Analýza rizika a bezpečnostní hrozby mládeže při práci s počítačem

Lucie Hladká

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lucie Hladká**
Osobní číslo:	**L18428**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Analýza rizika a bezpečnostní hrozby mládeže při práci s počítačem**

Zásady pro vypracování

1. Na základě studia odborné literatury zpracujte literární rešerši týkající se analýzy rizik a bezpečnostních hrozeb mládeže při práci s počítačem.
2. Proveďte analýzu rizik a bezpečnostních hrozeb při práci s počítačem u vybranné věkové kategorie.
3. Na základě výsledků analýzy zformulujte závěry a navrhněte vlastní opatření k eliminaci zjištěných rizik.

Forma zpracování bakalářské práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. JUŘÍČEK, Ludvík a Petr ROŽŇÁK. *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: Key Publishing, 2014. ISBN 978-80-7418-201-3.
2. LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7.
3. ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. ISBN 978-80-247-5010-1.

Další odborná literatura na doporučení vedoucí bakalářské práce.

Vedoucí bakalářské práce: **Ing. Kateřina Víchová, Ph.D.**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: **6.8. 2021**

Jméno a příjmení studenta: Lucie Hladká

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá analýzou rizik a bezpečnostními hrozbami mládeže při práci s počítačem. Cílem bylo identifikovat možná rizika a navrhnout případná opatření. Práce je rozdělena na teoretickou a praktickou část. Teoretická část obsahuje literární rešerši dané problematiky. V praktické části byla vyhodnocena rizika metodami Check list, What if a maticí rizik a dotazníkové šetření. Na základě výsledků analýzy a vyhodnocení dotazníkového šetření byla navrhnuta opatření k jejich eliminaci.

Klíčová slova: analýza rizik, bezpečnostní hrozby, riziko, sociální síť, počítač

ABSTRACT

This bachelor ‘s thesis deals with the risk analysis and security threats of young people when working with a computer. The aim was to identify possible risks and propose possible measures. This work contains a theoretical and practical part. The theoretical part contains literary recherche of the given issue. In the practical part, the risks were evaluated using the methods „Check list“, „What if“ and risk matrix and a questionnaire survey. Based on the results from analysis and evaluate of questionnaire survey were proposed measures for their elimination.

Keywords: risk analysis, security threats, risk, social network, computer

Zde bych chtěla poděkovat své vedoucí práce paní Ing. Kateřině Víchové Ph.D. za její odborné rady a připomínky při tvorbě práce. Dále bych chtěla poděkovat mému manželovi a dětem za velkou podporu během celého studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Tématem bakalářské práce je analýza rizika a bezpečnostní hrozby mládeže při práci s počítačem. Osobně si myslím, že je to aktuální téma, jelikož v každé rodině je minimálně jeden počítač a každý člen vlastní mobilní telefon nebo tablet. Dnešní mládež žije v době, kdy tyto moderní technologie využívá denně a bez nich si svůj život už ani nedokáže představit. Spousta mladých lidí už ani neví co je to poslat pohlednici z dovolené nebo dopis kamarádovi. Pohodlnější je přece poslat SMS zprávu nebo vyfotit fotografii a dát ji na sociální síť. V počítačovém světě je tolik lákadel, že je obtížné se v nich správně orientovat. Nebezpečí může být na první pohled skryto, avšak pravdou je, že na neopatrného uživatele číhá téměř na každém rohu.

Tohle téma jsem si vybrala, protože mě ihned zaujalo a jakož to pro matku dvou dětí je pro mě velice aktuální. Doufám, že i pro ostatní rodiče moje práce bude mít nějaký přínos.

Cílem práce je odhalit možná rizika a hrozby, které mohou nastat při práci mládeže s počítačem.

Bakalářská práce je rozdělena do dvou částí teoretickou a praktickou část. V teoretické části se nejprve zabýváme vymezení základních pojmů, poté následuje kapitola Legislativa kybernetické bezpečnosti, ve které je uveden zákon o kybernetické bezpečnosti. Druhou kapitolu Počítač a internet ve které je zahrnuta definice počítače, bezpečnost při práci s počítačem a jak bezpečně používat počítač vzhledem ke zdraví. Třetí kapitola obsahuje Sociální sítě a online hry. Poslední kapitola je zaměřené na hrozby v online prostředí jako jsou sociální inženýři, webcam trolling, sexting, kyberstalking, podvody a phishing. Praktická část obsahuje kapitolu zpracování analýzy. Zpracování analýzy za pomocí Check listu, What if, matice rizik a následné návrhy opatření k zjištěným výsledkům. Dále dotazníkové šetření a následně zjištěné poznatky. Cílem dotazníkového šetření bylo zjistit kolik času tráví mládež denně na počítači, jaké činnosti na počítači dělají a s jakými hrozbami se již setkali. Poslední kapitola se zabývá, kam se mládež může obrátit v případě, že se stydí řešit problémy s rodiči.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

V této kapitole jsou vymezeny základní pojmy pro bližší seznámení s danou problematikou. S těmito pojmy se budeme opakovaně setkávat v celé práci. Jsou zde vysvětleny pojmy jako jsou: aktivum, riziko, hrozba, nebezpečí, mládež, analýza rizik, kyberprostor

Aktivum

Je vše, co má pro subjekt hodnotu. Aktiva se dělí na hmotná např. nemovitosti, cenné papíry, peníze a nehmotná např. informace, autorská práva, morálka. (Smejkal, Rais, 2006, str.82)

Mládež

Je sociální věková skupina, charakterizovaná společnými znaky. (Sociologická encyklopedie, 2018)

Kybernetický útok

Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. (Jirásek at al., 2013, str.59)

Kybernetická kriminalita

Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení. (Jirásek at al., 2013, str.57)

Kybernetická bezpečnost

Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. (Jirásek at al., 2013, str.57)

Kybernetický prostor

Označení virtuálního světa vytvářeného moderními technologiemi. Kybernetický prostor je fenomén, díky kterému můžeme reálný svět redukovat. Je to prostor, který se otevírá ve chvíli, kdy se pomocí internetových sítí vstupuje do online prostředí. (Hulanová, 2012, str.27)

1.1 Hrozba

Představuje skutečnost, která se svým působením projevuje na určitém celku negativně. Může způsobit újmu nebo mít negativní dopad. Jedná se o negativní účinek, který může mít materiální nebo nemateriální povahu.

Materiální hrozba může mít fyzikální nebo chemickou povahu. Příkladem materiálního působení jsou války, krádeže, dopravní nehody, povodně atd.
Nemateriální hrozba má informační a logickou povahu. Promítá se do řady oblastí společnosti i osobního života jedinců. Může mít podobu spojenou s penězi, informacemi, dezinformacemi a zpravodajstvím, ekonomickými procesy, psychikou. (Lukáš, 2017, str. 24)
Škoda, kterou způsobí hrozba při působení na určité aktivum se nazývá dopad hrozby. Dopad hrozby může být odvozen od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo odstranění následků škod způsobených hrozbou. (Smejkal, Rais, 2006, str.82)
Hrozba ještě neznamená narušení bezpečnosti. Možnost samostatného narušení bezpečnosti se vyjadřuje rizikem. (Lukáš, 2017, str. 24)

1.2 Riziko

Pod názvem rizika se ukazuje, že jde o sémantický problém, který není univerzálně řešitelný. Záleží velice na odvětví, oboru a problematice. Právě proto neexistuje obecně uznávaná definice. (Tichý, 2006, str.15,16)

Pojem riziko je definován různě, např.:

- Nejistota vztahující se k újmě
- Nebezpečí psychické, fyzické nebo ekonomické újmy
- Osoba vystavená újmě
- Nebezpečí nějaké újmy

1.3 Nebezpečí

Významným pojmem je nebezpečí, které je jistou reálnou hrozbou pro poškození objektu nebo procesu. Stroje, materiály, technologie a pracovní činnosti se vyznačují tím, že mohou způsobit neočekávaný negativní důsledek např. poškození člověka a majetku.
Jde o:

- nebezpečí nebo nebezpečné činnosti.
- podstatnou, ale skrytou vlastnost nebo schopnost něčeho, která může zapříčinit vznik škody.
- zdroj možného ohrožení nebo škody.

Zdroj nebezpečí je schopen aktivovat nebezpečí v konkrétním prostoru a času. (Šefčík, 2009, str.8)

1.4 Analýza rizik

Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti. Výsledky hodnocení rizik pomohou určit odpovídající kroky pro zvládání jejich zvládnutí a také pro realizaci opatření určených k zamezení jejich výskytu.
Analýza rizik zpravidla zahrnuje:

1. Identifikaci aktiv – vymezení posuzovaného objektu
2. Stanovení hodnoty aktiv – určení hodnoty aktiv pro subjekt
3. Identifikace hrozeb a slabin – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv, určení slabých míst subjektu, které mohou umožnit působení hrozeb
4. Stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě (Stejskal, Rais, 2006, str.81)

Základní metody pro stanovení rizik:
Analýza rizik je ve své podstatě multikriteriálním hodnocením parametrů. Obecně lze metody analýzy rizik rozdělit na kvantitativní a kvalitativní metody.
Princip kvantitativní analýzy rizik je založen na dvou základních krocích, a to pravděpodobnosti výskytu jevu a pravděpodobnosti ztráty hodnoty. Principy kvalitativní

analýzy rizik jsou více využívány ke stanovení priorit mezi riziky. Pracují s daty, následky a ztrátami užitné hodnoty.
Pro analýzu a její vyhodnocení lze použít například tyto metody:

Event Tree Analysis – ETA (analýza stromu událostí) – graficko-statistická metoda. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout.

Human Reliability Analysis – HRA (analýza lidské spolehlivosti) – je postup na posouzení vlivu lidského činitele na výskyt pohrom, nehod, havárií, útoků či některých jejich dopadů.

Failure Modes and Effects Analysis – FMEA – identifikuje jednoduché poruchy, které mohou významně přispívat k havárii. (Ševčík, 2009, str.55,57,60)

Check list

Je seznam nebezpečí, rizik nebo neúspěchů, které vznikly na základě zkušenosti, případně z výsledků posouzení rizik a předešlých neúspěchů. Může být použit k identifikaci hrozeb i rizik, případně k posuzování efektivnosti rizikového řízení. Aplikace je možná v kterékoliv životní fázi produktu, procesu nebo systému. Jeho použití lze kombinovat s ostatními metodami posuzování rizik.

Výhody:
- Mohou být používány neodborníky
- Časová a pracovní nenáročnost
- Pomáhá zajistit kvalitu a komplexnost při plnění úkolů

Nevýhody:
- Absence potencionálních problémů
- Poskytuje pouze kvalitativní informace
- Mohou zde být položky, kdy je analýza časově náročná (Risk management – Risk assessment techniques, 2009, str.30,31)

What if

Jedná se o týmovou studii, při které se formou dotazů a odpovědí prověřují neočekávané události, které se mohou v procesu vyskytnout. Kdokoli může formulovat otázku: „Co se stane, když…“ následně se hledají odpovědi. Odhadují se následky vzniklého stavu nebo situace, navrhují se opatření a doporučení.

Výhody:

- Je to relativně rychlá metoda
- Lze ji použít k identifikaci příležitostí ke zlepšení procesů a systémů
- Lze ji použít k identifikaci rizik a nebezpečí, která lze zahrnout do kvantitativní studie

Nevýhody:

- k tomu, aby byla efektivní, potřebuje zkušeného a schopného pomocníka
- Pokud tým nemá povědomí o dané problematice, některá nebezpečí nemusí být identifikovatelná (Risk management – Risk assessment techniques, 2009, str. 38,39)

Matice rizik

Jde o prostředek, jak kombinovat kvalitativní a semikvantitativní klasifikaci následku a pravděpodobnosti s cílem vytvořit úroveň rizika nebo klasifikaci rizika.

Používá se k určení rizika, zda je přijatelné nebo nepřijatelné.

Výhody:

- metodu lze relativně snadno používat
- poskytuje rychlou klasifikaci rizik podle různých úrovní významnosti

Nevýhody:

- je obtížné jednoznačně definovat stupnice dopadu a pravděpodobnosti
- použití je velmi subjektivní a je tendence k výrazným výkyvům mezi pracovníky provádějícími klasifikaci, (Risk management – Risk assessment techniques, 2009, str. 82)

Z výše popsaných metod možných metod byly vybrány k bakalářské práci Check list, What if, matice rizik.

2 LEGISLATIVA KYBERNETICKÉ BEZPEČNOSTI

V současnosti je kybernetická bezpečnost v České republice jako druh bezpečnosti vymezena zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákon sice nedefinuje pojem kybernetická bezpečnost, ale vymezuje systém zajištění kybernetické bezpečnosti v rámci, kterého jsou definovaná bezpečnostní opatření jako souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech, dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. (Lukáš,2017, str.)

Za bezpečnostní opatření ve znění zákona je možné proto považovat:

1) Bezpečnostními opatřeními jsou

a) organizační opatření a

b) technická opatření.

(2) Organizačními opatřeními jsou

a) systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací,

i) řízení přístupu osob,

j) akvizice, vývoj a údržba,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit.

(3) Technickými opatřeními jsou

a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací a

l) bezpečnost průmyslových a řídících systémů. (zákon č. 181/2014 Sb.)

3 POČÍTAČ A INTERNET

Počítač v dnešní době nepředstavuje pouze zařízení složené z monitoru, klávesnice, myši a samostatné skříně počítače umístěné na velkém stole. Počítače v našem okolí se postupně proměnily do různých podob. Jednoznačně nejznámější varianta počítače je „smartphone“ tedy chytrý telefon, který je svým složením téměř totožný s již zmíněným počítačem, a především je dnes dostupný téměř pro kohokoliv. Zatímco v 90. letech minulého století stály počítače desetitisíce, dnes je možné zakoupit chytrý telefon i v řádech jednotek tisíců. Čímž se počítač, byť v jiné formě, stává masovou záležitostí pro celou společnost.

3.1 Definice počítače

Počítač je stroj určený k výpočtům a zpracování dat. Zpracovává vstupní data a produkuje výstup daných dat. Skládá se ze dvou hlavních částí; z hardwaru a softwaru. (Computer, 2020)

Hardware – jsou veškeré fyzické části počítače, které jsou potřebné pro jeho fungování. Mohou to být například: procesor, grafická karta, pevný disk, základní deska atd. Specifickým druhem hardware může být i klávesnice, myš a monitor. (Computer, 2020)

Software – je programové vybavení počítače. Rozděluje se na systémový a aplikační.Systémový software zajišťuje chod počítače a aplikační software jsou programy, s nimiž pracuje uživatel. Mezi software se řadí i uživatelská data. (Computer, 2020)

3.2 BEZPEČNOST PŘI PRÁCI S POČÍTAČEM

Bezpečností při práci s počítačem rozumíme možné napadení ale i správné sezení u počítače. Tím předcházíme možným únikům dat nebo zdravotním komplikacím.

