Kapitola

[Rodičovská kontrola]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: Silvia Prieto/Santiago Hernandez
Poslední úprava: 01.04.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

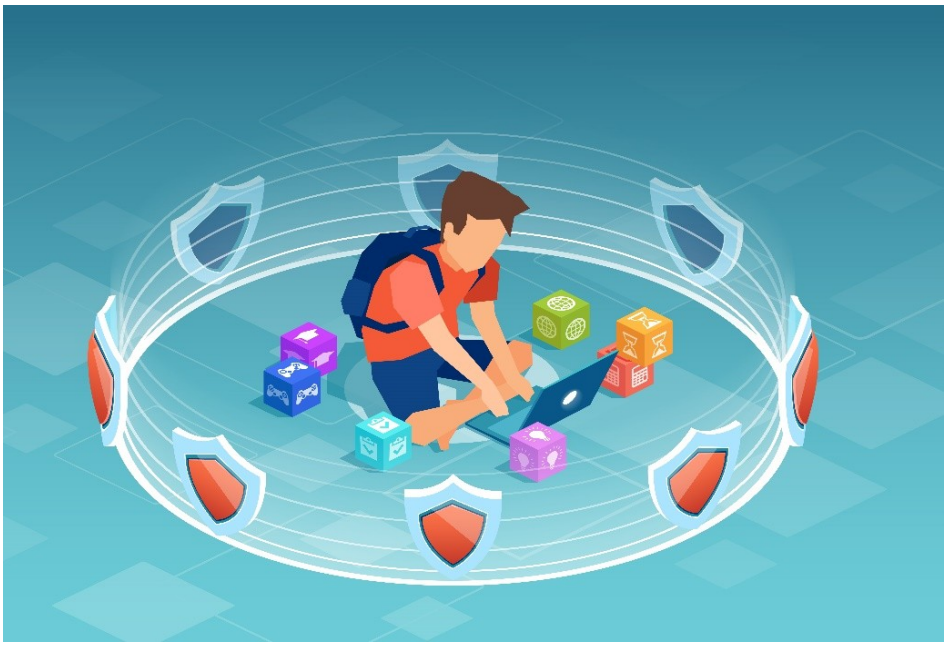
Rodičovská kontrola

Úvod

Ochrana a zajištění bezpečnosti dětí jsou jedny z nejhlavnějších a nejzákladnějších povinností každého rodiče či zákonného zástupce. V dnešní digitální době tato povinnost nabyla na důležitosti, jelikož se rozšířila i na užívání informačních technologií.

Děti se na internetu potýkají s velkým množstvím hrozeb jako jsou například sexting, grooming, kyberšikana, netolismus nebo únik informací. Tato nebezpečí zahrnují vystavování dětí sexuálnímu obsahu, obtěžování dospělými, šikanu, závislost na internetu či neúmyslné zveřejňování osobních údajů.

Všechny tyto nepříjemné zkušenosti mohou mít negativní dopad jak na jejich fyzické, tak na psychické zdraví. Je důležité, abyste Vy jako rodiče věnovali těmto nástrahám velkou pozornost a věděli, co dělat v případě, že se Vaše dítě v nějaké nebezpečné situaci ocitne.



Praktický význam – K čemu získané znalosti a dovednosti využijete

Nastudováním této kapitoly pochopíte důležitost využití nástrojů rodičovské kontroly při ochraně svých dětí a mladistvých před nástrahami internetu.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Jaké zásady rodičovské kontroly existují a k čemu je užitečná?

Díky velkému a neustálému pokroku v oblasti IT přicházejí v dnešní době děti, dospívající a mladí lidé stále častěji do kontaktu s novými technologiemi. Ve většině případů dokonce sami zaučují dospělé v jejich okolí v oblasti používání počítačů, tabletů či mobilních telefonů.

Je opravdu těžké a v některých případech i zcela nemožné dospívající mládež od těchto technologií odtrhnout. Používání internetu se stalo nezbytnou součástí zaměstnání i našeho každodenního života. Potřeba učit mládež, jak správně a efektivně používat tato zařízení, začala pronikat i do vzdělávacího systému. Ve skutečnosti jsou informační technologie základním pilířem vzdělávání – lze je využít při vyhledávání informací či vypracovávání školních úkolů. Mnoho škol a vzdělávacích středisek již do svých vzdělávacích programů zahrnulo platformy, prostřednictvím kterých poskytují svým studentům online zdroje, posílají jim úkoly nebo naopak chtějí po studentech, aby vypracované úkoly tímto způsobem odevzdávali. Jak je vidět, v tuto chvíli je nemožné nebo dokonce kontraproduktivní snažit se děti od informačních technologií udržet. Proto je na čase zvážit možná plynoucí rizika a způsoby, jak nezletilé uživatele ochránit.

Na internetu číhá hned několik různých nebezpečí, se kterými se mohou děti, náctiletí nebo mladiství setkat. Hrozbu představuje vše od kyberšikany a sextingu, při nichž může být pachatelem někdo z okolí oběti (ze školy, sousedství atd.), až po vnější hrozby, kdy je pachatelem někdo, koho oběť nezná. Neznámí lidé mohou shromažďovat informace o nezletilých osobách a navazovat s nimi kontakt, a to ne vždy s nejlepšími úmysly. Pomocí zařízení jako jsou mobilní telefony, notebooky nebo počítače mají navíc nezletilí možnost dostat se k nevhodnému obsahu, například k násilí, pornografii, nebo radikalismu. Sociální sítě jsou jednou z největších obav pro rodiče a děti se na nich mohou setkat s jakoukoli z výše zmíněných nástrah. Sociální sítě jsou přístupné nezletilým uživatelům od 13 let, není však problém, aby se zaregistrovaly i mladší děti, jelikož při registraci není požadováno žádné ověření uvedeného věku.

Před rozšířením nových technologií probíhal celý proces poznávání, experimentování a navazování nových vztahů, kterým si každý dospívající jedinec prochází, před zraky ostatních lidí. Pro rodiče bylo jednodušší ochránit své děti před nástrahami a dohlédnout na to, co dělají. Z těchto důvodů získal pojem rodičovská kontrola nový rozšířený význam, přestože jeho podstata zůstává stejná. Rodičovskou kontrolu můžeme tedy definovat jako:

Definice
Rodičovská kontrola je způsob, jakým rodiče dohlížejí na své děti a který jim v případě potřeby umožňuje zasáhnout, aby zajistili, že zkušenosti, procesy socializace a osobního růstu jejich dětí probíhají přiměřeně a bez rizik.

Podstata rizik, kterým jsou nezletilí vystavováni, se jako taková nezměnila, změnil se způsob a prostředky, kterými mohou být ohrožováni. Nové nástrahy však zároveň znamenají nové formy a metody rodičovské kontroly.

Příklad
Děti mohou být vystaveny šikaně ve formě urážek, odmítnutí, vyhrožování, výsměchu nebo šíření falešných zpráv, buď tváří v tvář nebo na internetu, kde šíření probíhá rychleji a zastihne větší množství lidí.

Rodičovská kontrola je nástroj, který umožňuje rodičům kontrolovat nebo omezit obsah, ke kterému mají jejich děti na internetu prostřednictvím počítačů, mobilních telefonů nebo tabletů přístup. Existuje několik různých nástrojů rodičovské kontroly, které lze použít jak na zařízení nezletilých osob, tak na zařízení dospělých. Pomocí těchto nástrojů mohou rodiče zakázat některé funkce, přístup k určitým webovým stránkám nebo obsahu.

