**ABY BYLO KYBERPEZPEČNO – Metodická příručka, online program a sborník aktivit pro následnou práci s tématem**

**Typ programu:** všeobecná specifická primární prevence

**Nástroje:** interaktivní online program, zážitkové aktivity mapující postoje žáků, jejich informovanost o daném tématu a upozorňující na specifika a rizika spojené s pohybem v online prostoru

**Cílová skupina:** 3.- 5. třída ZŠ, případně i žáci 2. stupně ZŠ

**Cíl programu:** Obecným cílem programu je umožnit dětem poznat rozdíly v chování lidí na internetu a mimo něj a na modelových situacích poznat možná rizika pohybu v internetovém prostředí. Cílem programu je také interaktivní a zážitkovou formou předat žákům základní informace o nebezpečných počítačových jevech, se kterými se mohou setkat nejčastěji (**kyberšikana, kybergrooming, kyberstalking, hoax a nepravdivé zprávy, rizika spojená s užíváním sociálních sítí**). Program pracuje s tématy: ochrana osobních údajů, anonymita na internetu, formy zneužití osoby prostřednictvím internetu a komunikačních technologií. V neposlední řádě je cílem programu diskuse nad způsoby ochrany před nebezpečnými počítačovými jevy.

**Časová dotace:** 90–120 minut

**Pomůcky:** přístup k online programu, pracovní karty s profily a rozhovory, reproduktory, dataprojektor, hudba jako podklad k některým aktivitám, fixy, nalepovací štítky, papíry, podložky, lístečky modelových situací (viz. příloha), papírky na poznámky, zpětné vazby

**před programem**

Je vhodné začít diskusí, nebo malou anketou směřující k využívání internetu mezi žáky: počet žáků využívajících email; počet žáků hrajících online PC hry; počet žáků, kteří mají účet na nějaké sociální síti aj.

Níže jsou také **dvě aktivity**, které je vhodné využít jako úvodní v rámci tohoto tématu – první dvě jsou screeningové a zabývají se povědomím o tématu a třetí využívá momentu překvapení pro diskusi nad tímto tématem.

|  |
| --- |
| KYBERŠKATULATA |
| Cíl: Úvod do tématu. Zmapování užívání a informovanost žáků v dané problematice.  Popis: Žáci sedí v kruhu na židlích. Po prvním kole je jedna z židlí odstraněna, v každém z následujících kol tedy na jednoho z žáků nezbude místo. Hru začíná lektor slovy: „Místa si vymění všichni ti, kteří…“ a doplní toto tvrzení. Například: „Místa si vymění všichni ti, kteří používají počítač.“ Úkolem žáků je se v rychlosti zamyslet, zda o nich dané tvrzení platí, postavit se a vyměnit si místo s jiným spolužákem, který se taktéž postavil. Důležitým pravidlem je, že se žák nesmí posadit zpět na svou židli, ani pravou/levou sousední židli. Po prvním kole lektor jednu z židlí odstraní. Žák, na něhož židle nezbyla, se postaví doprostřed kruhu a doplní větu „Místa si vymění všichni ti, kteří… “ A pokusí se najít si prázdné místo. Takto se hra opakuje. |

|  |
| --- |
| ROZSTŘEL |
| Cíl: Úvod do tématu. Zmapování užívání a informovanost žáků v dané problematice.  Popis: Žáci stojí v kruhu, jeden z lektorů ukazuje na jednotlivce, ti musí říct pojem, slovo, které se jim vybaví, když se řekne internet. Pokud žák rychle nezareaguje, vypadává a jde si dřepnout (ekvivalent motivace pro ty, kteří se příliš nechtějí zapojit). Hra se hraje až do posledního stojícího – experta na problematiku, nebo šťastlivce, na kterého lektor málo ukazoval. Druhý lektor zapisuje pojmy na tabuli nebo flipchartový papír, zároveň vytváří základní kategorizaci pojmu kladných, záporných a neutrálních co do vlivu na člověka.  REFLEXE: čeho je víc kladných nebo záporných? Proč tomu tak je? Nepřemýšlíme nad nimi tak často, možná o nich nevíme (pozn. většinou kladných, ale program je zaměřený spíše na ty záporné) |

|  |
| --- |
| JMENOVKY S HESLEM |
| Cíl: silný „aha“ zážitek, pojmenování rizik spojených s prozrazením hesla.  Popis: Žáci dostanou po úvodním představení instrukci, aby si vzali lepící štítek a napsali si na něj své jméno. Navíc ho mají doplnit o heslo, které používají na internetu. Mají na to čas jedné svižné písničky.  Metodická poznámka: Lektor si napíše třeba několik hvězdiček. Je potřeba sladit zadání s hudebním doprovodem, aby nebyl čas pro případné otázky (přeci jen se je snažíme nachytat).  Před samotným představením přiznáváme, že to na žáky byla „bouda“ a dáváme možnost si heslo zaškrtat a chvíli se bavíme o tom, jak vypadá bezpečné heslo.  Metodická poznámka: Možnou alternativou je zadání jmenovky s tématem „osoba, se kterou bych chtěl chatovat.“ Během jedné písničky si na lepící štítek žáci napíší své jméno a vymyslí osobu, se kterou by si chtěli dopisovat přes internet. Doplněním je téma takového rozhovoru.  Poté proběhne představení všech účastníků v kruhu s tím, že lektor se doptává na téma hovoru a důvod výběru. |

|  |  |
| --- | --- |
| JSNS: Interaktivní kvíz pro žáky pro vstup do tématu (TEST) |  |

**ONLINE PROGRAM**

Cílem programu je interaktivní a zážitkovou formou předat žákům základní informace o nebezpečných počítačových jevech, se kterými se mohou setkat nejčastěji (bezpečný pohyb na internetu, kyberšikana, kybergrooming, kyberstalking, hoax a nepravdivé zprávy, rizika spojená s užíváním sociálních sítí). Obsahem programu jsou jednotlivé lekce, které si žáci mohou jednotlivě projít. Součástí programu je také úvodní a závěrečný kvíz.