3.2.1 Bezpečnost dat

Pojem bezpečnost dat zahrnuje dva různé problémy. První z nich je zabezpečení dat proti ztrátě nebo zničení. K tomu může dojít mnoha způsoby: poškození počítače, havárie systému, neúmyslné smazání. Druhým problémem je zamezení krádeži a následnému zneužití dat. (Heller, Jelínek a Simr, 2011, str.15)

3.2.2 Zálohování dat

Zálohování dat zvyšuje bezpečnost uchovávaných informací a snižuje riziko jejich poškození nebo ztráty. Nejběžnějším způsobem zálohování dat je dvojité ukládání

důležitých souborů. Data by měla být ukládána na více než jedno záložní paměťové médium. Nejdůležitější je zálohovat data pravidelně a dlouhodobě. (Heller, Jelínek a Simr, 2011, str.15)

3.2.3 Uživatelské jméno a heslo

V počítačovém světě často pracujeme se systémy, kde se uživatel musí před vstupem identifikovat. Nejrozšířenější způsob identifikace je uživatelské jméno a heslo. Uživatel by měl používat co nejbezpečnější hesla. Bezpečné heslo je takové, které není snadno zjistitelné a uhodnutelné. Ideální heslo by mělo dostatečně dlouhé a obsahovat kombinaci malých, velkých písmen, číslic a symbolů. (Heller, Jelínek a Simr, 2011, str.15)

3.2.4 Škodlivé kódy

Malware je souhrnné označení pro všechny druhy škodlivého kódu. Jsou to programy pro vniknutí nebo poškození počítačového systému či jeho uživatele.

Počítačový virus je malý program, který připojí sám sebe k jinému programu nebo souboru, narušuje fungování počítače a pokouší se šířit na další počítače. Následky virů mohou být nepříjemné, ale hlavně i destruktivní. Nejsnadněji se šíří v přílohách emailových zpráv, stahováním dat a programů z internetu.

Trojský kůň je počítačový program, který se jeví jako užitečný software, ale místo toho naruší uživatelovo zabezpečení a napáchá spoustu škod.

Spyware je počítačový program, který slouží k zjišťování informací a o činnostech uživatelů. Program nijak nepoškozuje soubory, pouze shromažďuje specifická data, která posílá tvůrcům tohoto kódu. (Heller, Jelínek a Simr, 2011, str.16)

3.3 Jak bezpečně používat počítač vzhledem ke zdraví

Správné nastavení židle

Židle by měla mít možnost výškového nastavení a měla by umožňovat vzpřímené držení zad. (Jak správně sedět u PC + zásady ergonomie sezení na kancelářské židli, 2018)

Správné nastavení stolu

Důležité je, aby uživatel seděl ve správné výšce, tzn. mít správně vysoko desku stolu. Při sedu by měla být výška desky stolu totožná s výškou loktů. Předloktí a nadloktí by mělo svírat úhel 90°. Lýtko se stehnem by mělo svírat v koleni úhel 90°. Výška stolu by měla být

asi 72 cm nad podlahou, u žen o něco méně. (Jak správně sedět u PC + zásady ergonomie sezení na kancelářské židli, 2018)

Správná vzdálenost obrazovky

Vzdálenost monitoru od očí by měla být zhruba 45–70 cm. Střed obrazovky by měl být asi 20°- 35° pod horizontální osou očí a horní hrana mírně nad horizontální osou očí. (Jak správně sedět u PC + zásady ergonomie sezení na kancelářské židli, 2018)

Obrázek 1- Jak sedět u počítače (www.skolenibozp.cz)

3.4 Internet

Již v 60. letech v době studené války se začaly ve Spojených státech merických objevovat myšlenky na vytvoření sítě, která by propojovala nejdůležitější vojenské, vládní a akademické počítače tzv. ARPANET.

Období mezi lety 1983-1992 můžeme označit jako druhou etapu rozvoje internetu. Tato etapa je charakterizována prudkým růstem internetu, a především expanzí mimo americký kontinent. (Jak vznikl internet. Na počátku byl ARPAN, 2020)

Internet se v České republice objevil v roce 1990. V té době neexistovaly žádné linky mimo telefonních, tak se objevily první pokusy o vytvoření počítačové sítě. Až do roku 1995 lidé o existenci internetu neměli ponětí. Na přelomu let 1995 a 1996 vstupuje na český trh celá řada komerčních poskytovatelů internetu. Internet se ze začátku používal jen pro akademické a výzkumné účely. Dnes ale zastává důležitou roli v jakékoli lidské aktivitě, kterou si jen člověk dokáže představit. Na internetu se dá vyhledat cokoli např. dovolená, přátelé, knihy, slevy atd. V posledních letech je dynamika šíření internetu obrovská i díky tomu, že se dá připojit kdekoli a kdykoli. V každém restauračním zařízení, hotelu nebo na školách mají veřejnou síť. Dá se připojit i na ulici pomocí internetu v mobilu, jelikož všichni mobilní operátoři nabízí možnost internetu do mobilního telefonu. (Hulanová, 2012, str. 19)

Internet se v poslední době stává i snadno zneužitelným a nebezpečným nástrojem. Například útočníci, kteří na dálku infikují nezabezpečené počítače nebezpečnými viry. Množí se i případy, kdy útočníci pomocí zjištěných přístupů k bankovním účtům z nedokonale zabezpečených počítačů kradou peníze uživatelů. A v neposlední řadě i nebezpečný trend, kdy internet umožňuje šíření dezinformací za účelem ovlivňování veřejného mínění. (Jak vznikl internet. Na počátku byl ARPAN, 2020)

4 SOCIÁLNÍ SÍTĚ A ONLINE HRY

Online sociální sítě se řadí mezi specifické internetové služby, zaměřené primárně na získávání a udržování sociálních kontaktů s dalšími uživateli internetu. Uživatelům umožňují si založit veřejný nebo polo-veřejný profil. (Ševčíková, 2014, str. 58)

Pro sociální sítě jsou typické tyto vlastnosti:

- Obsah sociálních sítí vytvářejí sami uživatelé
- Umožňují vytvářet sociální vazby
- Obsahují velké množství osobních a citlivých informací, které o sobě zveřejňují a šíří sami uživatelé
- Podporují jednoduché a efektivní sdílení informací (Kopecký, 2015, str. 47)

4.1 Nejznámější sociální sítě

ČSFD

Největší sociální síť, která se zaměřuje na filmové fanoušky. (Kožíšek, 2016, str.25)

Facebook

Facebook vznikl na jedné z nejprestižnějších amerických univerzit Zakladatelem je bývalý student této univerzity Mark Zuckemberg, Facebook byl spuštěn 4. února 2004. Jeho vize byla taková, že službu budou používat k seznamování studenti. Už na konci roku 2004 měl Facebook 1 milion uživatelů. V roce 2005 koupil doménu Facebok.com a připojily se i další univerzity a školy. Tato síť přitahovala i soukromé uživatele. Proto se Mark zaměřil na rozšíření sítě. (Vznik a historie Facebooku, 2015)

Facebook je největší a nejrozšířenější sociální sítí a používají ho i děti. Věková hranice pro používání facebooku je 13 let, ale není to nijak kontrolováno. Po registraci může uživatel vyplnit svůj profil a uvést celou řadu údajů, například: datum narození, zájmy, telefonní číslo, bydliště. Na svém profilu může libovolně vkládat fotografie, videa, odkazy a psát vlastní texty. Tohle vše vidí tzv. přátelé. Přátelé jsou kontakty, které si uživatel sám přidal nebo se přidal do nějaké facebookové skupiny, na internetové platformě spolu komunikují nebo hrají hry. Tito přátelé mají přístup ke všemu, co uživatel o sobě napsal na svém profilu. (Rizika sociálních sítí a co by děti měly vědět, 2014*)*

Youtube

Je bezplatná sociální síť pro sdílení a sledování videí. Videa mohou být hudební, komediální, výukové atd. Děti už od útlého věku umí používat Youtube, většinou je to první sociální síť, se kterou se setkají. Na Youtube je spousta dostupných pohádek, písní a různě zajímavých videí. Samozřejmě i pro rodiče je to pohodlné, jelikož dítě tato sociální síť zabaví a rodiče mají klid. Jenže dítě se nevydrží dívat jen na jednu věc, a tak kliká na videa, které mu připadají zajímavá. Tímto se může doklikat na videa nevhodného obsahu plná násilí a vulgarit. Tohle neplatí jen u malých dětí, ale i u dospívajících. Youtube může být prospěšný, ale i špatný. (vlastní zpracování, 2021)

Twiter

Je sociální síť, která dostala svůj název od slova Tweet – pípat. Je založena na posílání krátkých textů s omezenou délkou, maximálně 280 znaků. Dále se může používat na odesílání odkazů na články, fotografie a videa. Každý uživatel si může vytvořit svůj okruh příjemců a zároveň přijímat sdělení od uživatelů, které si sám vybere. (Jak se prezentujeme na internetu, 2012)

Snapchat

Je mobilní aplikace pro sdílení fotek a videí. Od ostatních aplikací se liší tím, že odeslané fotky automaticky mizí za 1 až 10 sekund, dle konkrétního nastavení každého uživatele. Proto lze považovat sdílení za relativně bezpečné. Jediný způsob jak, odeslané fotky uchovat a případně sdílet mimo vědomí autora je tzv. otisk obrazovky. (The Dark Side of Snapchat and Teens, 2020)

4.2 Online hry

Počítačové hry jsou tu s námi již od minulého století a jejich obliba postupně stoupá. Dnes snad každý zná postavičku italského instalatéra jménem Mario. S rozšířením internetu se dnes nejčastěji mluví o online hrách, které jsou mezi mládeží velmi populární. V online herním prostředí se potkává více hráčů, kteří mohou hrát společně nebo proti sobě. Jedny z nejhranějších online her jsou Roblox a Minecraft. Jedná se o hry, které jsou na půli cesty k sociálním sítím. Obsah těchto her tvoří samy hráči pomoci virtuálních postav ve virtuálním světě. (Lorentz et al., 2015, str.153i

Online hry jsou pro mládež tolik lákavé, protože postavy ve hře se časem vyvíjejí jsou sofistikovanější, mocnější nebo prestižnější. Děti si ke svým postavám vytvářejí citová pouta, hra jim poskytuje prostor pro to stát se výjimečným. (Online hraní her)

Negativa online her:

- Závislost
- Zhoršené schopnosti komunikace
- Poruchy spánku a soustředění
- Hraní s cizími lidmi – pedofilové, zloději, podvody
- Nevhodné chování vyvolané hraním online her – vulgarita, násilí
- Nákupy v aplikacích vedoucí k finančním ztrátám
- Hraní her, které nejsou určeny věkové kategorii hráčů (Dočekal et al., 2019, str. 53)

Pozitiva online her:

- Učení se cizím jazykům
- Zlepšení prostorové orientace
- Možnost naučit se novým věcem
- Poznání ceny peněz v hrách, kde existují herní měny (Dočekal et al., 2019, str.53)

5 HROZBY V ONLINE PROSTŘEDÍ

Existuje mnoho způsobů, kterými nás mohou lidé na internetu podvést, okrást nebo zneužít. Internet jako takový je bezpečný, nebezpeční jsou na něm jen lidé. A ti vymýšlejí různé způsoby, jak dosáhnout svých cílů. Ve skutečném životě možná stačí vytrhnout peněženku z ruky, na internetu je tato metoda pouze vzdálená a útočníci se k ní musí dostat rafinovanou cestou. K tomu slouží propracované metody, které se velice často mění a zdokonalují s ohledem na úspěšnost útoků. Mnozí lidé žijí v přesvědčení, že k ochraně na internetu postačí dlouhé heslo, nainstalovaný antivirový program a bezpečné připojení z domova. Mít silné heslo, které je kombinací všeho, co najdete na klávesnici, nestačí. Většinu prolomení hesel nemají na svědomí neznámí útočníci, ale osoby, které jsou vám blízké. (Kožíšek, 2016, str. 36)

5.1 Sociální inženýři

Je několik úrovní toho, jak dobře útočníci zvládají svojí fiktivní roli. Některé jde velice snadno rozpoznat už pohledem na jejich profil, u některých je potřeba trochu důmyslnosti a poslední jsou ti, které odhalí až znalec v oboru. Sociální inženýři jsou útočníci, kteří se snaží získat informace nebo uspokojit svoje potřeby. (Kožíšek, 2016, str.36)

5.1.1 Náhodné útoky

Jejich cílem je oslovení co největšího počtu lidí, bez ohledu na jejich zájmy. Mnohdy je podobný typ útoků označován jako spam. Do tohoto typu útoků můžeme zařadit emailové zprávy, různé reklamní nabídky, které se tváří jako osobní zpráva. Dříve byly tyto útoky lehce rozpoznatelné díky špatné jazykové úpravě, poslední dobou jsou ale některé útoky vedeny brilantní češtinou a příběhem. Cílem tohoto útoku může být snaha o získání hesla, čísla platební karty, čísla nebo získání osobních údajů. (Kožíšek, 2016, str.37)

5.1.2 Vytipované útoky

Jsou využívané k oslovení určité skupiny lidí, u kterých útočník sleduje konkrétní cíl. Pokud jde o groomera (groomer je ten, co používá sociální sítě a snaží se navázat důvěrný vztah se svými obětmi, většinou dětmi) může jít například o dívky ve věku 16 let na sociálních sítích. Dalším případem útoku může být cílení na zájmy, jako je například záliba v autech nebo

telefonech. Útočník využívá údajů, které o sobě lidé uvedli, a snaží se přizpůsobit útok tak, aby cílovou skupinu zaujal. (Kožíšek, 2016, str.39)

5.1.3 Cílené útoky

Hlavním úkolem je dosažení cíle u konkrétní oběti. K jeho dosažení je nutná znalost oběti a prostředí, ve kterém se vyskytuje. U případů, které provádí někdo z blízkého okolí, jde převážně o pokusy získat heslo k účtu oběti. (Kožíšek, 2016, str.58)

5.1.4 Vytvoření důvěryhodného profilu

Před samotným oslovením si útočníci vytvářejí profil, který v oslovených budí zájem. Profil je tvořen informacemi, jako je věk podobný obětem, fotografiemi, zájmy a fiktivními přáteli. Právě přátelé vzbuzují v obětech dojem, že jde o skutečného člověka.

