTÍ

AKTIVITA: K ČEMU NÁM JSOU SOCIÁLNÍ SÍTĚ?

Sociální média neboli platformy, jako Facebook, Instagram, YouTube, TikTok nebo WhatsApp, jsou známé po celém světě a používají je miliardy lidí. Otázkou je, proč? Zamysli se, proč lidé na celém světě využívají tyto služby, a napiš tyto důvody do jednotlivých bublin.

Metodika k aktivitě: K čemu nám jsou sociální sítě?

Cílem aktivity je, aby se žáci zamysleli nad podstatou a smyslem sociálních sítí a našli důvody, proč jsou tyto online platformy tak populární a k čemu nám vlastně slouží.

Žáci by si měli uvědomit, že sociální sítě nejsou pouze zdroj zábavy či prostředek pro mrhání časem, ale že díky možnosti vytvářet uživatelské profily se můžeme v online světě také prezentovat a sdílet své myšlenky, názory, informace. Uživatelé z celého světa spolu mohou komunikovat (chat, hlasové zprávy, videohovor), seznamovat se, navazovat nová virtuální přátelství, vytvářet různé online komunity na základě společných zájmů nebo spolu sdílet jedinečné zážitky. Nezapomínejme, že sociální sítě se staly také revolučním prostředkem v podnikání. Ve světě digitálního marketingu jsou dnes mocným a nepostradatelným nástrojem.

AKTIVITA: POZITIVA A NEGATIVA SOCIÁLNÍCH SÍTÍ

? Sociální sítě mají celou řadu pozitiv. Vymysli alespoň 5 příkladů.

.....	.....	.....
.....	.....	.....

? Ovšem najde se i celá řada negativ. Se kterými z nich se můžeme při používání sociálních sítí setkat? Uveď alespoň 5 příkladů.

.....	.....	.....
.....	.....	.....

AKTIVITA: UŽIVATELÉ INTERNETU

? Víš, jaká je současná světová populace, tj. kolik lidí žije na Zemi? A kolik je mezi nimi uživatelů internetu?

1. Na světě je přibližně _____ lidí.

2. Na světě je přibližně _____ uživatelů internetu.

Naskenuj svým mobilním telefonem QR kód a podívej se na aktuální globální statistiky!

Poznáš sociální sítě a další online služby podle loga? Napiš, jak se jmenují a pokud aplikaci používáš, označ ji. ☑

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

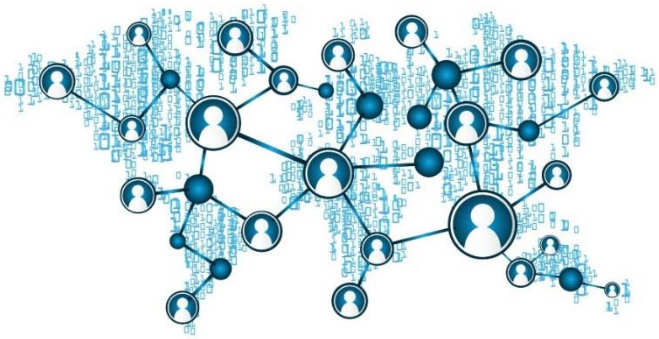
Název: _____

Používáš tuto aplikaci? ☐

Název: _____

Používáš tuto aplikaci? ☐

Používáš nějaké další online platformy? Které?



_____

_____

_____

_____

Pokuste se spojit tyto známé aplikace a služby s počtem jejich měsíčně aktivních uživatelů (srpen 2022).

Facebook Messenger

1,4 miliardy

Snapchat

YouTube

2,5 miliardy

Twitter

TikTok

617 miliónů

Instagram

WhatsApp

2 miliardy

Facebook

486 miliónů

Metodika k aktivitě: Pozitiva a negativa sociálních sítí

V aktivitě „**K čemu nám jsou sociální sítě?**“ jsme si popsali podstatu a smysl sociálních sítí, včetně mnoha pozitiv:

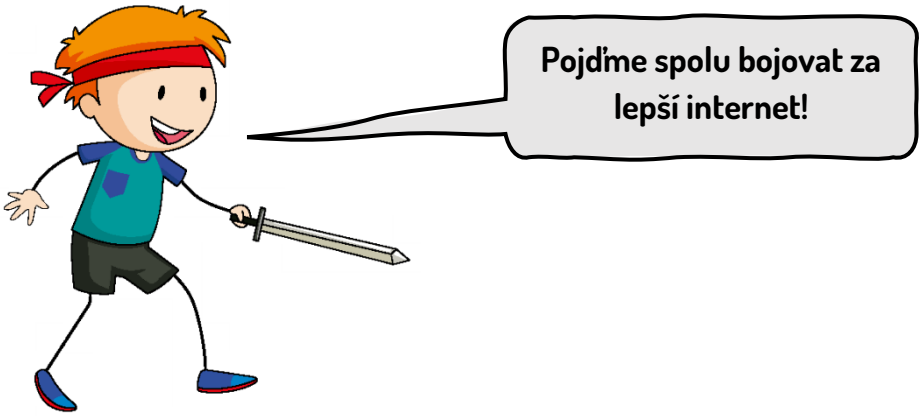
- sebeprezentace,
- svobodné vyjádření názorů a myšlenek,
- snadné a efektivní sdílení informací,
- rychlá a jednoduchá komunikace s ostatními uživateli,
- nástroj pro studium i podnikání,
- trávení volného času – zábava.

Přirozeně se můžeme setkat i s celou řadou nástrah a negativ, které s těmito komunikačními prostředky souvisí:

- online podvody,
- kyberšikana,
- kybergrooming (nebezpečné seznamování v online prostředí),
- závislostní chování (netolismus),
- šíření hoaxů a dezinformací,
- narušení soukromí.

Přestože sociální sítě na nás mohou působit jako nebezpečný nástroj, měli bychom žákům vysvětlit, že pokud budeme k online platformám přistupovat zodpovědně, není důvod se bát. Nezapomínejme, že **pozitiva internetu silně převyšují jeho negativa.**

Důležité je věnovat pozornost prevenci, která nám umožňuje minimalizovat vznik rizikové situace. Proto dodržujme pravidla online služeb, které používáme. Hlídejme si obsah, který zveřejňujeme na internetu a naučme se pracovat s informacemi, které čteme a sdílíme. Naučme se, jak chránit a regulovat naše soukromí na sociálních sítích a buďme obezřetní při online komunikaci s cizími uživateli, protože nikdy nemáme jistotu, kdo sedí na druhé straně.



Metodika k aktivitě: Uživatelé internetu

Aktivita je zaměřena na nejpopulárnější online platformy a jejich uživatele. Úkoly mají za cíl přiblížit žákům svět sociálních sítí z pohledu globálních statistik.

Pro pochopení síly konkrétních služeb nám poslouží první úkol, kde si žáci mohou tipnout, jaká je světová populace a kolik je přibližně na světě uživatelů internetu. Jelikož jde o stále rostoucí čísla, náš tip můžeme ověřit na webu **Internet Live Stats** nebo **Worldometer**, který poskytuje přibližné globální statistiky. Kromě světové populace zde nalezneme i zajímavá čísla z oblasti ekonomie, životního prostředí nebo zdravotnictví.