**Z hlediska jednotlivých témat je program rozdělený do následujících lekcí:**

1. **BEZPEČNÝ POHYB NA INTERNETU**

Velmi stručný kontakt s tématem „bezpeční na internetu“ – největší důraz je kladen na tvorbu bezpečného hesla.

**Při tvorbě hesla je třeba dodržet několik bezpečnostních standardů:**

1. Ideální heslo by mělo být dlouhé minimálně 8 znaků.
2. Při tvorbě hesla používejte číslice, velká i malá písmena abecedy a speciální znaky.
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.
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 dvojfázovým (dvojúrovňovým) ověřováním, které kombinuje heslo a kód 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.

**Odhadněte, jak dlouho by trvalo průměrně výkonnému počítači prolomit heslo dlouhé 6 znaků standardním útokem (tj. kombinace znaků), které:**

1. Bude složeno pouze z číslic? **Řešení: 3 hodiny**
2. Bude používat číslice a malá písmena abecedy? **Řešení: 8 měsíců**
3. Bude používat číslice, malá a velká písmena abecedy? **Řešení: 18 let**
4. Bude používat číslice, malá a velká písmena abecedy a speciální znaky? **Řešení: 120 let**

Navíc u drtivé většiny online služeb platí, že při opakovaném zadání hesla nás počítač automaticky odpojí a např. na několik hodin zablokuje přístup. Doba průniku na účet se tak násobí.

**Zkuste odhadnout žebříček tří nejčastějších hesel v ČR:**

**Řešení:** 12345, 123456, heslo, heslo123, 123heslo321, aaaaa a qwertz

**Navrhněte způsob, jak vytvořit zapamatovatelné, a přitom bezpečné heslo.**

**Řešení:** Např. zvolíme nějakou známou větu a písmena s diakritikou nahradíme číslicemi,

V Českých Budějovicích by chtěl žít každý = v4esk7chbud2jovic9chbycht2l69tka6d7

|  |
| --- |
| SEMAFOR „Bezpečně na YouTube“ |
| Popis: Žáci se rozdělí do tří skupin, které mají názvy ČERVENÁ – ORANŽOVÁ – ZELENÁ. Každá skupina dostane sadu 15 karet s příklady chování, s nímž se mohou setkat, pokud sledují/vytváří videa na YouTube.  2. Každá skupina má za úkol vybrat chování, které odpovídá barvě její skupiny:  ČERVENÁ: chování, které je na YouTube zakázáno a jehož porušením dochází zároveň k porušení zákona, které může být stíháno a vyšetřováno Policií ČR.  ORANŽOVÁ: chování, které není na YouTube dovoleno, ale dělá se a můžeme se s ním běžně  setkat.  ZELENÁ: chování, které je na YouTube dovoleno a je tedy správné.  3. Následně si žáci sednou do kruhu a zvolí žáka, který bude zaznamenávat. Lektor vyzve jednotlivé skupiny, aby postupně předčítaly, co vybraly. U každého tvrzení je nutné se zastavit a odpověď diskutovat, zejména pokud odpověď není správná nebo pokud zjevně vyvolává otázky.  OTÁZKY K DISKUZI:  Jak se vám tato aktivita líbila?  Dozvěděli jste se něco nového? Zaujalo vás něco?  Zaznělo zde něco, o čem bychom si měli říct více?  Chcete se na něco zeptat?  PRAKTICKÁ DOPORUČENÍ:  Po rozřazení do skupin je nutné obejít všechny skupiny a připomenout úkol skupiny s ohledem na její barvu. Žáci mají většinou problém s rozlišením, které chování je tzv. „oranžové“ a které už „červené“. Je potřeba žáky nabádat, aby nad tím zkusili zapřemýšlet. V následující diskuzi upozornit, že někdy je obtížné rozlišit, které jednání je „oranžové“ a které už „červené“. Tak je to i v reálném životě. Někdy je hranice mezi těmito druhy chování tenká a každý ji může chápat jinak.  Příloha č.1 – sada karet  Příloha č.2 – sada karet – řešení |