Až na několik málo výjimek jsou falešné profily tvořeny fotografiemi skutečných lidí. Fotografie celebrit zpěváků nebo modelů dokáže dítě lehce rozpoznat. K vytvoření profilu jsou tak velice často používány fotografie z vykradených účtů a veřejných fotek lidí, kteří ani netuší, že se za ně někdo cizí vydává. (Kožíšek, 2016, str. 40,41)

Mluva a zájmy

Útočníci, kteří lákají děti, se snaží přizpůsobit jejich mluvě. Napodobování mluvy dětí může místy připadat legračně, dítě až na výjimky nedokáže rozeznat, že nemluví s vrstevníkem. Útočníci velice často používají archaismy, nebo výrazy, které již tato generace dětí nepoužívá. (Kožíšek, 2016, str.41)

Přitvrzení

Pokud útočník vycítí, že oslovený subjekt je ochotný komunikovat i na citlivé téma, komunikaci na ně záměrně směřuje. Pokud docílí zaslání nějakého citlivého materiálu nebo videa, snaží se v této činnosti pokračovat. Pokud je odmítnut volí útoky, jak fotky z dotyčného dostat různým typem výhružek. (Kožíšek, 2016, str.41)

5.2 Webcam trolling

V poslední době se na internetu objevuje nový fenomén tzv. webcam trolling. Především děti jsou podvodem lákány na erotické video hovory přes oblíbené komunikační nástroje.

Získané intimní záběry pak podvodníci umisťují na internet, nebo je využívají k manipulaci a vydírání.

Podvodníci mohou člověka napálit velice jednoduše. Stačí, aby si na internetu zakoupil speciální program, který dokáže vytvářet virtuální webkameru. S nainstalovaným doplňkem, pak útočník může oslovit libovolného uživatele. Komunikace pak z pravidla probíhá v duchu lechtivých témat a útočník čeká, až mu protistrana ukáže svoje intimní partie. Oběť zpravidla ani netuší, že je hovor nahráván a že video může být zneužito. (Kožíšek, 2016. str.45,46)

5.3 Kybergrooming

Cílem kybergroomingu je vyvolat v dospělém/ dítěti pocit důvěry za pomocí falešné identity a vylákat ho na schůzku. (Kožíšek, 2016, str. 72)

Jinými slovy by se dalo říct, že jde o psychickou manipulaci realizovanou pomocí internetu, mobilních telefonů a dalších souvisejících technologií, jejímž cílem je vždy osobní schůzka. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie atd. (Kopecký, 2015, str. 25)

Charakteristické rysy kybergroomingu: (Szotkowski at al., 2013, str. 51,55)

1. Místa výskytu:

   kybergrooming je vázán na komunikační platformy. Nejčastěji se s nimi dá setkat v rámci služeb, které jsou mezi dětmi a mládeží zrovna nejpopulárnější. V současné době jde tedy o sociální sítě. Predátoři rovněž zneužívají veřejného chatu a seznamek. Dále si podávají různé inzeráty slibující práci modelek a navštěvují portály pro nezletilé např. herní portály.

2. Délka manipulace vyhlédnuté oběti:

   délka manipulace může být odlišná. Z reálných dat vyplývá, že psychická manipulace probíhá od tří měsíců až po několik let.

3. Charakteristika oběti

   oběťmi kybergroomingu se nejčastěji stávají děti a mládež ve věku 11 až 17 let. Co se týče pohlaví nejsou mezi nimi rozdíly tzn. chlapci jsou terčem útoku stejně jako dívky.

4. Mezi oběti patří zejména:
    - děti s nízkou sebeúctou nebo nedostatkem sebedůvěry.
    - děti s emocionálními problémy.
    - děti naivní a přehnaně důvěřivé.
    - adolescenti/ teenageři.

Specifické rysy kybergroomingu: (Kopecký, 2015, str. 26,28)

1. Manipulace

   Kybergrooming zahrnuje různé formy manipulativního jednání např. uplácení, lichocení, nabídka dárků či peněz. Způsoby, které volí útočníci v rámci manipulace, závisí na jejich osobnosti a osobnosti oběti. Na jedné straně mohou pachatelé u oběti vzbudit pozitivní emoce, pocity zamilovanosti či dokonce lásky, na straně druhé mohou s obětí manipulovat zastrašováním, vyhrožováním či vydíráním.

2. Budování vztahu s obětí

   V komunikaci s obětí je velmi důležité získat si její důvěru. Proto útočníci synchronizují svoje vlastní chování a styl komunikace s dětskými uživateli a vytvářejí si s dítětem výborný vztah, snaží se být co nejvíce pozitivní, důvěryhodný. Kybergroomři potřebují, aby jim dítě důvěřovalo.

3. Sexuální témata

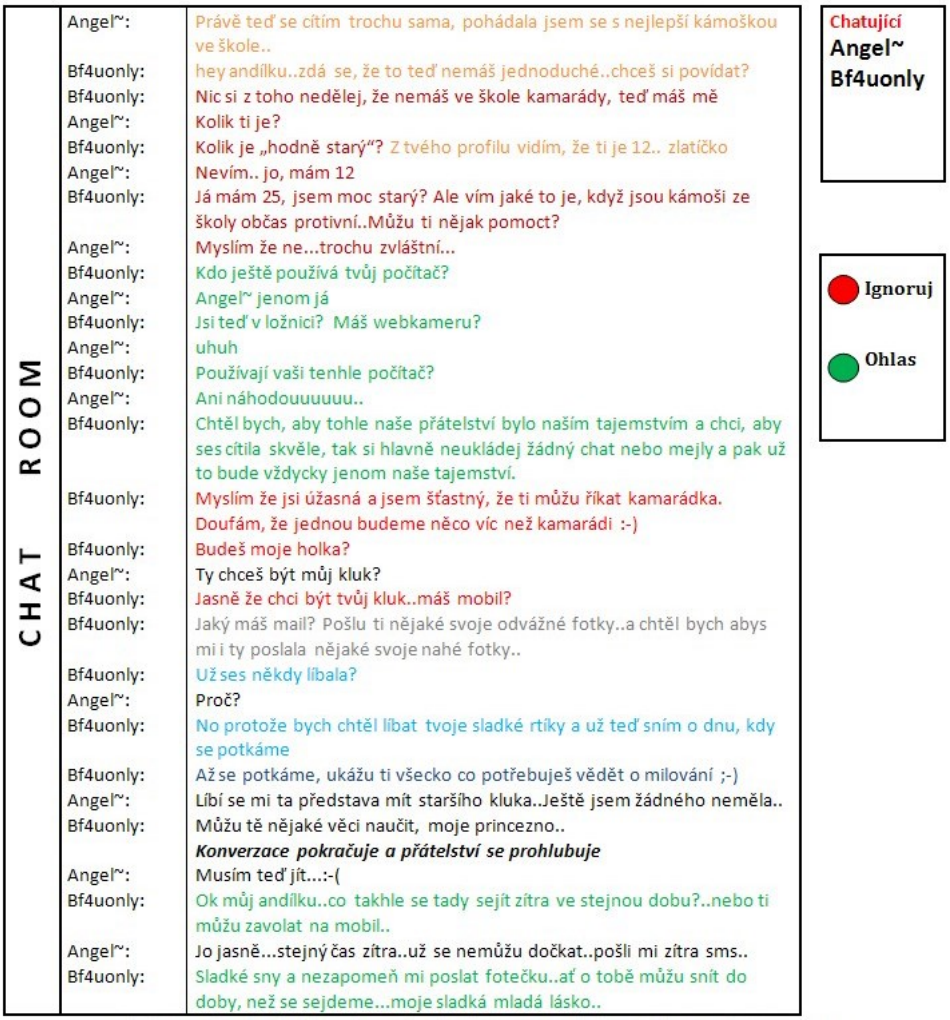
   Dříve nebo později se v komunikaci začnou objevovat sexuální témata, která útočník do konverzace záměrně zavádí. Komunikace může mít poté povahu např. flirtování, sexuální vulgarity, posílání pornografických materiálů (fotografií, videí, odkazů na pornografické stránky)

4. Posuzování rizik

   Je to velmi důležitá etapa, ve které se pachatel rozhoduje, jakým způsobem zajistit, aby nebyl odhalen, a aby se mu podařilo dítě zmanipulovat a sexuálně zneužít. Proto se snaží ochránit několika základními způsoby:

    - technická ochrana,
    - pachatelé používají více různých počítačů, mají celou řadu falešných identit atd.,

- přechod k soukromé komunikaci,
- pachatelé rychle opouští prostředí veřejných komunikačních služeb a preferují komunikaci pomocí privátních emailů či mobilních telefonů.
- zajištění osobní schůzky,
- pachatelé volí osobní schůzky daleko od domova dětí.



Obrázek 2 - ukázka kybergroomingu (www.e-nebezpečí.cz, 2008)

5.4 Sexting

Sexting představuje poměrně nový a rychle se rozmáhající fenomén. Založený na rozesílání fotografií zachycující nahotu. Pořízené fotografie mohou být rozesílány mobilním telefonem nebo prostřednictvím internetu a sociálních sítí. Je spojován především s mladou generací, která pořizuje sexuálně laděné fotografie. Mezi nebezpečí patří vysoké riziko zveřejnění citlivých fotografií potencionálním útočníkem, který může oběť vydírat, šikanovat nebo s ní manipulovat. (Szotkowski at al., 2013, str. 81)

Rizika sextingu:(Kožíšek, 2016, str. 83)

- po odeslání zpráv s citlivým materiálem nad nimi oběť ztrácí kontrolu. Tyto materiály se mohou objevit kdekoli na internetu,
- zaslaný materiál může být kdykoli zneužit proti oběti. Sexting je velice často spojen s jinými rizikovými jevy jako vydírání,
- v případě úniku citlivých materiálů do prostředí internetu oběť musí počítat s tím, že životnost materiálů nejde prakticky smazat, a během několika hodin se materiály mohou objevit kdekoli.

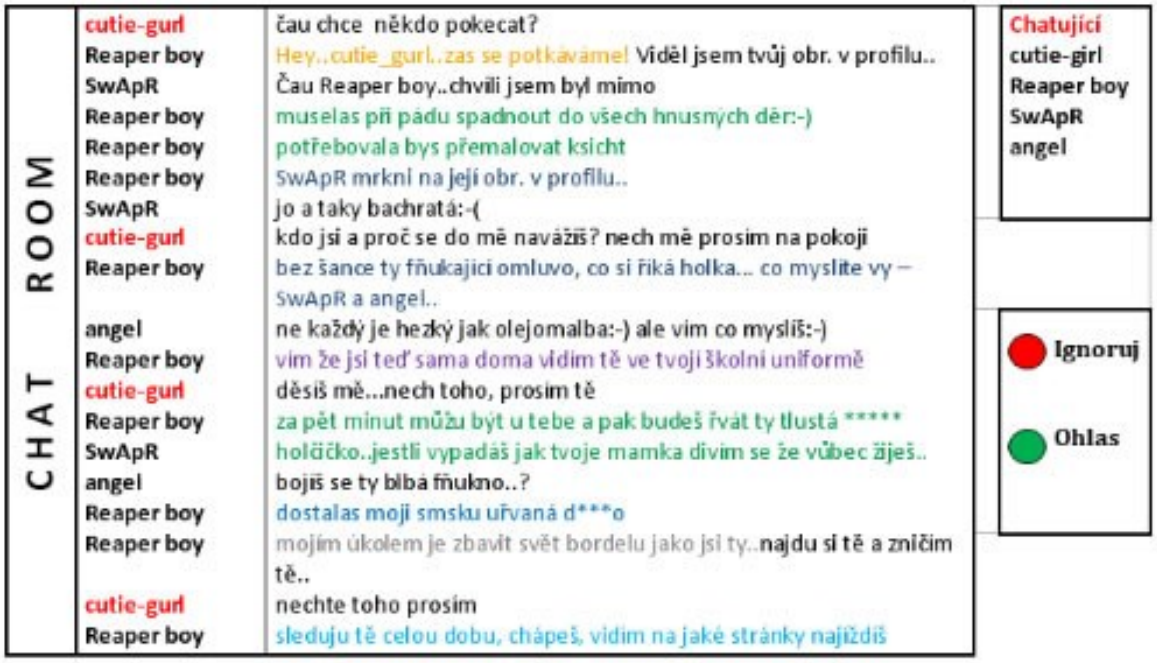
V České republice platí zákon, že děti mohou mít sex od patnácti let, ale pořizování lechtivých fotografií či videí je povoleno od osmnáctého roku života. Tohle ošetřuje zákon č.40/2009 Sb. Trestní zákoník.

Obrázek 3 - Ukázka sextingu (www.sancedetem.cz, 2021)

5.5 Kyberstalking

Je nebezpečné úmyslné a systematické pronásledování v online prostředí. Cílem je navázání a udržování kontaktu s obětí i přes její zjevný nesouhlas. Útočník k tomu může používat různé komunikační prostředky jako sms zprávy, emaily nebo kontaktování na sociálních sítích. Oběť může útočníka zablokovat nebo požádat zakladatele o zablokování útočníka. Kyberstalking může vygradovat až do fyzického pronásledování. Přímým následkem je závažné narušování soukromí, osobní svobody a lidské důstojnosti oběti. V závažných

případech poškození duševního a tělesného zdraví oběti. Oběť je vystavena permanentnímu strachu o svoje zdraví. Mnohdy má pronásledování pro oběť i finanční dopad. (Nebezpečné pronásledování (stalking), 2020)



Obrázek 4 - Ukázka kyberstalkingu (www.e-bezpečí.cz)

5.6 Podvody

Je protiprávní jednání, kdy se chce útočník obohatit na oběti. Zpravidla jsou to podvodné e-shopy nebo falešné inzeráty. Znakem falešných e-shopů je, že nemají odběrové místo na osobní vyzvednutí. Platby probíhají pouze bankovním převodem. Kontaktní telefon neexistuje nebo ho nikdo nezvedá. Po nějaké době e-shop mizí z internetu. Je to proto, že útočníci získají velký finanční obnos od obětí, které svoje objednané zboží samozřejmě nikdy neviděly. Obdobným podvodem jsou i falešné inzeráty, oběti často mohou vybírat z pohodlí domova. Vše bývá přehledné a nabídka je obrovská ale stejně jako u podvodných e-shopů oběť zboží zaplatí a nikdy zboží neuvidí. Profil potom zmizí z internetu. (Kožíšek, 2016, str.111)

Obrázek 5- Ukázka podvodních e-shopů (www.idnes.cz)

5.7 Phishing

Jedná se o speciální techniku používanou na internetu se snahou získat citlivé údaje. Principem phishingu je věrohodné napodobení oficiální žádosti banky nebo podobné instituce a tím získání od oběti její přihlašovací údaje. Po zadání údajů od oběti získává útočník veškeré přihlašovací údaje. Problémem phishingu je, že podvodné stránky jsou věrohodné a těžko rozeznatelné. (Phishing)

Předmět: [redacted] Informace o Vaši zásilce
Datum: Thu, 27 Nov 2014 09:28:50 +0100
Od: Ceská pošta <tracktrace@cs-post24.com>
Společnost: cs-post24.com
Komu: [redacted] .zcu.cz>

logo

[redacted]

Vaše zásilka *DR631396851C* dorazila na 24. listopadu 2014. Courier nebyl schopen doru`eit zásilku pro vás. Vytisknout informace o Vaší zásilky a ukázat, že v nejbližší pošt`i, aby si zásilku.

