INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt „ Vzdělávání dotykem“
CZ.1.07/1.3.00/51.0031

Autor: PhDr. Jan Černý

POČÍTAČOVÁ KRIMINALITA A KYBERŠIKANA

Obsah

Úvodní slovo realizačního týmu CVLK

Cílem projektu Vzdělávání dotykem je především inovovat IC zařízení ve školách pro zefektivnění výuky. V 21. století se IC neodmyslitelně stává součástí výuky na všech stupních škol. V žádném případě nemá toto zařízení sloužit k nahrazení standardní výuky, ale cílem je tuto výuku především inovovat a zefektivnit. Dnešní IC technika dokáže přitáhnout a motivovat žáky k předmětům, které nepatří mezi oblíbené pro svoji složitost. Pokud učitel dokáže propojit klasickou výuku s informačními technologiemi, může se i z neoblíbeného předmětu stát populární.

Uvědomujeme si, že využívání moderních IC zařízení klade na učitele nemalé nároky, a jedinou možností, jak v tomto obstát, je neustálé vzdělávání se. Proto jsme do tohoto projektu zařadili i množství kurzů, které jsme koncipovali tak, abychom co nejvíce pomohli učitelům se získáním praktických dovedností v této oblasti.

Kurzy jsme rozdělili do 4 vzdělávacích oblastí. První je zaměřena na problematiku zadávání veřejných zakázek při pořizování ICT zařízení do škol, druhá aktivita je zaměřena na obecné znalosti ovládání ICT, včetně ochrany autorských práv a nebezpečí počítačové kriminality a kyberšikany. Třetí a čtvrtá aktivita jsou již plně zaměřeny na využití ICT ve školách. Učitelé mají možnost seznámit se s využitím ICT technologií při vedení elektronických dokumentů, s tvorbou elektronických výukových materiálů, včetně jejich ukládání na virtuální uložiště. Dále se pedagogové seznámí s možností využití ICT zařízení při výuce cizích jazyků, matematiky, českého jazyka, odborných a přírodopisných předmětů.

Kurzy jsou koncipovány a přizpůsobeny vždy dané škole, protože jsme si vědomi, že existují značné rozdíly ve vybavenosti škol ICT zařízením a technických znalostí jednotlivých učitelů.

Cílem výukového materiálu není komplexní shrnutí dané problematiky, ale především shrnutí obecných informací, na kterých je možné dále stavět. Je důležité připomenout, že ICT technologie jdou neustále dopředu a pokud chce učitel využívat tato zařízení ve své výuce, je nutné se v této oblasti neustále vzdělávat.

Věříme, že tímto projektem pomůžeme učitelům v aplikaci ICT do výuky a usnadníme jim tuto nelehkou práci.

Realizační tým Centra vzdělanosti Libereckého kraje, p. o.

1. Kybernetická kriminalita současnosti

Základní pojmy

- Kyberprostor - označení pro virtuální svět propojených počítačových zařízení a sítí.
- Kybernetická kriminalita - jedná se o kriminální činnost spojenou s využitím počítače nebo telekomunikační sítě v podobě útoku proti jedinci, skupině či státu.

1.1. Typologie on-line kriminality

Spam

- Nevyžádané zprávy, které jsou nejčastěji distribuovány pomocí elektronické pošty, dále pak zejména v rámci sociálních médií, newsgroups, on-line her, blogů, chatovacích platforem a mobilních telefonů.
- Spam ve většině případů obsahuje:
- Obchodní nabídky od firem bez registrace u Úřadu pro ochranu osobních údajů (ÚOOÚ).
- Reklamní sdělení.
- Podvodné nabídky z Nigérie či dalších zejména afrických států (obchod s dětmi).
- Podvodné loterie.

Hoax

- Šíření poplašných zpráv.
- Hoax se dělí dle serveru Hoax.cz následovně:
- Popis nebezpečí (viru)

  Ničivé účinky viru

  Důvěryhodné zdroje varují

  Výzva k dalšímu rozeslání

Popis jiného nereálného nebezpečí

Petice a výzvy

Pyramidové hry a různé nabídky na snadné výdělky

Řetězové dopisy štěstí

Žertovné zprávy.