Globální statistiky:

www.worldometers.info/cz/

www.internetlivestats.com

Řešení – sociální sítě a online služby (logo, MAU – měsíční aktivita):

Název: **Facebook**
MAU: **2,9 miliard**

Název: **TikTok**
MAU: **1 miliarda**

Název: **Twitter**
MAU: **486 miliónů**

Název: **Instagram**
MAU: **1,4 miliardy**

Název: **Discord**
MAU: **150 miliónů**

Název: **WhatsApp**
MAU: **2 miliardy**

Název: **Reddit**
MAU: **430 miliónů**

Název: **Facebook Messenger**
MAU: **1 miliarda**

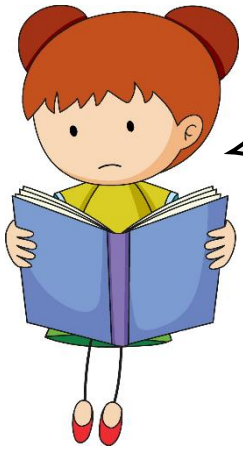
Název: **Snapchat**
MAU: **617 miliónů**

Název: **YouTube**
MAU: **2,5 miliard**

Zdroj:
Global Social Media Statistics
https://datareportal.com/social-media-users

AKTIVITA: SOCIÁLNÍ SÍTĚ VE SVĚTĚ

Jsou někde na světě sociální sítě nedostupné? Existují země, kde fungování sociálních sítí nějakým způsobem omezuje nebo zakazuje vláda? Pokud ano, uveď pár příkladů a zkus tyto země barevně vyznačit na slepé mapě.



Země, kde sociální sítě nefungují:

_____

_____

_____

Země, kde jsou určité sociální sítě omezené:

_____

_____

_____

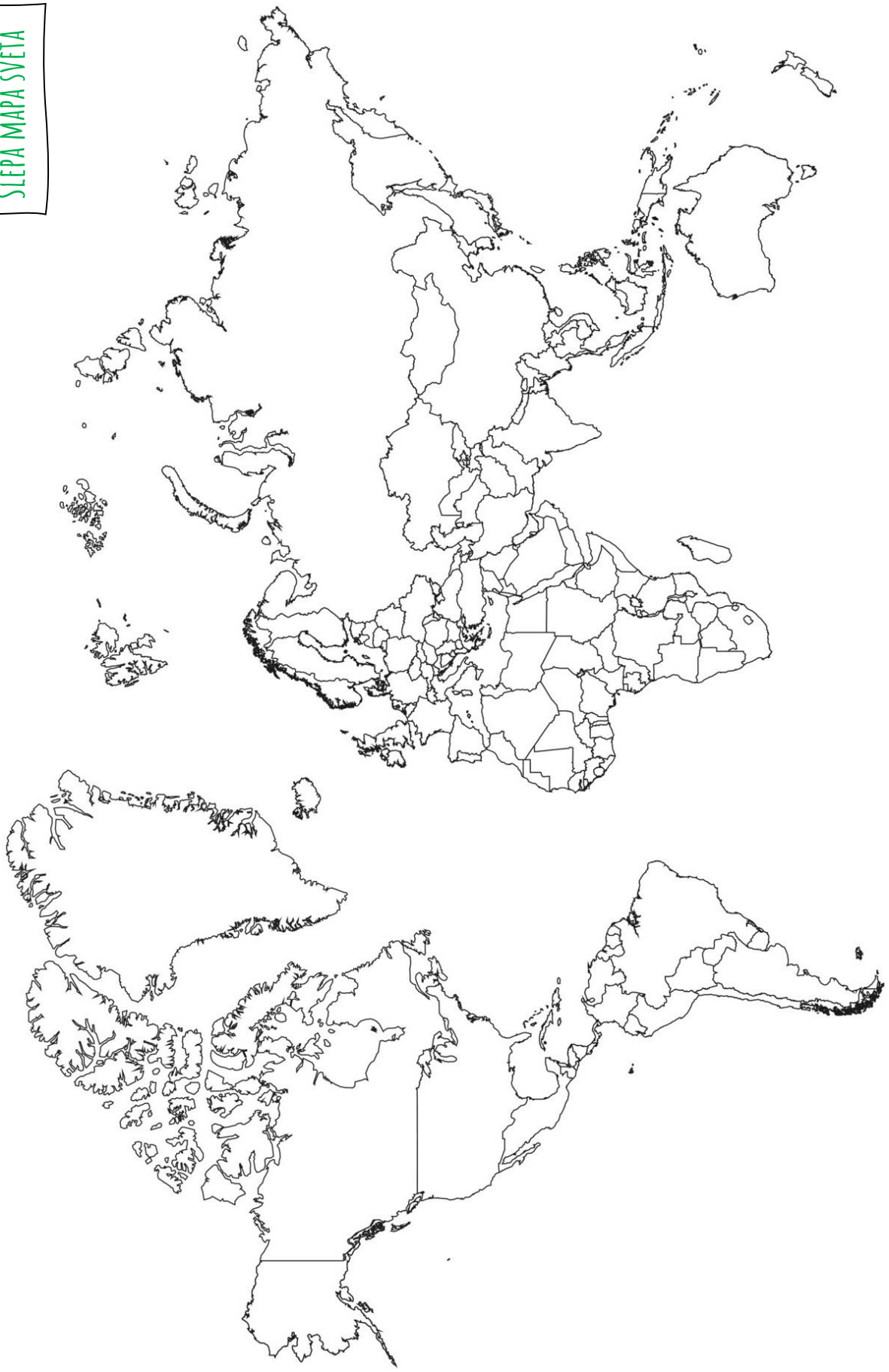
Země, kde jsou určité sociální sítě zakázané:

_____

_____

_____

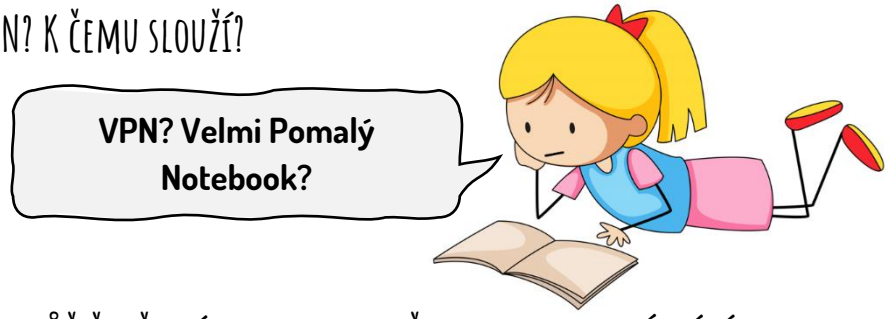
Slepá mapa světa



Proč myslíš, že jsou v některých zemích určité sociální sítě omezovány nebo úplně zakázány? A jak je to u nás, v České republice?

Představte si, že byste měli moc pročistit internet a smazat libovolnou sociální síť. Podle čeho byste se při mazání rozhodovali? A jaké sociální sítě byste smazali?

Víš, co je to VPN? K čemu slouží?



Od kolika let si můžeš v České republice založit profil na sociální síti bez svolení rodičů?

1	8	13	15	18	21

Jakým způsobem si sociální sítě ověřují věk svých uživatelů? A dokážeš toto ověřování nějakým způsobem překonat?

Metodika k aktivitě: Sociální sítě ve světě

Více než polovina světové populace má přístup k internetu. Zřejmě nenajdeme žádnou zemi, kde bychom se nikde na jejím území nedokázali připojit k sociálním sítím. Přesto mělo v minulosti mnoho zemí zakázán přístup k internetu (např. **Sýrie, Etiopie**) nebo jej dodnes výrazně omezují. Pokud bychom hledali vyloženě zemi bez přístupu k sociálním sítím, šlo by zejména o odlehlá místa bez signálu, tzn. bez možnosti připojení k internetu. Země s nejmenším počtem uživatelů internetu tak najdeme především v Africe nebo Asii.

