Autor	*Mgr. Martina Iskrová*
Pracovisko autora	*Základná škola pri zdravotníckom zariadení, Nám. L. Svobodu 4, 974 01 Banská Bystrica*
Názov záverečnej práce	*Digitálna bezpečnosť pre všetkých*
Hlavný cieľ	*Získavať nové vedomosti a informácie o digitálnej bezpečnosti.*
Špecifické ciele	*Zodpovedne používať technológie.* *Ovládať pojmy v oblasti kybernetickej bezpečnosti.* *Budovať bezpečné online prostredie pre deti.*
Cieľová skupina	*pedagógovia ZŠ pri zz*
Predmet/y	*všetky vyučovacie predmety ZŠ*
Kľúčové pojmy	*vírus, malvér, advér, ransomvér, zabezpečenie počítača*
Odporúčaná literatúra/zdroje	*Bezpečne na nete | ESET ; WebTesty.sk ; https://vosveteit.zoznam.sk/ ; Home*
Pomôcky	*počítač alebo tablet s napojením na internet, prezentácie, papier, fixky, mobil*
Trvanie	*v našej ZŠ október 2022 – január 2023* *(možnosť prispôsobiť podľa potrieb)*

Metodický postup:

Som učiteľkou v základnej škole v nemocnici a do edukačného procesu sú u nás zaradení žiaci – deti hospitalizované v DFNsP Banská Bystrica – žiaci rôznych typov škôl, ročníkov i sociálnych vrstiev a digitálnych zručností. V rozvrhu pre náš typ škôl nemáme informatiku, ale snažíme sa digitálne technológie a prácu s nimi využívať vo všetkých vyučovacích predmetoch. Práve preto sme sa po dohode s vedením školy rozhodli spustiť tento školský rok interné vzdelávanie pre pedagógov našej ZŠ a tým zabezpečiť, aby pracovali s technológiami zodpovedne a túto zodpovednosť i získané vedomosti a zručnosti prenášali na žiakov.

Vzdelávanie sme rozdelili do 4 modulov (stretnutí) a modul č.1 som rozpracovala podrobnejšie, ostatné sú spomenuté informatívne:

Modul č. 1

Téma: Úvod do problematiky, vysvetlenie pojmov

Cieľ - absolvent dokáže vysvetliť pojmy malvér, advér, ransomvér, kyberšikana, phishignový podvod

- pozná „Slovník kybernetických pojmov“ a aktívne s ním pracuje
- vie vyhľadať podcasty, ktoré pomáhajú deťom pri IT bezpečnosti

Modul č. 2

Téma: Dezinfo, hoaxy a fake news + ako správne na selfie

Cieľ: - absolvent dokáže rozoznať nepravdivé správy aj phishingové maily

- pozná základné pravidlá publikovania fotografií
- vie žiakom poradiť pri tvorbe a zverejnení „selfie“

Modul č. 3

Téma: Bezpečnosť prehliadača a mobilných zariadení

Cieľ: - absolvent pozná základné pravidlá zabezpečenia mobilných zariadení

- pozná Príručku o digitálnej bezpečnosti pre učiteľov 1. a 2. stupňa základných škôl a aktívne s ňou pracuje

Modul č. 4

Téma: Kybergrooming, kyberšikana a program Hrdinovia internetu

Cieľ - absolvent dokáže rozpoznať nebezpečné komunikačné javy realizované prostredníctvom informačných a komunikačných technológii

- vie žiakom poradiť ako sa pred nimi brániť
- pozná program Hrdinovia internetu ako aj iné nástroje a metódy potrebné pri učení základov digitálnej bezpečnosti

Modul č. 1

Evokácia

Na úvod sme si pomocou upravenej prezentácie od ESET-u objasnili pojem Digitálna bezpečnosť a vymedzili druhy ohrozenia, ktoré na nás v online priestore číhajú – SPAM, Vírusy, Online obchodovanie, Čet, Reklama, Hry, Sťahovanie z internetu, Zoznamky, Mobily, HOAX, Monitorovacie, filtrovacie programy.

Na základe pokynov v prezentácii si každý účastník na svojom tablete/počítači otvoril stránku WebTesty.sk a vypracoval Veľký test internetovej bezpečnosti - (ID – 5878, heslo – zszz) – Príloha č.1. Na test sa mali možnosť dostať aj pomocou QR kódu, čo bolo pre mnohých zaujímavé, lebo to skúšali prvýkrát.