Stáhn`ite si informace o zásilka
<http://cs-post24.com/service.php?id=027364718>

Pokud je zásilka neobdrží do 15 pracovních dn`u `Eeská pošta bude mít právo nárokovat odškodn`iní od si pro své udržení ve výši 52,5 K`e za každý den vedení.
M`užete si najít informace o postupu a podmínkách poi pozemku chov v nejbližší kanceláoi.

Toto je generován automaticky zprávu, pokud nechcete poijímat zprávy od nás prosím odhlásit <http://cs-post24.com/unsubscribe.php?id=625568844>

Obrázek 6- ukázka Phisingu (www.support.zcu.cz)

5.8 Kyberšikana

Kyberšikana je spjatá s tradiční šikanou. Tyto dva pojmy jsou si velice blízké. Nejdůležitější rozdíl mezi kyberšikanou a tradiční šikanou je ten, že kyberšikana je provozovaná v online prostoru. Není, ale vyloučeno, že se neprojeví v reálném světě.

Další rozdíl mezi kyberšikanou a tradiční šikanou je ten, že u tradiční šikany oběť útočníka zná a ví, jak vypadá a co od něj může čekat. U kyberšikany je útočník naprosto anonymní, a navíc může měnit svoji identitu. Navíc pod štítem anonymnosti je jednodušší sdělit něco přes internet než to říct druhému do očí. Dále je rozdíl v tom, že u tradiční šikany rozhoduje fyzická síla a u kyberšikany využívaní počítačových znalostí. Poslední rozdíl mezi kyberšikanou a tradiční šikanou je takový že, tradiční šikanu jde na oběti snadno vypozorovat, například na oběti jsou patrné známky násilí. Kyberšikana je těžko rozpoznatelná, jelikož oběť se často nepřizná, má pocit, že by ji nikdo nepochopil, a raději se to snaží vyřešit sama. (Kyberšikana a šikana – rozdíly, 2010)

		Tradiční šikana	Kyberšikana
JAK	Způsob	Tváří v tvář.	Za použití ICT.
	Forma	Fyzická, verbální, sociální, ekonomická.	Nevyžádaná, zraňující, vyhrožující sdělení, pořizování a šíření záznamů aj.
	Prostředek	Fyzická zdatnost, verbální obratnost, orientace v sociálních vztazích.	Mobilní telefon, PC, internet (SMS, MMS, e-mail, IM, web, sociální sítě, PC hry).
KDE	Místo	Školní prostředí.	Kdekoli dosahu ICT.
		Nejbližší okolí.	Celý svět.
KDY	Čas	Před/v průběhu/po školním vyučování.	Kdykoli 24 hodin/7 dní v týdnu.
	Trvání	Opakovaná akce.	Jednorázový akt.
	Expozice	Jednorázově.	Opakovaně.
KDO	Identita aktérů	Vzájemná znalost.	Anonymita.
	Agresor	Fyzická/sociální převaha.	Pokročilá znalost ICT.
	Publikum	Pasivní přihlížející, omezený počet.	Aktivní šiřitelé (stávají se agresory). Nekončící publikum (celý svět).
	Oběť	Fyzicky, sociálně slabší.	Kdokoli, příp.s menší znalostí ICT.
	Dospělí	Informování, zapojení, prevence i intervence.	Nedostatečná úroveň, nízká úroveň supervize.

Obrázek 7- Rozdíl mezi kyberšikanou a tradiční šikanou(www.medium.com, 2017)

Specifické projevy kyberšikany:

1. Publikování ponižujících záznamů nebo fotografií

   Publikováním je míněno zveřejňování ponižujících záznamů nebo fotografií na internetu nebo jejich posílání pomocí mobilních telefonů.

2. Ponižování a pomlouvání

   Útočník se snaží poškodit pověst oběti a narušit její vztahy tím, že o ní zveřejňuje nepravdivé informace nebo ji uráží a ponižuje.

3. Krádež identity, zneužití cizí identity ke kyberšikaně

   Tento projev kyberšikany je mezi útočníky jedním z nejoblíbenějších. Cílem je získat přístup do cizího elektronického účtu a ten následně zneužít ke kyberšikaně jeho majitele. (Szotkowski, 2013, str. 9,11,12)

Útočník kyberšikany:

Základní škola:

- sociálně a emocionálně nezralý, necitlivý.
- s poruchou pozornosti, hyperaktivitou a poruchami chování.
- fyzicky nebo psychicky zdatný, nadprůměrně inteligentní.

Střední škola:

- málo úspěšný, ale s vysokou potřebou sebeprosazení.
- pocházející z majetné rodiny nebo rodiny s významným společenským postavením.
- setkal se s šikanou na základní škole, ať už v roli agresora, svědka nebo oběti. (Martínek, 2015, str. 176,177)

Oběti kyberšikany:

Obětmi kyberšikany jsou většinou děti, které kolektiv přijímá jen obtížně, či je dokonce odmítá. Oběti o sobě na internetu ve větší míře uveřejňují osobní údaje. Díky tomu se se stávají zranitelnějšími, protože je útočník proti oběti může lehce použít. (Černá,2013, str. 63)

II. PRAKTICKÁ ČÁST

6 ZPRACOVÁNÍ ANALÝZY

V teoretické části byla rozebrána možná rizika a hrozby se kterou se mládež může setkat při práci s počítačem. V praktické časti se zaměřím na analýzu a vyhodnocení dotazníkového šetření. Jako první metoda bude použita Check list, ve kterém byli sestaveny otázky za pomocí poznatků z teoretické části a z otázek dotazníkového šetření. Po tomto kroku bude jako druhý nástroj analýzy rizik bude použita metoda What if ve které, budou řešeny otázky jako, „Co se stane, když mládež…“, v této metodě na ni budou vyhodnoceny možné následky a doporučená opatření. Dalším nástrojem bude matice rizik. Za pomocí tabulek pravděpodobnosti a dopadu, budou rizika roztřizena do tří kategorií, a to na přípustná, nebezpečná ale ještě přípustná a na nepřípustná rizika. K těmto výsledkům následně budou předloženy návrhy opatření. Posledním nástrojem je dotazníkové šetření, které bylo rozesláno elektronicky na cílové skupiny respondentů tzn. žákům základních škol a studentům středních škol. Dotazník byl sestaven tak aby bylo možné zjistit, zda se již setkali s nějakou hrozbou nebo mají povědomí o tom, že se při práci s počítačem na ně mohou narazit. Po vyhodnocení dotazníku byli výsledky rozděleny na podkategorie mužů a žen podle věkových kategorií. Dotazník bude také vyhodnocen a budou předloženy návrhy opatření.

6.1 Výzkumné šetření

Pro odhalení možných rizik jsem zvolila metodu Check list. Tabulka byla vypracována na základě poznatků z teoretické časti a odpovědí získaných z dotazníkového šetření.

Tabulka 1 – Check list

P.Č.	Otázka	ANO	NE
1	Zvládá mládež základy práce s počítačem?	X	
2	Má mládež čas strávený na počítači pod kontrolou?		X
3	Ví mládež, jak správně sedět u počítače?		X
4	Ví mládež, z jaké vzdálenosti se dívat do obrazovky počítače?		X
5	Používá mládež antivirový program?	X	
6	Používá mládež silná hesla k účtům?		X

7	Má mládež dostatečnou znalost možných bezpečnostních rizik?	X	
8	Ví, mládež, jak správě sdílet soukromá data?		X
9	Ví mládež, jak se chovat v prostředí internetu?	X	
10	Umíme rozpoznat cílený útok?		X
11	Umí mládež rozeznat, zda na sociálních sítích komunikujeme se svými vrstevníky?		X
12	Dbá mládež na věková doporučení sociálních sítí a online her?		X

V tabulce č.1 se uvádí možná rizika spojená s užíváním počítače. U otázky č. 1 byla zvolena odpověď „ANO“, protože žáci a studenti mají v rámci studia předmět informatika, kde získávají potřebné základní znalosti práce s počítačem. V otázce č. 5 je opět odpověď „ANO“, protože většina uživatelů využívá alespoň základní balíček antivirového programu. U otázky č. 7 je odpověď „ANO“, ale během dotazníkového šetření vyplynulo, že teoretické znalosti této problematiky neumí mládež využít v praxi. V otázce č. 9 byla zvolena odpověď „ANO“, tato odpověď vychází z otázek č. 1 a 7, protože žáci a studenti tyto informace získávání i během studia ve škole, ale někteří z nich tyto poznatky nerespektují.

Metoda What-if

Po zpracování tabulky č.1 CLA jsem navázala na metodu What-if, ve které jsem odpovídala na otázky, co se stane když…

Tabulka 2 - What-If

P.Č.	Co se stane když…. Mládež	Následek	Opatření
1	Nehodnoceno		
2	tráví na počítači příliš mnoho času	Závislost, zdravotní potíže	Kontrola času
3	u počítače nesedí správně	Zdravotní problémy zejména v oblasti zad a krční páteře	Kontrola nastavení židle a stolu

4	neví, jak správně mít umístěnou obrazovku počítače	Zhoršení zraku	Kontrola vzdálenosti monitoru od očí
5	Nehodnoceno		
6	nepoužívá silná hesla k účtům	Prolomení hesel k uživatelským účtům (sociální sítě, online hry, bankovní účty, email) , ztráta citlivých informací	Používání silných hesel, popřípadě generátorů hesel
7	Nehodnoceno		
8	nesdílí soukromá data správně	Únik citlivých dat do špatných rukou	Kontrola všech příjemců při sdílení dat
9	Nehodnoceno		
10	neví, že se můžeme stát obětí cíleného útoku	Snazší podlehnutí útočníkovi, krádež dat, kyberšikana, kybergrooming, sexting, vydírání, phising	obezřetnost
11	neví, zda komunikuje s lidmi z jeho věkové skupiny	Podání citlivých informací cizí osobě, kyberšikana, kybergrooming, sexting, vydírání	Nekomunikovat s lidmi, které neznáme
12	neřídí se doporučenou věkovou hranicí u sociálních sítí a online her	Přístup k obsahu, který není vhodný pro doporučený věk	Kontrola ze strany rodičů

Matice rizik

Matice rizik byla sestavena na základě metody What-if. Zde byla rozdělena pomocí pravděpodobnosti a dopadu roztřídila rizika na přijatelná, nebezpečná, ale ještě přípustná a nepřípustná, u kterých je potřeba uskutečnit nápravná opatření.

Tabulka 3 - Pravděpodobnost

I	Téměř nikdy	Stalo se 0x – 1x
II	Někdy	Stalo se 1x – 10x
III	Často	Stalo se více jak 10x

Tabulka 4 - Dopad

A	Nízký	Mírný dopad
B	Střední	Omezující
C	Vysoký	Problém

Tabulka 5 - Matice rizik

P/D	**A**	**B**	**C**
I	1	3	6
II	2	5	8
III	4	7	9

Hodnocení:

1-3 přijatelná rizika

4-6 nebezpečná, ale ještě přijatelná rizika

7-9 nepřijatelná rizika

Vyhodnocení rizik

V tabulce jsou zapsána vyhodnocená rizika, která jsou zvýrazněna barvou pro lepší orientaci. Zelená barva představuje přijatelná rizika, oranžová barva nebezpečná, ale ještě přípustná rizika a červená barva představuje nepřípustná rizika.

Tabulka 6 – Vyhodnocení matice rizik

P.Č.	Pravděpodobnost	Dopad	Hodnocení
2	III	C	9
3	II	B	5
4	II	B	5
6	III	C	9
8	III	C	9
10	III	B	7
11	II	C	8
12	II	B	5

Při vyhodnocení bylo zjištěno, že u otázek č. 2, 6, 8, 10, 11 byli zjištěny nepřijatelná rizika

6.2 Nápravná opatření

Návrh opatření u otázky č. 2: Mládež tráví na počítači příliš mnoho času.

Čas strávený mladistvými uživateli obrazovky je jeden s rizikových faktorů, které byly zjištěny. Tento problém je dost zásadní, jelikož uživatel může ztrácet kontakt s reálným světem a žít pouze virtuálně. Dále se zvyšují možná zdravotní rizika, kterými u mládeže mohou být obezita, další zdravotní obtíže či psychické potíže.

Proto je nutné:

- zavést časová omezení strávených na počítači stanovené rodiči,
- kontrola rodiči,
- trávit více času s vrstevníky v reálném světě,
- zájmové činnosti, kroužky,

- sportovní aktivity.

Návrh opatření u otázky č. 6: Mládež nepoužívá silná hesla k účtům

Mladiství uživatelé používají slabá hesla ke svým účtům, což vede k napadení účtů a následně ke krádeži. Mohou to být bankovní účty, případně profily na sociálních sítích nebo v online hrách.

Proto je nutné:

- používat generátor hesel,
- používat dlouhá silná hesla, která obsahují velká a malá písmena, číslice a speciální znaky.
- nikdy nepoužívat banální a snadno uhodnutelná hesla jako např. datum narození nebo naše jméno.

Návrh opatření u otázky č. 8: Mládež nesdílí soukromá data správně

Mladiství uživatelé nesdílí svá soukromá data správně, což může vést k úniku citlivých dat do prostřednictví internetu nebo do rukou útočníka, který poté může tyto materiály použít proti oběti.

Proto je nutné:

- zvýšit informovanost ze strany školy,
- pomoc rodičů,
- na internetu neuvádět všechny osobní informace.

Návrh opatření u otázky č. 10: Mládež neví, že se může stát obětí cíleného útoku

Pokud mladí uživatelé nerozpoznají, že se mohou stát obětí cíleného útoku, mohou útočníkovi nahrát v jeho prospěch.

Proto je nutné:

- větší informovanost ze strany školy o možných praktikách cíleného útoku,
- mít informace od rodičů o možných praktikách cíleného útoku,

- neodpovídat na podezřelé e maily, zprávy,
- nikdy nesdělovat osobní informace cizím lidem na internetu.

Návrh opatření u otázky č. 11: Uživatel neví, zda komunikuje s lidmi jeho věkové skupiny

Riziko, kdy mladí uživatelé neví, zda komunikují se svými vrstevníky je velmi vysoké. Mohou se stát obětí kyberšikany, kybergroomingu nebo sextingu. V podstatě nikdy neví, kdo sedí na druhé straně monitoru. Jestli je to opravdu jeho kamarád anebo nějaký útočník, který se za kamaráda pouze vydává.

Proto je nutné:

- kontrolovat profily kontaktů,
- nepřidávat si neznámé lidi do přátel,
- kontrolovat údaje,
- kontrola ze strany rodičů,
- apelovat na tuto problematiku ze strany školy videa, přednášky.

