Kapitola

[Ochrana před nevhodným obsahem]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: bit cz training
Poslední úprava: 24.6.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Ochrana před nevhodným obsahem

Úvod

V dnešní digitální době nám internet poskytuje neomezený přístup do virtuálního světa. Bohužel ne všechen obsah na internetu je vhodný pro všechny uživatele a neexistuje způsob, jak ho rozdělit do kategorií podle věkové vhodnosti. Určitý obsah na internetu může být nelegální, neslušný, urážlivý nebo nevhodný pro některé věkové skupiny. Na tento znepokojující obsah může bez dozoru narazit úplně kdokoliv, včetně malých dětí. Spousta nevhodných webových stránek není zakázána a nikdo na jejich obsah nedohlíží. Kontakt (ať už neúmyslný) s takto nevhodnou stránkou může mít traumatizující účinky, hlavně na děti. Příklady nevhodného obsahu jsou: propagace nenávisti vůči určité rase, náboženství, tělesnému postižení, sexuální preferenci, násilný extremismus, sexuálně explicitní obsah nebo násilí - skutečné či simulované. Vaší úlohou jakožto rodičů je Vaše děti o tomto obsahu poučit, dohlédnout na ně a doprovázet je při jejich začátcích na internetu tak, aby se z nich mohli stát samostatní a zodpovědní uživatelé.

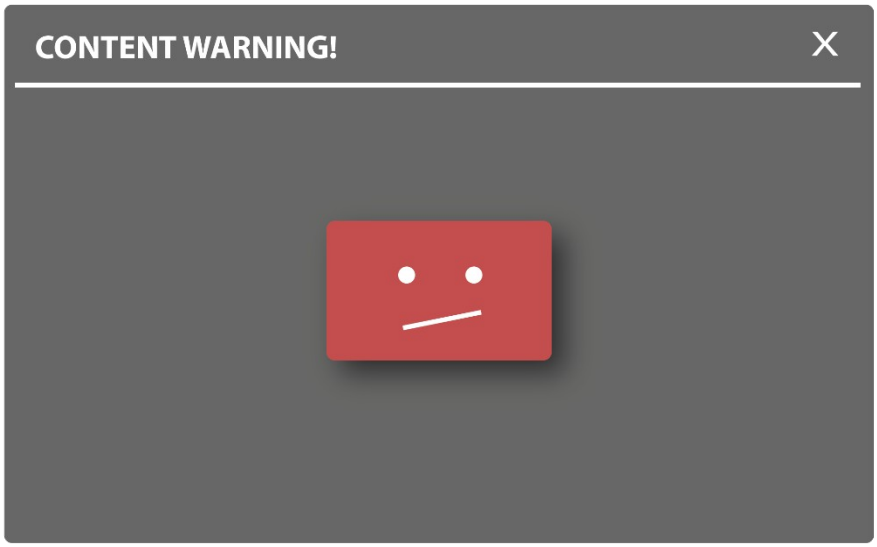
Praktický význam – K čemu získané znalosti a dovednosti využijete

Tato kapitola má za cíl naučit Vás, co je to nevhodný obsah, co tento pojem zahrnuje a jak se před takovým obsahem chránit.
Dále získáte znalosti o metodách šíření nevhodného obsahu a jeho působení na Váš každodenní život.

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

1. Co je to nevhodný obsah?

Pod pojem nevhodný obsah spadá velké množství obsahu na internetu, který je vyhodnocován jako pochybný či podezřelý.



Obecně je nevhodný obsah definován jako vše, co porušuje práva dětí vymezená dle Úmluvy o právech dítěte a vše, co porušuje lidská práva vymezená dle Základní listiny práv a svobod, zejména právo na život, soukromí, ochranu, právo účastnit se veřejného života a právo na ochranu před násilím a zneužíváním. Jako nevhodný obsah může být klasifikováno cokoliv od nenávistných projevů po obrázky sebepoškozování a pro-ana webové stránky. Termín nevhodný obsah zahrnuje tyto témata:

- Pornografie
- Násilí a extremismus
- Nebezpečné zboží
- Rasismus a nenávist
- Pro-Ana webové stránky
- Webové stránky s extremistickým obsahem

Abychom jednotlivým podtématům lépe porozuměli, podíváme se na ně zblízka:

Pornografie

Pornografie je charakterizována jako explicitní popis nebo vyobrazení, jehož účelem je podnítit sexuální pud. Pornografie však nemusí být vždy obscénní, a to v případě, kdy je možno polemizovat s tím, že dílo má literární, umělecký, politický nebo vědecký význam. Neshoda názorů však brání pokusům o objektivní definici tohoto pojmu.

Definice
Definice pornografie se mění v průběhu času a liší se podle místa. To, co bylo považováno před pár lety za pornografii, může dnes být označováno jako erotika. Pornografie na internetu je jakýkoliv pornografický obsah dostupný na internetové síti, hlavně na webových stránkách, v sdílených dokumentech nebo Usenet skupinách. K růstu pornografie na internetu vedlo rozšíření veřejného přístupu k “celosvětové síti” (World Wide Web) v 90. letech minulého století.

Příklady pornografie na internetu:

- Vyobrazení nahoty - osoba je nahá nebo oblečená pouze minimálně a toto vyobrazení nahoty neodpovídá vhodnému veřejnému kontextu.
- Vyobrazení, animace nebo ilustrace sexuálních praktik a sexuálně sugestivních póz.
- Obsah, který zobrazuje sexuální pomůcky a sexuální úchylky.
- Oplzlý či rouhavý obsah.
- Obsah, který vyobrazuje, popisuje nebo podporuje surovost.
- Aplikace, které propagují obsah se sexuálním zaměřením, eskortní služby nebo jiné služby, které poskytují sexuální praktiky výměnou za peníze či jinou odměnu.