|  |
| --- |
| SDÍLEJ SVŮJ OBSAH |
| Popis: 1.Rozdáme žákům papíry a vyzveme je, aby namalovali svůj jednoduchý portrét. Žáci obrázek  nepodepisují a během aktivity neříkají ani jinak nedávají najevo, který obrázek je jejich. Doporučujeme zdůraznit, že portrét má být opravdu jednoduchý, případně vymezíme přesný čas.  2.Doprostřed třídy dáme krabici/nádobu, na kterou napíšeme „internet“. Žáci umístí svůj obrázek do krabice. Upozorníme je, že právě „sdíleli svůj obsah na internet“. (Ověříme si, že žáci pojmu „sdílení na internetu“ rozumí, případně pojem vysvětlíme.)  3. Vyzveme je, aby si z krabice vylosovali obrázek a připsali na něj vzkaz. Tento obrázek „přepošlou“ (podají) někomu ze spolužáků. Nyní má každý obrázek, který od někoho dostal, a opět na něj napíší vzkaz (z kterékoliv strany a kamkoliv). Poté žáky vyzveme, aby obrázek umístili opět „na internet“ (do krabice) a znovu si vylosovali jiný.  4. Tentokrát obrázek trochu upraví, něco menšího k němu přimalují. Vhodí ho zpět do krabice a každý si naposledy vylosuje obrázek.  5. Vyzveme pět dobrovolníků, aby nalepili obrázky, které drží v ruce, na tabuli. K nalepeným  obrázkům připíšeme nadpis: „Lidi, kteří mají rádi pizzu s ananasem.“ Dalších pět žáků obrázky v ruce zmačká.  6. Ptáme se žáků, kde se nyní nachází jejich obrázek, většina by to neměla vědět. Vyzveme žáky, aby obrázky položili do kruhu na zem. Každý by měl svůj obrázek najít a podívat se na něj.  OTÁZKY K DISKUZI:  Co se stalo s vaším obsahem poté, co jste ho „umístili na internet“? Jakým způsobem se šířil? Měli jste kontrolu nad tím, kde se váš obrázek nachází? Jak jste se u toho cítili?  Co asi symbolizoval zmačkaný obrázek? Jak jste se cítili, když se u vašeho obrázku objevil komentář nebo jste byli označeni, že „máte rádi pizzu s ananasem“?  Můžeme námi sdílený obsah na internetu uhlídat? Co vše se s ním může stát?  Co je třeba si uvědomit, než něco budu sdílet?  Metodická poznámka: Snažíme se dovést žáky k tomu, aby si uvědomili, že vše, co sdílíme na internetu, se šíří bez naší kontroly a nelze to vzít zpět. Je třeba si řádně rozmyslet, co budeme sdílet. Na závěr se vrátíme k pravidlům slušného chování při komunikaci. Ptáme se: Jaká pravidla slušného chování při komunikaci platí v běžném životě i na internetu? (Na internetu, stejně jako v reálném životě, platí pravidla ohleduplného chování: Mluvíme slušně. Nikoho neurážíme apod.) |

|  |  |
| --- | --- |
| O2 Chytrá škola: Jak vytvořit bezpečné heslo a jak sním správně zacházet (VIDEO; 2:25) |  |

1. **kyberšikana**

Kybernetická šikana (cyberbullying) je šikana v digitálním prostředí. Stejně jako její klasická forma v reálném světě, i kyberšikana může potkat prakticky kohokoliv. Společný jmenovatel bývá nedostatek sebedůvěry oběti, její submisivita a neprůbojnost.

Děti i dospělí se mohou stát terčem šikany skrze mobil, sociální sítě, počítačové hry, chatovací aplikace, diskuzní fóra a skupiny, fotografie a videa. Cíl je jasný – ztrapnit, zesměšnit, ohrozit, zastrašit a celkově oběti ublížit.

**Co je kyberšikana:**

1. Pomlouvání, zastrašování, urážení nebo zesměšňování prostřednictvím e-mailu, SMS, chatu nebo v diskuzi.
2. Pořizování zvukových nahrávek, videí a fotek nebo jejich upravování a zveřejňování s úmyslem člověku ublížit.
3. Vytváření internetových stránek, které urážejí, pomlouvají nebo ponižují konkrétní osobu.
4. Vyloučení z online komunity.
5. Zneužívání cizího e-mailu nebo profilu a vydávání se za osobu, které patří.
6. Vydírání pomocí mobilu nebo internetu.
7. Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.

**Jak se chránit před kyberšikanou:**

1. Respektuj ostatní uživatele a chovej se k nim slušně.
2. Dobře si rozmysli, co komu posíláš.
3. Měj bezpečné heslo a nikomu ho nedávej.
4. Neposkytuj neznámým uživatelům své osobní údaje, podle kterých by tě mohli vystopovat.
5. Neposílej své fotky nebo fotky své rodiny.
6. Seznam se s pravidly dané služby, ať víš, co je zakázané dělat.
7. Pokud tě někdo šikanuje nebo vydírá, přestaň s ním okamžitě komunikovat.
8. Poraď se o tom s rodiči, učitelem nebo aspoň starším sourozencem či kamarádem.

**Jak poznat kyberšikanu od jednorázového útoku?**

* opakuje se
* má dopad na oběť (zesměšnit, „vyštípat“ z kolektivu)
* je záměrná
* je tu nepoměr sil mezi agresorem a obětí
* často je sama cílem – uspokojení přináší trýznění oběti

|  |
| --- |
| CO JE KYBERŠIKANA? |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Cíl: Cílem aktivity je 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 myšlenkových map.  Otázky:  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. Jaký je rozdíl mezi klasickou šikanou a kyberšikanou?  4. Zkuste popsat, co cítí oběť. (řešení: fyzické projevy, psychické projevy.)  5. Proč vlastně lidé páchají kyberšikanu? (řešení: z pomsty, upevnění pozice ve skupině nebo přeženou vtip apod.)  6. Páchají kyberšikanu pouze chlapci, nebo i dívky? (řešení: samozřejmě obě pohlaví)  7. Je kyberšikana trestným činem?  8. Na koho se obrátit, když mám s kyberšikanou problém? |