Příklad
Pokud si rodiče dělají starosti s bezpečností svých dětí, měli by zvážit, jaká zařízení dítě používá a kolik mu je let. Existují aplikace a softwary, pomocí kterých lze ovládat a kontrolovat aktivity na internetu, ne všechny jsou však k dispozici pro všechna zařízení. Dalším důležitým faktorem při výběru správného nástroje je věk dítěte, ne každý software bude totiž vyhovovat jejich potřebám. Pokud máte dvě děti s větším věkovým rozdílem, které používají stejné zařízení, je nutné vzít v potaz, co chcete monitorovat a před čím je potřeba je chránit. U mladších dětí je důležité zamezit přístup k nevhodnému obsahu, zatímco u náctiletých je nutnější hlídat, kolik času na internetu tráví a jaký obsah navštěvují. Nástroje rodičovské kontroly jsou k dispozici v každém zařízení, pokud však hledáte něco specifičtějšího, máte možnost si stáhnout nebo koupit pro Vás vhodnější nástroje nebo aplikace. Dále máte možnost si stáhnout nástroje nabízené pojišťovnami, bezpečnostními společnostmi a poskytovateli internetového připojení.

Obecně se současné systémy rodičovské kontroly užívají k zajištění bezpečnosti nezletilých osob na internetu, a tedy k prevenci možných hrozeb a špatných zkušeností. Konkrétněji se jedná o nástroje, jejichž účelem je filtrovat obsah či zamezit přístup k nějakému obsahu na internetu a k sledování aktivit. Tyto nástroje nabízejí stále více funkcí a lze je přizpůsobit potřebám rodičů. Dostupné funkce lze rozdělit do těchto skupin:

- Sledování: Mějte přehled o veškerých online aktivitách. Tato funkce umožňuje uživateli analyzovat, které stránky jeho dítě navštěvuje, a generuje varovnou zprávu, pokud vstoupí na nevhodný web.
- Ovládání kontaktu s ostatními lidmi: Tato funkce umožňuje zamezit dítěti v kontaktu s cizími lidmi, ke kterému podle INCIBE dochází v 40 % případů.

- Časové omezení používání: Umožňuje Vám kontrolovat jak maximální dobu, po kterou má dítě přístup k internetu, tak dobu, po kterou může být zařízení zapnuté.
- Správa přístupu k nevhodnému obsahu: Umožňuje uživateli ovládat nebo blokovat přístup ke stránkám, na kterých se nachází nevhodný obsah nebo které ohrožují jejich osobní údaje.
- Omezení aplikací: Tato funkce zabraňuje používání nebo stažení určitých aplikací.
- Vyhýbání se nákupům online: Umožňuje zakázat nákup aplikací nebo jiných položek na internetu, ať už k němu došlo úmyslně, či nikoliv.
- Geolokace: Umožňuje Vám zjistit přesnou polohu dítěte.
- Dvoufázové ověření: K odemknutí zařízení je kromě hesla vyžadován také kód, který je zaslán rodičům. Tímto způsobem je vždy na rodičích, aby umožnili dítěti přístup k zařízení.
- Blokování hovorů

Všechny zmíněné druhy rodičovské kontroly mají zaručit bezpečí nezletilých osob, ochránit je před cizinci na internetu a nevhodným obsahem či webovými stránkami. Navíc pomáhají chránit děti a náctileté před nevhodným užíváním internetu. Chránit je lze různými způsoby – například sledováním jejich aktivit na internetu či blokováním nebo ovládáním určitých funkcí.

Pro nejmenší děti jsou vhodné nástroje, které omezují nebo zamezují přístup k určitému nevhodnému obsahu, nebo které omezují čas strávený na aplikacích či celkově na zařízení. Tyto nástroje používají různé metody k dosažení stejného výsledku. Většina z nich používá listiny (seznamy) s webovými stránkami. Na černé listině (blacklist) jsou uvedeny stránky, které jsou pro děti nevhodné, zatímco na bílé listině (whitelist) se nacházejí stránky, které děti mohou bez problému navštěvovat. K blokování konkrétního obsahu je nejlepší využít klíčová slova (např. pornografie, drogy, nakupování atd.). Je však možné, že při použití této metody nástroj nesprávně vyhodnotí některé stránky, a tím pádem zablokujete i obsah, který pro děti nevhodný není. Tento druh rodičovské kontroly dále umožňuje zablokovat přístup k určitým aplikacím, umožňuje užití aplikací pouze bez připojení k internetu, lze pomocí něj zakázat chatování nebo reguluje dobu či časový plán přístupnosti zařízení.

Pokud jde o náctileté, existují nástroje, které monitorují jejich aktivity a zároveň neomezují používání zařízení. S postupem času potřebují děti větší svobodu při používání mobilních telefonů, počítačů či tabletů a zároveň roste i jejich porozumění technologií. Děti v tomto věku jsou zvídavé a chtějí mít možnost komunikovat s dalšími lidmi. Z těchto monitorovacích nástrojů rodičovské kontroly se rodiče

dozví, jaké služby jejich děti využívají, co na internetu dělají, s jakými lidmi komunikují a kde se do sítě připojují, což je možné díky zabudované GPS a technikám pro určování polohy.

Rodičovskou kontrolu lze aplikovat na různá místa:

- Router a DNS servery (Domain Name Systems): Router je zařízení, které umožňuje ve Vaší domácnosti připojení k internetu. Prostřednictvím routeru je možné spravovat navigační omezení všech připojených zařízení – regulovat a filtrovat dostupný obsah, upravovat časový limit připojení a použít filtry na webové stránky. Stejné funkce poskytují také DNS servery.

Analýza
Tato možnost je vhodná, chcete-li stejným způsobem spravovat všechna připojená zařízení. Nehodí se však, pokud chcete na jednotlivá zařízení použít pouze konkrétní omezení. Další nevýhodou je nemožnost ovládat zařízení, která nejsou připojená k serveru.

- Konkrétní zařízení: Všechna zařízení (počítače, tablety, mobilní telefony, dokonce i hračky) mají zabudovaný balíček rodičovské kontroly a umožňují ovládat online aktivity dětí a blokovat přístup k nevhodnému obsahu.

Analýza
Jelikož tento nástroj přichází přímo se zakoupeným zařízením, není potřeba hledat a platit za jinou rodičovskou kontrolu. Nicméně, u tohoto typu není většinou možné přizpůsobit nastavení Vašim potřebám.

- Software: Některé programy, které mají za úkol chránit naše zařízení před viry a malwarem, mají také funkci blokovat stránky, upravovat časový limit připojení a dostávat informace o chatech.

Analýza
Umožňuje ovládat jak obsah navštěvovaný na internetu, tak užívání samotného zařízení. Nevýhodou je, že může být méně intuitivní než jiné nástroje.

- Webový prohlížeč: Prostřednictvím prohlížeče je možné nastavit různé filtry, zabránit některým stránkám v otevření a blokovat vybrané domény.

Analýza
Velmi užitečný nástroj k blokování adres, které obsahují určitá klíčová slova, konkrétních stránek nebo všech stránek spadajících do určité kategorie. Nevýhodou je, že tento nástroj neumožňuje ovládat zařízení jako takové.

- Aplikace: Vhodné pro všechna mobilní zařízení, která nezletilí používají nejčastěji. S těmito aplikacemi je možné ovládat stránky, které mohou navštívit, čas strávený na zařízení, zamezit stahování aplikací, zamezit kontakt s cizími lidmi a předejít úniku informací.

Analýza
Velmi užitečný nástroj, existuje několik různých možností, z kterých si můžete vybrat, je jednoduchý k instalaci a k používání. Nevýhodou je, že většinou není možné ho použít na počítače a notebooky.

Úroveň dohledu, kterou tyto nástroje poskytují (hlavně poslední zmíněná skupina), je velmi vysoká a může být někdy vnímána jako zásah do soukromí. Stejně jako mají mladiství právo na ochranu před všemi formami zneužívání na internetu, mají také právo na soukromí. Doporučuje se tedy nezneužívat nástroje rodičovské ochrany. Zhodnoťte nutnost jejich užití v konkrétních případech, snažte se vybudovat s Vaším dítětem vztah plný důvěry a komunikujte s ním o těchto záležitostech.

1. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_01_01: Víte, jakým hrozbám jsou vystavováni nezletilí při používání informačních technologií.