Násilí a extremismus

Násilí se nevyskytuje pouze v počítačových hrách a filmech. Internet poskytuje prostor pro šíření videí a dalších multimédií s násilným obsahem, ať už hraným nebo skutečným, či záznamem reálných násilných událostí s často tragickým koncem. Existují dokonce stránky, které se specializují na shromažďování odkazů na videa a fotografie s takovým obsahem. Násilný obsah většinou neporušuje žádné předpisy a je tedy složité zamezit jeho šíření na internetu.

Násilí na internetu se většinou zaměřuje na grafické znázornění či popis násilí nebo násilných hrozeb mířených na určité osoby či zvířata. Dále také můžete narazit na aplikace, které obsahují projevy násilí. Tyto aplikace propagují sebepoškozování, sebevraždu, poruchy příjmu potravy a na první pohled neškodné hry, jejichž hraní však může vést k zraněním nebo i smrti.

V extrémních případech se můžete setkat s obsahem spojeným s terorismem, např. obsah, který podněcuje násilí, propaguje teroristické činy nebo je dokonce vyzdvihuje a oslavuje.

Zapamatujte si
Násilný obsah nebo obsah spojený s terorismem může mimo jiné sloužit pro vzdělávací, dokumentární, vědecké nebo umělecké účely. V tomto případě je důležité důkladně zvážit vhodnost užití takového obsahu a neopomenout vysvětlení jeho škodlivost.

Nebezpečné zboží

Mnoho lidí si neuvědomuje, že internet je prostředkem k snadnému prodeji výbušnin, střelných zbraní, střeliva a různého příslušenství k střelným zbraním. Na internetu je také možné sehnat součástky k výrobě výbušnin, střelných zbraní, střeliva, zakázané příslušenství k střelným zbraním a jiné zbraně nebo návody k tomu, jak přeměnit střelnou zbraň na automatickou nebo na zbraň, která simuluje automatickou střelbu.

Darknet market („temný trh") nebo cryptomarket je nelegální komerční webová stránka na speciálním neveřejném webu zvaném darknet, na který se lze dostat pouze se speciálním softwarem, konfigurací nebo oprávněním. Primárně funguje jako černý trh pro prodej nebo zprostředkování transakcí souvisejících s léky, kybernetickými zbraněmi, zbraněmi, padělanými penězi, údaji z ukradených kreditních karet, padělanými doklady, nelegálními drogami, steroidy a dalším nelegálním zbožím, ale i se zbožím legálním.

Rasismus a nenávist

Dalším typickým druhem nevhodného obsahu, který se vyznačuje systematickou diskriminací a marginalizací určitých skupin, je propagace a podněcování nenávisti vůči jednotlivcům nebo skupinám na základě jejich rasy, národnosti, náboženství, zdravotního postižení, věku, sexuální orientace, pohlaví, genderové identity a dalších. Cílem těchto tvrzení je dokázat, že tito jedinci nebo skupiny jsou méněcenné, podřadné a zaslouží si nenávist, které se jim dostává. Aktivity zaměřené proti těmto

jednotlivcům či skupinám zahrnují negativní charakteristiky, tvrzení, že určitá skupina představuje nějakou hrozbu, nebo proslovy, jejichž cílem je podnítit více lidí k jejich nenávisti a diskriminaci.

Internet poskytuje neomezený prostor k uveřejnění jakéhokoliv obsahu, textů, videí, fotek nebo hudby. Kdokoli, jednotlivec či skupina, organizace nebo firma, se může zvýraznit na internetu pomocí blogu, webové stránky nebo profilu na sociální síti. I přes veškeré snahy regulovat nevhodný obsah, lidé neustále nacházejí nové způsoby jeho šíření po internetu. Mezi nejčastější způsoby patří:

Pro-ana webové stránky

Pro-ana stránky, blogy, fóra a skupiny na sociálních sítích nevnímají anorexii jako nemoc ale jako životní styl. "Pro-ana jedinci" nevidí nic špatného na tomto způsobu života a před odmítavým postojem svého okolí se uchylují na internet, kde se navzájem podporují. Vyzdvihováním svého chorobného chování na webových stránkách a sociálních sítích si zajišťují pozitivní zpětnou vazbu a s tím související pocit uspokojení. Názory na pro-ana stránky se rozcházejí - jedna skupina tvrdí, že pro-ana hnutí existuje jako bezpečné prostředí pro jedince trpící anorexií, kde mohou diskutovat o své nemoci a vzájemně se podporovat na cestě k uzdravení, druhá skupina využívá pro-ana stránky k propagaci názoru, že mentální anorexie není nemoc, ale životní styl a že by tento pohled měl být respektován jak doktory tak jejich okolím.

Webové stránky s extremistickým obsahem

Stránky s extremistickým obsahem se na první pohled zdají být neškodné a často lidem poskytují zajímavé informace např. o různých historických událostech. Zmíněná fakta však bývají zkreslená a odkazují na zdroje, ve kterých jsou informace ovlivněny zvráceným pohledem na svět. Podobně extremisté užívají i texty písní, které mají většinou skrytý extremistický význam.

Sociální sítě

Stejně jako v televizi nebo v novinách, i na internetu je zakázáno šířit nelegální obsah jako je např. dětská pornografie nebo násilí. I přes veškeré snahy ho regulovat, se obsah tohoto typu na internetu vyskytuje. Kromě toho internet poskytuje prostor i pro distribuci legálního, ale nevhodného obsahu, jako je běžná pornografie nebo násilí, který může narušit zdravý vývoj dětí.

Dobrovolné posílání zpráv se sexuálně sugestivním obsahem, intimních fotek nebo videí se na internetu stává v dnešní době běžnou záležitostí. Rozvoj sociálních sítí značně přispěl k usnadnění šíření tohoto obsahu.

Někdy není úplně snadné rozpoznat, co je a co není nevhodný obsah.

Pornografie se často zaměňuje s výrazem erotika.

Jak se tyto výrazy od sebe liší?