Hacking

- Neoprávněný průnik do konkrétního informačního systému, provedený zvnějšku, zpravidla ze vzdáleného počítače.
- Pachatelé se zpravidla nepřipojují k objektu útoku (počítači) přímo, ale přes jeden i více internetových serveru v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, který byl při útoku užit.
- Jednotlivé případy takových incidentu se liší zejména svou motivací (vzrušení, zábava, msta, zvědavost, hmotný zisk).

Cracking

- Činnost spojená se šířením nelegálního software.
- Jedná se překonávání ochrany počítačových programů s cílem změnit jejich funkcionalitu, či eliminovat náklady spojené s plným využitím daného software.
- Příklad crackingu:
- Generátor sériových čísel.

Malware

- Počítačové programy, které jsou schopny kopírovat sama sebe a způsobovat v počítači, případně počítačovém systému nějaké škody. Jsou schopny se šířit i po počítačové síti.
- Druhy „špatných programů“:
- Bootviry

- Souborové viry
- Multipartitní viry
- Makroviry
- Trojské koně a červi.

Cybersquatting

- Kriminální činnost spojená s doménovými jmény.
- Nelegální obchodníci nakupují domény známých firem či ochranných známek a následně je nabízejí k odprodeji za astronomické částky.
- Obrana: WIPO.int.

Sniffing

- Odposlouchávání komunikace
- Zachycování hesel
- Získávání obchodních tajemství
- Získávání e-mailových zpráv v plném znění.

Browser sniffing

- Hrozba především pro osoby s nízkou počítačovou gramotností.
- Získávání osobních údajů skrze webové aplikace v internetových prohlížečích.
- Následný prodej osobních údajů.

Trollování

- Rozvracení diskuzních fór ve formě napadání, urážek a samozřejmě spamu
- Podobné příspěvky mají za cíl rozvinout další emotivní diskuzi

- Ignorace mnohdy již nezabírá
- Diskuzní fóra napadají začínající hackeři, kteří využívají pro svou činnost roboty.

Kyberšikana (cyberbullying, cybermobbing)

- Druh šikany, při které se využívají elektronické prostředky (mobilní telefony, e-maily, sociální média, …).
- Nejčastěji se jedná o zasílání urážlivých, obtěžujících a útočných zpráv s cílem dehonestovat oběť, popř. podpořit vlastní šikanu v reálném světě.
- Pachatelé využívají síťového efektu (př. upload videa na YouTube a následné sdílení s velkou komunitou lidí).
- Fyzické napadení oběti spojené s natáčením videozáznamu.
- Vyvedení oběti z rovnováhy spojené s natáčením videozáznamu.
- Vydírání s pomocí informačních a komunikačních technologií.

Kybergrooming

- Cílem kybergroomingu je vyvolat v dítěti falešnou důvěru, donutit ho k hlubší komunikaci (kybergroomer postupně stupňuje úroveň důvěrnosti), která vede k osobnímu setkání.
- Výsledkem setkání má potenciální scénáře: sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.

Sexting

- Zasílání fotografií a dalšího obsahu se sexuálním podtextem.
- Průzkum The National Campaign to Prevent Teen and Unplanned Pregnancy v roce 2008 odhalil, že 20 % uživatelů v rozmezí věku od 13-20 let zaslalo pomocí ICT svou fotografii, která obsahovala prvky nahoty či polonahoty. 33% uživatelů potom bylo v rozmezí 20–26 let.

- Číslo textových zpráv se sexuálním podtextem bylo prakticky dvojnásobné.
- Riziko zneužití zejména po partnerských rozchodech.

Phishing

- Phishing = rybaření
- Podstatou této metody je zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datum atd.).
- Pachatel vytvoří podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat.
- Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele.