7 DOTAZNÍKOVÉ ŠETŘENÍ

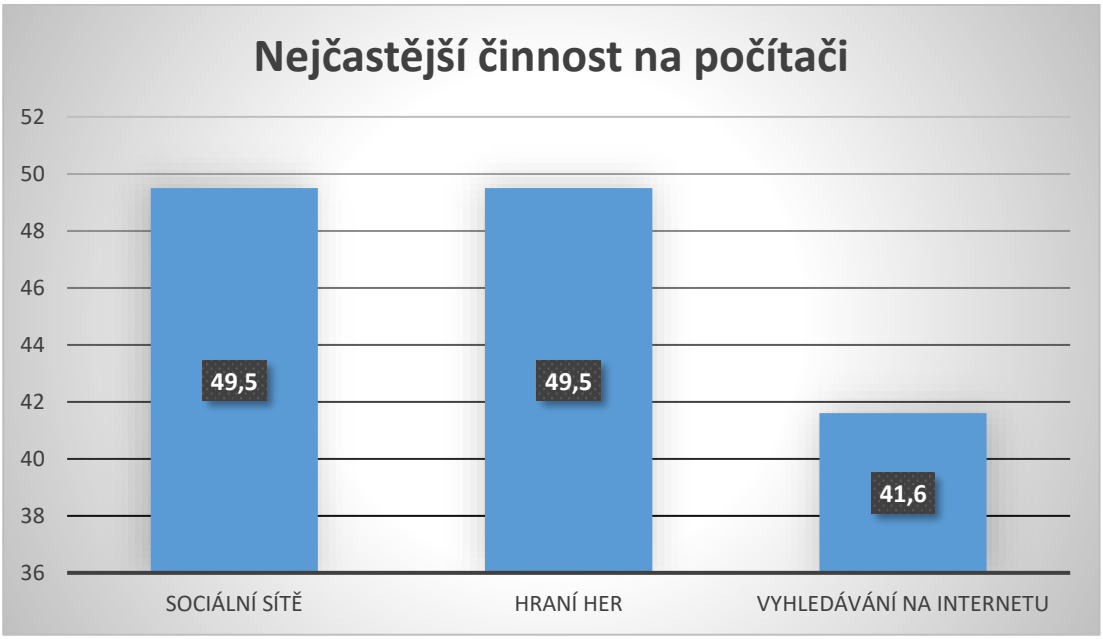
Dotazníkové šetření probíhalo u mládeže ve věkovém rozpětí 10-15 let a 15-18 let.
Cílem bylo zjistit, k čemu mládež počítač nejčastěji používá, kolik času tráví na počítači, zda mládež má nějaké zkušenosti s kybernetickými hrozbami. Dotazník vyplnilo 101 respondentů. Výsledky dotazníku se nejsou vázány ke konkrétním školám. Byly rozesílány lidem v mém okolí, kteří mají děti v požadovaném věku a dotazník se poté šířil mezi jejich spolužáky. U otázek bylo na výběr z více možností, a i možnost vyjádřit odpověď vlastními slovy, například v otázce „Jaké používáte sociální sítě?“. Dotazník byl elektronický, vytvořený na internetu v aplikaci Survio. V této aplikaci se sběr dat vyhodnocoval v grafech nebo v jednotlivých odpovědích. Jednotlivé odpovědi byly vypracovány podrobněji a hodnotily se i některé otázky podle pohlaví a věku respondentů. Cíleně byla zvolena dvě nejaktuálnější témata, a to sociální sítě a online hry, kde se domnívám, že dotazovaná mládež tráví nejvíce času.

7.1 Vyhodnocení otázek dotazníku

Z celkového počtu respondentů dotazník vyplnilo 60 žen a 41 mužů. Z toho bylo 66 % respondentů ve věku 10-15 let a 34 % ve věku 15-18 let. Jak je vidět v odpovědích dotazníku se účastnili zástupci obou pohlaví i věkových skupin. Věkově je u respondentů menší nepoměr ve prospěch mladší věkové skupiny. Více jak 40 % respondentů u počítače denně tráví 1 hodinu a méně. Pouze necelých 10 % uvedlo 6 a více. Po následném rozebrání dotazníku podle pohlaví a věku, bylo zjištěno, že ženy ve věkovém rozmezí 10-15 i ve věkovém rozmezí 15-18 let nejčastěji tráví na počítači 1 hod a méně. U věkové kategorii 15-18, ale stejné procento žen tráví 4-5 hodin. A u mužů bylo zjištěno, že muži ve věkové kategorii 10-15 let nejčastěji tráví na počítači 4-5 hodin. A muži ve věku 15-18 let 1 hodinu a méně. Při porovnání všech zúčastněných skupin, bylo vysledováno, že nejvíce času u počítače tráví muži ve věku 10-15 let, a ženy ve věku 15-18 let.

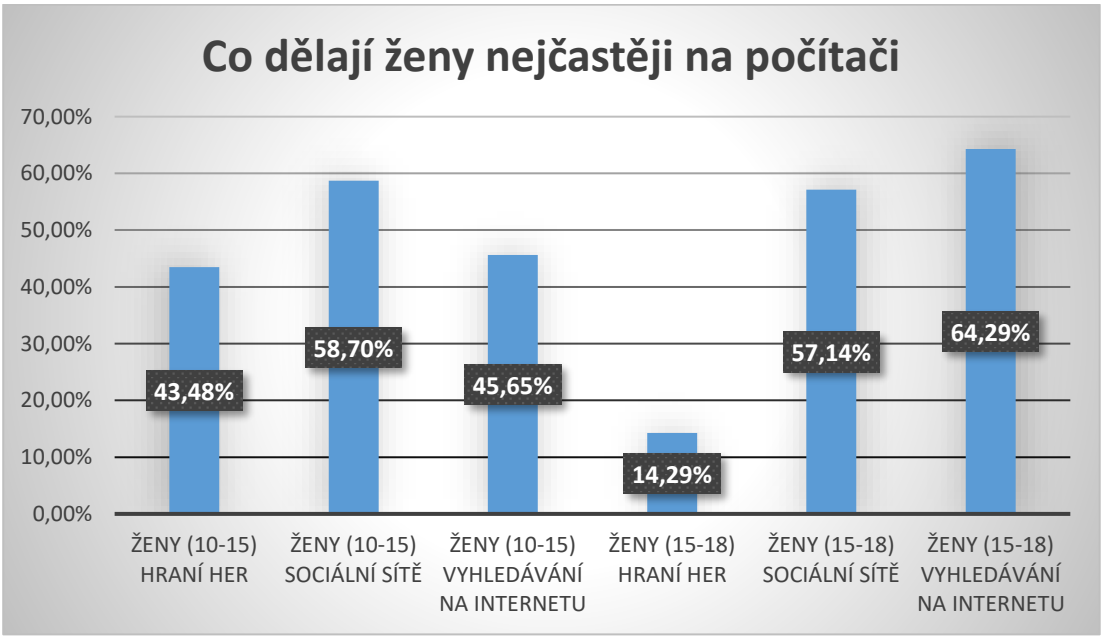
Otázka č.4: Co na počítači nejčastěji děláte?

Otázka, co na počítači nejčastěji děláte byla otevřená a respondenti při odpovědi mohli vybírat z více možností. Z grafu (obr. 8) lze vyčíst, že nejčastější činností jsou sociální sítě 49,5 %, zároveň s hraním her 49,5 % a jako třetí nejčastější činnost je vyhledávání na internetu. Zaznamenané odpovědi na otázky byly pro lepší posouzení následně rozděleny do dvou samostatných grafů podle pohlaví a věku.



Obrázek 8 - Graf "Nejčastější činnosti na počítači" (vlastní zpracování)

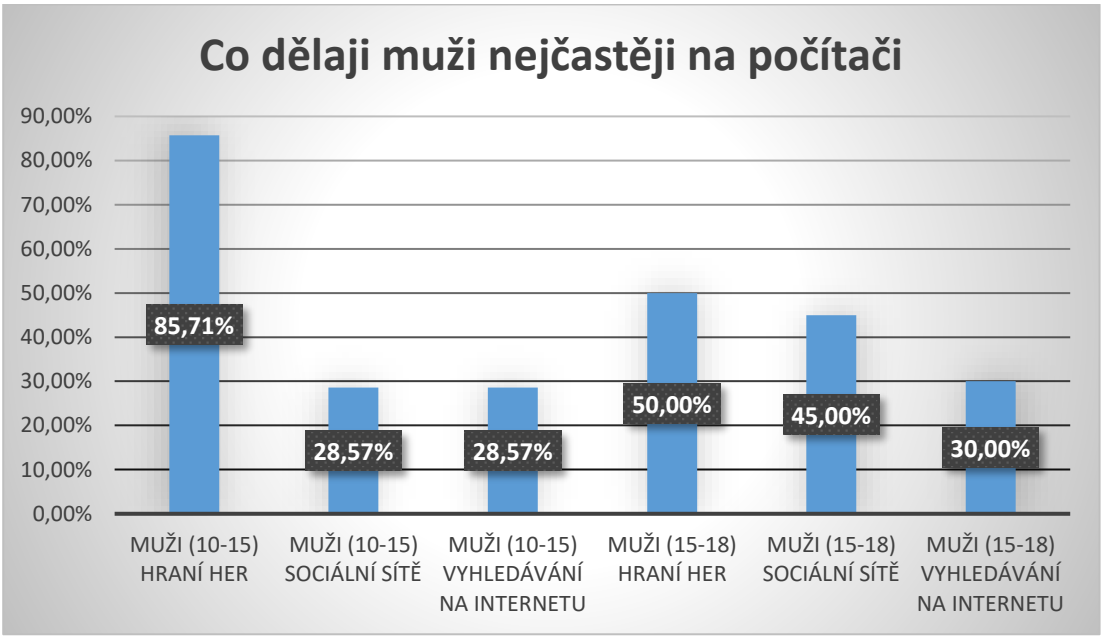
V grafu (obr. 9), který sleduje co, ženy nejčastěji dělají na počítači, vyplynuly následující výsledky. U věkové kategorie 10-15 let byly nejčastější činností sociální sítě, poté vyhledávání na internetu a jako poslední bylo hraní her. U věkové skupiny 15-18 let byly jako nejčastější činnost uvedeno vyhledávání na internetu, poté sociální sítě a jako poslední hraní her.



Obrázek 9 - Graf "Co dělají ženy nejčastěji na počítači" (vlastní zpracování)

U mužů obou věkových skupin je nejčastější činností na počítači hraní her viz (obr. 10). U věkové kategorie 10-15 let jsou poté sociální sítě a vyhledávání na internetu druhou nejčastější činností. U věkové kategorie mužů 15-18 let jsou sociální sítě jako druhá nejčastější činnost a následně vyhledávání na internetu.

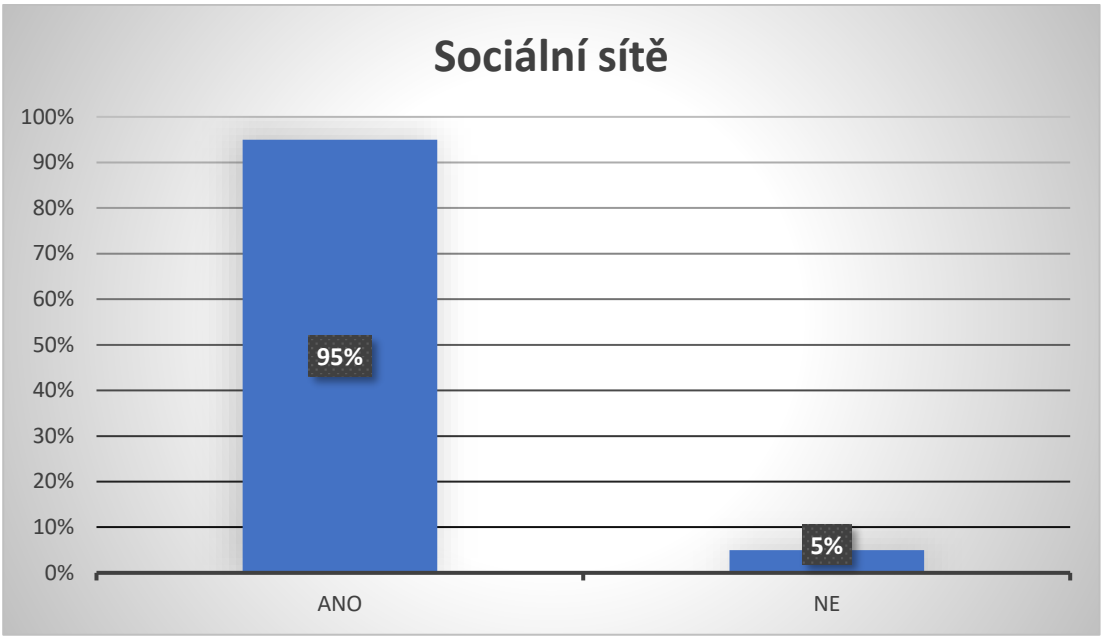
Při porovnání grafů mužů a žen bylo zjištěno, že muži na počítači dávají přednost počítačovým hrám a ženy sociálním sítím a vyhledávání na internetu.



Obrázek 10 - Graf „Co dělají nejčastěji muži na počítači“ (vlastní zpracování)

Otázka č.5: Používáte sociální sítě?

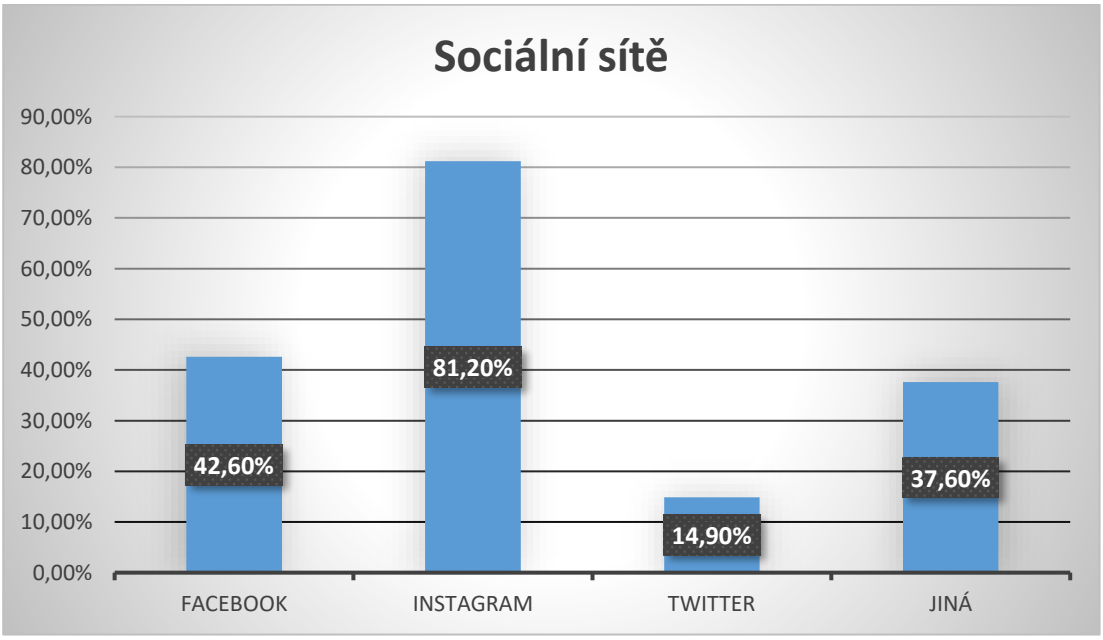
U otázky, zda používají sociální sítě odpovědělo 95 % respondentů, že ano a pouze 5 % odpovědělo ne. Zde je vidět, jakou roli hrají sociální sítě v životě mladých lidí.