Zadání: Jakým hrozbám čelí mladiství na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pouze kyberšikaně
- Existuje několik nebezpečí, se kterými se děti, náctiletí nebo mladiství mohou na internetu setkat (kyberšikana, sexting, grooming...)
- Při užívání informačních technologií nejsou mladiství vystavováni žádných hrozbám.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_01_02: Dokážete vysvětlit pojem rodičovská kontrola.

Zadání: Která z následujících možností nejlépe vystihuje pojem rodičovská kontrola?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Způsob, jakým rodiče dohlížejí na své děti a který jim umožňuje v případě potřeby zasáhnout, aby zajistili, že zkušenosti, procesy socializace a osobního růstu jejich dětí probíhají přiměřeně a bez rizik.
- Nástroj, který umožňuje rodičům kontrolovat nebo omezit obsah, ke kterému mají jejich děti na internetu prostřednictvím počítačů, mobilních telefonů nebo tabletů přístup.
- Hrozba pro mladistvé

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_01_03: Dokážete vysvětlit, k čemu je rodičovská kontrola dobrá.

Zadání: K čemu je rodičovská kontrola dobrá?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Umožňuje rodičům kontrolovat nebo omezit obsah, ke kterému mají jejich děti na internetu prostřednictvím počítačů, mobilních telefonů nebo tabletů přístup.
- Umožňuje dětem používat internet podle jejich představ.
- Umožňuje rodičům kontrolovat účty na sociálních sítích svých dětí.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_01_04: Víte, na jakých principech rodičovská kontrola funguje.

Zadání: Jak rodičovská kontrola funguje?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Zabraňuje dětem v přístupu k internetu.
- Zabraňuje používání elektronických zařízení v domácnosti.
- Rodičovskou kontrolu lze praktikovat z různých míst: vnější a DNS servery, servery zařízení, ze zařízení jako takového, software, internetový prohlížeč nebo aplikace.

2. Co je to sexting?

Sexting je činnost, při které osoba posílá fotografie či videa se sexuálním obsahem prostřednictvím mobilního telefonu a podobných zařízení. Jedná se o výraz, který spojuje slova sex a anglické texting (= zasílání textových zpráv). Tento výraz má počátky v Anglo-Saských zemích, poprvé byl použit v roce 2005 a poté se postupně rozšířil do celého světa.

Rozdíl mezi sextingem a groomingem je v tom, že fotografie či videa jsou v případě sextingu rozesílány či pořizovány se souhlasem zúčastněné osoby. V případě nezletilých, kteří provádějí sexting, při kterém jsou oklamáni druhou osobou nebo ke kterému jsou donuceni, se nejedná o sexting jako takový, protože ačkoli jej v některých případech provádějí dobrovolně, jsou při něm podvedeni. Sexting lze rozdělit do dvou skupin podle toho, jakou roli hraje zúčastněná osoba. Aktivního sextingu se dopouští osoba, která fotografie či videa pořizuje, a pasivního sextingu osoba, která tento materiál obdrží.

Někteří mladí lidí považují sexting za způsob flirtování nebo pokus o přilákání pozornosti, někdy fotografie posílají svým partnerům jako "dárek". Riziko představuje skutečnost, že si nikdy nemůžeme být jisti, zda se adresát nerozhodne podělit o obdržený materiál s dalšími lidmi. Někdy může tyto fotografie či videa dokonce použít k vydírání za účelem získání dalšího

podobného obsahu nebo dosažení nějakého cíle. A někdy k jejich distribuci může dojít pouhým omylem.

Definice
Sexting je dobrovolné rozesílání fotografií či videí se sexuálním obsahem. Většinou jsou tyto materiály vyměňovány mezi partnery. Pořizovatel a odesílatel tohoto obsahu je tatáž osoba.

Při aktivním sextingu osoba pořizuje sexuálně sugestivní obsah a posílá ho druhé osobě.
Při pasivním sextingu je osoba příjemcem výše zmíněného obsahu.
Proč je tedy sexting potenciálním rizikem pro děti a mladistvé? Po odeslání těchto fotografií či videí nad nimi původní majitel ztrácí veškerou kontrolu a může se stát, že se dostanou k lidem, kterým nebyly původně určeny. K tomu může dojít z několika důvodů:

- Příjemce úmyslně rozešle materiál dalším lidem, od kterých se šíří dál.
- Autor obsahu ho omylem pošle nesprávné osobě, která jej pak pošle někomu dalšímu.
- Někdo cizí k obsahu získá přístup tím, že ukradne mobilní telefon, tablet či počítač některé z osob, která jej má ve vlastnictví, a rozhodne se ho zveřejnit na internetu.
- Hacker získá obsah nabouráním se do mobilního telefonu či počítače osoby, která jej má ve vlastnictví, a zveřejní ho na internetu nebo zneužije k vydírání autora.

Tento obsah může skončit na několika místech:

- V rukou kamarádů či rodinných příslušníků původního autora.
- Na sociálních sítích, kde k nim má přístup kdokoliv.
- Na stránkách se sexuálním obsahem či pornografií.
- V rukách groomerů, kteří v nich vidí dokonalý způsob, jak ovládat svoji kořist (viz grooming).

Důsledky pro poškozenou osobu jsou:

- Ponížení a sociální lynčování.
- Veřejné ponížení a urážky, což může mít vliv hlavně na mladší osoby, jejichž osobnost se stále formuje, a to, jak je vidí druzí, je pro ně v tomto věku velmi důležité.
- Pocity bezmoci či viny, hlavně pokud se o skutečnosti dozví rodiče nebo učitelé.
- Všechny výše zmíněné faktory mohou vést k pocitům smutku, úzkostem, depresím, zvýšené či snížené chuti k jídlu a v extrémních případech k pokusům o sebevraždu.

Důležité
Odhalení situace může znamenat ztrátu důvěry od okolí. Problémy ve školních vztazích mohou vést k izolaci jedince ve snaze vyhnout se opovrhujícím pohledům a urážlivým poznámkám apod.

Snažit se předejít nepříjemným situacím spojeným se sextingem by mělo být v zájmu každého rodiče či zákonného zástupce. Existují však i preventivní opatření, která mohou podstoupit sami mladiství.

Rodiče či jiní zákonní zástupci by měli:

- Naučit své nezletilé děti, že by si měli dávat pozor na to, co se rozhodnou sdílet na internetu, protože jejich chování může mít nepříjemné následky a vést k velkému množství problémů.
- Naučit děti mít úctu k vlastnímu tělu a soukromí a vštípit jim, že je nikdo nemůže donutit udělat něco, co samy nechtějí.
- Podporovat děti v užívání počítačů či mobilních telefonů na místech sdílených s rodinou.

Mladiství by se měli vyvarovat posílání jakýchkoliv fotografií. S věkem je však tato funkce stále lákavější, je ale důležité mít pořád na paměti následující opatření:

- Nerozesílejte intimní fotografie, už vůbec ne lidem, které neznáte.
- Nepřidávejte kompromitující fotografie na sociální sítě, často je později těžké je smazat a mohou se dostat do rukou nevítaných osob.
- Pokud se přece pro zaslání fotografie rozhodnete, nemělo by z ní být snadno poznatelné, že jste to vy, tzn. neukazujte svou tvář, tetování či znaménka, podle kterých by Vás bylo snadné identifikovat.
- Nerozesílejte fotografie s geolokačními souřadnicemi. Některá zařízení mají možnost pomocí těchto údajů rozpoznat, kde byla fotografie pořízena, což zvyšuje nebezpečí a ulehčuje práci predátorům.
- Nejjednodušším způsobem ochrany je fotografie, které nechcete nikomu ukazovat, ze svého zařízení smazat.

2. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_02_01: Dokážete vysvětlit pojem sexting.

