PREVENCE RIZIKOVÉHO CHOVÁNÍ NA INTERNETU A SOUVISEJÍCÍ FENOMÉNY

KYBERŠIKANA, KYBERGROOMING, STALKING A KYBERSTALKING, RIZIKA SOCIÁLNÍCH SÍTÍ, SOCIOTECHNIKA A DALŠÍ RIZIKOVÉ JEVY

Doc. Mgr. Kamil Kopecký, Ph.D.

Základní tematický blok

STUDIJNÍ TEXTY K DISTANČNÍMU VZDĚLÁVÁNÍ

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Pedagogická fakulta

Univerzita Palackého v Olomouci

Tato publikace je výstupem projektu Kompetence leadera úspěšné školy, reg. č. CZ.02.3.68/0.0/0.0/16_032/0008145

Jméno řešitele: Ing. Alena Opletalová, Ph.D.

Název díla: Prevence rizikového chování na internetu a související fenomény
Autor: Doc. Mgr. Kamil Kopecký, Ph.D. a řešitelský kolektiv projektu Centra celoživotního vzdělávání Pedagogické fakulty Univerzity Palackého v Olomouci.

URL autora: www.ccv.upol.cz
URL odkaz na původní dílo: www.klus.upol.cz

PREVENCE RIZIKOVÉHO CHOVÁNÍ NA INTERNETU A SOUVISEJÍCÍ FENOMÉNY

OBSAH

CÍLE DISTANČNÍHO TEXTU

Cílem distanční textu je seznámit vedoucí pedagogické pracovníky s ústředními problémy spojenými s prevencí rizikového chování v online prostředí, především s fenomény:

- kybernetická šikana,
- kybergrooming,
- sexting,
- nebezpečné výzvy v online prostředí,
- rizikové služby a aplikace.

1 RIZIKOVÉ JEVY SPOJENÉ S VYUŽÍVÁNÍM INTERNETU

1.1 Úvod do problematiky rizikových forem chování v online prostředí

Děti a dospělí se v online prostředí setkávají s celou řadou rizikových fenoménů, které jim mohou způsobit psychickou i fyzickou újmu. K nejčastějším rizikovým formám chování, kterým jsou děti na internetu vystaveny, pak patří především kyberšikana, kybergrooming, rizikové online výzvy a problematický sexting.

1.2 Kybernetická šikana

Kyberšikana je forma agrese, která se uplatňuje vůči jedinci či skupině osobs použitím informačních a komunikačních technologií (počítačů, tabletů, mobilních telefonů a dalších moderních komunikačních nástrojů) a ke které dochází opakovaně ať už ze strany původního agresora, či dalších osob – tzv. sekundárních útočníků (např. opakované sdílení nahrávky, opakované komentování apod.).

Ačkoli je kyberšikana zpravidla definována jako činnost záměrná, může vzniknout i nezáměrně – např. jako nevhodný vtip, který se v on-line prostředí vymkne kontrole. Kyberšikana je často zaměňována s tzv. on-line obtěžováním. Termínem on-line obtěžování označujeme jednorázové útoky, jejichž dopad je pouze dočasný. „Opravdová" kyberšikana musí splňovat zejména kritéria opakovanosti, musí být dlouhodobá a musí být vnímána jako ubližující. Oběť se pak nedokáže útokům účinně bránit, existuje mocenská nerovnováha.

1.2.1 Základní formy kyberšikany a příbuzné fenomény

Kyberšikana mnohdy začíná jako tradiční šikana (psychická nebo fyzická), případně je jejím doprovodným jevem. Může však existovat zcela nezávisle na tradiční šikaně.

Mezi základní formy kyberšikany z pohledu propojení útočníků a obětí patří:

- **Kyberšikana přímá**

U přímé kyberšikany agresor útočí na oběť přímo, bezprostředně, začne např. dehonestovat oběť, založí o ní falešný profil, zveřejní její fotografie či video apod.