Následne sme spoločne test vyhodnotili a diskutovali o správnych odpovediach. Nakoniec si podľa počtu správnych odpovedí vypočuli hodnotenie:

1 – 4 správne odpovede
Hackeri nikdy nespia! Svoje znalosti o bezpečnom správaní sa na internete musíte čo najskôr zlepšiť.
5 – 7 správnych odpovedí
Na internete sa viete ochrániť pomerne dobre, ale stále je čo zlepšovať!
8 – 10 správnych odpovedí
Gratulujeme. Dosiahli ste skvelý výsledok! Ste majster v boji proti online podvodom a internetovú bezpečnosť by ste mohol sám učiť! Ale nezaspite na vavrínoch, podvodníci prichádzajú so stále novými trikmi. Pravidelne kontrolujte zabezpečenie svojho účtu*!*

Uvedomenie

Pokračovali sme v prezentácii, kde som vypichla a objasnila základné pojmy – vírus, červ, malware, spyware a phishing. Pri každom mali v prezentácii zdôraznenú aj prevenciu.

Z minulého roka sme si zopakovali aj zásady pri tvorbe silného hesla a mnohé kolegyne sa pochválili, že tieto vedomosti využili pri práci so žiakmi i vo svojej rodine.

V poslednom slide prezentácie sme si zhrnuli „Ako zabezpečiť svoj počítač pred napadnutím / zneužitím údajov“:

- používať len oficiálne zakúpený OS
- aktualizovať softvér
- zálohovať dáta
- používať silné heslá

- zapnúť firewall (bariéra medzi verejným internetom a súkromným počítačom, blokuje viaceré hrozby)
- nainštalovať a aktualizovať antivírusový program
- pozor na webové stránky a e-mailové adresy
- nezadávať citlivé údaje do verejného PC

Reflexia

Následne som prešla na „Slovník kybernetických pojmov“, ktorý je k dispozícii online - https://bezpecnenanete.eset.com/sk/kyberneticky-slovnik-pojmov/. Tento slovník mnohé kolegyne veľmi potešil, pretože v daných pojmoch tápajú nielen oni, ale často aj žiaci, a potom ich používajú nesprávne, lebo vôbec nevedia, čo znamenajú.

Nakoniec som účastníčky školenia rozdelila do trojčlenných skupín a ich úlohou bolo vyhľadať zaujímavé články a podcasty o internetovej bezpečnosti.

Ja sama som na záver vypichla niektoré stránky, ktoré ponúkajú podcasty na tému internetovej bezpečnosti a môžu byť veľmi nápomocné pri práci so žiakmi:

Archívy Podcast - Bezpečne na nete | ESET

Podcast o kybernetickej bezpečnosti na Slovensku - INFOSECURITY.SK

Úvod - incident podcast - Správy a podcasty o bezpečnosti

Bezpečnost v praxi - ▶ Podcasty na bezpečnostné témy (bezpecnostvpraxi.sk)

Modul č. 2

Evokácia

Na úvod každá účastníčka dostala 3 vytlačené emaily z phishingového testu - SAFELab - Phishingový test a ich úlohou bolo zhodnotiť, či sú to podvodné maily, alebo nie. Spoločne sme si ich prešli a povedali sme si, prečo sú niektoré falošné a ako ich rozpoznať. Upozornila som na základné znaky a následne si každá vyskúšala svoje znalosti online na CSIRT.SK (gov.sk).

Uvedomenie

Ďalej sme pomocou riadeného rozhovoru diskutovali o hoaxoch, s ktorými sa stretli v poslednej dobe oni osobne a opäť sme zhrnuli znaky a možnosti, ako si overovať pravdivosť správ.

Následne mali všetci za úlohu vytiahnuť mobil a nájsť akúkoľvek selfie, ktorú tam mali uloženú. Rozdelili sa do dvojíc a diskutovali, pri akej príležitosti bola daná fotografia urobená, prípadne či a kde ju zverejnili. Keďže som nechcela poukazovať na chyby na ich fotkách, zobrazili sme si obrázky - Príloha č. 2 a spoločnou diskusiou sme dospeli k záverom, že si máme pri zhotovovaní dávať veľký pozor na okolie, ale i na osobné údaje. Ďalej som im vložila chrobáka do hlavy otázkou, dokedy zostanú na nete fotky napríklad ich detí a či je možné ich zmazať. Každá dostala mailom odkaz a prečítala si článok - Je možné vymazať niečo z internetu? Tu je niekoľko možností, ako na to | Vosveteit.sk (zoznam.sk) .

Následne sme si povedali o cookies. Vysvetlila som, že ide v podstate o malé súbory, ktoré sa uložia na počítač alebo mobilné zariadenie v prípade, že tak určí konkrétna webová stránka.

Fixácia

Na záver sme prešli k digitálnej stope. Využili sme braintorming a zapisovali online pomocou odkazu na jamboard. Pri zhrnutí som si pomohla príručkou od Eset-u, zosumarizovala a rozdelila som ju na aktívnu a pasívnu.

Modul č. 3

Evokácia

Na úvod sme diskutovali o príkladoch z vlastných skúseností, keď sa nám niekto nabúral do počítača, mobilu, konta... alebo sa nám tam vyskytol vírus. Zhodli sme sa na tom, že mať bezpečnostný softvér na počítači v dnešnej dobe nestačí. Je toho oveľa viac.