|  |
| --- |
| KYBERŠIKANA NA FACEBOOKU |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Cíl: 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.  Popis: Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie dívky, která je důležitá k podpoře emočního prožitku dětí a identifikaci s obětí. Následně je necháme zodpovědět položené otázky a rozvedeme diskusi na téma, zda může verbální agrese v online prostředí člověku ublížit.  PŘÍBĚH:  Tři žáci 6. třídy nesnášeli svoji spolužačku Dorotu. Založili tedy skupinu na Facebooku s názvem „Dorota Nováková smrdí“. Ve skupině Dorotu uráželi, nadávali na ni, zveřejňovali různé její fotografie. Postupně do skupiny přidali celou třídu, a nakonec udělali skupinu veřejnou. Čím více dětí se do komunikace zapojilo, tím horší příspěvky se  ve skupině objevovaly, kluci si nakonec psali o tom, že Dorotu zavraždí, že ji rozřežou  na kusy, že její tělo spálí apod.  OTÁZKY:  1. Myslíte si, že své výhrůžky mysleli kluci vážně?  2. Jak byste se cítili, kdybyste byli Dorotou? Co byste prožívali?  3. Mohou nadávky a výhrůžky v online světě lidem ublížit? Jak?  4. Jak byste situaci řešili – z pohledu Doroty? (řešení: můžeme navést diskusi k technickým řešením – blokací, oslovením dospělého – učitele, rodiče, blokací obsahu na internetu, kontaktováním pachatelů atd.)  5. Představte si, že byste byli učitelem, kterému se Dorota 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?  SHRNUTÍ DISKUSE:  Závěrem diskuze 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/ROZŠIŘUJÍCÍ AKTIVITY:  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. Zpracováním „vlastní“ přednášky nebo prezentace pro své spolužáky o tom, co je kyberšikana.  DOKONČENÍ PŘÍBĚHU:  Výše uvedený příběh vychází ze skutečného příběhu kyberšikany a vyvíjel se následovně ve dvou liniích:  a) Ředitel školy se o existenci diskuzní skupiny dozvěděl, nechal ji zablokovat a potrestal žáky, kteří skupinu založili, sníženou známkou z chování.  b) Nezávisle na postupu ředitele se na Facebook podívala maminka Doroty (vyhledávala jméno a příjmení své dcery, protože chtěla vědět, zda nemá na Facebooku profil). Nalezla diskuzní 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.  Příloha č. 3 – fotka dívky |

|  |
| --- |
| KYBERŠIKANA NA YOUTUBE |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Popis: 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 již od útlého věku (cca 9 let), kolem 13 let věku přecházejí na Facebook a stále častěji na Instagram. Aktivitu proto věnujeme právě aktivitám spojeným s YouTube. Aktivitu je vhodné realizovat jako skupinovou práci. Žákům vytiskneme příběh včetně fotografie dívky, která je důležitá k podpoře emočního prožitku dětí a identifikaci s obětí. Následně je necháme zodpovědět položené otázky a rozvedeme diskusi na téma, zda může verbální agrese v online prostředí člověku ublížit.  PŘÍBĚH:  Třináctiletá 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 ji 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.  OTÁZKY:  1. Kdo z vás sleduje YouTube? Jaká videa na YouTube sledujete?  2. Sledujete youtubery? Chtěli byste být jako youtubeři? Proč?  3. Myslíte si, že má youtuberství nějaká pozitiva?  4. Myslíte si, že má youtuberství také nějaká negativa?  5. Jak byste reagovali, kdybyste byli Katkou? Co byste dělali na jejím místě?  6. Když je někdo na internetu slavný, má pouze své fanoušky, nebo i tzv. hatery?  SHRNUTÍ DISKUSE:  Závěrem diskuzí by mělo být sdělení, že sláva v prostředí internetu má svoje pozitiva i negativa a že v podstatě každý úspěšný youtuber/streamer/influencer má své nepřátele – tzv. 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.  Příloha č. 4 – fotka dívky |

|  |
| --- |
| KYBERŠIKANA V ONLINE HRÁCH |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Popis: Aktivita se věnuje kyberšikaně spojené s hraním online her 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. Následně je necháme zodpovědět na položené otázky a rozvedeme diskuzi na téma, zda může verbální agrese v online prostředí člověku ublížit.  PŘÍBĚH:  Jedenáctiletý 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 prostřednictvím běžného textového chatu, řada z nich však také využívala instant messenger s VoIP – Skype. Při objevování světa Minecraftu se Petr seznámil s třináctiletým Jakubem. Z obou chlapců se stali herní přátelé a večer spolu pravidelně hráli a komunikovali prostřednictvím Skype, stejně tak si nahrávali své herní pokroky a sdíleli je prostřednictvím YouTube. Ke komunikaci využívali rovněž 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 vysvlečeni předváděli různé fiktivní praktiky). 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 Facebooku a Instagramu.  OTÁZKY:  1. Hrajete online hry? A znáte nebo hrajete hru Minecraft?  2. Přečtěte si výše 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? (řešení: heslo, anonymizace 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? (řešení: ignorování, nahlášení videa, oznámení rodičům s radou o pomoc apod.)  7. Který osobní údaj je podle vás v online prostředí nejvíce zneužitelný? (řešení: otázku lze pojmout jako brainstorming, výsledek by měl být, že ten osobní údaj, který umožňuje naši jednoznačnou identifikaci – fotografie obličeje, případně intimní fotografie, na které je rozpoznatelný náš obličej.)  SHRNUTÍ DISKUSE:  Závěrem diskuze by mělo být sdělení, že v prostředí internetu je nutné chránit si své osobní údaje, protože mohou být zneužitelné 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. |

|  |
| --- |
| ANDĚLÉ A DÉMONI: HRANICE KYBERŠIKANY |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Popis: Aktivita „andělé a démoni“ 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.  VÝROKY:  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 jenom svět virtuální, ve kterém neplatí to, co ve světě reálném.  ŘEŠENÍ:  Výrok 1 se zaměřuje na svobodu slova (projevu) na internetu – ta však není neomezena. Svoboda projevu je jedním ze základních lidských práv, které je definováno v řadě dokumentů – ve Všeobecné deklaraci lidských práv, Mezinárodním patku 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 výroku 2 a výroku 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 my. 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 netikou (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.  Výsledkem argumentačního souboje by tedy mělo být, že i na internetu jsme odpovědní za vše, co děláme. |