- **Kyberšikana nepřímá (kyberšikana v zastoupení, tzv. cyberbullying-by-proxy)**

U nepřímé kyberšikany agresor k útoku využívá jinou osobu, která často neví o tom, že se stala nástrojem útoku – např. pomsty. Typický příklad představuje situace, kdy útočník pronikne na účet oběti (např. účet na sociální síti), prostřednictvím tohoto účtu začne dehonestovat ostatní uživatele, kteří začnou reagovat a mstít se za on-line urážky právě majiteli účtu, z něhož byly dehonestující zprávy odeslány. Majitel účtu se o tomto dozví až s časovou prodlevou.

V případě obou forem kyberšikany může pachatel využívat jak své vlastní identity, tak identity falešné.

Kyberšikanu lze dále rozdělit podle toho, zda je do ní aktivně zapojeno publikum, nebo zda probíhá v soukromí bez přítomnosti publika.

Mezi základní formy tedy patří:

- **Kyberšikana s přítomností publika (veřejná)**

Jde o kyberšikanu, jejíž podstatou je rozšířit informace o oběti mezi velké množství uživatelů. Do této kategorie lze

zařadit publikování ponižujících záznamů oběti, krádeže identity, verbální formy kyberšikany (dehonestování, urážení, provokování) apod. Přítomnost publika je základní obligatorní součástí kyberšikany. Komunikace probíhá prostřednictvím veřejných komunikačních kanálů.

- **Kyberšikana bez přítomnosti publika (soukromá)**

Jde o kyberšikanu, v níž zpravidla komunikuje pouze pachatel a oběť, přičemž jejich komunikace je soukromá, bez přítomnosti publika. V rámci této formy kyberšikany často dochází k výměně intimních materiálů – ať již dobrovolné, nebo pod nátlakem. Do této kategorie lze zařadit kyberšikanu ve formě vydírání či vyhrožování. Komunikace probíhá prostřednictvím soukromých komunikačních kanálů – soukromého chatu v rámci sociálních sítí, instant messengerů a VoIP komunikátorů (Skype), případně prostřednictvím SMS/MMS. Projevy kyberšikany (např. dehonestování, provokování, vyhrožování, vydírání v on-line prostředí atd.) se mohou vyskytovat ve formě jednorázového útoku (tzv. nepravá kyberšikana, kyberobtěžování, kyberagrese apod.) nebo dlouhodobého útoku se vzrůstající intenzitou (tzv. pravá kyberšikana). Mezi nejznámější projevy/formy kyberšikany (Kopecký, Szotkowski, & Krejčí, 2014; Krejčí, 2010; Willard, 2007) patří především útoky využívající fotografií, videozáznamů, audiozáznamů, ale také běžné verbální formy útoků.

Mezi kyberšikanu řadíme projevy tradiční psychické šikany posílené využitím ICT, například:

- Dehonestování (ponižování, nadávání, urážení) v on-line prostředí.
- Vyhrožování a zastrašování v on-line prostředí.
- Vydírání v on-line prostředí.
- Očerňování (pomlouvání) v on-line prostředí.

Mezi typické formy kyberšikany také patří:

- Publikování ponižujících videozáznamů, audiozáznamů nebo fotografií.
- Ponižování a pomlouvání (denigration).
- Krádež identity (impersonation) a její zneužití.
- Ztrapňování pomocí falešných profilů. Provokování a napadání uživatelů v online komunikaci (flaming/bashing).
- Zveřejňování cizích tajemství s cílem poškodit oběť (trickery/outing).
- Vyloučení z virtuální komunity (exclusion).
- Obtěžování (harassment).
- Specifické formy kyberšikany spojené s hraním on-line her.
- Happy slapping (v *překladu* „zábavné fackování").
- Kyberstalking (pronásledování ve spojení s využitím informačních komunikačních technologií).
- Webcam trolling (zneužívání webkamer pro manipulaci uživatelů internetu prostřednictvím podvržených videozáznamů).

1.2.2 Jak předcházet kyberšikaně

Kyberšikanu lze zařadit mezi základní oblasti rizikového chování, konkrétně mezi šikanu a extrémní projevy agrese (Miovský, 2010), dle Národní strategie primární prevence rizikového chování dětí a mládeže 2013-2018 se řadí mezi interpersonální agresivní chování (MŠMT, 2013).