Většina lidí ve svobodné zemi, obzvláště děti, si nedokáže představit, že jejich oblíbené aplikace nebo i sám internet může být nějakým způsobem omezen, nebo úplně zablokován. Pro obyvatele zemí s autoritářským režimem jde o běžný jev. Důvody se v jednotlivých zemích mohou lišit. Státní správa se např. snaží omezit jiné politické strany, odpůrce režimu, kritiky nebo svobodný tisk. Své jednání mohou oficiálně zdůvodňovat jako ochranu soukromí svých obyvatel nebo jako ochranu národní bezpečnosti. Avšak pravým důvodem bývá omezení svobodného přístupu k informacím nebo tendence své občany monitorovat a cenzurovat. K tomu ovšem nemusí sloužit pouze blokace populárních sociálních sítí, ale právě naopak podpora určitých sociálních médií.

Například **Čína** blokuje ty největší západní společnosti (Google, Meta Platforms atd.) a podporuje aplikace vytvořené (a pravděpodobně kontrolované) ve své zemi. Jde o nám ne moc známé aplikace jako **WeChat** (1,3 miliardy aktivních uživatelů měsíčně) nebo **Tencent QQ** (560 miliónů aktivních uživatelů měsíčně). Zajímavou aplikací je v tomto ohledu i **TikTok**, který na čínském trhu provozuje společnost **ByteDance** pod názvem **Douyin** (613 miliónů aktivních uživatelů měsíčně).

Nezapomínejme ale, že za cenzurou sociálních médií nestojí jen státní správa dané země. Na regulaci obsahu či uživatelů se na svých platformách mohou podílet i soukromé společnosti.

Mezi země, kde jsou určité sociální sítě omezené (především Twitter nebo Facebook), můžeme zařadit např. **Bělorusko**, **Sýrii**, **Ekvádor**, **Venezuelu** nebo **Spojené arabské emiráty** či **Brazílii**, kteří blokují především VoIP aplikace (volání přes internet), jako jsou **Skype** nebo **FaceTime**.

Mezi země, kde jsou konkrétní sociální sítě zablokovány, patří hlavně africké a asijské státy. Jako příklad si můžeme uvést **Severní Koreu**, **Čínu**, **Írán**, **Rusko**, **Turecko**, **Ugandu**, **Turkmenistán** nebo **Uzbekistán**.

V těchto a dalších zemích lidé obchází zákazy za pomoci služby **VPN** (virtuální soukromá síť), která vytváří zabezpečené šifrované připojení mezi uživatelem a sítí. VPN tak skryje naše online aktivity a zajistí nám anonymitu před online útočníky i před poskytovatelem připojení.

Kromě toho nám umožňuje přistupovat na požadovaný web odkudkoliv na světě, přestože se fyzicky nacházíme v zemi, kde je konkrétní webová stránka blokována. Nevýhodou VPN je pomalejší rychlost připojení a fakt, že v mnoha zemích je služba omezována nebo úplně zakázána (např. Čína, Bělorusko). Přesto jde o vhodný nástroj pro jakéhokoliv uživatele, který chce chránit své soukromí a mít svobodný přístup k informacím.

Otázky učitele (průvodce):

1. Kolik lidí má podle vás přístup k internetu?
2. Jaká je nejpoužívanější sociální síť v Evropě / Asii / Severní Americe?
3. Jsou někde na světě sociální sítě nedostupné?
4. Napadají vás nějaké důvody, proč se někde na světě nedokážeme připojit k Facebooku, přestože nám internet funguje?
5. Proč jsou v některých zemích určité sociální sítě omezené nebo nedostupné?
6. Myslíte si, že vedení země vysvětluje svým občanům, proč jim zakázalo určité služby?
7. Některé státy blokují zahraniční aplikace a upřednostňují ty, které vytvořily ve své zemi. Proč to dělají?
8. Proč bychom také v České republice neměli zakázat konkrétní sociální sítě?
9. Od kolika let si můžeš v České republice založit profil na sociální síti bez svolení rodičů?
10. Co je to VPN? K čemu slouží? Jaké má výhody a nevýhody?

Slepá mapa světa:

Diskusi ohledně svobodného přístupu k internetu a sociálním sítím můžeme obohatit aktivitou se slepou mapou světa. Žáci mohou do mapy barevně zaznačit například:

- Země, kde jsou sociální sítě omezovány, nebo blokovány.
- Země, kde státní správa cenzuruje internet.
- Země, které blokují službu VPN.
- Země, které blokují především VoIP aplikace, jako jsou Skype nebo FaceTime.
- Země, kde jsou blokovány aplikace společnosti Meta Platforms (Facebook, Instagram, WhatsApp atd.).
- Země, kde jsou blokovány aplikace a služby společnosti Google (YouTube, Gmail atd.).

Zdroje a užitečné odkazy:

These Countries Have Outlawed Social Media
www.cyberghostvpn.com/privacyhub/countries-ban-social-media/

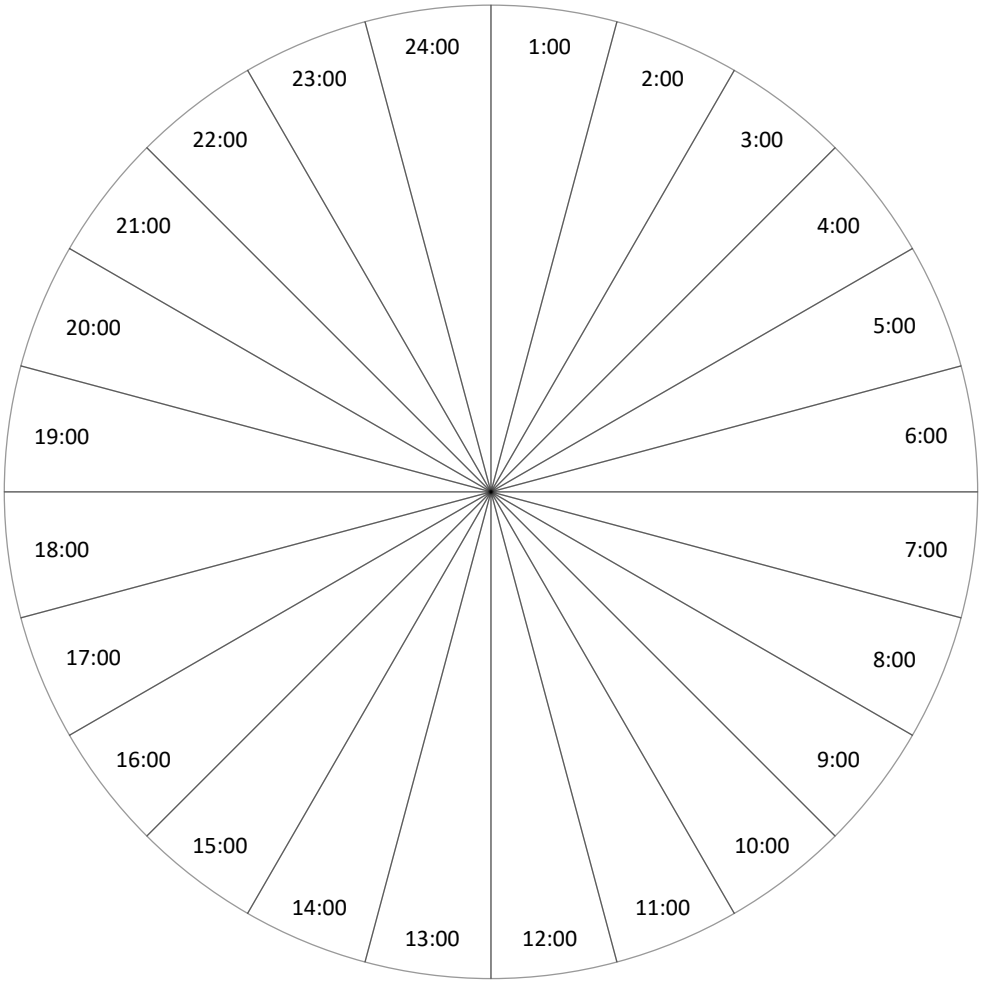
Internet Censorship 2022: A Global Map of Internet Restrictions
www.comparitech.com/blog/vpn-privacy/internet-censorship-map/

Internet shutdown tracker
www.surfshark.com/research/internet-censorship

AKTIVITA: MŮJ DEN

Přemýšlel/a jsi někdy nad tím, jak trávíš svůj čas? Kolik hodin denně se věnuješ škole, sportovním aktivitám nebo zábavě na internetu? Tento graf ti to ukáže! Zamysli se, jak vypadá tvůj běžný den a barevně ho zakresli do grafu. Jeden dílek znázorňuje jednu hodinu tvého dne. Nezapomeň na spánek!