Názory na to, co si představit pod pojmy pornografie a erotika, se liší mezi různými skupinami a jedinci. To, co bylo na začátku minulého století považováno za pornografické, může být dnes řazeno do kategorie erotiky.
Kritéria, podle kterých rozlišujeme pornografii a erotiku, se často odvíjejí od našich vlastních morálních, estetických a náboženských hodnot. Přestože se podle spousty lidí významy těchto dvou slov překrývají, existují mezi nimi značné rozdíly. Erotika se na rozdíl od pornografie nezaměřuje výhradně na naše smysly nebo tělesné pudy, ale také zapojuje naše estetické cítění a naše vnímání ideálu lidské krásy. Erotika se zaměřuje na umění a estetiku, pornografie na uspokojení sexuálních potřeb.

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

Dělení pornografie z psychologického hlediska:

- "měkká/lehká" pornografie = cokoliv erotické od uměleckého aktu po náznak pohlavního styku
- "tvrdá/drsná" pornografie = přímé zobrazení pohlavního styku včetně detailů pohlavních orgánů, jejich dráždění, erekce, penetrace a ejakulace
- úchylky = zobrazení sexuálních úchylek a praktik, které se běžně nevyskytují v sexuálním životě jedinců dané společnosti - dětská pornografie, sadomasochismus atd.

Pornografie vs dětská pornografie
Znázornění nahoty není vždy chápáno jako pornografie. Aby dílo jakékoliv formy (psané, fotografické, natočené atd.) bylo považováno za pornografické, musí být jeho účelem navození nebo posílení sexuálního vzrušení (za pornografii se nepovažuje zobrazení pohlavních orgánů v učebnici biologie). Proto je rozhodnutí, zda něco je nebo není pornografie, často založeno na morálním úsudku jedince. Dětská pornografie zobrazuje nebo jinak využívá dětí nebo osob, které lze za děti na první pohled považovat. Tento druh pornografie vyobrazuje děti v pózách, které znázorňují skutečný nebo simulovaný pohlavní styk, nebo děti v pózách, jejichž účelem je odhalení jejich genitálií. Dle evropských a vnitrostátních předpisů je výroba, šíření, export, import nebo držení dětské pornografie přísně zakázáno. Porušením právních předpisů zakazujících dětskou pornografii se pachatel dopouští vážného zločinu a čelí vysokým pokutám a trestům.

1.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Umíte charakterizovat nevhodný obsah.01_01: Dokážete vyjmenovat typy nevhodného obsahu.

Zadání: Která témata řadíme do nevhodného obsahu?
Úkol: Vyberte správné odpovědi. Více odpovědí může být správných.

- Erotické umělecké výjevy
- Webové stránky s rasistickým nebo nenávistným zaměřením
- Akční filmy
- Prodej nebezpečných výrobků
- Válečný dokumentární film s násilným obsahem

2. Jak rozpoznat webové stránky s nevhodným obsahem?

V dnešní době existuje několik organizací, které dohlížejí na obsah na internetu. Je ale dobré umět rozpoznat kvalitu a věrohodnost informací na internetu a vědět, jak se chovat, pokud na nějaký nebezpečný obsah narazíte.

Common Sense Media

Common Sense Media (common sense = selský rozum) je nezisková organizace zabývající se hodnocením filmů, seriálů, knih, aplikací a dalších médií a přiřazováním věkové vhodnosti k těmto jednotlivým obsahům. Rovněž samotným uživatelům nabízí možnost ohodnocení vhodné věkové příslušnosti určitého obsahu.

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

Kids-In-Mind
Kids-In-Mind podrobně popisuje, co děti v daném filmu uvidí, nedoporučuje však, pro kterou věkovou skupiny je obsah vhodný.

Další možnosti
Filmová databáze IMDb poskytuje spoustu užitečných informací. Při rozkliknutí detailů k filmu či seriálu si najděte odkaz "Parents Guide" (= příručka pro rodiče), který vás přesměruje na stránku s detailním rozpisem scén, které jsou pro diváky určité věkové kategorie nevhodné. Dále tento odkaz poskytuje věková doporučení podle jednotlivých zemí.

Existuje několik způsobů, jak zjistit, zda je určitý obsah vhodný pro Vaše dítě. Spousta platform na internetu používá hodnocení, které poukazuje na množství a míru násilí a explicitního obsahu vyskytující se v konkrétním díle.

Tyto údaje Vám pomohou vyhodnotit, zda je aplikace, webová stránka nebo určitý obsah vhodný pro Vaše dítě:

Hodnocení hudebních videí na internetu
Hodnocení videí podle věku nabízejí dvě největší platformy pro sdílení videí - VEVO a YouTube. Na YouTube se hodnocení nachází na videu nebo pod videem a dělí se do 3 kategorií: PG 12, 15 nebo 18, tzn. obsah ve videu je vhodný pro osoby starší 12, 15 nebo 18 let. Na VEVO se znak věkového ohodnocení nachází v levém horním rohu videa. Při rozkliknutí "i" se o něm dozvíte více informací.

Hodnocení počítačových her podle PEGI
Pan European Game Information neboli PEGI je organizace zabývající se věkovým hodnocením obsahu počítačových her. Podle tohoto hodnocení se posuzuje, zda je hra vhodná pro mladší nebo starší dospívající děti nebo pouze pro dospělé. Věkové hodnocení PEGI vzniklo v roce 2003 a má tyto kategorie: PEGI 3, PEGI 7, PEGI 12, PEGI 16 a PEGI 18. Číslo odkazuje na příslušný věk, od kterého je hra dostupná, např. hra s hodnocením PEGI 7 je vhodná pro děti od 7 let. Tato hodnocení jsou právně vymahatelná, což znamená, že hru s hodnocením PEGI 18 není možno prodat nezletilému dítěti. Hodnocení PEGI odkazuje pouze na věkovou přístupnost nikoli na hrací obtížnost hry.