Základním způsobem, jak lze předcházet kyberšikaně či minimalizovat její dopad, je především všeobecná primární prevence. Cílem primární prevence je předcházet rizikovému chování. Prevenci zaměřenou na oblast kyberšikany a dalších forem kybernetické agrese lze realizovat ve formě *specifické* i *nespecifické*.

Specifickou primární prevenci lze rozdělit do 3 úrovní na:

- **Prevenci všeobecnou** (zasahuje celou třídu, školu apod. bez rozdílu). Sem lze zahrnout aktivity typu dlouhodobé preventivní programy, interaktivní besedy, projektové dny atd. Zároveň lze témata primární prevence zahrnout do výuky, propojit s průřezovými tématy a klíčovými kompetencemi žáka.
- **Prevence selektivní** (zasahuje osoby, u kterých jsou ve zvýšené míře přítomny rizikové faktory pro vznik a vývoj různých forem rizikového chování, např. děti z vyloučených lokalit, děti s poruchami chování apod.).
- **Prevence indikovaná** (zacílena na situace, kdy se ve třídě/škole již kyberšikana vyskytla).

Nespecifická prevence je pak zaměřena na **rozvoj zdravého klimatu ve třídě a škole, posilování dobrých vztahů mezi dětmi** apod.

Jak předcházet kyberšikaně na úrovni školy:

- Zanést do školního řádu pravidla používání ICT, intranetu a mobilních telefonů (během vyučování, o přestávkách, v areálu školy).
- Informovat žáky o netiketě a „listině práv na internetu". O této listině by měli být informování i rodiče nezletilých žáků, např. vyvěšením na webových stránkách škol.
- Instalovat a využívat software, který v učebnách vyučujícímu umožňuje informovat se přes svůj počítač, co právě žák na své ploše dělá. (Informovat o tomto opatření žáky a systém nezneužívat!)
- Být vzorem vhodného užívání moderních technologií.
- Pracovat na povědomí žáků o rizikovém chování na internetu.
- Definovat kompetence v rámci školy a na akcích konaných školou mimo místo, kde se uskutečňuje vzdělávání.
- Začlenit témata spojená s rizikovým chováním na internetu do výuky.
- Vzdělávat pedagogy.
- Podporovat pozitivní využívání technologií.

Jak předcházet kyberšikaně na úrovni jednotlivých pedagogů:

- Posilovat empatii mezi žáky.
- Pracovat na klimatu třídy, školy.
- Vést k úctě k druhým lidem.
- Dávat žákům pozitivní zpětnou vazbu.
- Vytvářet dobré vztahy mezi žáky i kolegy.
- Důsledně zakročovat vůči rozeznatelným individuálním projevům agrese.

1.3 Kybergrooming

Termín kybergrooming (child grooming, online grooming) označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce v reálném světě. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Kybergrooming je vlastně druhem psychické manipulace, ve které komunikuje dospělý uživatel (často pod falešnou identitou) s dítětem, přičemž využívá celou řadu strategií, např. zrcadlení (mirroring), phishing, profilování oběti, vábení a uplácení (luring), strategie snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace, izolační metody, strategie manipulace dětí prostřednictvím fotografií opačného pohlaví, webcam trolling apod.

Kybergrooming zahrnuje řadu trestných činů, jako je nebezpečné vydírání, sexuální nátlak, navazování nedovolených kontaktů s dítětem apod.

1.4 Sexting

Termín sexting označuje dobrovolné sdílení vlastních intimních materiálů (fotografií, videí, má však i textovou podobu), a to zpravidla v on-line prostředí. Ačkoli se sextingu věnují především dospělí, a to především v rámci partnerských vztahů, stále častěji se s ním setkáváme také u dětí základních škol.

Se sextingem je spojena celá řada rizik – v on-line prostředí snadno ztratíme kontrolu nad šířeným materiálem, materiály mohou po internetu kolovat desítky let, sexting může poškodit naši prestiž a může způsobit dokonce ztrátu zaměstnání, v rámci sextingu se můžeme stát pachateli přestupků či trestných činů (výroba, přechovávání, šíření dětské pornografie, ohrožování výchovy dítěte, nově např. navazování nedovolených kontaktů s dítětem, sexuální nátlak apod.), sexting je součástí kyberšikany, kybergroomingu a dalšího rizikového chování v on-line prostředí.

