GYMNÁZIUM, NOVÝ BYDŽOV, KOMENSKÉHO 77

Seminární práce

2017 Roman Šedivý

GYMNÁZIUM, NOVÝ BYDŽOV, KOMENSKÉHO 77

Kyberkriminalita

Zpracoval: Roman Šedivý

Adresa: Selských Bouří 773/IV

503 51 Chlumec nad Cidlinou

**Prohlášení:**

Prohlašuji, že jsem seminární práci „Kyberkriminalita“ vypracoval samostatně s využitím literatury uvedené v seznamu použité literatury.

31. 3. 2017 Roman Šedivý

Anotace

Seminární práce se zaměřuje na páchání trestních činů pomocí sociálních sítí. V teoretické části práce jsou popsány jednotlivé trestné činy a způsob jak se proti nim bránit. V praktické části jsem zjistil, že většina lidí vystavuje fotografie a osobní údaje bez jakéhokoliv zabezpečení.

Klíčová slova

Kyberkriminalita, kyberšikana, kyberstalking, kybergrooming

Title

Cyber crimes

Annotation

Seminar work focuses on committing crimes using social networks. The theoretical part describes the various criminal acts and the way how to defend against them. In the practical part I have found that most people exhibits photos and personal information without any security.

Keywords

Cybercrime, cyberbullying, cyberstalking, cybergrooming

Obsah

[Úvod - 6 -](#_Toc478927171)

[1 Kyberkriminalita na sociálních sítích - 7 -](#_Toc478927172)

[1.1 Kyberšikana - 8 -](#_Toc478927173)

[1.2 Kybergrooming - 9 -](#_Toc478927174)

[1.3 Kyberstalking - 10 -](#_Toc478927175)

[1.4 Prevence - 11 -](#_Toc478927176)

[1.5 Obrana - 13 -](#_Toc478927177)

[2 PRAKTICKÁ ČÁST - 14 -](#_Toc478927178)

[Závěr - 18 -](#_Toc478927179)

[Použitá literatura - 19 -](#_Toc478927180)

Úvod

Trestná činnost způsobená prostřednictvím informačních sítí představuje závažný problém. Z důvodu nárůstu trestných činů souvisejících kromě jiného s neoprávněným zachycením informací, porušením autorského práva se jeví jako přirozený důsledek podrobnější zaměření právní normy na tuto oblast, kterou charakterizuje rychlý vývoj. Rychlost se tedy musí následně promítat i do tvorby právních norem. Závažná je i otázka možností vynucování postihu porušení těchto norem spojená s problematikou ukládání trestu zákazu přístupu k internetu či zákazu užívání počítače. V souvislosti s rozšiřujícími se kybernetickými hrozbami roste také potřeba prevence a je nutné zajistit dostatečné povědomí o souvisejících rizicích pro všechny uživatele kybernetického prostoru.