Platformy poskytující „video na vyžádání"
Při užívání služeb jako Netflix, BBC iPlayer nebo Amazon Prime najdete věkové hodnocení konkrétních filmů a seriálů přímo na přehrávači při spuštění. Hodnocení se může lišit od poskytovatele, ale vždy jste upozorněni, pokud je určitý obsah vhodný pouze pro starší publikum nebo pokud obsahuje vulgární výrazy.

Minimální věková hranice pro užívání sociálních sítí
Většina sociálních sítí ve svých podmínkách a zásadách užití uvádí jako doporučenou věkovou hranici 13 let a výše. Důvodem omezení není to, že by obsah na sociálních sítích nebyl vhodný pro osoby mladší 13 let, ale to, že tyto platformy spadají pod federální zákon COPPA (Zákon o ochraně soukromí

dětí na internetu) vydaný Spojenými státy americkými, který existuje za účelem ochrany soukromí dětí mladších 13 let.

Věkového omezení aplikací

Google Play Store stejně jako Apple Store používají hodnocení, které poukazuje na množství sexuálně explicitního obsahu, užití vulgárních výrazů, obsahu pro dospělé nebo vyobrazení zneužívání návykových látek, jež mohou aplikace obsahovat.

Zkratky označující přístupnost obsahu, se kterými se na internetu můžete setkat (zdroj: Filmový rating MPPA):

- G: Dětský film, zcela nezávadný a nevinný
- PG: Rodiče by měli zvážit, zda nechají své děti film zhlédnout
- PG-13: Rodiče musejí doprovázet děti mladší 13 let
- R: Mládež do 17 pouze v doprovodu dospělé osoby
- NC-17: Nevhodné pro diváky mladší 18 let

Zapamatujte si
„Rodičovská kontrola", „Nastavení soukromí" a různá hodnocení přístupnosti jsou užitečnými nástroji, jež pomáhají minimalizovat rizika, kterým mohou Vaše děti na internetu čelit. Jejich účinnost však není 100%. Důležité je poučit děti o možných nástrahách a naučit je kriticky myslet, aby věděly, co dělat, pokud se do nějaké nepříjemné situace na internetu dostanou. Důležité je také děti pobízet k tomu, aby se Vám svěřily, pokud na něco nepříjemného na internetu narazí.

O nástrahách, které ve virtuálním světě číhají, byste měli Vaše děti poučit hned v jejich začátcích užívání internetu. Vysvětlete jim, že existuje možnost, že při surfování po internetu narazí na něco, na co narazit nechtěly. Čím častěji s nimi budete toto téma probírat, tím lépe.

Doporučená opatření, jak kontaktu s nevhodným obsahem předejít:

- Vysvětlete dětem věková omezení určitého obsahu
- Komunikujte s dalšími rodiči a se zaměstnanci školy
- Stanovte dětem určitá pravidla
- Buďte rozvážní a povzbudiví
- Nastavte ověření věku na webových stránkách s pornografickým obsahem
- Povzbuzujte kritické myšlení Vašich dětí
- Mluvte o tom, co je na internetu skutečné a co ne
- Mluvte o pozitivním užití technologií

Zapamatujte si
Důležité je s dítětem komunikovat a zajímat se o to, co na internetu dělá.

2.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Umíte charakterizovat nevhodný obsah.01_02: Dokážete vyjmenovat metody šíření nevhodného obsahu a získávání citlivých údajů.

Zadání: Jaký obsah naleznete na pro-ana stránkách?
Úkol: Vyberte správné odpovědi - pouze jedna odpověď je správná.

- oplzlý, nemravný obsah
- odkazy na videa a fotografie zobrazující násilí
- propagace sebepoškozování, sebevraždy a násilných her
- diskuze o anorexii

3. Jaký obsah je pro moje dítě nevhodný?

Bez dohledu mají děti a náctiletí neomezený přístup do virtuálního světa. Proto by si rodiče měli uvědomovat všechny možné nástrahy, které internet přináší. Internet umožňuje komukoliv na něj cokoliv přidat, a tak je možné, že Vaše dítě narazí na něco, na co narazit nechtělo, nebo se ocitne na stránce, která pro něj není vhodná. Vhodnost a nevhodnost obsahu vnímá každý jinak a mění se s tím, jak Vaše dítě roste a dospívá. Nevhodný obsah může být vše od sprostého vyjadřování po pornografické obrázky a videa.
Používání internetu by mělo být pro děti příjemným a bezpečným zážitkem. Bohužel existuje spousta věcí, které pro ně mohou být znepokojující. Mezi nevhodný obsah nepatří pouze pornografie, ale také rasistický obsah, obsah vyzdvihující poruchy příjmu potravy nebo stránky s hazardními hrami.

Jaký obsah je pro děti nevhodný?
Nevhodný obsah zahrnuje informace nebo vyobrazení věcí, které mohou znepokojit nebo jinak poznamenat nezletilé uživatele. Patří sem také obsah s informacemi, které mohou navádět děti k protiprávnímu nebo nebezpečnému jednání. Řadíme sem:

- Pornografický obsah
- Obsah s vulgárními výrazy
- Stránky podporující vandalismus, trestné chování, terorismus, rasismus, poruchy příjmu potravy, sebepoškozování nebo sebevražedné chování
- Fotky, videa nebo hry, které vyobrazují násilí páchané na lidech nebo na zvířatech
- Stránky s hazardními hrami
- Chatovací místnosti, jejichž obsah není monitorován
- Sexistické stránky nebo stránky, které vyobrazují ženy v zastaralých tradičních rolích, které neodpovídají soudobým hodnotám a postojům

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

S nevhodným obsahem se setkává na internetu skoro každý. Podle věku a vhodnosti obsahu dělíme uživatele internetu do těchto kategorií:

- Předškolní věk (0 – 5 let)
- Mladší školní věk (6 – 11 let)
- Starší školní věk (12 – 15 let)
- Adolescence (15 – 18 let)
- Dospělost

Předškolní věk

Čím dál více předškoláků používá počítače, chytré telefony nebo tablety svých rodičů k hraní her, používání aplikací nebo sledování svých oblíbených seriálů a filmů. Existuje několik způsobů, jak se ujistit, že jejich počínání na internetu je bezpečné. Důležitá je spolupráce a asistence při jejich seznamování s online světem a vytvoření zdravého vztahu k internetu. Velice účinná je instalace rodičovské kontroly, užívání hesel, která zabrání přístup k určitému obsahu, a stanovení určitých pravidel pro používání internetu.