Obrázek 11- Graf "Používáte sociální sítě" (vlastní zpracování)

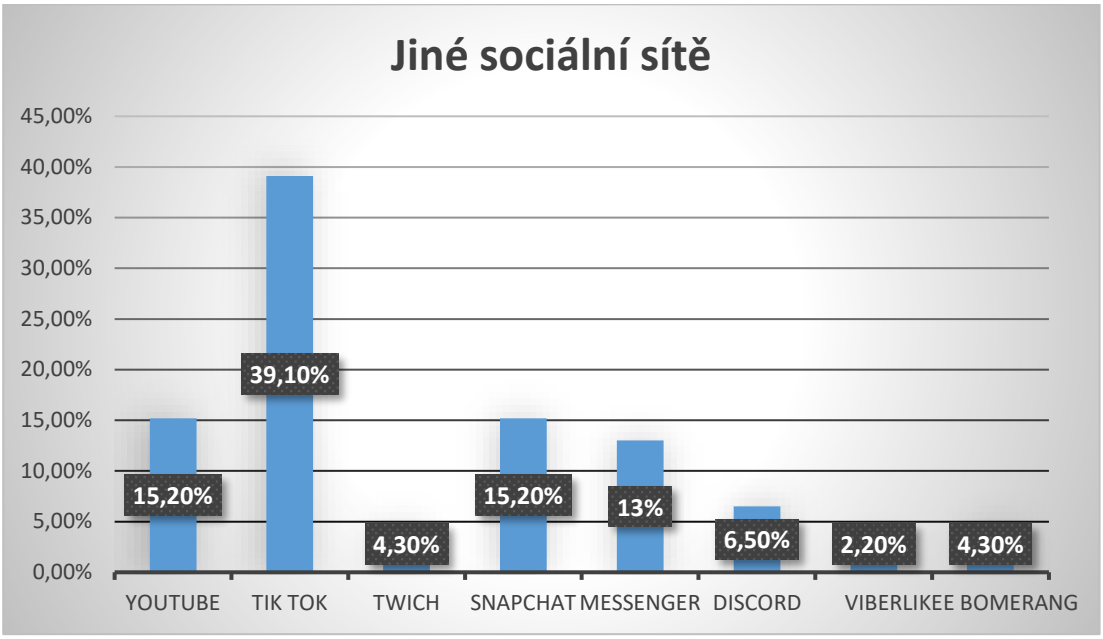
Otázka č. 6: Pokud ano jaké?

Jako nejčastěji používanou sociální síť zvolilo 81 % respondentů Instagram. Následovaný Facebookem, který používá více jak 42 % respondentů. Sociální síť Twitter obdržela necelých 15 %. Více jak 37 % respondentů uvedlo možnost „Jiná“. Sociální sítě, které byly specifikovány v poslední možnosti jsou rozebrány v další otázce.



Obrázek 12- Graf "Druhy sociálních sítí (vlastni zpracování)

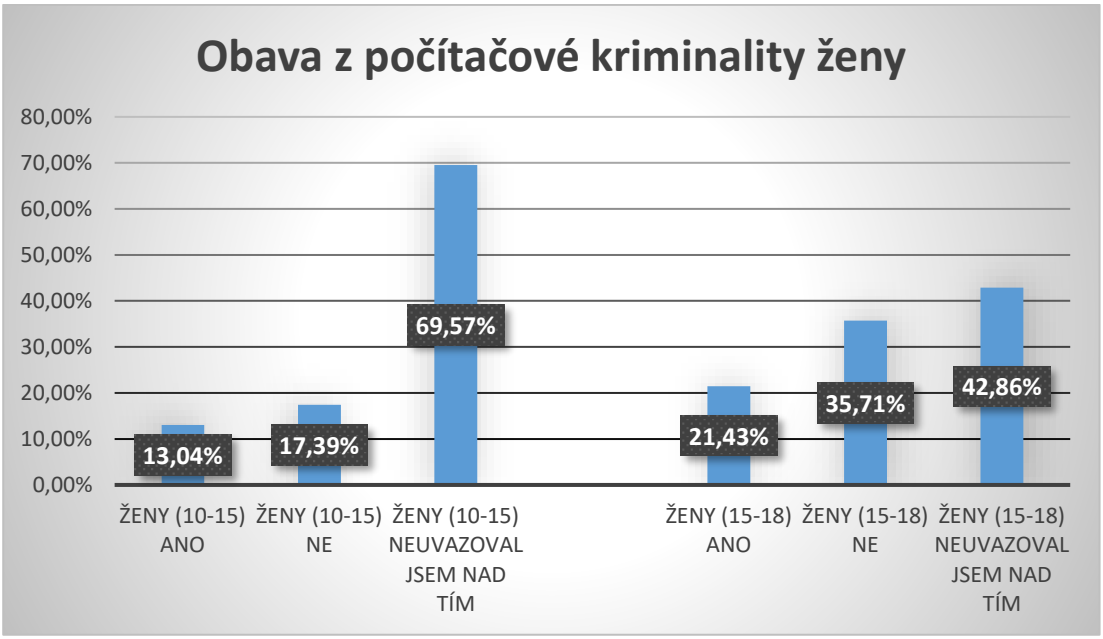
Z jiných sociálních sítí lze zmínit Tik Tok s 39 %, který nabírá v poslední době velkou popularitu. A určitě i stále populární YouTube a Snapchat s více jak 15 %.



Obrázek 13 - Graf "Jiné sociální sítě" (vlastní zpracování)

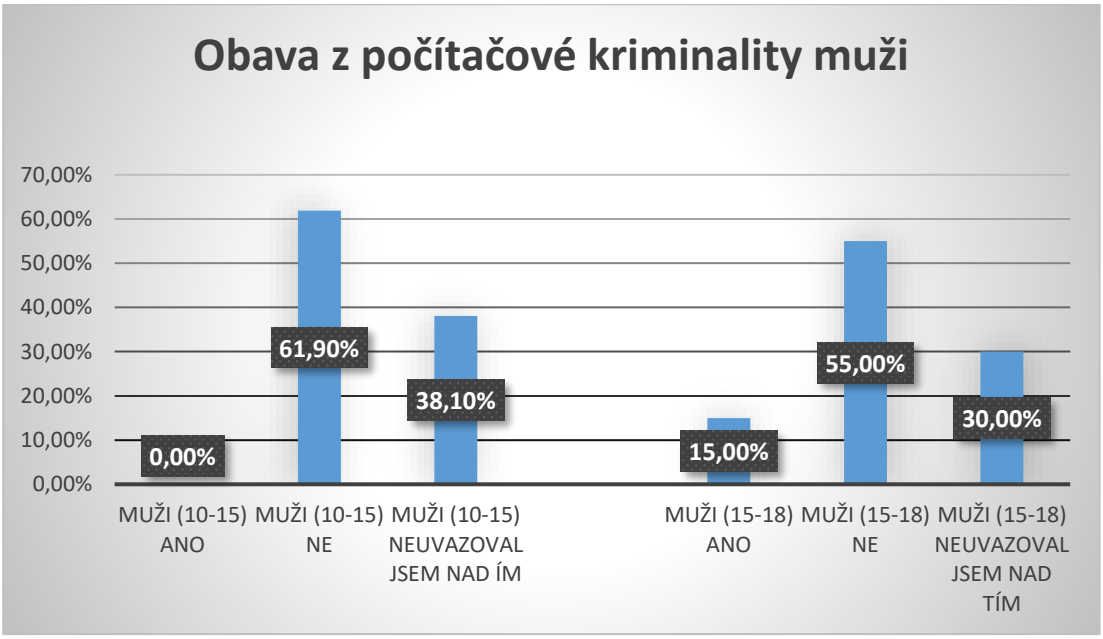
Otázka č.7: Máte obavu, že byste se mohli stát obětí počítačové kriminality?

Výsledky této otázky jsou u žen přinejmenším překvapivé (obr. 14). Kdy téměř 70 % žen ve věku 10-15 let a 42 % žen ve věku 15-18 let neuvažovala nad možností, že by se mohli stát obětmi kybernetické kriminality. A pouhých 13 % respektive 21 % žen uvedlo, že má obavy z toho, že by se mohly stát obětí kybernetické kriminality.



Obrázek 14 - Graf "Obava z počítačové kriminality ženy"

Zato u mužů je situace odlišná, tam jasně vítězí odpověď „ne“, tedy nemají obavu, že by se mohli stát obětí kybernetické kriminality. Pouze 15 % můžu ve věku 15-18 let má obavy z kybernetické kriminality.

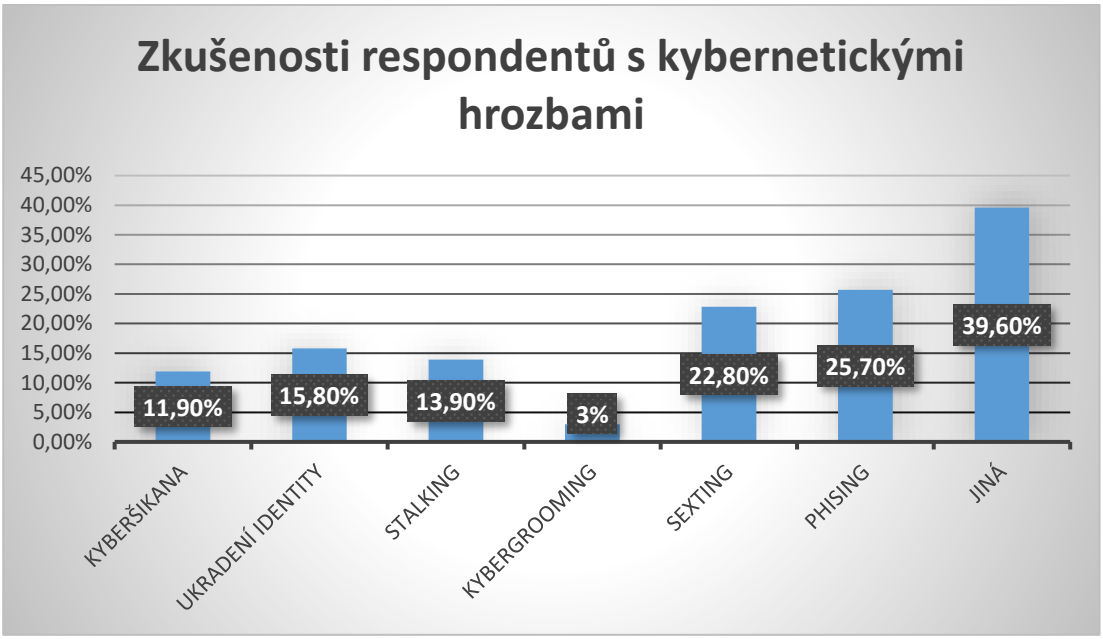


Obrázek 15 - Graf "Obava z počítačové kriminality muži"

Při porovnání grafů mezi muži a ženy bylo zjištěno, že pohled na riziko kybernetické kriminality se velmi liší mezi pohlavím a i věkem.

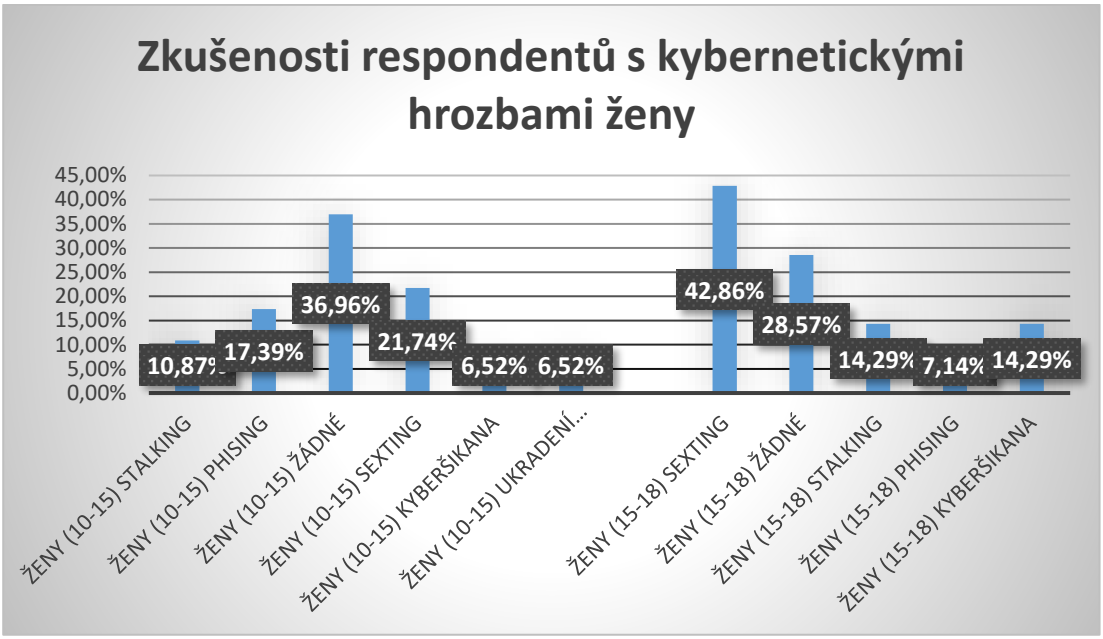
Otázka č. 8: S kterou kybernetickou hrozbou jste se již setkali?

V otázce, s kterou kybernetickou hrozbou jste se již setkali respondenti odpověděli pojmem jiná, která v tomhle případě znamenalo nic nebo žádná, byla vypsaná slovy 39,6 %. Nejčastější kybernetickou hrozbou je tedy podle respondentů phising 25,7 % a následně sexting 22,8 %.