Jak vypadá můj den?



spánek	škola	čas venku s přáteli
zájmové kroužky	PC hry / konzole	_____
četba knih	filmy, seriály, videa	_____
sport	online služby	_____

Metodika k aktivitě: Můj den

Vyzvěte žáky, aby se zamysleli nad tím, jak tráví svůj čas během obyčejného dne. Vyberte například pondělí. Nejprve, ať si žáci promyslí, jaké aktivity během dne vlastně provozují a porovnají je s vybranými aktivitami v legendě pod grafem. Následně ať vybarví celý graf. Ten je rozdělen na dvacet čtyři dílků. Jeden dílek znázorňuje jednu hodinu. Spánek a škola budou přirozeně zabírat přibližně polovinu grafu.

Pokud by v legendě chyběla nějaká důležitá aktivita, kterou žáci provozují, mohou pro ni využít vyznačené místo a doplnit název a barvu aktivity.

Úkol můžete modifikovat. Místo běžného dne vyberte třeba den, kdy mají děti volno a nemusí být ve škole (například sobota, neděle nebo svátek). Výsledky grafů následně porovnejte. Projevil se během volného dne nárůst některé z aktivit, nebo naopak došlo k poklesu? Nad výraznými rozdíly můžete rozvést diskusi a zkusit se dopátrat příčiny.

Žáků se také zeptejte, zda znají pojem **netolismus** (závislostní chování na tzv. virtuálních drogách). Mezi typické projevy patří např. nadměrná aktivita na sociálních sítích, hraní online her, internetové nakupování, online sázení, sledování virálních videí nebo i surfování na internetu. Ovšem abychom někoho mohli označit za závislého, musel by vykazovat všechny typické znaky netolismu. Pokud tedy dítě neprovozuje online aktivity na úkor spánku, školních či domácích povinností, hovoříme pouze o nadměrném užívání. V opačném případě může jít o první příznaky netolismu.

Jestliže v grafu budou převažovat aktivity typu online služby, PC hry, videa nebo konkrétní sociální sítě, vyzkoušejte si i aktivitu „**Kolik času trávíš na internetu?**“, kde se zaměřujeme na čas strávený s konkrétními online službami.

Více informací o netolismu najdete na www.netolismus.cz.

AKTIVITA: KOLIK ČASU TRÁVÍŠ NA INTERNETU?

MÁŠ PŘEHLED, KOLIK VOLNÉHO ČASU TRÁVÍŠ NA INTERNETU? NAŠE TABULKA TI POMŮŽE! VYTVOŘ SI SEZNAM VŠECH SLUŽEB, KTERÉ POUŽÍVÁŠ, A GRAFICKY ZNÁZORNI, KOLIK ČASU S NIMI TRÁVÍŠ. JEDEN DÍLEK ZNÁZORŇUJE PŮL HODINY TVÉHO VOLNÉHO ČASU.

Instagram						
TikTok						
YouTube						

TVÁ TABULKA:

ONLINE SLUŽBA	MŮJ STRÁVENÝ ČAS									
	0:30	1:00	1:30	2:00	2:30	3:00	3:30	4:00	4:30	5:00

PLATÍŠ NĚCO ZA TO, ŽE POUŽÍVÁŠ SOCIÁLNÍ SÍTĚ, NEBO NE? JAK TO, ŽE FIRMY, KTERÉ PROVOZUJÍ SOCIÁLNÍ SÍTĚ, JSOU TAK BOHATÉ?

Metodika k aktivitě: Kolik času trávíš na internetu?

Aktivita nabízí dětem i dospělým možnost vytvořit si přehlednou tabulku, do které si zapíšou všechny online služby, jež denně aktivně využívají. Úkol je podobný předchozí aktivitě „**Můj den**“, ve které z aktivit celého dne vytváříme koláčový graf.

Vypište si všechny používané sociální sítě, jako jsou Facebook, Instagram, TikTok nebo YouTube, a nezapomeňte ani na herní a jiné oblíbené aplikace. Vše se počítá. Následně se zamyslete, kolik času denně přibližně strávíte s vybranými aplikacemi a na základě těchto denních hodnot vybarvěte příslušný počet čtverečků v tabulce.

Jeden dílek znázorňuje půl hodiny volného času, který jste aplikaci věnovali. Když někdo sleduje videa na YouTube přibližně hodinu denně, vybarví dva čtverečky. Pokud alespoň hodinu a půl, vybarví tři čtverečky a tak dále. Jestliže si nejste jistí, kolik času denně trávíte na svém mobilním zařízení, můžete si tyto hodnoty vyhledat přímo v telefonu.

Uživatelům **Apple** zařízení stačí otevřít možnost **Nastavení** -> **Čas u obrazovky** a zde si zobrazit celou aktivitu, případně funkci Čas u obrazovky aktivovat.

Uživatele mobilních zařízení se systémem **Android** to mohou mít složitější. U novějších verzí operačního systému by tuto funkci měli nalézt pod možností **Nastavení** -> **Digitální rovnováha a rodičovská kontrola**. Pokud ve svém telefonu nic takového nemáte, vyzkoušejte třeba nějakou aplikaci, která je k tomu určena.

Možná vás překvapí, kolik volného času věnujete svému telefonu. Podle analýzy společnosti data.ai (dříve App Annie) z roku 2021 trávíme s aplikacemi ve smartphonech v průměru **4 hodiny a 12 minut denně**. A jaký je váš průměr?

Zdroj:

Winning the Attention War: Consumers in Nine Major Markets Now Spend More than Four Hours a Day in Apps
www.data.ai/en/insights/market-data/q1-2021-market-index

Videa k aktivitě

Digitální wellbeing

Sociální bubliny a sociální sítě

DALŠÍ AKTIVITY

Aktivita: Rizika spojená s online hrami

- Hraješ na internetu nějaké hry? Pokud ano, sestav žebříček svých pěti nejoblíbenějších online her.

1.

2.

3.

4.

5.

- Potřebuješ mít pro hraní svých oblíbených online her založený herní účet, který je chráněn přihlašovacím jménem a heslem?

- Hraješ hry společně s dalšími hráči (multiplayer)? A vyměňujete si spolu herní předměty, případně je prodáváte?

- Hraješ v online světě hry, které jsou zdarma, nebo spíše hry, za které platíš (jednorázově či v podobě předplatného)?

- Umožňuje tvá oblíbená online hra nákup nejrůznějších virtuálních předmětů (skiny, zbraně, virtuální peníze apod.) pomocí kreditní karty (tzv. mikrotransakce)? A nakoupil sis někdy něco do své oblíbené hry?