Zadání: Co znamená pojem sexting?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Rozesílání výhružných zpráv se sexuálním obsahem dětem nebo mladistvým.
- Rozesílání fotografií či videí se sexuálním obsahem, ve kterých vystupuje sám odesílatel.
- Rozesílání fotografií či videí se sexuálním obsahem, které vytvořil útočník.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_02_02: Víte, jaký je rozdíl mezi aktivním a pasivním sextingem.

Zadání: Co je to aktivní sexting?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Činnost, při které osoba pořizuje sexuálně sugestivní obsah a posílá ho druhé osobě.
- Snaha útočníka přimět svou oběť, aby mu poslala fotografie či videa se sexuálně sugestivním obsahem.
- Útočník vyhrožuje oběti, že rozešle fotografie se sexuálně sugestivním obsahem, ve kterých oběť vystupuje.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_02_03: Víte, jaké rizika plynou z podílení se na sextingu a šíření sextingového obsahu.

Zadání: Z jakého důvodu může autor ztratit kontrolu nad rozeslaným obsahem?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Kvůli velkému množství důsledků, které pro poškozenou osobu z rozesílání takového obsahu plynou.
- Útočník získá nad obětí moc.
- Obsah se může dostat do špatných rukou a rozšířit se dál.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_02_04: Dokážete vysvětlit 3 základní strategie prevence sextingu.

Zadání: Jaká opatření lze pro prevenci sextingu podstoupit?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Rodiče by měli naučit své nezletilé děti, aby si dávaly pozor na to, co se rozhodnou sdílet na internetu, jelikož jejich chování může mít nepříjemné následky.
- Rodiče by měli hlídat, co jejich děti na internetu dělají.
- Jejich vrstevníci by měli nezletilé naučit respektovat své tělo.

3. Co je to grooming?

Grooming je definován jako kyberšikana, kterou záměrně provádí dospělá osoba za účelem navázání vztahu a získání emoční kontroly nad dítětem či mladistvým. Hlavním cílem predátora je sexuální zneužívání.

Ke groomingu může docházet i mezi dvěma nezletilými osobami, ve většině případů je mezi nimi větší věkový rozdíl a predátorem je starší z dvojice.

Hlavním cílem predátora je získat důvěru nezletilé osoby, přimět ji k pořízení a zaslání fotografií či videí se sexuálním obsahem nebo se s ní dokonce setkat. Takovéto jednání představuje trestný čin dětské prostituce či sexuálního zneužívání mladistvých.

Grooming je úzce spjat s pedofilií. Pachatelé navíc často využívají získané fotografie k vydírání či zastrašování svých obětí.

Definice
Grooming je činnost, při které se dospělá osoba snaží navázat důvěrný vztah s nezletilou osobou, nejčastěji za účelem sexuálního zneužívání. Většinou se grooming odehrává na internetu, v některých případech se pachatel pokusí navázat kontakt se svou obětí i offline.

Pachatel ("groomer") většinou postupuje tímto způsobem:

- **Nalákání** oběti: Pachatel se snaží získat co nejvíce informací o oběti – věk, bydliště, škola. Dalším krokem je zjistit, jaké má oběť záliby, koníčky, čeho se bojí, a celkově se jí přizpůsobit a najít "společné zájmy" za účelem získání její důvěry. Pachatel udělá cokoliv pro to, aby vybudoval s obětí silný přátelský vztah. V této fázi není cílem predátora oběť zastrašovat.
- Navázání **důvěrného vztahu** s obětí: Poté, co se pachatel úspěšně s dítětem spřátelí, chce se ujistit, že má oběť nadále zájem udržovat s ním kontakt. Pokračuje tedy v přátelském chování, snaží se bavit o tom, co oběť zajímá, o společných zálibách (sporty, filmy, hudba atd.) a postupně přejde na osobnější témata týkající se rodiny – jaká je její rodinná situace, kolik má sourozenců, co dělají její rodiče apod.
- **Svedení** oběti: S velkým množstvím informací a vybudovanou důvěrou se pachatel odhodlá k dalšímu kroku – svedení dítěte. Začne do konverzace častěji začleňovat sexuální témata a vyměňovat si s obětí intimní fotografie. Je možné, že oběť ze začátku fotografie posílat nechce, postupným sváděním, lichocením a pocitem, že pachateli něco dluží, nakonec oběť všem požadavkům pachatele vyhoví.
- **Obtěžování** oběti: V tuto chvíli má predátor dobrou představu o tom, co může z dítěte vymámit. Zná jeho osobní údaje, informace o rodině, zájmy, obavy a má ve vlastnictví jeho intimní fotografie. Hlavním cílem je teď pro pachatele navázání sexuálního vztahu s obětí, často nejdřív pouze po internetu. Pokud oběť nechce jeho požadavkům vyhovět, začne pachatel s vydíráním, vyhrožováním a manipulací pomocí získaných informací a fotografií, aby svého cíle dosáhl.

Občas mohou první dvě fáze proběhnout tváří v tvář s člověkem, kterého oběť již zná.

V některých případech může mít celý proces další dvě fáze:

- **Vyhlédnutí si** oběti: Předchází první fázi. Nezletilé osoby často uvádějí velké množství osobních informací na sociálních sítích, v chatovacích místnostech nebo na fórech, což pachatelům značně usnadňuje jejich práci. Pachatel při vyhlížení oběti bere v potaz faktory jako zranitelnost, emocionální potřeby, nízké sebevědomí, samota nebo nedostatečná pozornost od rodičů.
- **Izolace** oběti: K této fázi může dojít mezi nalákáním a svedením oběti. Pachatel zneužije vzniklé důvěry a získaných informací a pokusí se dítě izolovat od rodiny a přátel. Takto jej může snadněji ovládat a manipulovat, sblížit se s ním a zabránit mu, pokud se pokusí se situací někomu svěřit.

Změny, které je možné na oběti zpozorovat, lze rozdělit do těchto 4 kategorií:

1. Změny v chování v různých oblastech:

    - v užívání komunikačních technologií nebo internetu
    - v školní docházce, např. chabé důvody absence
    - nepřítomnost či úplné opuštění zájmových aktivit
    - výkyvy v učení a školních výkonech
    - změny ve volnočasových aktivitách
    - změny v stravovacích návycích
    - snížená soustředěnost a paměťová kapacita

- zatajování toho, co dělají a s kým komunikují na internetu

2. Změny nálady:
    - změna humoru
    - chvíle smutku, lhostejnosti či apatie
    - neobvyklé střídání fází relaxace a napětí, někdy dokonce i agresivní reakce
    - krátkodobá výbušnost a agresivita

3. Změny ve vztazích:
    - neobvyklé změny v přátelských vztazích – náhlý nedostatek či ztráta přátel a jiných společenských vztahů
    - nedostatek obrany nebo přehnané reakce na vtipy nebo postřehy od okolí; na první pohled může jít o neškodné poznámky, které však pro oběť mají hlubší význam
    - strach či vzdor při opouštění domova
    - omezení komunikace
    - změny ve vztahu k dospělým z hlediska jejich četnosti a závislosti
    - nestálost skupin nebo vzorů, které oběť sleduje a napodobuje

4. Fyzické a psychosomatické změny:
    - změny v řeči těla v přítomnosti určitých osob – vyhýbání se kontaktu či uzavírání se do sebe
    - nižší výskyt na veřejnosti či na viditelných místech (např. ve školních prostorách)
    - projevy nemocí nebo častá onemocnění
    - častá fyzická poranění, pro která nemá oběť jasné vysvětlení, ztráta nebo poškození oblečení
    - časté závratě s neobvyklými příznaky
    - bolesti hlavy nebo břicha, které znamenají zhoršení školní docházky či nepřítomnost při určitých aktivitách

Co dělat, aby se dítě do takovéto situace nedostalo:

Důležité je mezi dětmi a rodiči podporovat vzájemnou komunikaci, a tím usnadnit rozhovory týkající se internetu, sociálních sítích a jejich potenciálních hrozeb, jejichž nedílnou součástí je i varování před tím, jaké údaje by neměly děti na internetu sdělovat.