Podle zákona je dítětem osoba mladší 18 let. Pokud osoba mladší 18 let pořizuje nebo zveřejňuje materiály sexuální povahy (textové, obrazové, videa apod.), může se sama dopustit výše uvedených trestných činů.

1.5 Nebezpečné výzvy v online prostředí (challenges)

V prostředí internetu se setkáváme s velkým množstvím výzev, které často nabádají k nebezpečnému chování, které může způsobit uživatelům internetu (především dětem a dospívajícím) vážnou zdravotní újmu.

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

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

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

1.6 Rizikové služby a aplikace

1.6.1 Tik Tok (Musical.ly)

V minulých letech poměrně pravidelně poradna projektu E-Bezpečí zachycovala případy kyberšikany, které se odehrály v prostředí online služby Musical.ly. Služba Musical.ly byla primárně zaměřena na sdílení krátkých několikavteřinových videí, zaměřených většinou na hudební produkci či reprodukci. Každý uživatel Musical.ly pak mohl sdílet s ostatními třeba svá domácí videa a amatérské hudební videoklipy doplněné o různé filtry a efekty. Původní síť Musical.ly byla před více než rokem nahrazena novou službou/aplikací/sítí s názvem Tik Tok. A právě na ni se v textu zaměříme.

V roce 2017 se Musical.ly přerodilo ve službu Tik Tok (akvizicí čínskou společností ByteDance, čínská verze Tik Toku se jmenuje Douyin), přičemž původní uživatelské účty byly zachovány, proměnila se samotná aplikace, změnila se také podoba on-line portálu a přibylo několik nových funkcí. V současnosti Tik Tok využívá měsíčně přibližně půl miliardy

uživatelů z celého světa. Tik Tok patří k 6 nejstahovanějším aplikacím světa, v roce 2018 dokonce dominoval mezi aplikacemi pro iPhony (AppStore).

Tik Tok používá také stále více uživatelů z ČR, a to především děti, přičemž Tik Tok častěji využívají dívky (poradna E-Bezpečí zachytila případy, v nichž byly oběťmi útoku téměř výhradně nezletilé dívky). Veškerá videoprodukce, kterou děti (i dospělí) na Tik Tok umisťují, se v základním nastavení aplikace stává zcela veřejnou a snadno šiřitelnou. Aplikace je extrémně jednoduchá – nepotřebujete žádné uživatelské účty, máte okamžitý přístup k nekonečnému streamu videí, vše lze snadno sdílet, lajkovat, komentovat, tagovat, uploadovat, aplikovat filtry apod.

Velmi lákavou funkcí Tik Toku představují tvz. duety (duets) – uživatelé natočí pouze část videa (s využitím funkce lip-sync, tj. synchronizace hudby/slova a pohybu rtů) a pomocí hashtagu #duetwithme propojí své video s dalšími uživateli, kteří vytvořili druhou část hudebního videa. Výsledkem je pak video složené z obou částí. Samozřejmě tato funkce svádí k velkému množství parodování (tzv. ironic memes) a velkou část obsahu na Tik Toku tvoří právě různé druhy parodických videí.

Stejně jako u ostatních služeb, ve kterých děti sdílejí svůj vlastní videoobsah, se i v prostředí Tik Toku objevuje celá řada problémů – od kybernetické agrese a kyberšikany, přes úniky či cílené nahrávání sexuálně laděného (či přímo pornografického) obsahu, po různé druhy obtěžování, vydírání, zesměšňování apod. Ačkoli má Tik Tok nastaven věkový limit 16 let (nemluvě o regulaci EU v rámci GDPR), je – stejně jako ostatní služby podobného typu – využíván podstatně mladšími uživateli. Podle údajů DigiDay tvoří polovinu uživatelů Tik Toku věková skupina 13 až 24 let.