On-line zneužívání dětí

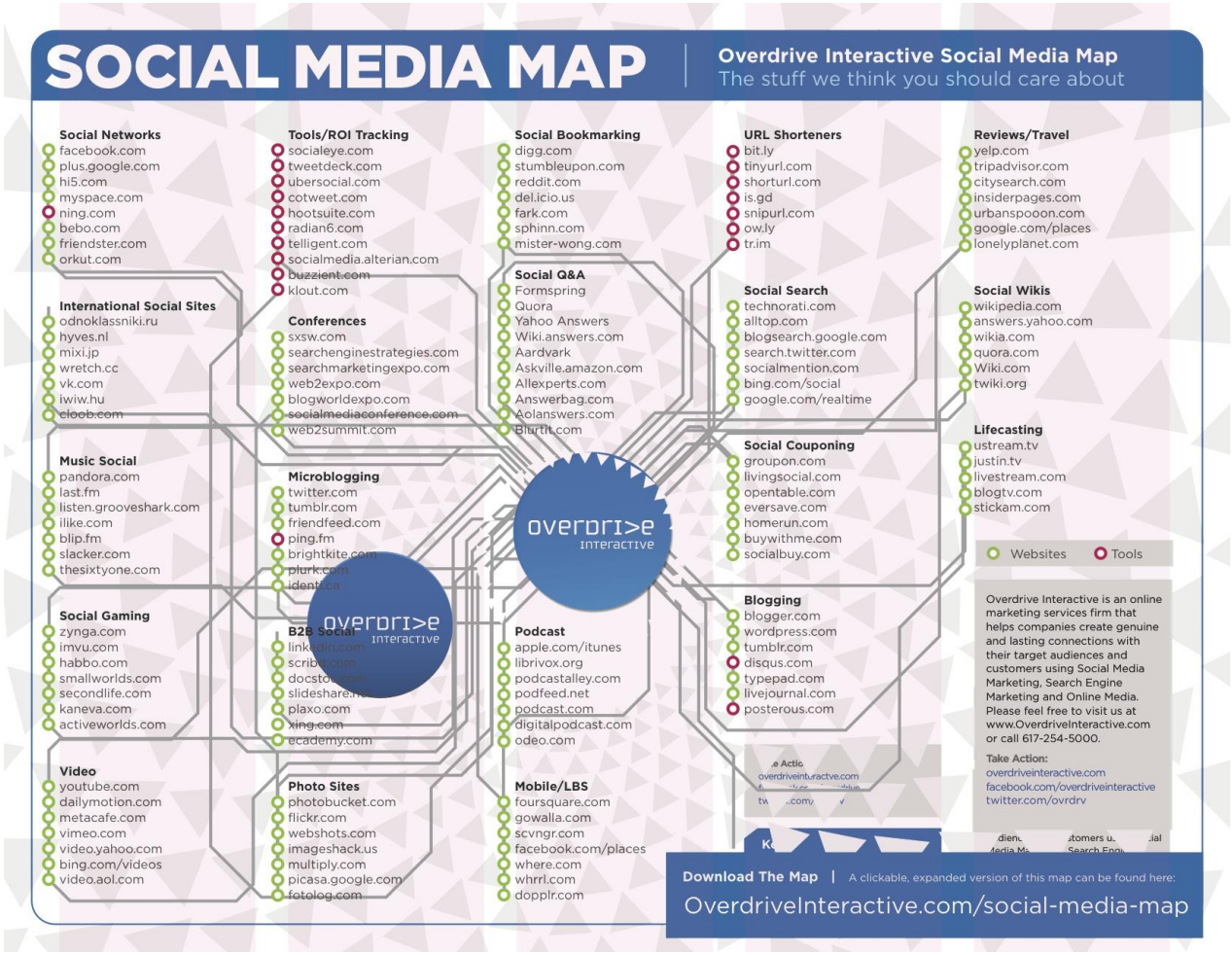
- Sexuální zneužívání dětí
- Komerční sexuální zneužívání dětí
- Dětská prostituce
- Dětská pornografie
- Obchod s dětmi
- Dokumenty, z kterých vychází EU pro boj se zneužíváním dětí:
- Úmluva o tom, kterak potírat rozšiřování necudných publikací (1910) vyhlášena pod č. 116/1912, Úmluva o potlačování obchodu s necudnými publikacemi a jejich rozšiřování (1923), Čl. 34 Úmluvy o právech dítěte (1989), Úmluva o zákazu a okamžitých opatřeních k odstranění nejhorších forem dětské práce (1999) a rámcové rozhodnutí Rady Evropské unie č.2007/68/VV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, Úmluva o počítačové kriminalitě.