Dále je vhodné poučit nezletilé o tom, jak bezpečně používat internet, nástroje, služby a sociální sítě a mít při tom neustále na paměti již zmíněné doporučení – nesdělovat informace a nekomunikovat s cizími lidmi. Cílem je zaškolit je pomocí potřebných znalostí a nástrojů tak, aby byli při používání internetu stále více samostatní. Dohled a kontrolní opatření musí být přizpůsobeny věku dítěte či mladistvého.
Vzdělávací střediska mohou vypracovat konkrétní opatření proti groomingu a počítat s odborníky z řad pedagogického personálu, kteří usměrňují a usnadňují předávání informací a technické fungování mechanismů a zařízení. Dále mohou také přijmout postupy, které usnadní začlenění problematiky groomingu a opatření zaměřená na jeho prevenci do učebních osnov.
Pokud jde o nezletilé, je nutné, aby se vyhnuli sdílení kompromitujících fotografií a informací, odmítali pornografické zprávy či zprávy se sexuálním obsahem. V každém případě je důležité, aby požádali o pomoc, ocitnou-li se v neznámých či choulostivých situacích, zejména pokud tyto situace v dítěti vyvolají nejistotu či citovou újmu.

3. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_03_01: Dokážete vysvětlit pojem grooming.

Zadání: Která z následujících možností nejlépe definuje pojem grooming?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Kyberšikana, kterou záměrně provádí dospělá osoba.
- Kyberšikana, kterou záměrně provádí vrstevník.
- Kyberšikana, kterou záměrně provádí spolužák na internetu.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_03_02: Znáte fáze a znak groomingu.

Zadání: Postup groomingu se skládá z několika fází. Která z následujících možností nejlépe vystihuje fázi nalákání oběti?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pachatel upevňuje vztah s obětí.
- Pachatel se snaží o oběti dozvědět co nejvíce informací.
- Pachatel si vyhlíží oběť na internetu a snaží se o ní najít dostupné informace.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_03_03: Dokážete pomocí symptomů rozpoznat oběť groomingu.

Zadání: Změny, které lze na oběti pozorovat, dělíme do 4 kategorií. Které to jsou?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Chování, nálada, koníčky, zdraví.
- Chování, nálada, vztahy, zdraví.
- Chování, nálada, vztahy, fyzické a psychosomatické změny.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_03_04: Dokážete vysvětlit 3 základní strategie prevence groomingu.

Zadání: Jaká opatření lze zavést pro prevenci groomingu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Kontrolovat, co děti dělají na internetu, sledovat, kde se pohybují, a nenechat je samostatně užívat internet a elektronická zařízení.

- Podpora vzájemné komunikace mezi dítětem a rodičem – rodiče by měli naučit své děti, jak správně užívat sociální sítě, elektronická zařízení a různé nástroje.
- Dovolit dětem užívat internet pouze pokud jsou dostatečně samostatné.

4. Co je to kyberšikana?

Definice
Kyberšikana je jakýkoliv druh šikany, který probíhá prostřednictvím digitálních zařízení (notebook, tablet, mobilní telefon atd.).

Cílem útočníka je poškodit na internetu jméno oběti šířením falešných zpráv prostřednictvím sociálních sítí (Facebook, Instagram, Twitter atd.), uveřejňováním klamných či urážlivých příspěvků na blozích nebo rozesíláním informací prostřednictvím e-mailů, SMS nebo aplikací jako jsou WhatsApp a WeChat.

Jedním z prvních kroků kyberšikany je urážení či vyhrožování oběti útočníkem, který hrozí tím, že vyzradí informace, které by mohly poškodit reputaci oběti. V tomto případě není až tak důležité, zda jsou informace pravdivé, útočník je ve snaze uškodit oběti tak či tak vypustí do světa. Pokud informace nejsou pravdivé, jedná se o dezinformaci.

Příklad
Dívka obdrží na WhatsAppu zprávu s odkazem na stránku, na které se nacházejí její nahé fotografie. Útočník stanoví ultimátum – dívka za něj musí vypracovat domácí úkol, jinak tento odkaz pošle jejím kamarádům a rodině.

Mezi nejběžnější způsoby kyberšikany patří:

- napadání či urážení druhých na internetu
- navádění osob k sebepoškozování či dokonce k sebevraždě
- vyhrožování
- vytvoření webové stránky či blogu, který obsahuje ponižující informace o oběti
- hackování profilů na sociálních sítích, tzv. sockpuppet
- vypouštění soukromých údajů o oběti
- sdílení fotografií, na kterých je oběť nahá
- šikana ze žárlivosti
- obtěžování na základě náboženství, rasy nebo sexuální orientace

Obecně platí, že agresor, známý též jako kyberstalker, je někdo blízký oběti: spolužák, někdo, koho oběť zná ze zájmových aktivit apod. Ve velkém množství případů se nejedná pouze o jedince, ale o celou skupinu útočníků. Kyberšikana je pro oběť velmi vyčerpávající, zejména kvůli těmto faktorům:

1. Vytrvalost: Žijeme v nepřetržitě připojeném světě, kde komunikace nikdy neustává.
2. Stálost: Většina obsahu zůstane na internetu navždy a je přístupná komukoliv. Navíc, jakmile útočníci začnou oběť obtěžovat, jen tak sami od sebe nepřestanou.
3. Skrývání: Oběti se často ze strachu samy nesvěří, a tak je pro rodiče, učitele nebo příslušné orgány těžké rozpoznat, že k nějakému obtěžování dochází.

Pokud se děti ocitnou v roli oběti kyberšikany, často je jejich prvotní reakcí stažení se do sebe, čímž agresor nepřímo ovlivňuje jejich život i mimo svět internetu.
Oběti kyberšikany se snaží vyhýbat místům, která jim připomínají traumatizující zážitky, a tak často opustí aktivity, které dříve milovaly. V některých případech dokonce začnou chodit za školu nebo předstírat nemoc, aby do školy nemusely jít, což ohrožuje jejich dobré výsledky. Někdy se u nich objeví nemoci jako poruchy příjmu potravy nebo deprese. Zvýší nebo sníží se u nich používání komunikačních technologií a začnou se více zajímat o své soukromí a skrývat před rodiči, co dělají na internetu. Někdy dokonce úplně smažou své původní profily a vytvoří si nové.

Pro prevenci kyberšikany je dobré podstoupit tato opatření:

- Rodiče a učitelé by měli s dětmi hovořit o kyberšikaně, poučit je nejen o útočnících, ale i o přihlížejících, a snažit se podpořit a odměňovat dobré chování vůči ostatním.
- Rodiče by měli stanovit pevná pravidla ohledně toho, jaký obsah mohou jejich děti na internetu navštěvovat a kolik času mohou na sociálních sítích u telefonů či počítačů strávit. Kromě toho by měli stanovit pravidla a očekávání správného chování na internetu.
- Školy by měly zavést anonymní boxy, do kterých mohou děti šikanu nahlásit a pomocí kterých se začne celý problém řešit.
- Rodiče a učitelé jsou povinni dohlížet na jakékoliv sebemenší změny v chování a náladách dětí a zasáhnout, pokud situaci vyhodnotí jako neobvyklou.

4. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_04_01: Dokážete vysvětlit pojem kyberšikana.

Zadání: Která z následujících možností nejlépe vystihuje pojem kyberšikana?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Obtěžování, urážení nebo vyhrožování, jak fyzické, tak po internetu.
- Obtěžování druhých na sociálních sítích, webových stránkách, mobilních aplikacích nebo jakýmkoliv jiným způsobem za použití komunikačních technologií.
- Přihlížení nevhodnému chování na internetu.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_04_02: Dokážete charakterizovat role účastníků kyberšikany.