Jedním z problémů, který postihuje Tik Tok (ale na nějž narazíme např. i na serveru YouTube), patří úniky videí velmi malých dětí (do 11 let věku), která obsahují sexuálně explicitní obsah. Tik Tok totiž cílí především na taneční/hudební videa, kde se děti pohybují – třeba poskakují na posteli, dělají různé taneční kreace apod. Na záznamu se pak často objeví i obnažené části těla dítěte, které přitahují pozornost sexuálních abuzérů. A právě tato videa mají velmi vysokou návštěvnost a jsou cíleně vyhledávána, sdílena a rozšiřována. Děti se pak stávají vyhledávaným cílem a jsou prostřednictvím Tik Toku oslovovány dospělými uživateli. Následují žádosti o zaslání dalších sexuálně explicitních fotografií apod.

Na tento problém upozorňuje např. reportáž ABC News: Tatínek 7leté uživatelky Tik Toku upozorňuje na to, že byla jeho dcera neznámým uživatelem prostřednictvím mobilní aplikace oslovena a vyzývána k poskytnutí erotické fotografie s tím, že to bude jejich společné tajemství. Nejde o ojedinělý případ, na rizikovou komunikaci tohoto typu upozorňuje celá řada organizací, které se online bezpečností zaměřenou na dětské uživatele internetu zabývají. Varování před sexuálními predátory na Tik Toku vydala také např. francouzská policie, která v souvislosti s Tik Tokem zachytila řadu obdobných případů.

Na Tik Toku nalezneme také velké množství nevhodného obsahu, jako např. stovky sexuálně explicitních videí zachycujících velmi malé děti (pod 12 let věku), klasickou pornografii zachycující dospělé (např. záznamy masturbujících mužů podle vzoru známého videochatu Omegle), videa zachycující tzv. killingstalking („umělecká videa" zachycující chlapce, kteří si vzájemně přikládají nože na hrdla, předstírají vzájemné týrání apod. – zde je zjevná inspirace stejnojmenným manga-komiksem Killing Stalking o sadistickém vrahovi, který unese a následně týrá svou oběť; na Tik Toku zpracováno jako cosplay). Tik Tok také obsahuje videa zaměřená na sebepoškozování (hashtagy #selfharm, #cutter, #selfhate), videa zachycující různé způsoby, jak spáchat sebevraždu (#suicide), videa zaměřená na anorexii (hashtag #anorexic), ale také morbidní obezitu. Všudypřítomný je samozřejmě hating všeho druhu.

Samotnou kapitolu videí pak tvoří různé druhy výzev – ať již jde o výzvy bezpečné a zábavné, až po výzvy nebezpečné (např. salt and ice challenge). Velmi časté jsou různé druhy adrenalinových videí, ve kterých jejich tvůrci žádají lajky (hearts,

srdíčka) právě za to, že riskovali svůj život – ve snaze získat adrenalinové video pro publikaci na Tik Toku se např. procházeli po nebezpečných římsách domů, vylézali na mosty, skákali před rozjetá auta a autobusy (např. v rámci populární výzvy Nillu Nillu Challenge) aj. Za svou „odvahu" pak získávají lajky/srdíčka, a to daleko snadněji než např. na Facebooku či Instagramu. Aby toho nebylo málo, k přístupu ke konkrétnímu typu závadného obsahu jsou využívány speciální hashtagy, v řadě případů totiž umělá inteligence videa, která jsou tagována srozumitelným způsobem, blokují. Proto se pro přístup k závadnému obsahu využívají např. hashtagy: #sxy, #thot, #whooty, #sin, #proana, #asset apod.