|  |  |
| --- | --- |
| Kyberšikana - proč vzniká a jaké jsou její nejčastější motivy (VIDEO; 12:26) |  |

|  |  |
| --- | --- |
| Kyberšikana – metodický list pro učitele (MŠMT – METODIKA) |  |

|  |  |
| --- | --- |
| Druhy kyberšikany (VIDEO; 4:51) |  |

|  |  |
| --- | --- |
| ONEMANSHOW Foundation – Cizí zeď (prod. Fiedlerski) (VIDEO; 4:49) |  |

|  |  |
| --- | --- |
| Nenech to být (NNTB) - nejpoužívanější platforma na whistleblowing v ČR (WEB) |  |

1. **kybergrooming**

Obětí podvodu, tedy i kybergroomingu, se může stát každý z nás. Děti a teenageři jsou ale vůči online manipulacím daleko citlivější. Nejčastější průběh kybergroomingu je ten, že se útočník pod falešnou identitou snaží dostat svou oběť na osobní schůzku. Tam pak dochází k sexuálnímu zneužití a výrobě dětské pornografie. Výjimečné nejsou ani fyzické útoky.

Kybergrooming představuje jednání osoby, která se snaží zmanipulovat oběť a donutit ji k osobní schůzce. Útočník s obětí komunikuje převážně skrze digitální technologie. Oběť může být vyzvána k osobní schůzce za účelem sexuálního zneužití nebo jiné formy agrese. Mezi sexuálními predátory je tento typ agresivního útočníka v menšině. Většina predátorů se spokojí „pouze“ s nevhodnou komunikací, masturbací na dálku atd.

|  |
| --- |
| CHAT |
| Cíl: Cílem aktivity je vytvořit atmosféru pro chatování, vytvořit podklady pro další aktivitu. Zvědomit, že nikdy nevíme, kdo je na druhé straně.  Popis: Aktivitu motivujeme jako hru na chat. Můžeme v úvodu využít zkušenosti účastníků s chatováním, případně použít název některé konkrétní aplikace (často využíváme Messenger). Zároveň zdůrazníme, že někteří budou mít možnost si zažít chatování i z pohledu počítače.  Rozdělíme účastníky na dvě poloviny – z jedné se stanou uživatelé chatu, druzí jsou chat sám o sobě. Všichni dohromady se dozví základní informace – chatovat budete 15 minut, úkolem uživatelů je si dobře o čemkoli pokecat, úkolem chatu je přenášet vzkazy od jednoho uživatele ke druhému. Polovina uživatelů si sedne na jednu stranu místnosti a druhá na druhou, dostanou instrukci, že se mají po celou dobu dívat směrem od druhé poloviny uživatelů – na chatu přeci také nevidíte člověka, se kterým si píšete, jenom svůj počítač případně jeho fotku, kterou má v profilu. Jedné polovině (nebo i oběma polovinám) uživatelů navíc dáme tajnou instrukci, aby se vydávali za někoho jiného ze svojí skupiny. „Zkuste toho, s kým si budete psát, zmást tak, aby si myslel, že jste někdo jiný.“  Polovina účastníků, kteří dělají chat, dostanou následující instrukce:  - budete přenášet vzkazy po celou dobu pouze mezi dvěma uživateli  - vzkaz vždycky vy sami zapíšete na papír, na kterém bude probíhat chat  - za žádných okolností nesmíte prozradit nebo naznačit, kdo s kým si píše  Na začátku je u každého uživatele jeden člověk, který dělá chat. Ten si náhodně vybere, ke komu z druhé strany místnosti půjde. Potom už chodí stále mezi těmi samými dvěma lidmi.  K chatování pustíme nějakou hudbu, pomáháme řešit případné nejasnosti v průběhu, snažíme se dosáhnout toho, aby se opravdu nedívali na druhou stranu.  V průběhu hry aktivně sledujeme dění, můžeme drobně interagovat s účastníky, kteří dělají chat, podpořit je. Po uplynutí 15 minut vyzveme všechny k ukončení chatu a dostanou pár minut na to, zjistit, s kým si doopravdy psali, případně si říct, jaké to bylo. Po chvilce všechny svoláme do kruhu a uděláme krátkou reflexi, kdy se zaměřujeme na to, jestli bylo poznat, s kým si píší, podle čeho to poznali. Chaty si od nich vezmeme.  METODICKÁ POZNÁMKA: Je vhodné začít aktivitu rozhovorem s dětmi na téma specifik komunikace přes síť, co vše využíváme a z jakého důvodu. Poté jeden z lektorů předvede úkoly přenašeče zpráv přede všemi. Je vhodné vyzdvihnout důležitost této role – nebude možné se vyměnit, často se jedná spíše o nepopulární roli.  REFLEXE: V reflexi se obvykle dotkneme toho, že se poznali hlavně díky tomu, že se dobře znají z každodenního života. Zároveň je obvykle několik lidí, kteří přiznají, že nevěděli, s kým si píšou. Pokud se to hodí, můžeme zmínit, že podobný poměr jako tady platí i v realitě na internetu („Každý pátý člověk se vydává za někoho jiného.“) Podobně, pokud se to hodí, můžeme mluvit i o tom, že řada z nich se na internetu vydává za starší (často mají Facebook s falešným věkem apod.). |