- Víš, co je to Merch? A máš nějaký merch spojený se svou oblíbenou hrou?

Bohužel při hraní online počítačových her můžeš narazit na nejrůznější podvodníky. Přečti si následující článek a zodpověz na otázky.

V roce 2020 se na darknetu prodalo více než 2 miliardy hacknutých účtů hry Fortnite

31. srpna 2020

Díky obrovské popularitě hry Fortnite v posledních několika letech (přes 350 milionů hráčů) se tato hra stala cílem počítačových zločinců. V roce 2020 se na darknetu prodalo více než 2 miliardy hacknutých účtů, ročně si pak zločinci prodejem těchto účtů vydělali více než 1,2 milionů dolarů.

Účty byly nejčastěji hacknuty prostřednictvím prolomení přihlašovacího hesla, buď šlo o tzv. prolomení hrubou silou (brute force), nebo se útočníci dostali do účtu díky tomu, že řada uživatelů používá jedno heslo pro přístup ke všem svým účtům. Pokud pak toto heslo unikne z jakékoli služby, může být snadno zneužito.

Epic Games se snaží omezit počty povolených přihlášení na IP adresu ve snaze zabránit prolomení hesel k účtům, kyberzločinci však toto dokážou obejít. K oblíbeným terčům hackerů patří také Roblox, Runescape a Minecraft.

Zdroj: ThreatPost.com

Jakým způsobem se kyberzločincům podařilo hacknout herní účty hráčů hry Fortnite?

Někteří z hráčů, kterým byl odcizen účet, se svým heslem nenakládali zrovna bezpečně. <u>Co udělali špatně</u>?

? V článku se píše o tzv. Darknetu. Co je to vlastně Darknet? Dokázali byste vysvětlit tento termín?

? Nyní si přečtěte další článek, který se věnuje online hrám a podvodům, které jsou s nimi spojeny. Poté zodpovězte na otázky.

Za krádež virtuálního nože za 30 000 hrozí pachateli až osm let vězení

29. 1. 2021

Kuriózní krádež vyšetřují kriminalisté v Plzni. Obrátil se na ně hráč populární hry Counter-Strike, který za téměř 30 000 korun prodával vzácný virtuální prvek. Od jiného hráče ale dostal pouze zálohu. Policie na Plzeňsku podobný případ nepamatuje, v celém Česku ale není ojedinělý. Videoherní obsah totiž může mít i vyšší cenu.

Virtuální nože či další vybavení a výstroj ve hře Counter Strike: Global Offensive jsou cennou herní komoditou. Má-li hráč štěstí, může vzácné variace takových předmětů získat přímo hraním. Pokud štěstí nemá, může si je pořídit na trhu za reálné peníze. Za unikátní design jsou sběratelé ochotni platit značné sumy.

Hráč z Plzeňska takto nabízel nůž za téměř třicet tisíc korun. Obdržel od kupujícího čtyři tisíce korun jako zálohu a při předání mělo dojít k zbylému doplacení částky. Do současné doby poškozený prodávající neobdržel zbylou část.

Videoher, s jejichž obsahem lze obchodovat, je na trhu nespočet. A byť je ochrana takových obchodů mnohdy zevrubná, prostor pro podvody existuje. Za virtuální podvod hrozí reálný trest – v době nouzového stavu podle policistů až osmileté vězení.

Zdroj: ČT24

- Jakým způsobem pachatel v tomto případě podvedl hráče? Napadá vás, jak by šlo tomuto podvodu zabránit?

- Pokud hrajete online hry, máte na svém herním účtu také nějaký virtuální předmět, který považujete za vzácný? Jak moc si jej ceníte?

- U nakupování virtuálních předmětů ještě chvilku zůstaneme. Přečtěte si následující příběh a pokuste se zodpovědět na otázky.

Noční můra rodičů. Dívka použila tátovu kreditku ve videohře, utratila 300 tisíc

11. 1. 2022

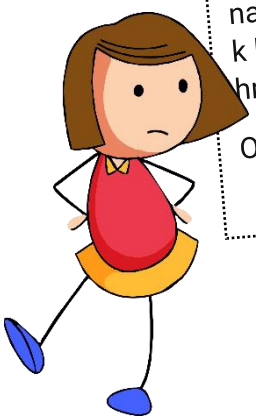
Tichou domácnost musí prožívat osmnáctiletá fanynka počítačové hry Genshin Impact, která použila otcovu kreditní kartu k nákupu 89 mikrotransakčních balíčků (loot boxů), a tím ho připravila o více než 317 tisíc korun. Stačilo jí k tomu jen pár týdnů.

Genshin Impact je mobilní i počítačová hra, která je prakticky zadarmo (free-to-play). Obsahuje ale mikrotransakce za reálné peníze. Díky nim mohou hráči získat další herní obsah, jako jsou např. speciální postavy, silnější předměty nebo kosmetické věci na úpravu vzhledu. Jenže hra využívá tzv. gacha mechaniky, kdy hráči nekupují přímo to, co by chtěli, ale výměnou za hotovost získají náhodný předmět. Odhaduje se, že právě díky tomu tvůrci Genshin Impact vydělali miliardy dolarů za pouhých pár let své existence.

Gacha mechanika využívá strachu z toho, že o něco přijdeme (Fear of Missing Out = FOMO), a tím vytváří nátlak na hráče, aby nakoupili další předměty. Tyto hry jsou přirovnávány k hazardním hrám a mají stejnou psychologickou taktiku jako hrací automaty, aby u lidí vyvolaly závislost.

Otci se nakonec podařilo z banky získat polovinu částky.

Zdroj: Denik.cz



GENSHIN IMPACT

? V textu se objevuje několik cizích slov (mikrotransakce, loot box, gacha mechanika, fomo), která možná neznáte. S využitím textu článku se je pokuste vysvětlit.

MIKROTRANSAKCE	
LOOT BOX	
GACHA MECHANIKA	
FOMO	

? Dokázali byste přijít na to, co mají společného tyto předměty?

Kinder vajíčko

Sběratelské karty

Loot boxy

? V našem příběhu hráčka nakupovala loot boxy s využitím kreditní karty svého tatínka a utratila více než 300 000 Kč. Dokázali byste přijít na to, <u>v čem jsou mikrotransakce rizikové</u>?

? Kolik byste byli ochotni zaplatit za 1 loot box s jedním náhodným virtuálním předmětem (skin, zbraň apod.)?

Méně než 100 Kč	100-499 Kč	500-999 Kč	1 000 Kč a více

Teď se zkusme zamyslet nad tím, jaká pozitiva a jaká negativa má hraní počítačových her. Své nápady doplň do příslušných bublin.

Pozitiva hraní počítačových her

Negativa hraní počítačových her

? Dokážeš vymyslet 5 základních pravidel, jak zajistit svoje bezpečí v prostředí online her?

Bezpečnostní pravidla pro hráče online her

1.

2.

3.

4.

5.

Jinx – League of Legends

? Dá se hraním online her uživit? A víte, co znamená termín esport?

? Vyjmenujte 5 vlastností, které musíte jako profesionální hráči online her mít, abyste byli úspěšní.

Metodika k aktivitě: Rizika spojená s online hrami

Online hry jsou u dětí velmi populární a v herním prostředí tráví velké množství času. Bohužel i tam ale mohou narazit na celou řadu rizik.

Úvodní sada otázek je určena především k rozehřátí žáků a k ověření, zda počítačové hry v online prostředí hrají. Zároveň tak získáme informace o tom, které hry jsou u dětí oblíbené (své žebříčky např. mohou přečíst spolužákům), zda mají herní účty (přihlašovací jména a hesla), zda hrají hry s více hráči (multiplayer), zda si vyměňují či prodávají herní předměty, jestli např. vědí, co jsou to **mikrotransakce** (nákupy za „drobné" částky, zpravidla pomocí kreditní karty), a zda si kupují **merch** (reklamní předměty, např. reklamní hrnky, oblečení apod.).