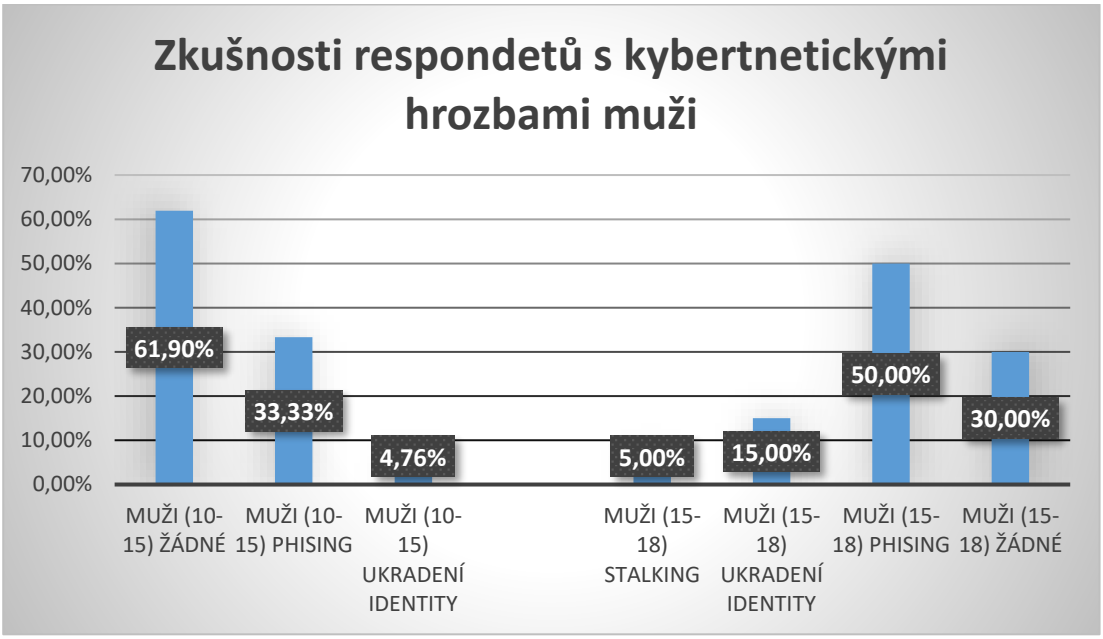
Obrázek 16 - Graf " zkušenosti respondentů" (vlastní zpracování)

U obou věkových skupin se jako nejčastější hrozba objevuje sexting. U mladších žen, lze pozorovat vyšší procento těch, které nemají žádnou zkušenost s kybernetickými hrozbami (téměř 37 %). Ve skupině starších, již toto procento klesá (28 %).



Obrázek 17 - Graf " zkušenosti žen" (vlastní zpracování)

U mužů je situace odlišná, nejčastější hrozba vyplývající z odpovědi žen úplně vypadla. Více jak 60 % z mladších respondentů nemá žádnou zkušenost s kybernetickými hrozbami. U starších toto procento kleslo na polovinu a nejčastější hrozbou je pro ně phising s 50 %.

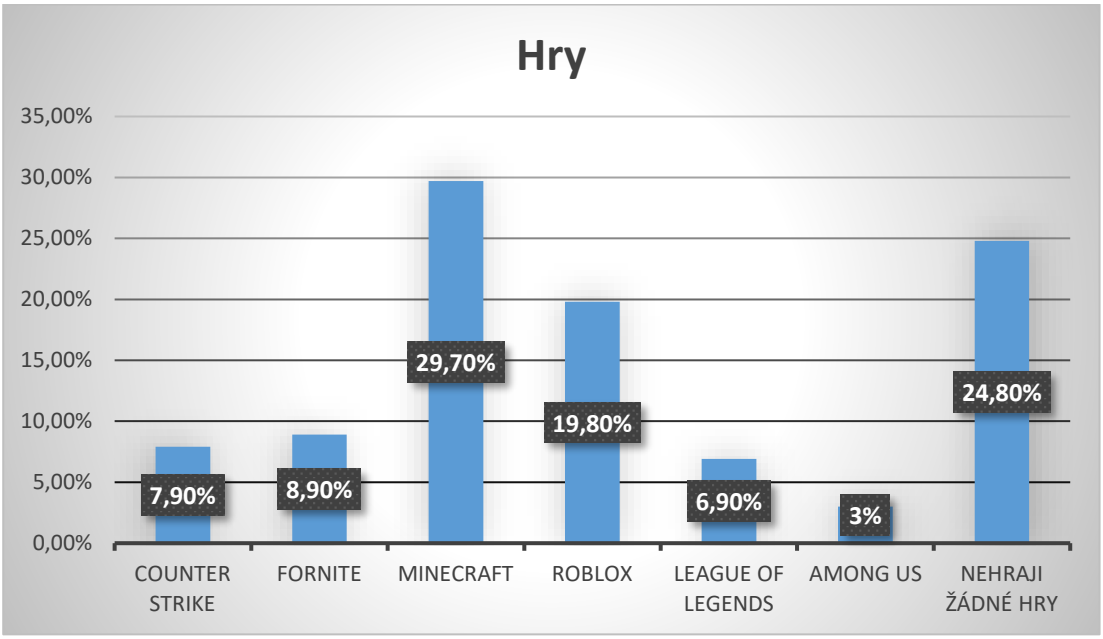


Obrázek 18 - Graf "zkušenosti mužů" (vlastní zpracování)

Pouze 37 % dotázaných žen ve věku od 10 do 15 let nemá žádnou zkušenost se zmíněnými kybernetickými hrozbami, tato hodnota je více než neuspokojivá. U starších žen pokles na 28 % dorovnává hranici u mužů ve stejné věkové kategorii. Avšak u mužů je propad mezi věkovými skupinami daleko dramatičtější, celých 30 %.

Otázka č. 9: Pokud hrajete počítačové hry, jaké to jsou?

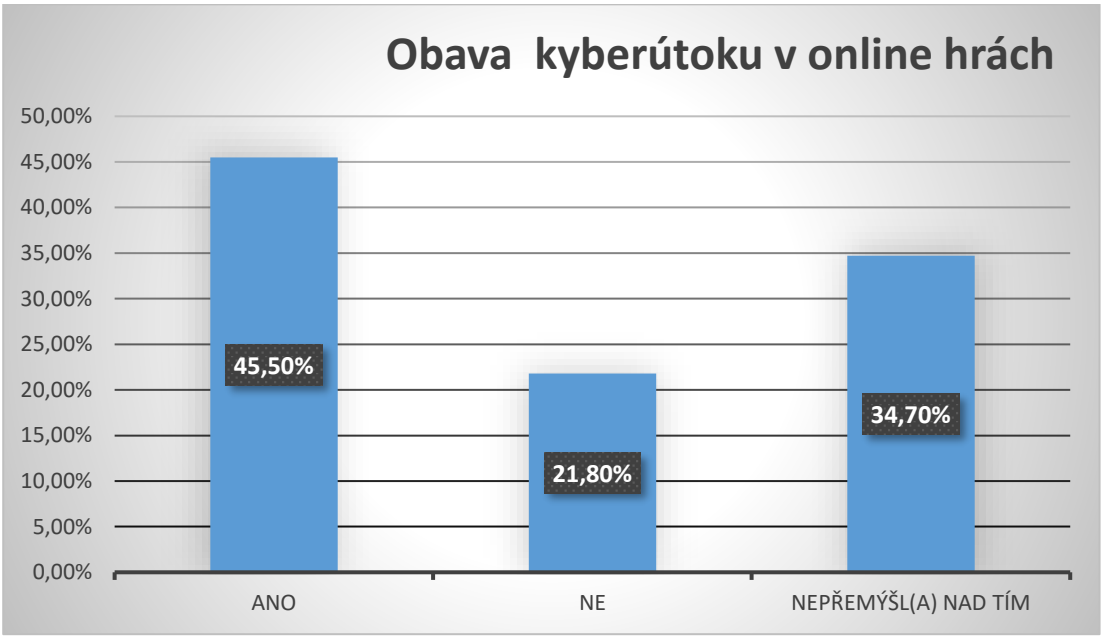
Otázka byla vytvořena tak, aby respondenti mohli do pole vypsat libovolný počet her, které hrají. Z velkého množství odpovědí byli vybrány ty nejčastější. Většina zvolených her spadá do kategorie online her, kde hráči mají možnost spolu komunikovat. Jako nejhranější hru uvedli respondenti hru Minecraft s více jak 29 %. Překvapivě druhá nejčastější odpověď byla, nehraji žádné hry.



Obrázek 19 - Graf "hry" (vlastní zpracování)

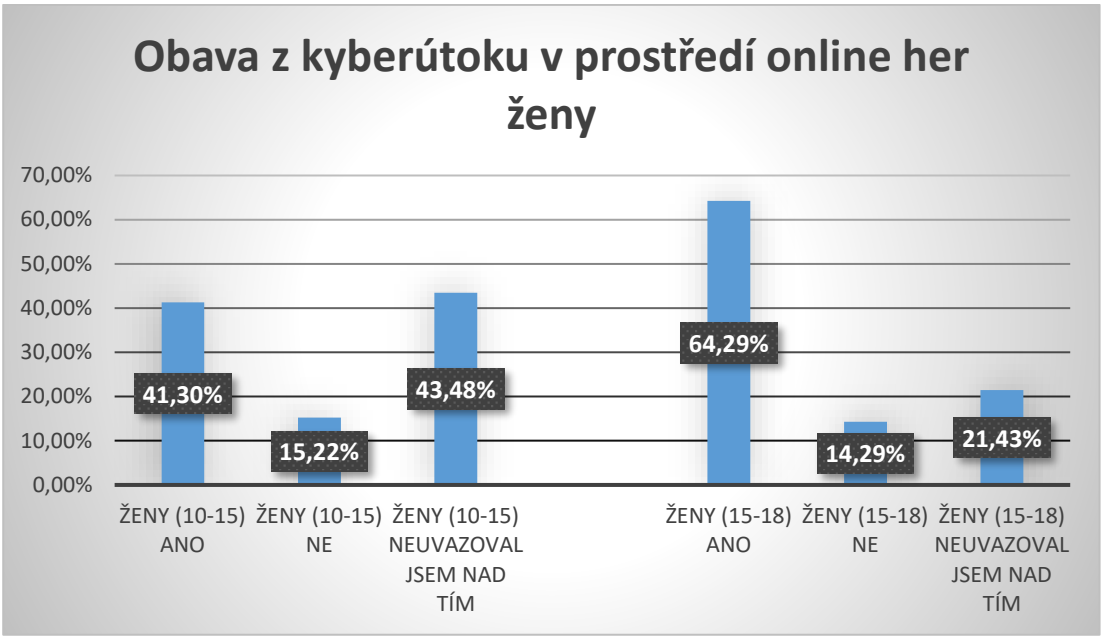
Otázka č. 10: Myslíte si, že při online hrách se můžete stát obětí kyberútoku?

Z celkového počtu respondentů byla nejčastější odpověď ano 45 %.



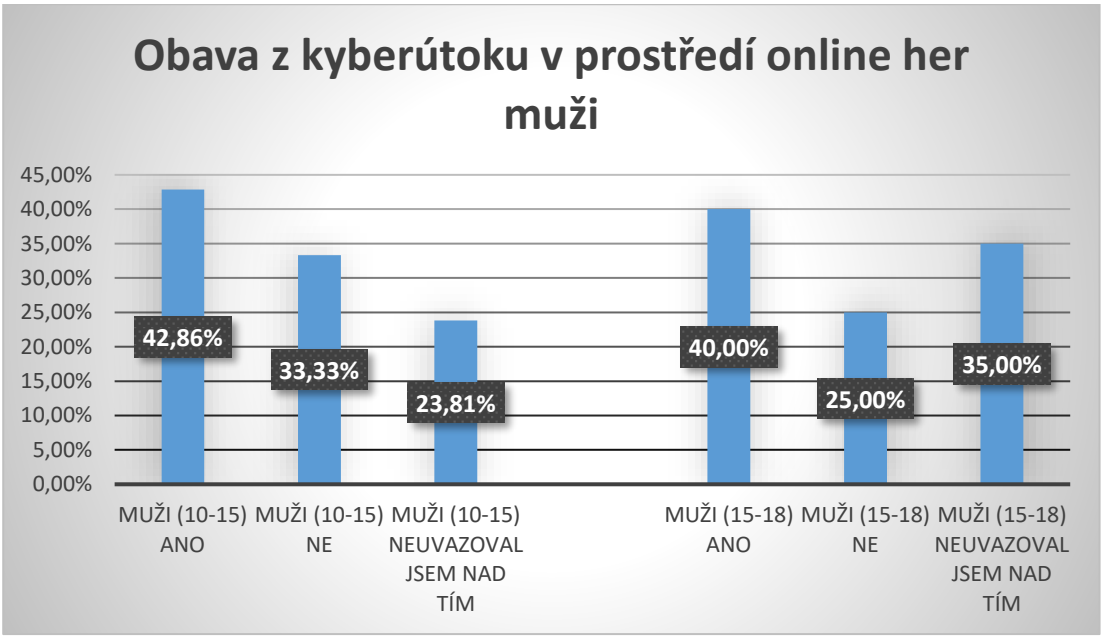
Obrázek 20 - Graf " Máte obavu z kyberútoku v online hrach" (vlastní zpracování)

I když u odpovědí respondentů ženského pohlaví nedominovala odpověď, že na počítači nejčastěji hrají hry, tak i přes to bylo u starších žen odpovězeno, že mají obavu z kyberútoku v online hrách a to celých 64 %. U mladší skupiny žen byla odpověď Neuvažovala jsem nad tím, a to v zastoupení 43 %.



Obrázek 21 - Graf " Kyberútok v online hrách ženy (vlastní zpracování)

Muži jako nejčastější činnost na počítači uvedli hraní her. A to se projevilo i v tomto grafu, kde více jak 40 % respondentů z obou věkových skupin odpovědělo kladně k obavám z kyberútoku v prostředí online her.



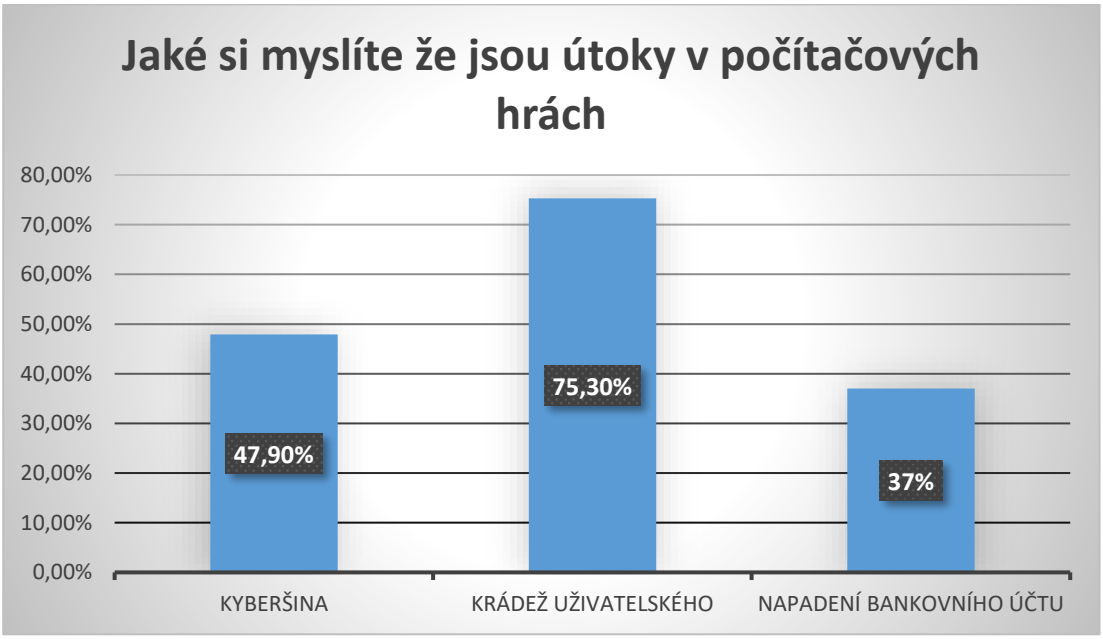
Obrázek 22 - Graf " kyberútok v online hrách muži (vlastní zpracování)

Tento rozdíl mezi ženami a muži z obav kyberútoku v online hrách je dán tím, že muži podle předešlých výsledků tráví více času na počítači hraním her. I když zajímavé zjištění u žen

ve věku 15-18 let, které neuvedly jako nejčastější činnost na počítači počítačové hry, má obavy z kyberútoku, a to celých 64%.