|  |
| --- |
| FIKCE NEBO REALITA |
| Cíl: Cílem hry je ukázat si na příkladech, které žáci sami v předchozí aktivitě (CHAT) vytvořili, rozdíly mezi běžnou komunikací tváří v tvář a komunikací prostřednictvím chatu.  Popis: Techniku uvedeme tak, že nyní tady máme záznamy několika chatů, což je jedinečná šance vyzkoušet, jestli rozhovory, které se odehrávají na internetu, jsou opravdové nebo ne. Jestli by se lidi takhle bavili i v normálním životě. Řekneme, že to vyzkoušíme na třech z chatů, které máme k dispozici, ale že se budeme snažit, aby žádný člověk nebyl dvakrát. Potom losujeme (pokud je ta možnost, necháme losovat TU).  METODICKÁ POZNÁMKA: Zpravidla je vhodné před touto aktivitou zařadit přestávku, někdy je vhodné předem vybrat chaty, které budeme číst, abychom z nich dostali co nejvíce informací, příp. témat. Žáci neřeší, zda se chaty losují, nebo ne, stačí je brát shora hromádky.  Po vylosování daný chat přečteme a společně pak krátce diskutujeme, zda by se takhle lidi bavili i v normálním světě, případně v čem se tedy normální rozhovor od toho internetového liší.  Na konci se můžeme zeptat, co chtějí se zbylými chaty udělat. Pokud se na tom neshodnou všichni, jenom krátce vysvětlíme, že nechceme nikoho k ničemu nutit, a že věci z tohoto programu zůstávají tady. Potom chaty roztrhneme a vyhodíme. K roztržení chatů můžeme ještě doplnit, že přesně tohle člověk na internetu udělat nemůže, protože všechno mohou mít ostatní uživatelé archivované, stejně jako se to i po smazání archivuje na serverech – „Co jednou na internet dáš, nemůžeš už nikdy s jistotou vzít zpět.“.  METODICKÁ POZNÁMKA: V dobré třídě je tato aktivita obvykle dobrá sranda. Někdy se může stát, že sranda začne převyšovat cíl programu – je vhodné na to žáky upozornit, celou situaci reflektovat, případně aktivitu ukončit. Ukončení aktivity je možné také pokud žáci některý z chatů využijí pro to, aby se některému ze spolužáků posmívali.  METODICKÁ POZNÁMKA: Při čtení dáváme jako první možnost oběma autorům chatu. Pokud to sami číst nechtějí, vyzveme toho, kdo mezi nimi přenášel zprávy (chat), aby to přečetl společně s jedním z lektorů. Samotný papír jim vždycky držíme. Při čtení je motivujeme, aby četli opravdu všechno (problémy dělají sprostá slova, vyznání lásky a smajlíky).  V reflexi u každého chatu se nejčastěji ukáží tyto rozdíly:  o větší tendence přehánět (na chatu se zvyšuje agresivita i projevy náklonnosti – je snazší nadávat i říkat „miluju tě“)  o je snazší lhát, předstírat nebo si dobře promyslet, co řeknu (opravovat si to)  o je těžší dát najevo emoce, zjednodušujeme si je (využíváme menší škálu)  o někdy se na chatu bavíme úplně o ničem (nesmyslně), přesto tím trávíme čas  rozhovor je jiný, protože nevidíme toho druhého |

|  |
| --- |
| NEZNÁLEK MAXIM |
| Cíl: Cílem je procvičení uplatňování zásad pravidel bezpečné online komunikace  Popis: 1. Žáci jsou rozděleni do dvojic/trojic. Každá dvojice má za úkol přečíst si úryvek rozhovoru  na sociální síti a zaznačit, které informace by o sobě Neználek Maxim neměl prozradit, když si píše s Chameleonem.  2. Žáci prezentují zvolené odpovědi a skupinově je diskutují. Jednotlivé odpovědi je potřeba  vztáhnout k pravidlům bezpečné online komunikace.  REFLEXE:  Zdál se vám tento chat reálný?  Komunikace mezi útočníkem a obětí vypadá v řadě případů takto. Útočník se snaží oběti zalíbit, někdy používá techniky manipulace a nátlaku. Velmi rychle většinou dojde na žádost o zaslání nevhodných fotografií či videí.  Shodli jste se ve skupině na tom, které informace by Neználek Maxim neměl zasílat a proč? Informace o tom, jakou navštěvuje školu; bydliště; telefonní číslo; fotografie a zejména ty s nevhodným obsahem; souhlas s videohovorem přes webovou kameru – útočník může mít nastavenou tzv. smyčku, která na PC/mobilu oběti vypadá jako spuštěná webová kamera, ale je to pouze záznam.  Co se nám může stát, pokud bychom tyto informace někomu sdělili? Řada těchto informací jsou osobními údaji, díky nimž nás může kdokoliv identifikovat. Pokud se jedná o dítě, může si na něj útočník počkat například před školou, když se bude vracet z kroužku a ublížit mu.  Co se nám může stát, pokud vyrazíme na schůzku s neznámým člověkem?  Může nám ublížit. Jak?  METODICKÁ POZNÁMKA: Věnujte se rozboru textu do hloubky. Žáci často opomíjí informaci typu „bydlím blízko školy“, protože to nepovažují za riziko (nikomu přece nesdělují přesnou adresu). Nicméně spolu s dalšími informacemi, může být i tato informace pro útočníka cenná.  Příloha č. 5 – Neználek Maxim  Příloha č. 6 – Text rozhovoru k řešení |

|  |  |
| --- | --- |
| Kybergrooming – nebezpečné seznamování v online prostředí (VIDEO; 6:03) |  |

|  |  |
| --- | --- |
| Kybergrooming - Triky sexuálních útočníků na internetu (VIDEO; 8:35) |  |

|  |  |
| --- | --- |
| Internetem bezpečně – Kybergrooming (VIDEO; 6:27) |  |

|  |  |
| --- | --- |
| On-line interaktivní vzdělávací aktivita pro žáky 4. a 5. tříd ZŠ  Tato vzdělávací aktivita se věnuje tématům digitální stopy, digitálního soukromí, sextingu a kybergroomingu. Cílem aktivity není encyklopedická znalost jednotlivých témat, ale především prožitek. |  |