Mladší školní věk

Používání digitálních technologií od nízkého věku prokazatelně zlepšuje jazykové dovednosti, sociální vývoj a kreativitu dítěte. Užívání internetu není bez rizika, malé děti často mohou narazit na nevhodný obsah nebo se snažit napodobovat to, co na internetu dělají jejich starší sourozenci. Pro děti v mladším školním věku je účinné zavést stejná opatření jako pro předškoláky a navíc využít tzv. režim letadlo, který jim zabrání komunikovat s lidmi prostřednictvím konkrétního zařízení. Komunikujte se staršími dětmi o tom, co na internetu dělají a co ukazují mladším sourozencům, a kontrolujte věkovou vhodnost obsahu, se kterým Vaše dítě přichází do styku.

Starší školní věk

Žáci druhého stupně základní školy jsou největší skupinou dětí užívající moderní technologie, a přesto většinou nejsou dostatečně poučeni o číhajících nástrahách. Rodiče nad jejich aktivitami většinou nemají dostatečnou kontrolu a dohled, děti v tomto věku jsou lehce manipulovatelné a naivní a ve snaze najít samy sebe často unikají ze skutečného světa do světa virtuálního, kde můžou být kýmkoliv chtějí. Rodiče na jejich online aktivity často dohlížejí pouze minimálně nebo vůbec, děti jsou ve většině případů zdatnější a zkušenější s užíváním internetu než jejich rodiče, kteří mají k moderním technologiím odtažitý postoj a své děti nechají užívat internet jako způsob relaxace. I proto má velké množství mladých uživatelů pocit, že na internetu mohou dělat cokoliv, aniž by z toho pro ně plynuly jakékoli následky.

Adolescence

Žáci středních škol jsou skupinou, která se vyznačuje hlubším porozuměním moderních technologií a jejich nadměrným užíváním, hlavně co se internetu a sociálních sítí týče. Zároveň si však uvědomují nástrahy, které na ně na internetu čekají. Vaše děti by si měly upravit nastavení soukromí na sociálních sítích tak, aby je mohli najít a označovat na fotkách pouze blízcí přátelé a rodinní příslušníci. Upozorněte je na to, že vše, co sdílí, napíší nebo odešlou, s velkou pravděpodobností zůstane na internetu navždy. Řekněte svým dětem, aby na internet přidávaly pouze příspěvky, u kterých by jim nevadilo, kdybyste na ně narazili vy, jejich učitelé nebo budoucí zaměstnavatelé. Veďte je k tomu, aby za sebou zanechávaly pozitivní digitální stopu. Připomeňte jim, že je důležité nepodlehnout nátlaku okolí a neposílat nevhodné obrázky a nepřidávat nevhodné komentáře. Je důležité, abyste jim důvěřovali. Ukažte, že se zajímáte, a snažte se s nimi vybudovat přátelský vztah. Sdílejte se svými dětmi své příspěvky a aktivity na internetu a pobídněte je k tomu, aby s vámi na oplátku sdílely ty jejich.

Dospělost

Nevhodný obsah představuje hrozbu i pro dospělé. Plno webových stránek s obsahem pro dospělé, např. pornografické stránky, obsahuje viry, které si často uživatel při jejich návštěvě omylem stáhne do svého počítače. Právě tyto stránky mají velké množství uživatelů a tím pádem jsou lákavé pro zločince, kteří na ně virus umístí. Uživatelé postiženi takovýmto virem většinou útok nenahlásí, protože se stydí za to, jak k viru přišli. Mezi nejčastější internetové útoky patří trojský kůň, clickjacking, falešné účty na Tinderu, za kterými se schovává počítačový program, catfishing, ransomware, počítačový červ, pornware nebo spyware.

3. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Jste poučeni o hrozbách a následcích zneužití citlivých údajů.02_03: Dokážete charakterizovat cílové skupiny, které by se mohly stát oběťmi nevhodného obsahu.

Zadání: Pro kterou skupinu lidí představuje nevhodný obsah největší hrozbu?
Úkol: Vyberte správné odpovědi - pouze jedna odpověď je správná.

- staří lidé
- děti mezi 12 a 18 lety
- všechny děti mladší 15 let
- všechny děti starší 15 let

4. Jak ochráním sebe a své děti před nevhodným obsahem?

Rodičovská kontrola a podobné nástroje jsou dobrým způsobem, jak ochránit děti před nevhodným obsahem, nikdy však nebudete mít naprostou kontrolu nad tím, na co na internetu narazí. Důležité je naučit je se nevhodnému obsahu vyhýbat a jak se v případech, kdy se s ním setkají, zachovat. Komunikace je v těchto případech klíčová.

Většina webových stránek s nevhodným obsahem není nelegální, a proto je pouze na Vás jako na rodičích kontrolovat, co děti na internetu dělají. Představte si internet jako velké město, ve kterém žijí dobří i zlí lidé. Stejně jako byste nenechali své dítě potulovat se v noci venku po městě bez dozoru, tak ho také nenechejte samotné “potulovat se” po internetu a dohlédněte na jeho aktivity.

Co mohu dělat, když rozpoznám obsah na webové stránce jako nevhodný?

- Informovat správce příslušné aplikace (webový prohlížeč, sociální síť atd.)
- Informovat policii nebo jinou instituci
- Začít používat software, který blokuje nevhodný obsah (např. rodičovská kontrola)
- Poučit děti o tomto tématu

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

Při užívání aplikací máte možnost kontaktovat správce dané aplikace (např. Google, Facebook) a informovat ho o nevhodném obsahu, na který jste narazili. Většinou najdete příslušné tlačítko, které Vám zprostředkuje kontakt se správcem, v nastavení aplikace.