1. Kyberkriminalita na sociálních sítích

Sociální sítě neustále nabývají na významu a v současnosti ovlivňují život téměř každého člověka. Jejich prostřednictvím můžete být v kontaktu s kýmkoliv a v podstatě kdykoliv a kdekoliv. Není proto divu, že „být online“ je pro někoho alfou a omegou každého dne. Bezesporu jsou návykové a ne každý si uvědomuje, co a s kým na sociálních sítích sdílí. „Emailová adresa, datum narození včetně měsíce a dne a další, jsou tak návnadou pro zneužití informací třetí stranou. Pocit bezpečí, intimity a do jisté míry i anonymity nabádá uživatele k neomezené otevřenosti a sdílnosti. Píší tak o sobě věci, které bychom druhé osobě při osobním kontaktu jen stěží prozradili nebo naopak sdělují věci pro ostatní uživatele nezajímavé (např. co měli k obědu, co se jim v noci zdálo apod.). Průměrný dnešní uživatel Facebooku má 133 přátel a vzhledem k množství příspěvků, kdy každý den jeden každý jeho přítel napíše několik příspěvků, je obtížné z nich vyfiltrovat ty kvalitní a informačně přínosné. Přitom zaregistrovat se na sociální síti zvládne skoro každý. Díky tomu se na sociálních sítích shromažďují obrovská množství cenných osobních dat, u kterých uživatel často ani neví, kdo si je může přečíst a jak s nimi dále naloží. A to s sebou přináší nebývalá rizika. Proto je třeba dbát na to, co vlastně chcete zveřejnit a zda je vůbec rozumné takový příspěvek zveřejňovat. K publikování informací vás nikdo nenutí, publikujete je tedy sami a dobrovolně. Uživatel sám rozhoduje, jaké informace dá o sobě vědět světu. Může se tak snadno stát obětí kyberstalkera, protože mu všechny informace, které může zneužít, lehce dodá. U informací, které o vás zveřejňují vaši přátelé to tak jednoduché není. Uživatel sociální sítě si nemusí všimnout, že o něm kamarád napsal status, vložil fotografii nebo video. To může danou osobu doslova kompromitovat nebo se zveřejněním nemusí souhlasit. I když to uživatel po dohodě smaže, vždy se tak stane ať s určitým prodlením (pár minut, ale i měsíce), v rámci kterého si takové informace ostatní uživatelé mohou prohlédnout, komentovat nebo sdílet. To může vést ke stažení kompromitující fotografie nebo videa s možným následným vydíráním nebo ke kyberšikaně. Ne vždy se na síti setkáte s profilem, který vlastní právě ta osoba, která je na fotografiích. Může se jednat o podvodný profil vytvořený někým cizím, klidně i z jiného kontinentu a jím prezentovaná identita je kradená. Často bývá falešný profil vytvořen se záměrem někoho pošpinit, způsobit škodu nebo ji zneužít. Profily mohou působit velmi věrohodně a odhalit falešný profil je tak obtížné. Profily na sociálních sítích mohou být vytvořeny i na fiktivní identitu, tedy na neexistujícího, vymyšleného člověka.

* 1. Kyberšikana

Kyberšikana je palčivý problém, který se rychle rozšiřuje i do českých škol a dětských kolektivů. Obecně se jako kyberšikana označuje užití komunikační a informační technologie, zejména mobilních telefonů a Internetu, k úmyslnému ublížení druhým. Přečtěte si, jak konkrétně se může kyberšikana projevovat. Kybernetická šikana má stejný cíl jako klasická fyzická šikana: ublížení a ponížení oběti. Kybernetická šikana přitom ale používá jiné prostředky, kromě toho se ale od klasické šikany liší dalšími rysy.

Rysy kyberšikany :

**ANONYMITA**– Agresor se méně bojí přistižení a trestu.

**NEOMEZENOST ÚTOKU**  
- časová – 24 hodin denně, 7 dní v týdnu.  
- prostorová – Osobní setkání není nutné, je možné šikanovat online.  
**PROFIL AGRESORA A OBĚTI** – fyzická převaha nebo věkový rozdíl nehrají roli, obětí útoků nemusí být jen outsider.

**„OSLOVENÍ“ ŠIROKÉHO PUBLIKA** – prostřednictvím Internetu a mobilních telefonů se

útočná informace rychle rozšíří k mnoha lidem. Ti ji potom mohou léta uchovávat.

**OBTÍŽNÁ KONTROLOVATELNOST** – Šikana těžko zjistitelná rodiči, učiteli, chybí obvyklé znaky šikanování, dítě nemá modřiny, zničené věci apod.