1. **kyberstalking**

Stalking je termín, který představuje dlouhodobé, opakované a systematické obtěžování (pronásledování). Útočník svou oběť sleduje a zasypává ji zprávami, e-maily, telefonáty, nechtěnou pozorností apod.

Kyberstalkting pak představuje verzi stalkingu, kde hrají hlavní úlohu digitální technologie. Pronásledovatel využívá především sociálních sítí a informací z dalších otevřených zdrojů, aby si našel informace o své oběti a aby jí jejich prostřednictvím dále ubližoval.

Sledovat a obtěžovat někoho na internetu je ještě snazší než v reálném životě. Moderní informační technologie usnadňují život nejen nám všem, ale i kyberstalkerům. Sociální sítě jsou pro stalkera skvělý zdroj informací o případné oběti. Navázat kontakt navíc nikdy nebylo snazší. Chat, e-mail nebo telefon? Stačí si vybrat.

V českém prostředí potvrzuje nějakou zkušenost se stalkingem asi desetina populace. Nejčastěji se vyskytuje mezi expartnery, setkávají se s ním ale i celebrity a politici. Určité procento případů bohužel může gradovat až ke smrti. Od roku 2010 klasifikuje český legislativní systém jakýkoliv stalking, tedy i kyberstalking, jako trestný čin nebezpečného pronásledování.

Díky internetu (a občas i lidské důvěřivosti) se stalker ani nemusí moc namáhat, aby získal dostatek informací o nás a naší každodenní rutině. Ochotně je celému světu servírujeme přes příspěvky a fotky na svých sociálních sítích. I s roztomilými a o to cennějšími detaily.

|  |  |
| --- | --- |
| Kyberstalking – virtuální nápadník (VIDEO; 25:02) |  |

1. **sociální sítě**

**Vodítkem, že se jedná o falešný profil, může být např.:**

* podivně znějící jméno profilu
* falešná nebo žádná profilová fotka
* absence reálných přátel/sledujících
* nemá skoro žádné sledující či přátele, ale sám sleduje hodně účtů
* velmi malá, případně podivně vypadající aktivita
* velmi malá interakce s přáteli a sledujícími, žádné lajky, žádné komentáře
* mezi sledujícími jsou pouze profily, které vypadají podezřele či falešně
* osoba podezřele často mění jméno profilu nebo profilovou fotografii
* obsah, který profil přidává, se často mění, příspěvky mizí atd.
* na svém profilu uvádí další zvláštně vypadající linky, kam kliknout dál

**Fotografie** – že se jedná o falešnou fotografii poznáme podle následujících signálů:

* fotografie je veřejně dostupná např. z fotobanky
* fotografii je možné najít na jiných profilech
* fotografii je možné nalézt v různých jiných kontextech na internetu
* na žádné z fotografií není dané osobě vidět plně do obličeje
* na profilu se objevují fotografie různých osob
* na profilu chybí fotografie dané osoby s přáteli / více lidmi
* U zaslaných fotek v rámci komunikace:
* můžeme danou osobu požádat, aby se vyfotila s nějakým konkrétním textem či předmětem v reálném čase, aby
* neměla čas případně fotografii editovat
* můžeme zaslané fotografie vyhledat přes Google obrázky, abychom zjistili, zda se nejedná o fotografii použitou již
* v minulosti v jiných kontextech či převzatou z fotobanky (postup: klikneme na fotografii pravým tlačítkem a zvolím
* možnost „vyhledat obrázek na webu “)

**Osobní komunikace** – mohli byste si nějak osobně ověřit, že to je opravdu tato osoba?

* vhodným způsobem je např. video hovor s danou osobou, kdy při vzájemné interakci nemá šanci skrýt svou skutečnou identitu
* zde je důležité pracovat s možností, že žáci budou navrhovat osobní setkání, musí být jasně formulována a zdůrazněna nebezpečnost této varianty (a pokud bychom se o této možnosti bavili, je nutné zdůraznit uskutečnění možného setkání vždy pouze na veřejném místě, kde se běžně pohybují lidé)

**Důvody pro používání falešných profilů-**falešné profily mohou lidé či skupiny lidí zakládat z různých důvodů:

* může se jednat o vylákání fotek či získání osobních a citlivých údajů, na jejichž základě vás poté podvodník může vydírat
* zároveň mohou falešné profily sloužit i k trolení (tzv. troll je v internetovém slangu účastník online diskuzí či chatů,
* komentátor, který se záměrně snaží vyprovokovat ostatní uživatele k emotivní odezvě či odklonit debatu od tématu
* a narušit ji) a díky tomu šířit provokativní, urážlivé příspěvky a komentáře k různým tématům