Zadání: Kdo je to obětí kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Osoba, která napadá druhou osobu urážkami, vyhrožováním nebo vypouštěním škodlivých informací.
- Osoba, která trpí kyberšikanou a často se v důsledku uzavře sama do sebe
- Pojem „oběť kyberšikany“ neexistuje.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_04_03: Víte, s jakými následky se potýkají útočník i oběť.

Zadání: Která z následujících možností není ukazatelem kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Oběť se rozhodne soustředit na studium a vylepšit si své výsledky ve škole.
- Oběť smaže své původní profily na sociálních sítích a založí si nové.
- U obětí dochází k změnám nálady a často se uzavírají samy do sebe.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_04_04: Dokážete popsat 3 základní strategie prevence kyberšikany.

Zadání: Co můžete udělat pro prevenci kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pokud máte sebemenší podezření, že je někdo obětí kyberšikany, ihned kontaktujte policii.
- Nepoužívejte doma elektronická zařízení.
- Stanovte dětem pevná pravidla pro to, jaký obsah mohou na internetu navštěvovat a kolik času mohou u telefonů či počítačů strávit.

Co-funded by the
Erasmus+ Programme
of the European Union

5. Co je to netolismus?

Internet rozšířil svět dětí a teenagerů a přinesl jim spoustu nových možností – umožnil jim se seznamovat a socializovat, svobodně vyjádřit svou osobnost, rozšířil jejich zdroje pro vzdělávání a zavedl způsob spolupráce a učení založený na peer-to-peer principu. Může se tedy zdát, že je internet pouze pozitivním místem plným všemožných příležitostí, opak je však pravdou. Jako každý jiný aspekt našeho života, má i internet svoji temnou stránku, kterou nelze ignorovat.

Existují dva druhy závislosti: látková závislost a nelátková neboli behaviorální závislost, při které se jedinec stává závislý na nějakém procesu či aktivitě. Tento druh je často označován jako "nová závislost" či "nechemická závislost". Tento typ závislosti si můžete vypěstovat, pokud trávíte velké množství času prováděním nějaké aktivity. Závislost na internetu se nazývá netolismus.

Definice
Netolismus je závislost na internetu vyznačující se chorobným užíváním internetu. Podstatou této závislosti není, kolik času užíváním internetu strávíte, ale zda Vám toto užívání zasahuje do každodenního života a nedokážete bez něj normálně fungovat.

S rostoucím počtem uživatelů internetu, roste i počet případů této nemoci. Na internetu jste v dnešní době schopni sehnat cokoliv a kdykoliv. Nenašli jste v kamenném obchodě správnou velikost trička, které se Vám líbilo? Nevadí, kupte si ho přes internet! Nemáte zrovna náladu na vaření? O nic nejde, můžete si vybrat z bezpočtu restaurací a jídlo Vám dovezou přímo před dveře! Nemáte s kým hrát Vaši oblíbenou hru? Na internetu je plno cizích lidí, kteří jsou na tom stejně, jako Vy! Potřebujete se učit, ale nechce se Vám shánět všemožné materiály? Žádný problém, na internetu jednoduše seženete všechny dostupné knihy, články a jiné zdroje!

Z těchto běžných situací není jednoduché vyčíst, zda je nezletilá osoba na internetu závislá, či nikoliv. Existují však způsoby, které Vám usnadní případnou závislost odhalit. Zeptejte se sami sebe na tyto otázky:

- Je moje dítě neschopné odtrhnout se od sociálních sítí?
- Jedná moje dítě kompulzivně při online nakupování?
- Tráví moje dítě příliš času hraním videoher?
- Hraje moje dítě na internetu hazardní hry?

- Tráví moje dítě u počítače celý den?
- Má moje dítě problémy navazovat vztahy v reálném světě?
- Má moje dítě problémy s přípravou do školy nebo se mu zhoršily výsledky ve škole?

Pokud Vaše odpověď na některou z otázek zněla "Ano", měli byste se více zaměřit na chování Vašeho potomka a jeho vztah k internetu. Možná právě on začíná propadat závislosti na internetu.

Nicméně, není možné celou diagnózu stavět pouze na těchto otázkách. Žijeme ve světě, který je neustále připojený k síti, a je tedy často těžké rozeznat běžné užívání internetu od toho chorobného. Je důležité zkontrolovat, zda užívání internetu nějakým způsobem negativně ovlivňuje každodenní život Vašeho dítěte. Pokud není schopné dát přednost svým povinnostem před sezením u počítače či mobilního telefonu, je jasné, že něco není v pořádku.

Příklad
Je čas večeře a Vy svoláváte svou rodinu k jídelnímu stolu. Váš syn nereaguje na opakovanou výzvu a je neustále přilepen k obrazovce svého mobilního telefonu. Dokonce i když se Vám ho konečně povede dostat do kuchyně, není ochotný se započatou činností přestat a mobilní telefon má v ruce i u večeře. Mobil mu tedy seberete a schováte si ho do kapsy, což zapříčiní, že je Váš syn po zbytek večeře nepokojný a rozrušený.

Dalším účinným způsobem, jak rozpoznat závislost na internetu, je analyzovat, kolik času Váš potomek na internetu tráví, jak často je připojený a jaké jsou jeho emoční projevy a chování, pokud zrovna na internetu není. Jestli se zdá být nervózní, rozrušený, úzkostný nebo dokonce v depresích nebo jestli u něj dochází k častým výkyvům nálad, může být na vině netolismus.

Závislost na internetu se může projevovat také prostřednictvím fyzických příznaků jako například nedodržování pitného a stravovacího režimu, bolest zad, nespavost, suchost očí nebo špatná osobní hygiena.

Existuje několik užitečných opatření, která Vám pomohou závislosti na internetu předejít:

- Stanovte přesná omezení pro užívání internetu a elektronických zařízení. Kromě vyhraněného časového limitu zaveďte také různá pravidla, která určí dítěti, kdy může internet používat – např. nikdy nesmí používat počítač po večeři.
- Zorganizujte na škole vzdělávací semináře o používání internetu.
- Naučte své dítě, aby dávalo přednost trávení času s rodinou.
- Nejmladší děti by měly používat internet vždy pouze pod dohledem dospělé osoby.
- Nainstalujte na Vaše zařízení nástroje rodičovské kontroly (viz podkapitola 1) a zabraňte dětem a mladistvým v přístupu na pornografické stránky či stránky s hazardními hrami.

5. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_05_01: Znáte definici pojmu netolismus.

Zadání: Která z následujících možností nejlépe vystihuje pojem netolismus?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Nemoc, při které jedinec tráví velké množství času na internetu.
- Závislost na internetu, která zasahuje do každodenního života jedince.
- Činnost, při které útočník vyhrožuje své oběti sdílením jejich nahých fotografií.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_05_02: Dokážete rozpoznat příznaky závislosti na internetu.

Zadání: Která z následujících možností nepatří mezi varovné signály závislosti na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Dítě či mladistvý nechce používat internet, protože se bojí někoho, kdo ho šikanuje.
- Dítě či mladistvý tráví velké množství času hraním videoher.
- Dítě či mladistvý má potíže s navazováním vztahů v reálném světě.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_05_03: Dokážete popsat 3 základní strategie prevence netolismu.

Zadání: Která z následujících možností představuje nejlepší způsob prevence závislosti na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Stanovte přesná omezení pro užívání internetu a elektronických zařízení.
- Dejte dětem naprostou volnost při používání internetu.
- Spravujte účty na sociálních sítích svých dětí.

6. Co je to únik informací?

V současné době se celý náš život postupně přesouvá na internet. Nabouráním se do Vašeho počítače hacker získává velké množství všemožných informací – údaje o kreditní kartě, přístup k účtům na sociálních sítích, k Vašim e-mailům nebo historii vyhledávání v prohlížeči.

Kvůli tomuto přílišnému vystavování našich životů si musíme dávat veliký pozor na naše údaje a data a vyhnout se tak jejich úniku. A pokud máte pocit, že jste v této oblasti dostatečně zabezpečeni, je Vaším úkolem naučit Vaše děti stejné odpovědnosti při užívání internetu, hlavně pokud s nimi sdílíte svá zařízení.