O svém nálezu můžete také informovat policii. Je potřeba podrobně popsat zdroj, kde jste na obsah narazili.

Rodičovská kontrola jsou softwary, s jejichž pomocí mohou rodiče kontrolovat aktivity svých dětí na internetu. Jejich hlavním úkolem je zamezit dětem v přístupu k nevhodnému obsahu na internetu. Lze je aplikovat na vyhledávače, servery pro sdílení videí nebo přímo u poskytovatele internetového připojení. Nejčastějšími typy rodičovské kontroly jsou:

- Nastavení rodičovské kontroly přes Wi-Fi router
- Aplikace monitorující aktivity dětí na internetu
- Omezení přístupu na internet v nastavení Wi-Fi
- Rodičovská kontrola na webových prohlížečích

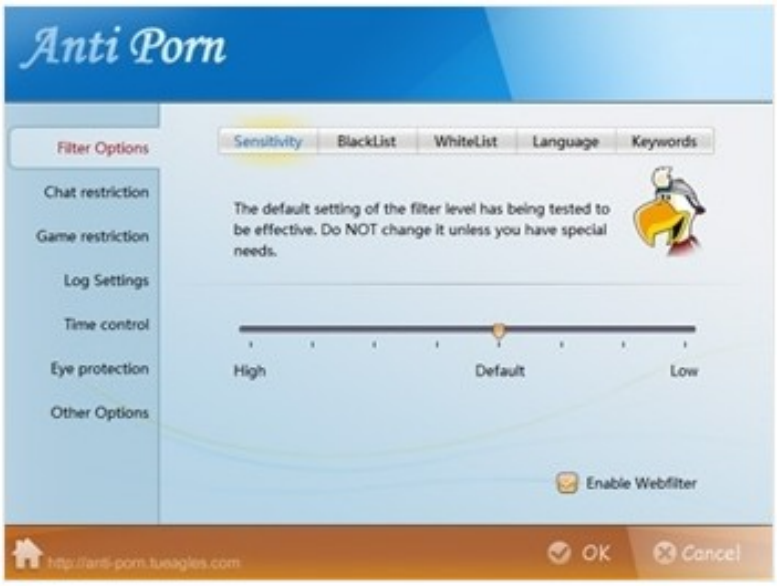
Existuje několik způsobů internetové ochrany, které dokáží zamezit v přístupu k nevhodnému obsahu nejen dětem, ale i Vašim zaměstnancům, jež by stránky s např. pornografickým či extremistickým obsahem mohly rozptylovat v práci.

Který program, filtr nebo doplněk je nejlepší pro zamezení přístupu k nevhodným webovým stránkám?

Anti-Porn

Anti-Porn je díky své možnosti přizpůsobení a jednoduché ovladatelnosti jeden z nejznámějších a nejpoužívanějších programů k zamezení přístupu k pornografii na internetu. Tento program sám automaticky rozpozná a označí obsah jako pornografický a okamžitě k němu zamezí přístup. Další výhodou tohoto programu je jeho velká databáze, která obsahuje seznam několika tisíc nevhodných stránek a která je pravidelně aktualizována.

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



K9 Web Protection

Další program, který filtruje obsah a chrání Vás před skrytými nástrahami internetu. Je zdarma a je možné ho nainstalovat jak na zařízení Windows, tak na zařízení Mac OS. Lze ho využít k ochraně před malwarem i k filtrování nevhodného obsahu. Snadno se instaluje, nastavuje a ovládá. Nevhodné stránky třídí do kategorií podle obsahu - pornografické, sociální sítě, násilný obsah atd.

Kurupira Web Filter

Méně známý a rozšířený program, který však zvládá svou úlohu třídění obsahu velmi dobře a zároveň je orientovaný na začínající uživatele. Výhodou je, že licence k tomuto programu je zdarma. Přístup do programu je chráněn heslem, takže pouze ti, kteří ho znají, mohou nastavovat a upravovat filtry.

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

iWebFilter

iWebFilter obsahuje širokou databázi nevhodného obsahu, klíčových slov a webových stránek. Každý uživatel má možnost tuto databázi rozšířit o vlastní obsah, který považuje za nevhodný. Filtrování obsahu lze nastavit na webové prohlížeče, Instant Messengers (= služba pro okamžité zasílání zpráv), e-mailové klienty a další aplikace. Dále tento program poskytuje možnost časově omezit přístup k internetu, limit pro přenos dat a detailní záznamy o událostech.

V případě, že na něco nevhodného na internetu narazíte, vypněte obrazovku nebo od ní odejděte a dále se na obsah nedívejte. Pokud zjistíte, že se Vaše dítě při surfování po internetu dostalo k nevhodnému obsahu, nevyčítejte mu to. Jestli ale zjistíte, že se Vaše dítě úmyslně dívá na pornografický či násilný obsah, měli byste tento problém začít řešit. Je nutné vzít v potaz věk dítěte a závažnost obsahu a případně vyhledat odbornou pomoc, např. v pedagogicko-psychologické poradně.

Organizace Insafe a INHOPE spolupracují prostřednictvím sítě Center pro bezpečnější internet (SIC), která se nacházejí po celé Evropě. Tato centra se obvykle zahrnují informační středisko, linku bezpečí, horkou linku a panel pro mládež. Horké linky, které se věnují odstraňování nelegálního obsahu na

internetu, se nacházejí ve 30 evropských zemích a snaží se zaručit bezpečný internet pro děti a mládež. Prostřednictvím řady služeb SIC reagují na nejnovější problémy na internetu, snaží se je řešit a pomáhají propagovat množství příležitostí, které online svět nabízí.