1.2. Kyberterorismus

- Nejdestruktivnější forma kybernetické kriminality.
- Definice (D.E. Denning):
- Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaných v případě, že útok je konán za účelem zastrašit nebo donutit vládu nebo obyvatele k podporování sociálních nebo politických cílů.
- Kybernetický terorismus si klade za cíl především kolaps infrastruktury.

2. Sociální média – vítejte v džungli

- Sociální média je skupina internetových aplikací, které vychází z principů Web 2.0 a umožňují tvorbu a **výměnu** uživateli generovaného obsahu (UGC).
- Web 2.0 charakterizují především blogy, wikis a kolaborativní platformy.
- UGC stojí především na **publicitě**, kreativitě a originalitě (příspěvky, videa, články,…).



Zdroj: OverdriveInteractive.com/social-media-map

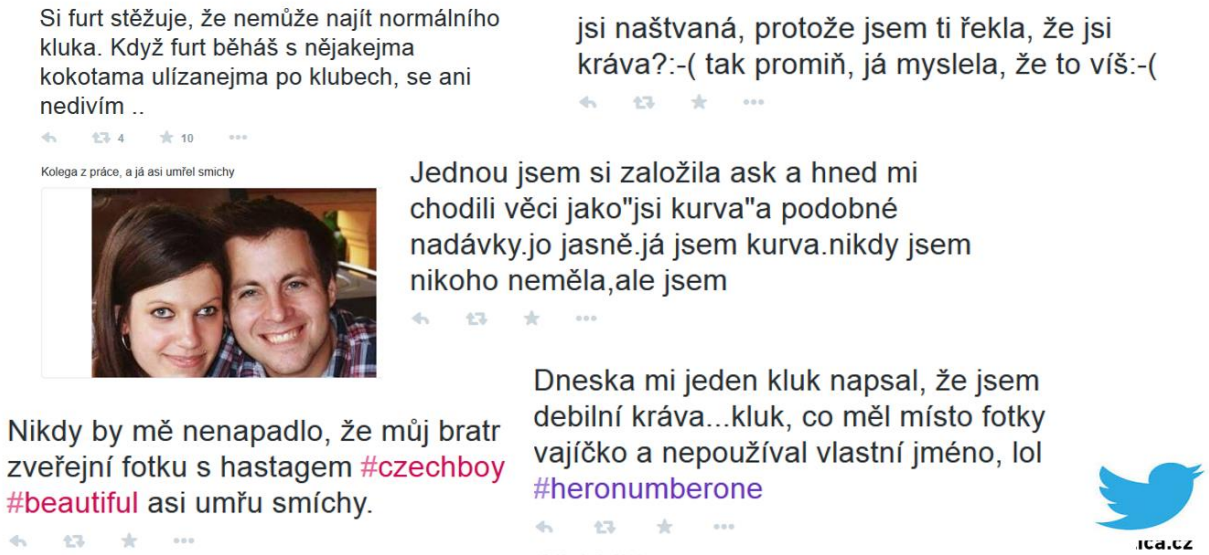
2.1. Typologie sociální médií

- Kolaborativní platformy
- Blogy (blogosféra)
- Mikroblogy (microblogging)
- Sociální sítě
- Content communities
- Virtuální sociální světy.

2.2. Twitter

- Nejznámější platforma pro microblogging
- Nejrychlejší médium současnosti pro přenos informace
- Krátké zprávy – 140 znaků
- Lze přidávat i fotografie
- V Česku cca 200 tisíc uživatelů
- 80 procent uživatel přistupuje na Twitter z mobilu.