Otázka č. 11 Pokud jste odpověděli Ano jaké to jsou?

Nejvíce respondentů uvedlo, že nejčastější hrozbou v online hrách je krádež uživatelského účtu, a to v zastoupení 75 %. Následně kyberšikana v zastoupení 48 % a jako poslední napadení bankovního účtu 37%



Obrázek 23 - Graf " útoky v počítačových hrách" (vlastní zpracování)

Vyhodnocení

V dotazníkovém šetření bylo zjištěno, že ženy ve věkové skupině 15–18 let a muži ve věkové skupině 10-15 let tráví na počítači 4-5 hodin. U mužů ve věkové skupině 15-18 let bylo zastoupení ve 20 % více jak šest hodin. Tento poznatek z dotazníkového šetření dokazuje fakt, že mladiství uživatelé tráví spoustu času na počítačích. A je zjevné riziko závislosti a zdravotních problémů. Dle mého názoru by měl být striktně zaveden čas trávený na počítači a omezen rodiči jen na určitou dobu.

Dalším znepokojivým zjištěním bylo, že respondenti nemají obavu nebo neuvažovali nad možností kyberútoku. Toto zjištění je téměř totožné s otázkou č. 10, ve které byla řešena otázka, zda uživatelé ví, že se mohou stát obětí cíleného útoku. A otázka č. 11 zda uživatel neví, že komunikuje s lidmi z jeho věkové kategorie. Největším rizikem je nerozpoznání

možné hrozby a snadnější podlehnutí útočníkovi. U mladistvých to může vést ke zhoršení psychického stavu (změny nálad, deprese, úzkosti), finančním ztrátám, změnám v chování. Proto by na školách měli apelovat na možné rizika, a i rodiče by měli mít povědomí o možných hrozbách a mluvit s mládeží o hrozbách v online prostředí.

Bylo zjištěno, že ženy se setkaly v online prostředí s hrozbou zvanou sexting, což je rozesílání intimních fotografií. Tato hrozba je velmi závažná, jelikož citlivé fotografie se mohou objevit kdekoli na internetu, pokud půjde příjemci o to ublížit odesílateli obsahu. Proto doporučuji vyvarovat se posílání intimních fotografií. Dále bylo zjištěno, že muži se nejčastěji setkali v online prostředí s hrozbou zvanou phising, což je rozesílání falešných zpráv s cílem získat citlivá data oběti. Tato hrozba je též velmi závažná, protože může dojít ke ztrátě citlivých údajů nebo hesel. Proto doporučuji neodpovídat na nevyžádané emaily.

8 DOPORUČENÍ KAM SE MOHOU MLADISTVÍ OBRÁTIT V PŘÍPADĚ JAKÉHOKOLI PROBLÉMU

Pokud mladiství nechtějí nebo se stydí řešit problémy se svými rodiči existují anonymní poradny, které mohou využít při řešení jejich problému. Většinou se jedná o bezplatné a anonymní poradny. Kontaktovat poradnu můžeme telefonicky, emailem nebo prostřednictvím chatu. Cílem pracovníků poraden je poradit nejzásadnější kroky k řešení problému mladistvého.

Linka bezpečí

Posláním linky bezpečí je poskytovat telefonickou krizovou pomoc a poradenství dětem a mladým lidem, kteří se nacházejí v tíživé životní situaci. Je určena dětem do 17 let a pro studenty denního studia do 25 let.Linka důvěry pomáhá řešit situace ve všech oblastech jako jsou rodina, vztahy, škola, kamarádi, ubližování, šikana atd.Linku důvěry mohou kontaktovat prostřednictvím telefonního čísla 116 111, emailu pomoc@linkabezpečí.cz, kontaktního formuláře nebo chatu. (Eckertová a Dočekal, 2013, str.181)

Poradna E – bezpečí

Poradna je určena zejména mladým uživatelům internetu, kteří se dostali do obtížné situace. Na poradnu se mohou písemně obrátit v případě vyhrožování, vydírání či zastrašování. Poradenská činnost je poskytována anonymně a zdarma. (Eckertová a Dočekal, 2013, str.183)

V závažných případech se mladiství mohou obrátit i na Policii České republiky na telefonním čísle 158.

ZÁVĚR

V teoretické části byla zpracována literární rešerše tykající se analýzy rizik a bezpečnostních hrozeb mládeže při práci s počítačem. V rámci této rešerše, byli představeny základní pojmy analýzy, legislativa České republiky, přesněji zákon o kybernetické bezpečnosti, počítač a internet, sociální sítě a online hry a rizika spojená s online prostředím. V práci byli vybrány sociální sítě a online hry jako zástupci nejčastějších činností mládeže na počítači. Byli představeny jejich pozitiva, negativa, a především hrozby s nimi spojenými. V praktické části, byli tito zástupci navíc doplněni o obecná témata spojená s práci na počítači. Načež byla provedena analýza rizik za pomocí metod Check list, What if a zpracováním matice rizik. Z analýzy vyšla jako potencionálně nebezpečná rizika, čas strávený u počítače, nedostatečná znalost práce na počítači a lehkovážnost základních bezpečnostních pravidel. Druhá část praktické části práce, se zabývá dotazníkovým šetřením. Dotazník sestavený pro účely této práce byl poskytnut náhodně zvolené skupině mladých lidí ve věku od 10 do 18 let. Z vyhodnoceného dotazníkové šetření bylo zjištěno, že mládež na počítači tráví přinejmenším hodinu denně a ve velké většině i více, a má slabší obavy o svoji bezpečnost na internetu. Dalším znepokojivým zjištěním bylo, že ženy jsou častěji vystaveny jiným druhům útoků než muži. U žen se jedná především o útoky se sexuálním podtextem, u můžu potom za účelem získaní soukromých údajů. V poslední kapitole je uvedeno, na koho se může dítě obrátit v případě, že potřebuje poradit v oblasti kyberkriminality.

Cílem práce bylo zpracovat literární rešerši a analyzovat rizika a hrozby při práci na počítači u mládeže ve věku od 10 do 18. Cíle byli splněny, rešerše je zpracovaná v teoretické části a analýza rizik v praktické. Byli představeny možné hrozby a navrhnuto řešení, jak je eliminovat nebo jim alespoň předcházet.

V dnešní digitálně době je i pro dospělého člověka těžké se bezpečně pohybovat po internetu a orientovat se v možných hrozbách. Postupně jak se naše běžné činnosti budou více přesouvat do online prostředí budeme muset být schopni čelit dalším hrozbám. V závěru bych chtěla říct, že klíčem ke zvládnutí digitální doby je dobrá znalost jak výhod, které nám online prostředí přináší, tak i rizik z nich plynoucích ať už ze strany rodičů a školy v případě mladistvých nebo ze strany zaměstnavatelů a státu u dospělých.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje

ČERNÁ, Alena, 2013. Kyberšikana: průvodce novým fenoménem. Praha: Grada. Psyché (Grada). ISBN 978-80-247-4577-0.

DOČEKAL, Daniel et al., 2019. Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace. Praha: Mladá fronta. Flowee. ISBN 978-80-204-5145-3.

ECKERTOVÁ, Lenka a Daniel DOČEKAL, 2013. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press. ISBN 978-80-251-3804-5.

HULANOVÁ, Lenka, 2012. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton. ISBN 978-80-7387-545-9.

KOPECKÝ, Kamil, 2015. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-4861-9.

KOŽÍŠEK, Martin, 2016. Bezpečně na internetu: průvodce chováním ve světě online. Praha: Grada. ISBN 978-80-271-9074-4.

LORENTZ, Pascaline et al., 2015. Living in the digital age. Brno: Masarykova univerzita. ISBN 978-80-210-7810-9.

LUKÁŠ, Luděk. Teorie bezpečnosti. I.. Zlín: Radim Bačuvčík - VeRBuM, 2017. Teorie a praxe ochrany majetku a fyzické bezpečnosti. ISBN 978-80-87500-89-7.

MARTÍNEK, Zdeněk, 2015. Agresivita a kriminalita školní mládeže. 2., aktualizované a rozšířené vydání. Praha: Grada. Pedagogika (Grada). ISBN 978-80-247-5309-6.

SMEJKAL, Vladimír a Karel RAIS, c2006. Řízení rizik ve firmách a jiných organizacích. 2., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 80-247-1667-4.

SZOTKOWSKI, René, Kamil KOPECKÝ a Veronika KREJČÍ, 2013. Nebezpečí internetové komunikace IV. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-3911-2.

ŠEFČÍK, Vladimír, 2009. Analýza rizik: analýza a management. 2., aktualiz. a rozš. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně. Beckova edice ekonomie. ISBN 978-80-7318-696-8.

ŠEVČÍKOVÁ, Anna, 2014. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada. Psyché (Grada). ISBN 978-80-247-5010-1.

TICHÝ, Milík, 2006. Ovládání rizika: analýza a management. V Praze: C.H. Beck. Beckova edice ekonomie. ISBN 80-717-9415-5.

Online zdroje

Computer, 2020. Technopedie [online]. [cit. 2021-8-3]. Dostupné z: https://www.techopedia.com/definition/4607/computer

HELLER, Lukáš, Jindřich JELÍNEK a Pavel SIMR, 2011. Práce s počítačem: Windows 7, Office 2010 [online]. Ústí nad Labem: Univerzita J.E. Purkyně v Ústí nad Labem [cit. 2021-8-2]. ISBN 978-80-7414-368-7. Dostupné z: https://chemistry.ujep.cz/userfiles/files/Prace%20s%20pocitacem%20-%20Finall%20v2.pdf

Jak správně sedět u PC + zásady ergonomie sezení na kancelářské židli, 2018. BOZP.cz [online]. [cit. 2021-8-2]. Dostupné z: https://www.skolenibozp.cz/aktuality/jak-spravne-sedet-u-pc/

Jak se prezentujeme na Internetu 2012 [online]. [cit. 2021-8-3]. Ke stažení dostupné z: https://bezpecne-online.ncbi.cz/vyukove-materialy/ke-stazeni/send/3-materialy-pro-ucitele/15-soukromi-na-siti-facebook-lide-cz

Jak vznikl internet. Na počátku byl ARPAN, 2020. Seniorclub [online]. [cit. 2021-7-28]. Dostupné z: https://www.seniorclub.cz/jak-vznikl-internet/

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze [cit. 2021-7-21]. ISBN 978-80-7251-397-0. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

Kyberšikana a šikana - rozdíly [online], 2010. [cit. 2021-01-29]. Dostupné z: http://www.kybersikana.eu/2010/12/kybersikana-sikana-rozdily.html

Nebezpečné pronásledování (stalking) [online], 2020. policie České republiky [cit. 2021-01-29]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-nebezpecne-pronasledovani-stalking.aspx

Online hraní her. Www.eduzin.cz [online]. [cit. 2021-8-4]. Dostupné z: https://www.eduzin.cz/wp-content/uploads/2018/12/07_online_hrani_her.pdf?fbclid=IwAR1kdGizfJJqQm2SCY3LSxdawmQ3SGnik1Nz5apUKM68rgIlLLI-mCIex9c

Phishing [online]. [cit. 2021-01-29]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

Risk management – Risk assessment techniques 2009 [online]. [cit. 2021-8-3]. Ke stažení dostupné z: https://bambangkesit.files.wordpress.com/2015/12/iso-31010_risk-management-risk-assessment-techniques.pdf

Rizika sociálních sítí a co by děti měly vědět 2014 [online]. [cit. 2021-8-3]. Ke stažení dostupné z: https://bezpecne-online.ncbi.cz/vyukove-materialy/ke-stazeni/send/3-materialy-pro-ucitele/71-metodika-rizika-socialnich-siti-a-co-by-deti-mely-vedet

Sociologická encyklopedie, 2018. Sociologická encyklopedie [online]. [cit. 2021-8-3]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Mládež_(MSgS)

The Dark Side of Snapchat and Teens, 2020. Verywell family [online]. [cit. 2021-8-3]. Dostupné z: https://www.verywellfamily.com/what-is-snapchat-and-its-use-1270338

Vznik a historie Facebooku, 2015. Vznik a historie Facebooku [online]. [cit. 2021-6-24]. Dostupné z: https://www.zdenekblazek.cz/vznik-a-historie-facebooku/

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lid* [online]. [cit. 2021-8-3]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

% Procenta

° Stupeň

IT Informační technologie

CLA Check list

ETA Event Tree Analysis

HRA Human Reliability Analysis

FMEA Failure Modes and Effects Analysis

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Bezpečnostní hrozby práce mládeže s počítačem

1 Jaké je vaše pohlaví

☐ Muž ☐ Žena

2 Jaký je váš věk

☐ 10 - 15 ☐ 15- 18

3 Kolik času na počítači denně trávíte?

☐ 1 hodinu a méně ☐ 2 - 3 hodiny ☐ 4 - 5 hodin ☐ 6 a více hodin

4 Co na počítači nečastěji děláte?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Sociální sítě ☐ Hraní her ☐ Vyhledávání na internetu

5 Používáte sociální sítě?

☐ Ano ☐ Ne

6 Pokud ANo jaké?

Nápověda k otázce: *pokud jiná prosím specifikujte*

☐ Facebook ☐ Instagram ☐ Twitter

☐ Jiná...

7 Máte obavu, že by jste se mohli stát obětí počítačové kriminality?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Ano ☐ Ne ☐ Neuvažoval(a) jsem nad tím

8 S kterou kybernetickou hrozbou jste se již setkali?

Nápověda k otázce: *pokud jiná prosím specifikujte*

☐ Kyberšikana ☐ Ukradení identity ☐ Stalking (pronásledování) ☐ Kybergrooming (vylákání na schůzku podvodným agresorem)

☐ Sexting (posílání lechtivých zpráv) ☐ Phising (podvodný email z důvěryhodné instituce s cílem získat vaše citlivé údaje)

☐ Jiná...

9 Pokud hrajete počítačové hry jaké to jsou?

10 Myslíte, že při online hrách se můžete stát obětí kyberútoku?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Ano ☐ Ne ☐ Nepřemýšlel(a) jsem nad tím

11 Pokud jste odpověděli ANO jaké to jsou?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Kyberšikana ☐ Krádež uživatelského účtu ☐ Napadení bankovního účtu