**NEZÁMĚRNOST**– V některých případech si agresor neuvědomuje, že ubližuje, nepozná, že vtip už přestal být vtipem.

* 1. Kybergrooming

Jako kybergrooming se označuje chování, kdy si pachatel na internetu vytipovává oběť, snaží se získat její důvěru, vybudovat s ní blízký vztah a vylákat ji k osobní schůzce. Cílem setkání je oběť zneužít. Do takové situace se děti a teenageři mohou dostat snadno: s cizími lidmi na internetu komunikují takřka denně. Pak stačí, aby se vaše dítě cítilo trochu osaměle, právě přišlo o kamaráda nebo první lásku. Když nový (ale cizí) virtuální přítel správně zvolí slova a trochu zahraje na city, je na potíže zaděláno.  
Pachatelé kybergroomingu se obvykle nejprve snaží získat osobní kontakty na svou oběť (telefonní číslo, adresu nebo číslo ICQ apod.). V další fázi potom zjišťují životní situaci oběti (Žije s oběma rodiči? Má sourozence? Má hodně kamarádů?) a na tom pak staví další komunikaci: snaží se navázat přátelský a důvěrný vztah, potom už je snadné navrhnout osobní schůzku. Pachatelé se často vydávají za někoho úplně jiného, než ve skutečnosti jsou: pokud se chtějí dostat do přízně osmileté dívenky, často si hrají na stejně starou holčičku a povídají si s ní třeba o domácích mazlíčcích. U starších děvčat se jim může vyplatit vydávat se za osmnáctiletého chlapce apod. Důležitým rysem komunikace je **trpělivost**: pachatelé si vydrží i dlouhé měsíce jen tak povídat, aby si k sobě svou oběť pevně připoutali a s jistotou získali její důvěru. Často k tomu využívají i dárky a podplácení, dítěti například posílají kredit na mobilní telefon. Součástí kybergroomingu může být i vydírání – pachatel od oběti získá např. intimní fotografie. Jakmile je má jednou v ruce, může dítě pod pohrůžkou zveřejnění nutit k čemukoliv – třeba k opakovanému osobnímu setkání, kde pachatel oběť zneužívá.

* 1. Kyberstalking

**Stalking (lov, pronásledování) je termín, který označuje opakované a stupňované obtěžování v různých formách. Pronásledovatel svou oběť například bombarduje SMS zprávami, e-maily, telefonáty či "dárky", obtěžuje oběť nechtěnou a nevyžádanou pozorností. Pokud pronásledovatel používá výše zmíněné informační a komunikační technologie (ICT), potom hovoříme o kyberstalkingu.**

**Znaky:**

1. Pachatel se dlouhodobě snaží kontaktovat svou oběť přes SMS zprávy, emaily, dopisy, telefonáty, zasílání zpráv přes chaty či Skype, apod., může také posílat dárky a pozornosti domů či do zaměstnání.
2. Charakter kontaktování může být ze začátku příjemný, obdivný a pozorný, pachatel si získává o oběti informace (kde žije, s kým žije, co má ráda). Pokud oběť nereaguje na kontakt dle představ pachatele, dochází k intenzivnějšímu kontaktování s prvky agrese, urážek, zastrašování či nevkusných komentářů, pachatel vyvolává v oběti pocity viny, vydírá ji a vyhrožuje.
3. Stalker dává oběti najevo svou sílu a moc skrze výhrůžky, ať přímé či nepřímé, které vyvolávají v oběti strach. Pokud komunikuje přes informační a komunikační technologie (ICT), většinou oběti vyhrožuje tím, co o ní zjistil v předešlé, ještě příjemné, komunikaci (vím kde jsi, co děláš, co máš na sobě, s kým se stýkáš, …). Patří sem také fyzické pronásledování oběti cestou do práce, na nákup, domů, čekání před domem, pronásledování autem, ale i výhrůžky přímého fyzického napadení či zabití. Pokud se jedná o zvlášť nebezpečného pachatele např. se sadistickými sklony, může dojít ke skutečnému napadení a zvyšuje se i riziko usmrcení oběti. Pronásledovaná oběť pak bývá častou obětí sexuálně motivované vraždy.
4. Další fází stalkingu je poškozování věcí oběti přímo – rozbitá okna, propíchnuté pneumatiky, poškozování osobních věcí nebo nepřímo – posílání např. virů emailovou poštou, elektronické nabourávání se do osobních údajů nebo rozšiřování nepravdivých informací po internetu, či dokonce vytvoření webové stránky o oběti, za účelem jejího poškození před rodinou, přáteli, zaměstnavatelem.
5. Stalker může dojít i k tomu, že sám sebe začne označovat za oběť.
   1. Prevence

**ZVAŽTE** **ODESÍLÁNÍ CITLIVÝCH ÚDAJŮ**

Opatrní bychom měli být zejména při odesílání jakýchkoliv citlivých informací, ať už se týkají nás, naší rodiny nebo známých.