Poté se podrobněji zaměříme na tři typy podvodného jednání, které je s online hrami spojeno:

a) krádeže účtů prostřednictvím získání hesla,
b) podvody, které jsou spojeny s nákupem a prodejem herních předmětů,
c) zneužití mikrotransakcí.

V případě hacknutí účtů ve hře Fortnite pachatelé jednak využili technické prostředky = brute force attack (útok hrubou silou, tj. odhalení hesla pomocí testování různých kombinací znaků prostřednictvím speciálních aplikací). A jednak toho, že **mnoho hráčů používá tzv. univerzální hesla** (1 heslo pro přístup k více službám). S žáky tedy můžeme probrat také to, zda používají jedno heslo, nebo více hesel pro různé služby.

V článcích, které si žáci přečtou a zanalyzují, najdeme informaci o tom, že se nabídka prodeje hacknutých herních účtů dostala na **darknet**. **Darknet** je označení pro počítačové sítě, které jsou přístupné pouze pomocí speciálního software, zpravidla speciálního prohlížeče webových stránek (např. TOR Browser). Ten umožňuje anonymně využívat celosvětovou síť serverů, přičemž komunikace je šifrovaná a prochází náhodnými uzly rozmístěnými po celém zemském povrchu. Na darknetu existuje celá řada nelegálních tržišť, kde je možné koupit např. drogy, zbraně, údaje k ukradeným kreditním kartám, ukradené herní účty, falešné doklady apod. Viz podrobně v naší animaci.

Třetí článek se věnuje problematice **mikroplateb** a hrám, které aktivně mikroplateb využívají. **Mikroplatba** je vlastně platba malé finanční částky, zpravidla prostřednictvím kreditní karty. Pomocí miokroplateb lze platit jak za reálné věci či služby, tak za virtuální předměty, čehož využívá řada počítačových her a umožňuje hráčům snadno a rychle nakoupit virtuální zboží.

Základním rizikem mikrotransakcí je, že si neuvědomujeme, jak velké částky ve finále utrácíme, protože vnímáme především cenu jednotlivých plateb (desítky, stovky korun). Navíc nám nedochází, kolikrát jsme tuto cenu byli ochotni zaplatit.

S tím souvisí i termíny, na které se dětí ptáme a které jsou schopny odvodit z textu:

Loot box = jde o balíček, který obsahuje náhodný virtuální předmět a který si můžeme zakoupit (či získat jiným způsobem). Existují také tzv. **mystery boxy**, které mohou obsahovat reálné předměty, zpravidla reklamní merch (hrnky, kšiltovky apod.).

Gacha mechanika = nákup virtuálního balíčku (loot boxu), u nějž nevíme, co se v něm ukrývá (balíček má náhodný obsah). Je to podobné jako např. u nákupu Kinder vajíček, sběratelských karet apod. Uživatelé nakupují loot boxy ve snaze získat jedinečný, raritní herní obsah.

FOMO = jde o zkratku slov „fear of missing out", tedy strach z toho, že něco propásneme, že o něco přijdeme. Syndrom FOMO nás vede k tomu, abychom např. pravidelně kontrolovali internetový obsah na sociálních sítích, aby nám nic neuniklo, abychom si pravidelně kontrolovali naše komunikační nástroje, nebo třeba nakupovali loot boxy, které jsou zrovna v akci a které nám nabízejí možnost získat exkluzivní obsah, o nějž nechceme přijít.

V rámci dalších aktivit věnujeme pozornost pozitivům i negativům hraní online her. **Pozitiva:** Trénování reflexů, spolupráce mezi hráči, odpovědnost, rozvoj jazykových kompetencí (angličtina), u nejlepších hráčů také možnost dobrého finančního ohodnocení. **Negativa:** Časová náročnost, drahé počítačové vybavení, vliv na zdraví (oči, obezita, nemoci kardiovaskulární soustavy), poruchy koncentrace, rizika spojená s podvodným chováním a rizikovým seznamováním atd.

Esport je zkratka pro elektronický sport, který je **organizovaný**. V rámci esportu fungují nejrůznější soutěže amatérských či profesionálních hráčů (šampionáty), funguje zde také sponzoring, možnost zajímavého finančního ohodnocení apod. V ČR existuje Česká asociace esportu (www.esport.cz).

Zdroje:

Noční můra rodičů. Dívka použila tátovu kreditku ve videohře, utratila 300 tisíc. Deník.cz. https://www.denik.cz/ze_sveta/divka-pouzila-tatovu-kreditku-ve-videohre-utratila-pres-tri-sta-tisic-20230111.html

Za krádež virtuálního nože za 30 tisíc pachateli hrozí až osm let vězení. ČT24. https://ct24.ceskatelevize.cz/regiony/3262330-za-kradez-virtualniho-noze-za-30-tisic-pachateli-hrozi-az-osm-let-vezeni

Stolen Fortnite Accounts Earn Hackers Milions Per Year. Threatpost.com. https://threatpost.com/stolen-fortnite-accounts-earn-hackers-millions/158796/

Co je syndrom FOMO. E-Bezpečí. https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1229-co-je-syndrom-fomo

Videa k aktivitě

Darknet

Rizika spojená s online hrami

Aktivita: Nebezpečné výzvy (challenge)

Přečtěte si článek o tom, co se stalo 13leté Destini Cranové, nadšené uživatelce TikToku. Poté zodpovězte na navazující otázky.

To, co si Destiny vyzkoušela, byla jedna z tzv. nebezpečných výzev (challenge), která koluje TikTokem. Dokázali byste uvést, v čem je vlastně tato výzva nebezpečná?

Proč vlastně lidé tyto výzvy plní, co je k tomu motivuje?

Jak byste se zachovali, kdybyste byli Influencerem a zjistili, že si nějaké dítě ublížilo, protože se pokusilo napodobit vaše video?

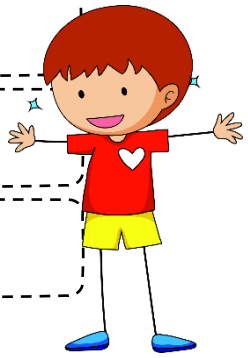
? Kdo je vlastně zodpovědný za to, co se Destini stalo? A proč?

? Měl by TikTok (a další sociální sítě) tento typ obsahu blokovat? A proč?

? Zkoušeli jste někdy vy sami napodobit chování nějakého influencera, kterého znáte ze sociálních sítí? Dokázali byste popsat, co jste si zkusili? A bylo to podle vás nebezpečné?

? Setkali jste se i vy sami s nějakými nebezpečnými výzvami, aniž byste je třeba plnili? A kde na ně na internetu narazíme?

Název challenge	Kde se s ní můžeme setkat?



? Challenge můžou být určitě i pozitivní. Dokázali byste uvést příklad nějaké pozitivní výzvy?

? Některé challenge můžou být i docela strašidelné a děsivé, příkladem takové výzvy je třeba MOMO Challenge, která se rozšířila do celého světa. Posuďte sami…

MOMO si tě našla! Jestli nesplníš její příkazy, přijde si pro tebe a vezme život tobě i tvým blízkým. Nyní začneš plnit úkoly, které ti přinesou hodně bolesti a utrpení. MOMO tě už teď sleduje a ví o každém tvém kroku, neunikneš. Pokud selžeš, zemřeš tak, jako mnoho dalších před tebou… nikdo neunikne MOMO.