Cílení Tik Toku na dětské uživatele je zřejmé hned po spuštění aplikace – důraz je kladen na audiovizuální složku, videa jsou velmi krátká (15 sekund), poutavá, energická, často velmi bizarní, plná efektů (filtrů), textová složka téměř úplně chybí. Pozornost není vůbec potřeba, jako uživatelé jste doslova zahlceni nekonečným tokem audiovizuálních dat – sledujete poměrně šílený spektákl, který zvláště vynikne v podobě různých kompilací toho „nejlepšího" z Tik Toku. Ale mladé uživatele online služeb Tik Tok zcela jasně bavit bude…

1.6.2 Instagram

Z Instagramu se stala nejrychleji rostoucí sociální síť na světě. Aplikace, která patří společnosti Facebook, v loňském roce překročila 1 miliardu aktivních uživatelů, čímž dosáhla na třetí místo pomyslného žebříčku. Z obyčejné fotogalerie se tak stal účinný marketingový nástroj, který se potýká s rizikovými jevy.

Instagram je sociální síť ve formě volně dostupné aplikace, která slouží ke sdílení fotografií či videí. Vznikla v roce 2010 a o dva roky později ji koupila americká společnost Facebook, která ji proměnila v jednu z nejrychleji rostoucích sociálních sítí na světě. Aplikaci lze používat na chytrém telefonu (smartphonu) či tabletu s operačním systémem iOS (Apple), Android, Windows Phone ad. Instagram má i svou webovou podobu, ovšem nejedná se o plnohodnotnou náhradu aplikace.

Tato sociální síť se v základu neliší od těch ostatních. Jakmile si vytvoříte vlastní profil, můžete jej začít plnit audiovizuálním obsahem. Stejně jako na Facebooku i zde najdeme zeď, na které se zobrazují fotografie a videa ostatních uživatelů. Abyste tento obsah viděli, je potřeba ostatní uživatele vyhledat a potvrdit odběr pomocí tlačítka Sledovat. Příspěvkům můžete dát „lajk" v podobě srdíčka nebo je doplnit komentářem. Každý profil, včetně popisu (BIO), obsahuje tři základní údaje: počet příspěvků, počet uživatelů, kteří sledují daný profil, a počet profilů, které dotyčný sám sleduje.

K čemu je Instagram vlastně dobrý? Primární funkcí je zábava. Lidé s touto aplikací tráví i několik hodin denně a hledají atraktivní materiál, který je díky této sociální síti daleko dostupnější. Díky svému minimalistickému vzhledu a bohaté nabídce funkcí se pro mnoho uživatelů stal náhradou za tradiční blog. Pokud ovšem nechcete, aby vás na Instagramu sledoval někdo, koho neznáte, máte možnost nastavit svůj účet jako soukromý. Vaše příspěvky poté uvidí jen ti, kterým jste v aplikaci udělili povolení.

Celebrity a další veřejně známé osobnosti využívají tuto platformu jako sdělovací prostředek. Důležitou roli v tom hrají tzv. hashtagy, označované znakem #. Slova, která jsou takto označena, pod sebou sdružují veškerý obsah, který uživatelé na Instagramu takto označili. Díky tomu vznikají komunity, které mají společné zájmy a chtějí se podělit o své fotografie, zážitky či zkušenosti (např. cestovatelé).

Velké popularitě se těší i novinka z roku 2016 – Instagram Stories. Tuto funkci přebral Instagram z aplikace Snapchat a najdeme ji dnes i na Facebooku. Příběhy (Stories) tvoří fotky a videa s možnostmi úprav, které u běžných příspěvků provádět nelze. Takto zveřejněný obsah bude viditelný max. 24 hodin, poté zmizí.

Instagram během roku 2018 přesáhl 1 miliardu aktivních uživatelů za měsíc. V České republice jde přibližně o 2,2 miliónů uživatelů. Díky tomu sez něj stal silný hráč na poli digitálního marketingu. Spousta firem a podnikatelů tak za pomoci

speciálních funkcí a placené reklamy oslovuje značnou část uživatelů. S těmi dále komunikují skrz komentáře a soukromé zprávy (direct messages). To jim zvyšuje popularitu a následně prodej. Účinným nástrojem jsou také influenceři, tzv. „vlivní uživatelé", kteří díky své popularitě a velikosti svého publika dokážou ovlivnit chování uživatelů.