**NEUVÁDĚJTE** **SVOU SKUTEČNOU IDENTITU**

Jméno, věk, adresu, telefon… žádné údaje o sobě a blízkých, podle kterých bychom byli pro agresora identifikovatelní. Vystupovat pod obecnou nic neříkající přezdívkou (tzv. nickname).

**ZVOLTE** **SI SPRÁVNÉ HESLO A CHRAŇTE SI HO**

Správné heslo je základem každého uživatele. Hesla by se totiž neměla u našich účtů opakovat. Měla by to být náhodná kombinace písmen a čísel, která je tajná a těžko uhodnutelná. Rozhodně bychom si neměli dávat jako heslo např. své křestní jméno. Na svých virtuálních účtech (např. účtu k e-mailu, k chatu, účtu do vzdělávacího prostředí apod.) se útočník jejich prostřednictvím může dostat k našim osobním údajům a ty zneužít, může s účtem manipulovat, popř. může zneužít naši virtuální totožnost. Heslo by mělo obsahovat minimálně jednu číslici, jedno velké písmeno, jeden speciální znak a jeho délka by měla být minimálně 6 znaků.

**ZABEZPEČTE** **SI SVOJE ÚČTY**

Na sociálních sítích, jako je např. Facebook, o sobě zveřejňujeme spoustu osobních informací. Některé z informací by ale rozhodně neměly být přístupné cizím lidem, proto je důležité, abychom měli svůj účet dobře zabezpečený. Tuto možnost u Facebooku naleznete vpravo nahoře > Hlavní stránka > Nastavení účtu.

**SEZNAMTE SE S PRAVIDLY** **CHATU, ČI DISKUZE**

Seznámením se s pravidly se jednak můžete sami vyvarovat jednání, které je v rozporu s používáním dané služby, a pak také budete vědět, co si mohou ostatní uživatelé dovolit k vám, případně jak se proti nevhodnému chování bránit a na koho se s problémy obrátit. V pravidlech se dočtete mimo jiné, které příspěvky mohou být správcem smazány nebo jak máte nebezpečný příspěvek nahlásit správci.

**ZVAŽTE** **OBSAH SVÉHO SDĚLENÍ**

Něco, co chápete jako legrácku nebo vtip, může druhý pochopit jako urážku nebo ponížení. Uvědomte si, kolik lidí si příspěvek, který zveřejníte, přečte a kolik lidí se tak bude na účet ponížené osoby bavit.

* 1. Obrana

**NEREAGUJTE A UKONČETE** **KOMUNIKACI**

Pokud budete odpovídat, útočník bude mít radost, že někoho ulovil a jen tak nepřestane. Lze předpokládat, že se útočník po čase vzdá, protože jeho námaha nenachází odezvu. Ačkoliv se jedná o zdánlivě jednoduchý krok, pasivní reakce na útok je pro člověka něco nepřirozeného a tedy i složitého.

**BLOKUJTE** **ÚTOČNÍKA**

Zamezte útočníkovi přístup k vašemu účtu nebo telefonnímu číslu (zablokujte si přijímání útočníkových zpráv či hovorů, změňte svou virtuální identitu) a je-li to v dané situaci možné, i k nástroji či službě, pomocí které své útoky realizuje (kontaktujte poskytovatele služby). Jde spíše o to znesnadnit mu jeho počínání. Vzhledem k tomu, že útočník může své virtuální identity jednoduše měnit,  blokování mu nemůže definitivně zabránit v dalších útocích.

**ZMĚŇTE** **SI SVOU IDENTITU**

Změňte si svou virtuální identitu – vystupujte pod jinou přezdívkou, vytvoř si jiný email, změň SIM kartu…

**NECHÁVEJTE** **SI DŮKAZY**

Nemažte to, co vám útočník poslal, poslouží vám to jako důkaz. To znamená uložit, vytisknout, popř. jinak uchovat emaily, SMS, odkazy na webové stránky s problematickým obsahem apod. Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování.