Příklady zpráv na Twitteru

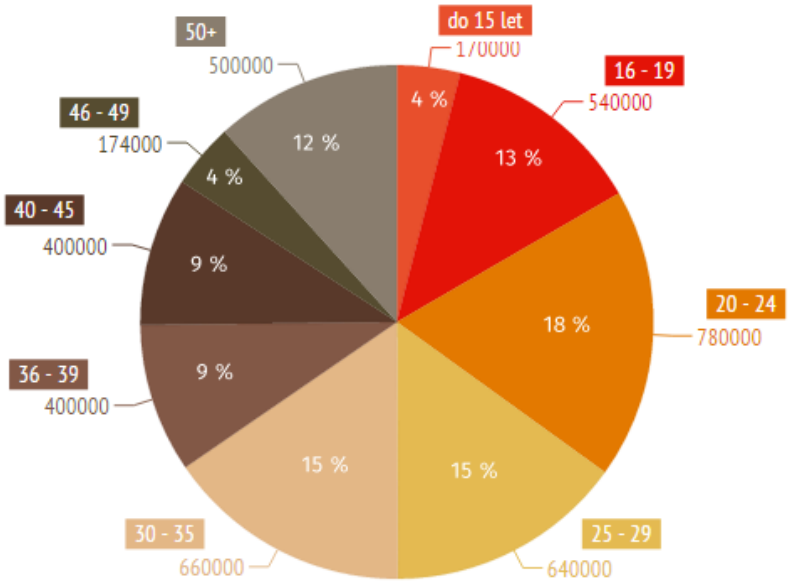


Zdroj: Klaboseni.cz

2.3. Facebook

- V Česku přes čtyři miliony uživatelů.
- Číslo stále narůstá a to zejména díky seniorům.
- Od 1. 1. 2015 nové podmínky pro zpracování a nakládání s osobními údaji.

Věkové složení českého Facebooku



Zdroje:
https://www.facebook.com/Effectix/photos/a.301856163511.148502.240346398511/10152489336598512/

Facebook a vztah rodičů a dětí

- Společnost Lab42 provedla zajímavý průzkum role Facebook v rámci rodiny.

Zdroj: Facemag.cz

Příklady negativních trendů poslední doby:

- Pražské roztahovačky
- Klátiči
- „Privátek“

- Den šikanování tlustých holek.

Zdroj: Facebook.com

Vlastní nás Facebook?

- Úprava pravidel nakládání s osobními údaji povede k absolutnímu ovládnutí digitální identity uživatele.
    - Pozor, s novými pravidly souhlasíte pouhým přihlášením se na Facebook.

Ochrana soukromí na FB v detailu

Facebook od roku 2015 rozlišuje:

- **Které z vašich informací vidí ostatní**

➢ Ovlivňování okruhu lidí, kteří uvidí váš příspěvek.

➢ Možnost smazání příspěvku.

➢ Váš profil pro každého podle vašich pravidel.

➢ Odstranění „označení“.

- **Jak s vámi komunikují ostatní**

➢ Váš příspěvek mohou hodnotit a komentovat pouze ti, kterým jste ho zveřejnili.

➢ Možnost blokace a odstranění „přátel“.

- **Co vidíte vy**

➢ Reklamy

➢ Ovlivňování obsahu v příspěvcích

Sice vše vypadá dobře, ale…

- Facebook – ve chvíli, kdy jste přihlášení – ví o tom, které stránky navštěvujete, co vyhledáváte, na co se díváte, co píšete.
- Facebook bude znát vaši GPS polohu a bude ji využívat pro cílení reklam.
- Facebook bude vlastnit všechny vaše napsané příspěvky, fotografie, videa a bude je moci použít.
- Facebook bude prodávat získaná data a zároveň získávat další informace o vás (třeba, co jste nakoupili a jak jste s produktem spokojení).
- Facebook vám nicméně bude určovat i to, co byste si měli koupit.

A dále…

- Facebook vlastní kompletní balík osobních informací o vás: jméno, telefonní číslo, e-mail, zájmy (i když je neprozrazujete).
- Vše Facebooku zůstane, i když svůj účet deaktivujete, ale i pokud se to rozhodnete odstranit.

2.4. Google+

- Sociální síť založená na sdílení obsahu v kruzích.
- Možnost vytvářet si vlastní soukromé i veřejné komunity.
- Neomezená záloha fotek z mobilního zařízení.
- Párty mód.
- Veřejné hangouty.

2.5. Youtube

- Počet českých uživatelů se odhaduje přes 5 milionů.
- Upload, sdílení, komentování videí, audio souborů.
- Striktní pravidla pro eliminaci nevhodného materiálu.
- Možnost omezení publikace komentářů.
- Příspěvky propojené se sítí Google+.