Jak nahlásit nevhodný obsah?
Co dělat, pokud se Vy nebo Vaše dítě dostanete do kontaktu s nevhodným obsahem, který podněcuje násilí či nenávist:

- Pokud se jedná o nelegální obsah, kontaktujte policii
- Kontaktujte organizace zabývající se bezpečností na internetu, která Vám pomůže s odstraněním či zablokováním obsahu (např. Centrum pro bezpečnější internet (SIC): https://www.bezpecnenanetu.cz/cs/stoponline/)
- Nahlaste svůj nález správci stránky či aplikace
- Upravte nastavení Vašeho počítače
- Obraťte se na odborníka, který pomůže Vašemu dítěti se s traumatickým zážitkem vyrovnat
- Promluvte si se svým dítětem
- Zůstaňte v klidu

Krátká videa s návody, jak správně upravit nastavení na nejužívanějších platformách:

Kontrola soukromí na Facebooku
https://www.youtube.com/watch?v=wN3jz2Mv_ME&feature=emb_title

Omezený režim na YouTube
https://www.youtube.com/watch?v=XuXnatkASTQ&feature=emb_title

Bezpečné vyhledávání Google
https://www.youtube.com/watch?v=LK-MIwjQz20&feature=emb_title

Zabezpečení a spyware
Většina počítačů, které jsou k dispozici na veřejně přístupných místech (např. knihovny, kavárny, školy,atd.), obsahuje monitorovací software, který sleduje aktivity na počítači a zachycuje vše, co se na obrazovce děje. Tyto softwary a podobné sledovací nástroje monitorují všechny druhy činností na počítači a tím pádem ohrožují citlivé osobní údaje osob, které s počítačem pracovaly. Antiviry a firewally neposkytují dostatečnou ochranu před spywary a útoky na soukromí uživatelů. Spyware se nejčastěji dostane do počítače stažením nějakého programu, ke kterému byl připojen, prostřednictvím e-mailových příloh nebo se může tvářit jako skutečný program a po instalaci může být téměř nemožné ho odhalit a odebrat bez pomoci speciálního nástroje určeného k jeho odstranění. Ochrana a preventivní opatření hrají důležitou roli v ochraně Vašeho soukromí před spywary a podobnými vnějšími útoky. Zmíněné monitorovací programy lze nainstalovat i do Vašeho soukromého počítače, a tedy mít neustále přehled o tom, co Vaše dítě na internetu dělá.

Tipy, jak rozpoznat podezřelé stránky a aplikace:

- Zkontroluje, zda URL stránky je stejná jako ta, kterou vždy používáte.
- Dávejte si pozor na e-maily od lidí, které neznáte. Pokud si nejste jistí, o co se jedná, neotevírejte odkazy a přílohy v e-mailech.
- Zkontrolujte, zda se značka jeví stejná na všech svých platformách a zda její logo není náhodou rozmazané.
- Pokud obdržíte e-mail s chybami, ve kterém Vás odesílatel žádá o zadání přihlašovacích údajů a aktualizaci informací na Vašem profilu, s největší pravděpodobností se jedná o podvod.

- Podívejte se na hodnocení aplikací předtím, než se je rozhodnete stáhnout do Vašeho zařízení. Pokud má aplikace hodně uživatelů a kladných hodnocení, není se čeho bát. Nemá-li žádné hodnocení, pokuste si ji prověřit na internetu. Podvody jsou obvykle identifikovány poměrně rychle a lidé o nich prostřednictvím internetu informují ostatní.
- Jestli Vás aplikace žádá o zadání velkého množství osobních údajů nebo o poskytnutí přihlašovacích údajů k Vašim účtům na sociálních sítích, jedná se nejspíš o podvrh.

Osobní údaje

Další problém, který souvisí s nevhodným obsahem, je zveřejňování osobních údajů. Cokoliv se rozhodnete přidat na internet si může kdokoli a kdykoli zobrazit nebo stáhnout a použít v jiném kontextu nebo Vaše údaje nějakým způsobem zneužít.

Osobní údaje jsou typem informací, které potřeba chránit nejvíce.

Definice
Americká nezávislá vládní agentura General Services Administration (= Správa obecných služeb) definuje osobní údaje jako "údaje, s pomocí kterých lze rozeznat či dohledat totožnost jedince, a to buď za použití jednoho nebo kombinace několika údajů, které jsou spojeny nebo je lze spojit s konkrétním jedincem."

Za osobní údaje se považují:

- Jména: Vaše jméno a příjmení, Vaše rodné příjmení a rodné příjmení Vaší matky
- Čísla dokladů: číslo sociálního zabezpečení, číslo řidičského průkazu, číslo pasu, číslo pojištěnce, číslo daňového poplatníka, číslo kreditní karty nebo číslo bankovního účtu
- Adresy: adresa bydliště a e-mailová adresa
- Biometrie: snímek sítnice, otisky prstů, geometrie obličejových rysů nebo hlasová biometrie
- Telefonní čísla
- IT údaje: MAC adresa (Media Access Control) nebo IP adresa (Internet Protocol)

Proč je ochrana osobních údajů tak důležitá? Zabezpečením svých osobních údajů snižujete riziko krádeže identity, chráníte své finanční údaje, svou zaměstnatelnost a reputaci podniku, předcházíte možnosti, že budete okradeni, a mnoho dalšího.

Tipy, jak zabezpečit své účty a udržet své soukromí na internetu pod kontrolou:

- Zkontrolujte nastavení soukromí u všech svých účtů na sociálních sítích
- Nastavte si silná hesla a pravidelně je aktualizujte
- Nesdílejte s nikým svá hesla
- Stáhněte a nainstalujte si nové aktualizace operačního systému nebo softwaru do svého telefonu, tabletu či počítače ,jakmile budou k dispozici
- Nepřidávejte si do svých kontaktů na sociálních sítích osoby, které mimo internet neznáte
- Pokud Vás stránka nebo aplikace žádá o zadání osobních údajů, prověřte si, že se nejedná o podvod

Evropská komise přijala doporučení o opatřeních k účinnému boji proti nelegálnímu obsahu na internetu. Témata, jako podněcování k terorismu, nezákonné nenávistné projevy nebo pohlavní zneužívání dětí, stejně tak jako porušování práv duševního vlastnictví a ochrany spotřebitele na internetu, vyžadují silný koordinovaný přístup celé EU. Tento přístup je plně v souladu se Směrnicí EU o

autorském právu, která zahrnuje široce diskutované aspekty odpovědnosti platforem na internetu. Je také plně v souladu s revizí Směrnice o audiovizuálních mediálních službách.