Velké množství trestných činů souvisí s únikem či smazáním dat a děti a mladiství jsou skupinou uživatelů, která nejčastěji sdílí své osobní údaje na internetu, a to z těchto dvou důvodů:

1. Tráví na internetu více času než jiné generace uživatelů.
2. Necítí se být na internetu ohroženi.

Co-funded by the
Erasmus+ Programme
of the European Union

Existuje několik metod, pomocí kterých se útočníci bez Vašeho vědomí dostanou k Vašim datům a následně je vypustí do světa. Často se tyto metody skrývají pod běžnými požadavky různých služeb na internetu, např. reklamy, které Vás žádají o zadání informací, kvůli vizualizaci dat, nebo internetové služby, které Vás pro přístup žádají o zadání hesla. Ve velkém množství případů však k úniku dat dochází kvůli lehkomyslnosti mladistvých, kteří si možné nástrahy online světa neuvědomují.

Definice
Únik dat je neúmyslné zveřejnění soukromých či důvěrných informací, ke kterým by neměli mít cizí lidé přístup. K úniku dat může dojít nabouráním se do systému (hackováním) nebo neinformovaností jedince o důležitosti ochrany osobních údajů.

Činnost, při které osoba záměrně vystavuje své důvěrné informace na místech, kde k nim má přístup leckdo, aniž by si uvědomovala rizika plynoucí z takového jednání, se nazývá zveřejňování či vystavování informací.

Případů úniku dat výrazně přibývá díky neustálému zlepšování metod hackování, které jsou čím dál více sofistikovanější a propracovanější. Mezi nejznámější patří spyware a malware. Největším problémem jsou však sami uživatelé, kteří jsou ochotni o sobě sdílet velké množství osobních informací. Tato ochota hraje do karet mobilním aplikacím, které se z nás snaží vymámit co nejvíce údajů a požadují přístup k často nesouvisejícím informacím, jako jsou naše údaje o poloze nebo seznam kontaktů. V televizi Vám zobrazují obsah výměnou za Vaši pozornost. Internet Vám zase poskytne přístup k aplikacím a službám výměnou za Vaše osobní data. Jedná se o jiný typ médií, princip však zůstává stejný.

Únik dat by nebyl problém sám o sobě, pokud by se nejednalo o citlivé osobní údaje. I dospělí mají často problém rozeznat, které údaje jsou citlivé a které ne, jak můžeme tedy chtít po dětech a mladistvých, aby je dokázali odlišit? Abyste odhalili potenciální únik dat, zeptejte se svých dětí na tyto jednoduché otázky:

- Jaké stránky navštěvuješ?
- Které aplikace stahuješ do telefonu?

- Chtěl po tobě někdo, abys mu sdělil(a) nějaké informace (e-mailovou adresu, číslo kreditní karty apod.) výměnou za užívání služby?

Příklad
Pavel si chce na svůj mobilní telefon stáhnout aplikaci, pomocí které by mohl komunikovat se svými přáteli. Přestože je aplikace poskytována zdarma, je po něm požadováno, aby vyplnil formulář a uvedl informace o své kreditní kartě.

Vždy buďte obezřetní, chce-li po Vás nějaká aplikace nebo online služba osobní údaje, které s jejím užíváním nijak nesouvisí, nebo pokud po Vás někdo požaduje neobvyklé soukromé informace, jako je např. adresa Vašeho trvalého bydliště. Je totiž možné, že se vystavujete riziku úniku informací.

Někdy může k úniku dat dojít prostřednictvím viru, který se nazývá Trojský kůň. Pokud máte o nějakém programu sebemenší pochybnosti, je rozumné ho nestahovat. Dávat pozor byste si měli také na stránky, které Vám umožňují sledovat filmy a seriály zdarma, nebo na bezplatné herní weby a aplikace.

Tipy, jak předejít úniku informací:

- Naučte své děti, aby bez Vašeho souhlasu nikde neuváděly osobní údaje.
- Pokud Vaše dítě používá stejné zařízení jako Vy, nikdy nepovolte stránkám možnost zapamatovat si Vaše přihlašovacích údajů.
- Nainstalujte si rodičovskou kontrolu (např. Qustodio, Kaspersky Safe Kids, Norton Family a další)
- Varujte děti před sdílením fotografií, pomocí kterých by cizí lidé mohli zjistit jejich adresu bydliště či školy.

Jako vždy je však nejlepším možným preventivním opatřením komunikace. Varujte děti před lehkomyslným sdílením osobních údajů na internetu, povězte jim, jaká rizika.

6. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_06_01: Dokážete definovat únik informací.

Zadání: Která z následujících možností nejlépe vystihuje pojem únik informací?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Závislost na digitálních zařízeních.
- **Neúmyslné zveřejnění citlivých údajů.**
- Zveřejňování nepravdivých informací na internetu.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Rodičovská kontrola_06_02: Dokážete rozpoznat situace, kdy Vaše děti sdílejí důvěrné informace.

Zadání: Která z následujících možností nepředstavuje nebezpečí pro Vaše osobní údaje?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Vaše dítě si chce stáhnout mobilní aplikaci.**
- Po Vašem dítěti je požadováno, aby uvedlo údaje ke kreditní kartě.
- Vaše dítě přidá na svůj účet na sociální síti fotografii, z které je poznat, kde bydlí.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: Vyberte správné odpovědi – pouze jedna odpověď je správná.

Zadání: Jak nejlépe zabránit úniku informací?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Nepovolujte stránkám, aby si zapamatovaly Vaše přihlašovací údaje.**
- Dovolte dětem stahovat jakékoliv aplikace.
- Přidávejte osobní fotografie na sociální sítě.

Zdroje

Garaigordobil, M. (2019). Prevención del cyberbullying: variables personales y familiares predictoras de ciberagresión. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=7041022

Garcia Ganchon, J. O. Seguridad y riesgos: Ciberbullying, grooming y sexting. Retrieved from: http://openaccess.uoc.edu/webapps/o2/handle/10609/72526

Stuttgen, K., McCague, A., Bollinger, J., Dvoskin, R., & Mathews, D. (2020). Whether, when, and how to communicate genetic risk to minors:'I wanted more information but I think they were scared I couldn't handle it'. Journal of Genetic Counseling. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1002/jgc4.1314

Villanueva-Blasco, V. J., & Serrano-Bernal, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género. Revista de Psicología y Educación, 14(1), 16-26. Retrieved from:https://www.almendron.com/tribuna/wp-content/uploads/2020/05/patron-de-uso-de-internet.pdf

Zapamatujte si

Shrnutí

Hlavním cílem této kapitoly je zdůraznit důležitost rodičovské kontroly a ochrany dětí a mladistvých na internetu.

S vývojem technologií přicházejí nové způsoby, prostřednictvím kterých je ohrožováno soukromí a bezpečí dětí a mladistvých. Tato rizika se zvlášť rychle šíří pomocí internetu.

Abyste mohli své děti před těmito nástrahami ochránit, je nutné být s nimi obeznámeni a vědět, jak v případě takovýchto situací postupovat a co dělat pro jejich prevenci. Je proto důležité uvědomit si, jakými způsoby se nebezpečí může dostat k těm nejmladším (sociální sítě, hry, video platformy atd.) a nainstalovat dostupné nástroje k jeho zastavení nebo detekci.

Co-funded by the
Erasmus+ Programme
of the European Union

Poté, co objevíte různé způsoby, jakými se nebezpečí na internetu může dostat k dětem a dospívajícím, a seznámíte se s nástroji a funkcemi, které mají za úkol udržet je pod kontrolou pod kontrolou, je nutné blíže specifikovat případná rizika a jejich následky. Některými z těchto nástrah, kterým mohu čelit nezletilí na internetu, jsou sexting, grooming, kyberšikana, netolismus nebo únik informací. Tato rizika by měla být pochopena do takové míry, že se s nimi dokážete vypořádat nebo je včas odhalit.