3. Zásady publikování a sdílení informací

Základní doporučení pro žáky, či studenty

- Už i celé jméno je poměrně hodně citlivá informace.
- Příspěvky spojené se jménem jednoduše navádí k lokaci.
- Určení lokace je přitom jedním z hlavních nebezpečí.
- Prakticky i nevinná informace o tom, co člověk snídal, může být počátkem různých forem on-line násilí. Fotografie jsou dnes hlavní entitou, která se sdílí. Zvažte opět ve vztahu k prozrazení místa působnosti, případně prozrazení absence v místě trvalého bydliště.
- Braňte slabší.

Základní doporučení pro pedagogy

- Komunikujte se žáky, či studenty v rámci sociálních médií.

- Používejte publikační nástroje v případě, že budete na více sítích.
- Otevřeně projevte zájem o sdílení v rámci nějaké ze sítí či platforem.
- Komentujte.
- Vzdělávejte je, řešte s nimi některé úlohy dálkově.
- Sdílejte i obsah, který zajímá vás (zpravodajství, videa ...).
- Nemějte strach z mnohdy opravdu pokročilých funkcionalit.
- Reagujte na negativní projevy.
- Osvěta od prvního stupně (i pro rodiče).
- Zvyšovat informační gramotnost.

Základní doporučení pro rodiče

- Sociální média nelze zakazovat, či nějak omezovat.
- Od útlého věku je třeba mluvit o jejich existenci a vlivech na společnost.
- Rozhodnutí, zda zveřejňovat fotografie s dětmi, důsledně promyslet.
- Neřešit rodinné problémy v rámci sociálních sítí.
- Zvolit pevná pravidla, co mohou děti sdílet.
- Aplikovat monitorovací nástroje pro sledování činnosti – celé rodiny.
- …a samozřejmě, nepodceňovat žádné riziko vzniku nebezpečné situace.

4. Bezpečné hledání na internetu

4.1. Webové prostředí

Rozlišujme:

- Povrchový web (Surface web)
- Hluboký web (Deep web)
- Temný internet (Dark internet).

Povrchový web

- Tvoří ho informace, které jsou schopny být indexovány.
- Obrovské množství informačního smogu a spamu.
- Avšak nepodceňovat z hlediska hodnotných informací.
- Časově náročné rešerše.
- Hlavní představitelé pro hledání: Google, Bing.

Deep web

- Dynamicky tvořená data a informací
- Prostředí pro získávání hodnotných analytických výstupů
- Zároveň místo pro nelegální činnosti
- Doporučení chránit svou identitu
- Databáze, databázová centra
- Pokročilý rešeršní jazyk
- Zdarma či placené.

Dark web

- Prostředí nedosažitelné pro běžného uživatele.
- Realizuje se zde nelegální obchod se zbraněmi, informacemi, drogami, ale rovněž lidmi.
- Pohyb výhradně s ukrytou identitou.

Nebezpečí povrchového webu

- Prostředí povrchového webu je velmi líbivé, problém je, že většina uživatelů neví, co je v pozadí.
- Problém vágního právního prostředí.
- Malé soubor cookies.
- Neprůhledný obchod s osobními daty v rámci tzv. třetích stran.
- Lze se bránit?

Digitální stopa

- Dva různé pohledy na problematiku digitální stopy, kterou za sebou tak, či onak zanecháváte:
    - Prozkoumejte, co jste publikovali, popřípadě, co o vás bylo zveřejněno.
    - Lze vědět, kdo nás sleduje právě v tuto chvíli?

4.2. Lepší informační bezpečnost

Základní nástroje a práce s nimi

Použitá literatura a zdroje

MEHAN, J. E. (2014). *Cyberwar, Cyberterror, Cybercrime & Cyberactivism (2nd Edition) An in-depth guide to the role of standards in the cybersecurity environment*. Ely, Cambridgeshire, IT Governance Ltd.

COHEN-ALMAGOR, R. (2015). *Confronting the Internet's dark side: moral and social responsibility on the free highway*.

NAVARRO, J. N., CLEVENGER, S., & MARCUM, C. D. (2015). *The intersection between intimate partner abuse, technology, and cybercrime: examining the virtual enemy*.

DENNER, J., & MARTINEZ, J. (2015). Children and Youth Making Digital Media for the Social Good.

https://www.facebook.com/

https://www.overdriveInteractive.com/social-media-map

https://www.klaboseni.cz

https://www.facemag.cz