|  |
| --- |
| ŠKÁLA CHOVÁNÍ |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Popis: Žákům dáme list s následující tvrzeními. Ti ho rozstříhají na proužky tak, aby se jeden proužek rovnal jedné větě. Jejich úkolem je seřadit chování od nejméně k nejvíce zraňujícímu. Proužky v tomto pořadí pak nalepí na papír, naskenují/vyfotí a pošlou, případně nasdílí během společné výuky.  TVRZENÍ:   * Napsat přes internet spolužákovi do zprávy, že ho všichni nesnáší. * Vyfotit učitele ve směšné pozici a dát to na internet. * Dát na internet fotku sourozence, když brečí vzteky. * Nemluvit se spolužákem. * Nemluvit se sourozencem. * Vyhrožovat spolužákovi fackou. * Dát spolužákovi facku. * Dát sourozenci facku. * Říct spolužákovi, že je hloupý. * Říct mámě, že je hloupá. * Říct sourozenci, že je hloupý. * Křičet na spolužáka. * Křičet na sourozence.   Společně si pak s žáky povídáme o tom, proč seřadili činnosti v tomto pořadí a snažíme se je vést k argumentaci. Popsané situace jsou záměrně vybrané tak, aby nebylo jednoznačné, které chování je více či méně přijatelné. |

|  |
| --- |
| PŘIDEJ SI DO PŘÁTEL |
| Cílová skupina: 5. třída + 2. stupeň ZŠ  Cíl: Cílem je zprostředkovat odpovědi na otázky: Proč se lidé vydávají za někoho jiného? Jaké má vydávání se za někoho jiného výhody a nevýhody? Téma osobní údaje: které to jsou a proč je potřeba osobní údaje chránit.  Popis: Žáci jsou rozděleni do skupin po 3 lidech, každá skupina si vylosuje obálku se svým profilem, který sdílejí veřejně na internetu. Stávají se nyní touto osobou a chtějí získat co nejvíce kamarádů, zároveň si je může kdokoli přidat do přátel, některé sdílené profily ovšem nejsou úplně pravdivé, skutečné informace o osobě se skrývají uvnitř obálky a může do nich nahlédnout pouze osoba, které obálka patří. Žáci mají dvě písničky na to, aby si vybrali mezi své přátelé, někoho z nabízených profilů.  REFLEXE: kolik lidí jsme si přidal/a mezi své přátele, podle čeho jsem si vybíral/a, proč se lidé na internetu vydávají za někoho jiného – odtajnění pravé identity, jaké výhody, jaké nevýhody může mít vydávání se za někoho jiného? Vydával/a jsem se někdy za někoho jiného? Co o sobě uvádět na veřejný profil, co ne, co mi může ohrozit?  Příloha č. 7 – sada profilů |

**další AKTIVITY a informace VHODNÉ PRO PRÁCI S TÉMATEM**

|  |
| --- |
| MILÁ SALLY |
| Cíl: Cílem hry je na modelových situacích poznat možná rizika pohybu v internetovém prostředí. Zároveň pak předat žákům dovednosti pro řešení problematických situací v on-line prostoru.  Popis: Na úvod rozdělíme účastníky náhodně na malé skupiny (po dvou nebo po třech). Řekneme jim, že jsou redaktory internetového portálu, na kterém radí, jak se na internetu chovat. Dostali od šéfa za úkol zpracovat správné reakce na modelové situace, které si vylosují. Je jen na nich, jak to pojmou. Mají teď jednu písničku na přípravu.  METODICKÁ POZNÁMKA: na rozdíl od většiny dělení žáků na skupiny není nutné dělit je náhodně, či rozpočítávat, pro tuto aktivitu stačí jen projít kruh a ukázat skupinky podle žáků tak, jak sedí u sebe.  Necháme je vylosovat jednotlivé situace, nabídneme papírky a fixy, pustíme hudbu.  Potom každá skupina prezentuje svoji odpověď na popsanou situaci. Až domluví, ostatní se k tomu mohou krátce vyjádřit. Každá skupina pak vybírá, kdo půjde po ní.  METODICKÁ POZNÁMKA: Modelové otázky, na které žáci odpovídají, lze mít již připravené nebo využít dotazů samotných žáků, kteří je mohou zformulovat na základě svého zájmu nebo vlastní zkušenosti.  Příloha č. 8 – modelové otázky |

|  |  |
| --- | --- |
| Kurz Technologie a prevence (KURZ PRO UČITELE) |  |

|  |  |
| --- | --- |
| Phishing (ONLINE KVÍZ) |  |

|  |  |
| --- | --- |
| Příznaky problémového užívání internetu (TEST) |  |

|  |  |
| --- | --- |
| CLASHING (ONLINE HRA) |  |

|  |  |
| --- | --- |
| Buď safe online (ONLINE KURZ) |  |

|  |  |
| --- | --- |
| Interland – hra určená dětem školního věku. Hra je složená ze čtyř základních lekcí, které tvoří jednotlivé minihry. Během cesty se děti naučí, jak si poradit s hackery, phishery, kyberšikanou nebo sdílením informací na sociálních sítích. |  |

|  |  |
| --- | --- |
| Interhighway - interaktivní vzdělávací hra, která seznamuje žáky základních škol s pravidly bezpečného chování na internetové dálnici. V herním prostředí se děti seznamují prostřednictvím virtuálních průvodců s klíčovými tématy internetové bezpečnosti, překonávají překážky a odhalují skrytá tajemství herního prostředí. |  |

**ZDROJE**

<https://o2chytraskola.cz/>  
<http://www.kybergrooming.cz/#kybergrooming>   
<https://www.nukib.cz>  
<https://www.kybertest.cz/>  
<https://www.jsns.cz/>  
<https://www.internetembezpecne.cz/>  
<https://bezpecne-online.saferinternet.cz/>   
<https://sitevhrsti.cz/socialni-site/>

<https://poradenskecentrum.cz/>