? Báli byste se, kdyby vám přišla zpráva s tímto obrázkem třeba na Messenger? Nemusíte, jde o obyčejný hoax a tzv. městskou legendu, která vás má jen vyděsit a vystrašit. Internetem koluje mnoho podobných příběhů, které si vymysleli uživatelé internetu pro pobavení, ale třeba také proto, aby ostatní uživatele vystrašili…

? Co myslíte, že je vyfoceno na obrázku „MOMO"? Využijte internet a zkuste to sami zjistit, třeba pomocí reverzního vyhledávání.

Metodika k aktivitě: Nebezpečné výzvy (challenge)

V prostředí internetu se setkáváme s velkým množstvím výzev (challenges), které **nabádají k často nebezpečnému chování, které může způsobit uživatelům internetu** (především dětem a dospívajícím) vážnou zdravotní újmu. Výzvy jsou šířeny především v prostředí sociálních sítí, např. ve formě videa. K populárním platformám, prostřednictvím kterých se výzvy šíří, patří především TikTok, Instagram či Facebook.

Online výzvy uživatele často nutí k zapojování se do nebezpečných úkolů, u jejichž plnění se uživatelé fotí či natáčejí, výsledek sdílejí a motivují tak další online diváky k zapojení se. Většina výzev v prostředí internetu existuje v latentní formě – pokud nejsou medializovány, zasahují velmi omezený okruh uživatelů. V případě medializace a masivního virálního šíření však mohou uživatelům internetu způsobit vážnou újmu.

To, že se dítě do rizikových výzev zapojuje, lze rozpoznat prostřednictvím různých fyzických příznaků – poškození rtů, poškození kůže, očí apod., v závislosti na typu výzvy, kterou dítě na internetu vyzkoušelo. **Rodiče a učitelé by měli sledovat, zda se u jejich dítěte či žáka varovné příznaky, které tyto jevy doprovázejí, nevyskytují**. Adekvátně pak na situaci reagovat a poskytnout dítěti informace o tom, jak nebezpečné toto chování je a jaké následky může způsobit.

Komunikace rodiče, učitele či vychovatele s dítětem o problematice rizikových výzev v prostředí internetu musí probíhat citlivě, aby informování o rizikových výzvách nevedlo k případné nápodobě.

Komentáře k úkolům:

1. Příběh Destini Cranové je příkladem napodobení výzvy, která se nazývá TikTok Fire Challenge. Podrobnosti o celém případu a samotné výzvě najdete na webu E-Bezpečí (odkaz viz zdroje). Nebezpečí této výzvy spočívá především v tom, že si děti neuvědomují, jak snadno se mohou hrátky s ohněm v kombinaci s natáčením mobilním telefonem zvrtnout a jak rychle může dojít k tragické nehodě.
2. K napodobování výzev vede uživatele celá řada motivů: **zvědavost, touha po úspěchu v online prostředí a touha po ocenění, vyhecování, touha vyniknout, získat nové příznivce, pochlubit se s tím, co dokážeme, prokázat odvahu** apod. Žáky přirozeně necháme vymyslet vlastní motivy, můžeme k tomu využít např. brainstorming.
3. Co se týče odpovědnosti a nebezpečných výzev:
   - odpovědnost má samozřejmě ten, kdo výzvu realizuje,
   - odpovědnost nese i samotný tvůrce, který tvoří obsah, který může vést k poškození zdraví (především v situaci, kdy má mnoho fanoušků mezi dětmi),

- diskutuje se také otázka odpovědnosti samotné služby, tj. sociální sítě a jejího provozovatele – ta sice deklaruje, že poskytuje prostor pro tvorbu, zároveň by však měla nést odpovědnost i za závadný obsah, který může uživatelům ublížit. Některé služby (např. YouTube) proto automaticky nebezpečné výzvy blokují nebo mažou. A dokonce omezují i vzdělávací videa, která se tématem nebezpečných výzev zabývají.

4. K pozitivním výzvám patří třeba Ice Bucket Challenge, v době pandemie vzniklo také mnoho sportovních výzev atd.
5. **MOMO challenge** byla velmi populární v roce 2018, kdy se masově šířila internetem. Děti vyzývala k sebepoškozování, dokonce i k sebevraždě, šlo však o klasický hoax, městskou legendu, která se stala populární především kvůli fotografii, která ji doprovázela. MOMO challenge deklaruje, že způsobila sebevraždy stovek dětí – nic z toho však není pravda a k žádným sebevraždám pod vlivem tohoto fenoménu nedošlo. Socha „Mother Bird" byla vytvořena pro japonskou firmu zabývající se speciálními efekty (Link Factory) a vytvořil ji umělec Keisuke Aiso (Aisawa) v roce 2016. A právě fotografie obličeje této sochy byla součástí „MOMO Challenge". Sám umělec sochu později zničil.

Celá socha „Mother-Bird" a její autor, Keisuke Aiso (Aisawa)

Zdroje:

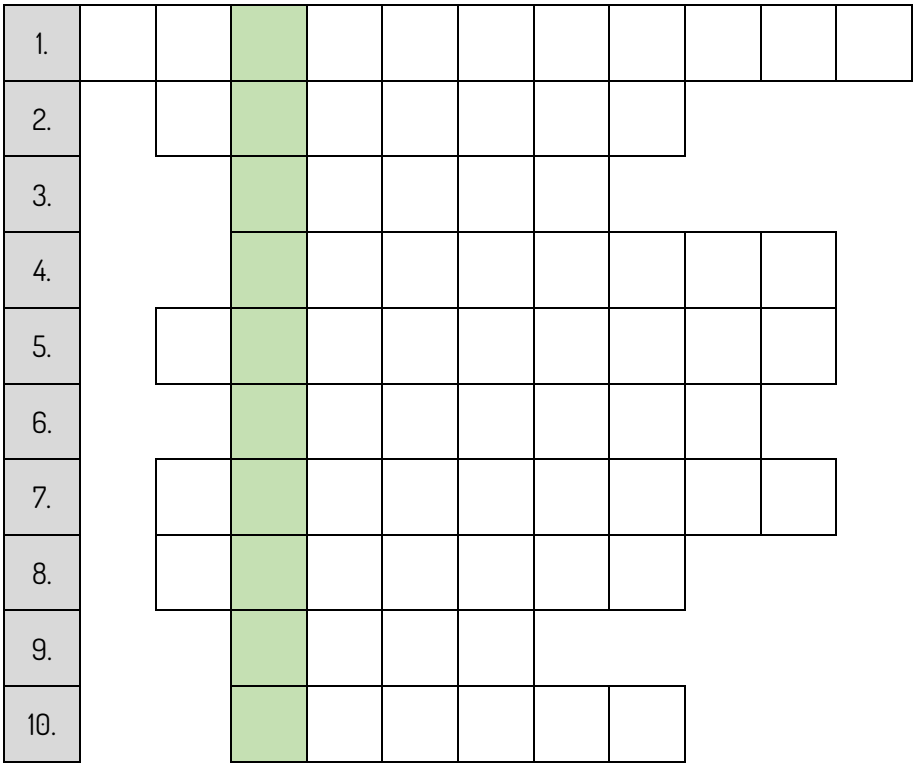
Riziková výzva TikTok Fire Challenge – hrátky s ohněm na TikToku. E-Bezpečí.
https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/2230-rizikova-vyzva-tiktok-fire-challenge-hratky-s-ohnem-na-tiktoku

Rizikové výzvy v online prostředí (fenomén online challenges). E-Bezpečí.
https://www.e-bezpeci.cz/index.php?view=article&id=1618

MOMO challenge – nový druh rizikové výzvy. E-Bezpečí.
https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sociotechnikax/1318-momo-challenge-novy-druh-rizikove-vyzvy

Aktivita: Křížovka

Zvládneš vyluštit naši bezpečnostní křížovku?