Je nutné, aby internetové platformy byly odpovědnější za správu svého obsahu. Zmíněné doporučení navrhuje společný přístup k rychlému a iniciativnímu zjišťování, odstraňování a prevenci opětovného výskytu určitého obsahu na internetu:

- Jasnější postupy pro podávání zpráv a preventivní opatření
- Efektivnější nástroje a proaktivní technologie
- Silnější záruky pro zajištění základních práv
- Zvláštní pozornost věnovaná malým podnikům
- Bližší spolupráce s veřejnými orgány

4.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_ Víte, jak se chránit před nevhodným obsahem. 03_05: Dokážete vyjmenovat osobní údaje, které by neměly být zveřejňovány na internetu.

Zadání: Jaké jsou základní způsoby ochrany osobních údajů?
Úkol: Vyberte správné odpovědi - více odpovědí může být správných.

- Neposílejte své fotografie lidem, které neznáte.
- Neprozrazujte svá hesla ani blízkým přátelům.
- Neotevírejte přílohy zpráv a e-mailů, jejichž odesílatele neznáte.
- Nenavštěvujte žádné sociální sítě.

Zdroje

Internet matters.org: https://www.internetmatters.org/issues/inappropriate-content/learn-about-it/#age-ratings

CNET.com: https://download.cnet.com/Anti-Porn/3000-27064_4-10207334.html

K9 Web Protection: https://www.downloadsource.net/1771222/k9-web-protection/

Soft free download (Soft 32): https://kurupira-web-filter-and-parental-control.soft32.com/

Softpedia: https://www.softpedia.com/get/Internet/Other-Internet-Related/iWebFilter.shtml

Zapamatujte si

Shrnutí

Existuje mnoho druhů nevhodného obsahu. Mezi nejčastější patří:

- Pornografie
- Násilí a extremismus
- Nebezpečné zboží
- Rasismus a nenávist

- Pro-Ana webové stránky
- Webové stránky s extremistickým obsahem

Přestože je tento obsah často nežádoucí a škodlivý, nemusí být vždy nelegální. Setkání s nevhodným obsahem může být nepříjemné, ať už je nebo není legální.

Obecně se doporučuje obrátit se s nelegálními nálezy na policii. Nejdůležitější je však jednat rychle a zabránit dalšímu šíření nevhodného a nelegálního obsahu. Pokud se setkáte s nelegální pornografií či stránkami s extremistickým obsahem, nahlaste svůj nález na policii.
Děti určitého věku by s nevhodným a nebezpečným obsahem vůbec neměly přijít do styku. Různé filtry, které lze použít na webové prohlížeče, jsou velmi užitečným nástrojem, jak tomu předejít (např. pokud jako klíčové slovo uvedete slovo “porno” nebo “pornografie”, filtr zablokuje přístup ke všem stránkám obsahující tento výraz).

Rodičovská kontrola jsou softwary, s jejichž pomocí mohou rodiče kontrolovat aktivity svých dětí na internetu. Jejich hlavním úkolem je zamezit dětem v přístupu k nevhodnému obsahu na internetu. Lze je aplikovat na vyhledávače, servery pro sdílení videí nebo přímo u poskytovatele internetového připojení. Nejčastějšími typy rodičovské kontroly jsou:

- Nastavení rodičovské kontroly přes Wi-Fi router
- Aplikace monitorující aktivity dětí na internetu
- Omezení přístupu na internet v nastavení Wi-Fi
- Rodičovská kontrola na webových prohlížečích

Nejdůležitějším a nejúčinnějším prostředkem ochrany před nevhodným obsahem je komunikace a starost o to, co Vaše děti dělají, o co se zajímají a jaké jsou jejich koníčky. Nástroje ochrany jako jsou různá zákonná opatření, rodičovská kontrola, softwary a podpůrné instituce jsou užitečnou prevencí, klíčová je však vzájemná důvěra mezi Vámi a Vaším dítětem.

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

Správné odpovědi

Zadání: Která témata řadíme do nevhodného obsahu?
Úkol: Vyberte správné odpovědi. Více odpovědí může být správných.

- Erotické umělecké výjevy
- **Webové stránky s rasistickým nebo nenávistným zaměřením**
- Akční filmy
- **Prodej nebezpečných výrobků**
- Válečný dokumentární film s násilným obsahem

Zadání: Jaký obsah naleznete na pro-ana stránkách?
Úkol: Vyberte správné odpovědi - pouze jedna odpověď je správná.

- oplzlý, nemravný obsah
- odkazy na videa a fotografie zobrazující násilí
- propagace sebepoškozování, sebevraždy a násilných her
- **diskuze o anorexii**

Zadání: Pro kterou skupinu lidí představuje nevhodný obsah největší hrozbu?
Úkol: Vyberte správné odpovědi - pouze jedna odpověď je správná.

- staří lidé
- **děti mezi 12 a 18 lety**
- všechny děti mladší 15 let
- všechny děti starší 15 let

Zadání: Jaké jsou základní způsoby ochrany osobních údajů?
Úkol: Vyberte správné odpovědi - více odpovědí může být správných.

- **Neposílejte své fotografie lidem, které neznáte.**
- **Neprozrazujte svá hesla ani blízkým přátelům.**
- **Neotevírejte přílohy zpráv a e-mailů, jejichž odesílatele neznáte.**
- Nenavštěvujte žádné sociální sítě.