1. PRAKTICKÁ ČÁST

(tabulka č. 1)

|  |  |  |
| --- | --- | --- |
| Znění otázky | Možné odpovědi | Počty odpovědí |
| Jaké je vaše pohlaví? | Muž | 12 |
| Žena | 14 |
| V kolika letech jste se zaregistrovali na nějakou ze sociálních sítí? | 6-11 | 0 |
| 11-13 | 25 |
| 14-18 | 1 |
| 19 a více | 0 |
| Zveřejňujete své fotografie? | Ano | 26 |
| Ne | 0 |
| Zveřejnili jste někdy fotografii, která někoho zesměšňuje? | Ano | 12 |
| Ne | 14 |
| Přidali jste si na Facebooku někoho koho neznáte? | Ano | 22 |
| Ne | 4 |
| Máte profil přístupný pouze pro své kamarády nebo pro všechny? | Pro všechny | 23 |
| Pouze pro přátele | 3 |
| Jak často se přihlašujete ke svému účtu? | Jsem neustále přihlášen | 3 |
| Několikrát denně | 22 |
| Několikrát týdně | 1 |

(Graf č. 1) Jaké je vaše pohlaví?

(Graf č. 2) V kolika letech jste se zaregistrovali na nějakou ze sociálních sítí?

(Graf č. 3) Zveřejňujete své fotografie?

(Graf č. 4) Zveřejnili jste někdy fotografii, která někoho zesměšňuje?

(Graf č. 5) Přidali jste si na Facebooku někdy někoho, koho neznáte?

(Graf č. 6) Profil máte přístupný pro všechny, nebo pouze pro přátele?

(Graf č. 7) Jak často se přihlašujete na Facebook?

(Graf č. 8) Setkali jste se někdy s nějakým druhem obtěžování na internetu?

Závěr

1. Většina lidí si založila nějaký profil na sociálních sítích ve velmi brzkém věku.
2. Všichni z dotazovaných si dávají na svůj Facebook fotografie.
3. 46% z dotazovaných někdy zveřejnilo fotografii, na které jejich kamarád vypadá směšně. Mnohdy si lidé neuvědomí, že tím někomu ubližují.
4. 85 % z dotazovaných si někdy přidalo někoho, koho v životě neviděli
5. 88 % z dotazovaných má své fotografie a osobní údaje pro všechny.
6. Pouhá 4 % respondentů se někdy setkala s nějakým druhem obtěžování.

V mém průzkumu se tedy ukázalo, že kyberkriminalita na sociálních sítích je méně rozšířená, než by se mohlo zdát ze zpráv českých médií, či popularizujících informací od firem zabývajících se školením ohledně tohoto fenoménu. Na druhou stranu, fenomén online obtěžování a kyberšikany není možné podceňovat. S ohledem na účinnost technické zvládací strategie se jeví jako vhodné, aby žáci byli vzděláváni v tom, co vše je možné v případech online obtěžování technicky udělat, aby se taková situace již neopakovala anebo jí byli schopni účinně předcházet. Do takových znalostí patří např. schopnost nahlásit závadný obsah administrátorovi webových stránek, blokování telefonního čísla, účtu či profilu a znalost nastavení soukromí a zabezpečení svých účtů a profilů tak, aby nedocházelo k nežádoucím kontaktům.

Použitá literatura

Internetové zdroje:

http://psychickeobtezovani.webnode.cz/news/kybersikana/

http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

http://www.linkabezpeci.cz/poradna/ublizovani,-zneuzivani,-sikana/kybersikana/?gclid=CNKQism6\_tICFQ26GwodEJEBmw

http://www.kybersikana.eu/2010/12/kybergrooming.html

https://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/361-prevence-kybersikany

http://www.profem.cz/clanek.aspx?a=97

https://cs.wikipedia.org/wiki/Kyberšikana

**Seznam příloh:**

Tabulka č. 1 (zdroj: autor)

Graf č. 1 (zdroj: autor)

Graf č. 2 (zdroj: autor)

Graf č. 3 (zdroj: autor)

Graf č. 4 (zdroj: autor)

Graf č. 5 (zdroj: autor)

Graf č. 6 (zdroj: autor)

Graf č. 7 (zdroj: autor)

Graf č. 8 (zdroj: autor)