V čem spočívají rizika Instagramu? Stejně jako jiné sociální sítě i Instagram se potýká s rizikovými jevy, jako jsou kyberšikana, kybergrooming nebo šíření poplašných zpráv a dezinformací (fake news). Problémem může být i nadměrně strávený čas na Instagramu. V souvislosti se stále novými možnostmi a funkcemi aplikace se značně zvyšuje doba, kterou zde uživatel tráví, což ve výsledku je i cílem této platformy. Instagram proto může napomáhat k závislostnímu chování – netolismu.

Velkým rizikem, které s sebou nese tato a podobné sociální sítě, je pořizování perfektních snímků. Mnoho uživatelů se nebojí proniknout na nepřístupná či nebezpečná místa a jdou až za hranu svých schopností jen proto, aby získali unikátní fotografii. Ta jim totiž zaručí hromadný přísun „lajků" v podobě srdíček a nemálo nových sledujících. Že jde o nebezpečný trend, dokazují i statistiky. V letech 2011 – 2017 zemřelo na celém světě více než 260 lidí kvůli selfie. Nejčastější příčinou těchto úmrtí bylo utonutí, například pád do prudké řeky, nebo dopravní nehody, pády z výšek a útoky zvířat.

V neposlední řadě se můžeme setkat i s krádeží uživatelského účtu. Tyto útoky jsou nejčastěji cíleny na veřejně známé osoby, ale nevyhýbají se ani běžným uživatelům. Ne vždy je totiž napadený účet ukraden, ale jen tiše využíván např. pro sledování dalších účtů. Lehce se tak může stát, že budete sledovat stovky profilů, které budou fake nebo zcela nevhodné. Předejít těmto útokům lze pomocí dvoufázového ověření, jež Instagram nabízí. Vyplatí se také být obezřetný a neposkytovat podezřelým aplikacím přístup k vašemu účtu.

SHRNUTÍ

- Internet může být dobrým sluhou, ale zlým pánem, proto je třeba chránit si v online světě své soukromí a nesdílet informace, které by nás mohly v budoucnu poškodit.
- Dávejme vždy pozor na to, s kým se v online prostředí seznamujeme. Uživatel či uživatelka, s nimiž v online světě komunikujeme, nemusí být těmi, za které se vydávají!

POUŽITÁ LITERATURA

KOPECKÝ, Kamil. Kybergrooming. [online]. Olomouc: E-Bezpečí, 2019 [cit. 2019-04-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/trivium/71-trivium/1421-co-je-kybergrooming

KOPECKÝ, Kamil. Kybernetická šikana (kyberšikana) [online]. Olomouc: E-Bezpečí, 2019 [cit. 2019-04-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/trivium/71-trivium/1418-co-je-kybersikana

KOPECKÝ, Kamil. Problém zvaný Tik Tok. [online]. Olomouc: E-Bezpečí, 2019 [cit. 2019-04-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1403-problem-zvany-tik-tok

KOPECKÝ, Kamil. Sexting. [online]. Olomouc: E-Bezpečí, 2019 [cit. 2019-04-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/trivium/71-trivium/1422-co-je-sexting

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. *Nebezpečí internetové komunikace III.* 1. vyd. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2012, 60 s. ISBN 978-80-244-3087-4.

KREJČÍ, Veronika. KYBERŠIKANA: KYBERNETICKÁ ŠIKANA [online]. Olomouc, 2010 [cit. 2019-04-22]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studieatd?download=14%3Akybersikana-studie

KUBALA, L. Facebook umírá, žezlo přebírá Instagram. [online]. Olomouc: E-Bezpečí, 2019 [cit. 2019-04-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1440-facebook-umira-zezlo-prebira-instagram

MIOVSKÝ, Michal et al. *Primární prevence rizikového chování ve školství: [monografie*. Vyd. 1. Praha: Sdružení SCAN, ©2010. 253 s. ISBN 978-80-87258-47-7.

WILLARD, Nancy. *Cyberbullying and cyberthreats. Responding to the challenge of online social aggression, threats and distress.* USA: Research Press, 2007.

PdF UP v Olomouci, Žižkovo nám. 5, 771 40 Olomouc

CENTRUM
CELOŽIVOTNÍHO
VZDĚLÁVÁNÍ

Centrum celoživotního vzdělávání

www.ccv.upol.cz