Některé z těchto rizik s sebou totiž nesou následky, které mohou přímo ovlivnit emoční, a dokonce i fyzické zdraví nezletilých. Pokud věnujete problému zvýšenou pozornost, všimnete si viditelných znaků, které Vás mohou dovést k jeho podstatě a napovědět Vám, jaká opatření je potřeba přijmout.

V lepším případě bychom měli být schopni úplně předejít situacím spojeným se sextingem, groomingem, kyberšikanou, netolismem či únikem informací než následně řešit jejich dopady. Za tímto účelem je potřeba zaměřit se na způsoby vykonávání rodičovské kontroly na internetu a jiných technologických zařízeních a na nástroje, které lze k této kontrole využít. Důležité jsou také tipy, jak ochránit nezletilé osoby před každým z výše uvedených nebezpečí.

Co-funded by the
Erasmus+ Programme
of the European Union

Správné odpovědi

Zadání: Jakým hrozbám čelí mladiství na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pouze kyberšikaně
- **Existuje několik nebezpečí, se kterými se děti, náctiletí nebo mladiství mohou na internetu setkat (kyberšikana, sexting, grooming...)**
- Při užívání informačních technologií nejsou mladiství vystavováni žádných hrozbám.

Zadání: Která z následujících možností nejlépe vystihuje pojem rodičovská kontrola?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Způsob, jakým rodiče dohlížejí na své děti a který jim umožňuje v případě potřeby zasáhnout, aby zajistili, že zkušenosti, procesy socializace a osobního růstu jejich dětí probíhají přiměřeně a bez rizik**.
- Nástroj, který umožňuje rodičům kontrolovat nebo omezit obsah, ke kterému mají jejich děti na internetu prostřednictvím počítačů, mobilních telefonů nebo tabletů přístup.
- Hrozba pro mladistvé

Zadání: K čemu je rodičovská kontrola dobrá?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Umožňuje rodičům kontrolovat nebo omezit obsah, ke kterému mají jejich děti na internetu prostřednictvím počítačů, mobilních telefonů nebo tabletů přístup.**
- Umožňuje dětem používat internet podle jejich představ.
- Umožňuje rodičům kontrolovat účty na sociálních sítích svých dětí.

Zadání: Jak rodičovská kontrola funguje?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Zabraňuje dětem v přístupu k internetu.
- Zabraňuje používání elektronických zařízení v domácnosti.
- **Rodičovskou kontrolu lze praktikovat z různých míst: vnější a DNS servery, servery zařízení, ze zařízení jako takového, software, internetový prohlížeč nebo aplikace.**

Zadání: Co znamená pojem sexting?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Rozesílání výhružných zpráv se sexuálním obsahem dětem nebo mladistvým.
- **Rozesílání fotografií či videí se sexuálním obsahem, ve kterých vystupuje sám odesílatel**.
- Rozesílání fotografií či videí se sexuálním obsahem, které vytvořil útočník.

Zadání: Co je to aktivní sexting?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Činnost, při které osoba pořizuje sexuálně sugestivní obsah a posílá ho druhé osobě.**
- Snaha útočníka přimět svou oběť, aby mu poslala fotografie či videa se sexuálně sugestivním obsahem.
- Útočník vyhrožuje oběti, že rozešle fotografie se sexuálně sugestivním obsahem, ve kterých oběť vystupuje.

Zadání: Z jakého důvodu může autor ztratit kontrolu nad rozeslaným obsahem?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Kvůli velkému množství důsledků, které pro poškozenou osobu z rozesílání takového obsahu plynou.
- Útočník získá nad obětí moc.
- **Obsah se může dostat do špatných rukou a rozšířit se dál.**

Zadání: Jaká opatření lze pro prevenci sextingu podstoupit?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Rodiče by měli naučit své nezletilé děti, aby si dávaly pozor na to, co se rozhodnou sdílet na internetu, jelikož jejich chování může mít nepříjemné následky.**
- Rodiče by měli hlídat, co jejich děti na internetu dělají.
- Jejich vrstevníci by měli nezletilé naučit respektovat své tělo.

Zadání: Která z následujících možností nejlépe definuje pojem grooming?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Kyberšikana, kterou záměrně provádí dospělá osoba.**
- Kyberšikana, kterou záměrně provádí vrstevník.
- Kyberšikana, kterou záměrně provádí spolužák na internetu.

Zadání: Postup groomingu se skládá z několika fází. Která z následujících možností nejlépe vystihuje fázi nalákání oběti?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pachatel upevňuje vztah s obětí.
- **Pachatel se snaží o oběti dozvědět co nejvíce informací.**
- Pachatel si vyhlíží oběť na internetu a snaží se o ní najít dostupné informace.

Zadání: Změny, které lze na oběti pozorovat, dělíme do 4 kategorií. Které to jsou?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Chování, nálada, koníčky, zdraví.
- Chování, nálada, vztahy, zdraví.

- Chování, nálada, vztahy, fyzické a psychosomatické změny.

Zadání: Jaká opatření lze zavést pro prevenci groomingu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Kontrolovat, co děti dělají na internetu, sledovat, kde se pohybují, a nenechat je samostatně užívat internet a elektronická zařízení.
- Podpora vzájemné komunikace mezi dítětem a rodičem – rodiče by měli naučit své děti, jak správně užívat sociální sítě, elektronická zařízení a různé nástroje.
- Dovolit dětem užívat internet pouze pokud jsou dostatečně samostatné.

Zadání: Která z následujících možností nejlépe vystihuje pojem kyberšikana?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Obtěžování, urážení nebo vyhrožování, jak fyzické, tak po internetu.
- Obtěžování druhých na sociálních sítích, webových stránkách, mobilních aplikacích nebo jakýmkoliv jiným způsobem za použití komunikačních technologií.
- Přihlížení nevhodnému chování na internetu.

Zadání: Kdo je to obětí kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Osoba, která napadá druhou osobu urážkami, vyhrožováním nebo vypouštěním škodlivých informací.
- Osoba, která trpí kyberšikanou a často se v důsledku uzavře sama do sebe
- Pojem „oběť kyberšikany“ neexistuje.

Zadání: Která z následujících možností není ukazatelem kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Oběť se rozhodne soustředit na studium a vylepšit si své výsledky ve škole.
- Oběť smaže své původní profily na sociálních sítích a založí si nové.
- U obětí dochází k změnám nálady a často se uzavírají samy do sebe.

Zadání: Co můžete udělat pro prevenci kyberšikany?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Pokud máte sebemenší podezření, že je někdo obětí kyberšikany, ihned kontaktujte policii.
- Nepoužívejte doma elektronická zařízení.
- Stanovte dětem pevná pravidla pro to, jaký obsah mohou na internetu navštěvovat a kolik času mohou u telefonů či počítačů strávit.

Zadání: Která z následujících možností nejlépe vystihuje pojem netolismus?

Co-funded by the
Erasmus+ Programme
of the European Union

Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- Nemoc, při které jedinec tráví velké množství času na internetu.
- **Závislost na internetu, která zasahuje do každodenního života jedince.**
- Činnost, při které útočník vyhrožuje své oběti sdílením jejich nahých fotografií.

Zadání: Která z následujících možností nepatří mezi varovné signály závislosti na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Dítě či mladistvý nechce používat internet, protože se bojí někoho, kdo ho šikanuje.**
- Dítě či mladistvý tráví velké množství času hraním videoher.
- Dítě či mladistvý má potíže s navazováním vztahů v reálném světě.

Zadání: Která z následujících možností představuje nejlepší způsob prevence závislosti na internetu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

- **Stanovte přesná omezení pro užívání internetu a elektronických zařízení.**
- Dejte dětem naprostou volnost při používání internetu.
- Spravujte účty na sociálních sítích svých dětí.