1. Kybernetická šikana.
2. Sdílení vlastních intimních fotografií či videí s jinými uživateli.
3. Symbol, který označuje v prohlížeči zabezpečené připojení k www stránce.
4. Vylákávání osobních a dalších citlivých údajů prostřednictvím podvodných odkazů a falešných stránek.
5. Populární komunikační nástroj firmy Facebook/Meta.
6. Silné heslo musí obsahovat velká a malá písmena, speciální znaky a ...
7. Velmi oblíbená sociální síť, jejímž základem je sdílení fotografií.
8. Malé textové soubory, které si webové stránky ukládají do našich prohlížečů a které obsahují informace o tom, co na dané webové stránce děláme.
9. Internetový podvod, jehož cílem je vylákat z nás peníze.
10. Populární sociální síť, jejímž základem je sdílení krátkých videí.

Metodika k aktivitě: Křížovka

Řešení:

1.	K	Y	B	E	R	Š	I	K	A	N	A
2.		S	E	X	T	I	N	G			
3.			Z	Á	M	E	K				
4.			P	H	I	S	H	I	N	G	
5.		M	E	S	S	E	N	G	E	R	
6.			Č	Í	S	L	I	C	E		
7.		I	N	S	T	A	G	R	A	M	
8.		C	O	O	K	I	E	S			
9.			S	C	A	M					
10.			T	I	K	T	O	K			

Závěrečné slovo

Vážený a milý čtenáři či čtenářko,

dostali jste se na konec naší malé knížečky o bezpečném chování na internetu. Doufáme, že jste se na naší procházce světem internetu něco naučili a že jste mnoho z aktivit úspěšně vyzkoušeli v praxi. Tím ale nekončíme! Na našem portálu E-Bezpečí naleznete mnoho dalšího užitečného obsahu ze světa online bezpečnosti! Takže neváhejte a pokračujte na naše webovky www.e-bezpeci.cz. Pokud nás chcete sledovat na sociálních sítích, máte šanci třeba na Facebooku (facebook.com/ebezpeci), Instagramu (Instagram.com/ebezpeci), Twitteru (Twitter.com/ebezpeci), YouTube (Youtube.com/ebezpeci) či TikToku (Tiktok.com/@ebezpeci).

Děkujeme za přízeň a buďte v bezpečí.

Kamil, René a Lukáš
autoři, E-Bezpečí

Napsali o nás

Nová publikace Bezpečné chování na internetu pro kluky a pro holky obsahuje kvalitní vzdělávací aktivity a informace napříč nejdůležitějšími tématy ze světa kyberbezpečnosti. Publikace je zaměřena na jednu z nejzranitelnějších cílových skupin – žáky základních škol. Přesto jde o univerzální příručku, kterou díky pracovním listům s různorodými aktivitami a úkoly může využít každý z nás. Témata jsou přehledně uspořádána a v rámci školní výuky či volnočasových aktivit s nimi lze jednoduše pracovat, případně je rozvíjet i nad rámec této publikace. Velmi oceňuji, že složitější témata, například kyberšikana či kybergrooming, jsou odborně a zároveň srozumitelně vysvětlena. Celkově tak jde o velmi přínosný materiál, který bych v první řadě doporučila dětem a dospívajícím. Ovšem nahlédnout do této příručky doporučuji každému, kdo se chce chránit před nástrahami, které na nás číhají nejen v online světě, ale i v každodenní realitě.

Lucie Kosová, Ministerstvo vnitra ČR

Vzdělávání v oblasti kyberprevence a kyberbezpečnosti je nedílnou součástí rozvoje digitální kompetence. Jak snadné je v online světě lhát? Rozeznáte na první pohled sexuálního útočníka od běžných lidí? Proč nepoužívat technologie těsně před spaním? To vše je možné se v publikaci Bezpečné chování na internetu pro kluky a pro holky dozvědět. Bezprostřední realita online světa je zde hezky ukázaná na konkrétních příkladech. Oceňuji i provázanost s fungujícími projekty v oblasti rizikového chování v online prostoru a interaktivnost doplněnou o přehledné tematické metodiky. Skvělá práce celého týmu autorů!

Lucie Gregůrková, Ministerstvo školství ČR

Publikace přináší velké množství námětů a aktivit pro žáky základních škol, kteří se v několika tematických blocích dozví, jak se pohybovat bezpečně na internetu. Díky srozumitelně popsaným příběhům, příkladům i hravé formě jsou mnohdy těžká témata lehce pochopitelná i pro menší děti. Hravost, která se knihou prolíná, je z mého pohledu výbornou příležitostí pro rodiče, kteří mohou se svými dětmi mluvit o tom, co prožívají na internetu.

Martin Kožíšek, Safer Internet Centrum ČR, CZ.NIC

V dnešní době si život bez informačních technologií již nedovedeme představit. Možnosti, které nám svět internetových služeb přináší, jsou ohromné a nikdo z nás si nedovede představit jejich limity. Propojení reálného světa s tím tvořeným z jedniček a nul je již běžnou realitou. Proto je ale dnes nutné být na toto propojení připraven. Uvědomovat si rizika spojená s užíváním technologických možností, být připraven na možná nebezpečí a leckdy i skryté hrozby, které se mohou v digitálním světě objevit. Je nutné na tato nebezpečí upozorňovat již v rámci základního školního vzdělávání – a právě tomu pomáhá i knížka Bezpečné chování na internetu pro kluky a pro holky. Návyky a pravidla bezpečného chování online si děti musí osvojit již od počátku svého vstupu do digitálního světa.

Václav Písecký, Policie ČR

Vážení uživatelé internetového prostředí, dostává se Vám do rukou přehledně zpracovaný soubor základních pravidel, jak se v online prostředí chovat bezpečně. Kriminalita se poslední roky po celém světě přesouvá více do prostředí internetu. To, jestli se stanete obětí nějakého kyber zločinu, však značně záleží na Vás samotných právě tím, jestli se sami budete chovat bezpečně a zodpovědně. Byla bych opravdu potěšena, kdyby už každý uživatel internetu používal bezpečná hesla, nezneužíval fotografie druhých a ani ty své nedával všanc predátorům. Aby si osvojil pravidlo, že nikomu nesděluje žádná přístupová data k herním či bankovním účtům a i profily na sociálních sítích zabezpečuje a prověřuje. A ta opravdu důležitá pravidla najdete právě v téhle přehledné příručce, kterou zpracovalo Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci. Tak neváhejte a pusťte se do práce.

Zuzana Pidrmanová, Policejní prezidium ČR

Rejstřík

Poradna pro oběti kybernetické kriminality

www.napisnam.cz

BEZPEČNÉ CHOVÁNÍ NA INTERNETU PRO KLUKY A PRO HOLKY

(náměty na výukové aktivity)

Kamil Kopecký, René Szotkowski, Lukáš Kubala

Vydala:
Univerzita Palackého v Olomouci

Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta Univerzity Palackého v Olomouci
Žižkovo náměstí 5, Olomouc, 779 00

www.e-bezpeci.cz

ISBN: 978-80-244-6197-7 (print)
ISBN: 978-80-244-6198-4 (online: PDF)

Ilustrace a fotografie využité v publikaci byly zakoupeny prostřednictvím služeb Vecteezy a Shutterstock.

Jazyková úprava: Pavla Dobešová

E-BEZPEČÍ

WWW.E-BEZPECI.CZ