Uvedomenie

Využila som upravenú prezentáciu „PKDK Bezpecnost mobilnych zariadeni“. Pomocou nej som objasnila mnohé pojmy a vysvetlila, že je dôležité vytvárať si unikátny prístupový kód - heslo je nepraktické, vzor je fajn, PIN je lepší, odtlačok/tvár je ideál. Prešli sme si však aj možné riziká. Na záver prezentácie sme si spoločne zhrnuli a zapísali aj na papier Bezpečnostné desatoro, ktoré je možné využiť na ďalšiu prácu so žiakmi – Príloha č.3.

Fixácia

Ďalej som online oboznámila kolegyne s Príručkou o digitálnej bezpečnosti a aj s pdf. materiálom - Aktivity k Príručke digitálnej bezpečnosti, ktorá obsahuje zoznam aktivít navrhnutých odborníkmi ESETu, učiteľmi informatiky a detskými psychológmi, ktoré

zaujímavou a praktickou formou ilustrujú problémy v oblasti digitálnej bezpečnosti a bezpečného používania internetu deťmi. Všetky prítomné kolegyne sa rozdelili do dvojíc, vybrali a prešli aspoň jednu konkrétnu aktivitu a informovali o nej ostatných.

Modul č. 4

Evokácia

Prítomní sa rozdelili do 2 skupín a ich úlohou bolo za pomoci internetu vysvetliť pojmy:

1.skupina – KYBERGROOMING,

2. skupina – KYBERŠIKANA.

Spoločne sme si to zosumarizovali a prešli sme si film „Kyberšikanovanie, zatočme s ním spoločne!“ (Let's Fight It Together) – trvanie 6:30 min. Pozreli sme si aj 5 videorozhovorov s jednotlivými postavami z filmu.

Následne sme vytvorili plagát a pripravili dokument pre žiakov na diskusiu - Príloha č. 4.

Potom som oboznámila kolegyne s IPčko.sk - Internetová poradňa pre mladých ľudí; a tiež som im predtavila https://www.beznastrah.online/online-poradna/

Uvedomenie

Ďalej som ich zoznámila s programom Hrdinovia internetu i s hrou Interland, ktorú si potom každý sám aj vyskúšal, konkrétne prejdením aspoň jedného z ostrovov.

Fixácia

Na záver sme si vymenili skúsenosti z jednotlivých ostrovov a v diskusii sme si ukázali ďalšie stránky, ktoré ponúkajú krátke videá nápomocné pri práci so žiakmi a kolegyne pridali i vlastné odskúšané online aktivity.

- Home | Sheeplive.eu
- Zvireracia galaxia Animália | ESET
- Elias medzi dvoma svetmi | ESET
- Archívy Wizard videá | Bez nástrah (beznastrah.online)

Vlastné skúsenosti: Ja sama som počas školení PKDK bola často prekvapená novými vedomosťami. Dozvedela som sa zaujímavé a potrebné i podnetné informácie. Považovala som za dôležité podeliť sa s nimi. V našej škole všetky kolegyne aktívne využívajú IKT pri práci. Keď som minulý rok s nimi robila niektoré aktivity inšpirované PKDK, mala som úspech a videla som, že ich s radosťou využívajú pri práci. Práve preto som privítala a využila ponuku vedenia našej ZŠ realizovať takéto interné vzdelávanie. Aktivity i informácie sa všetkým zúčastneným kolegyniam páčili a považovali ich za užitočné. Vnímam ako veľký prínos celé školenie digitálnych koordinátorov, všetky webináre a som vďačná za možnosť šíriť osvetu digitálnej bezpečnosti ďalej. Foto prikladám v prezentácii.

Zoznam príloh:

Príloha č. 1 – Veľký test internetovej bezpečnosti

Príloha č. 2 – foto /selfie

Príloha č. 3 – Bezpečnostné desatoro

Príloha č. 4 – Čo všetko je kiberšikana?

Príloha č.1

Veľký test internetovej bezpečnosti: Vyskúšajte sa, či sa viete brániť!

Ako zabránite neoprávnenému prístupu do zariadenia?

a. Obrazovku uzamknete PINom, heslom, kresleným vzorom alebo odtlačkom prsta

b. Nosíte telefón neustále pri sebe (máte ho na špeciálnej šnúrke)

c. Na jednom zariadení nastavíte niekoľko hesiel

Správna odpoveď: a

Ak nechcete, aby ktokoľvek, komu sa dostane do rúk váš telefón alebo tablet, získal prístup k vašim údajom, zamykajte displej na zariadení. Môžete si vybrať z nasledujúcich spôsobov: PIN, heslo, gesto, kreslený vzor, odtlačok prsta alebo rozpoznanie tváre (dostupnosť jednotlivých možností závisí od výrobcu a modelu vášho telefónu alebo tabletu).

2. Kedy majú zločinci najväčšiu šancu získať vaše heslo?

a. Keď používate rovnaké heslo v rôznych službách

b. Keď používate silné heslo obsahujúce čísla aj symboly

c. Keď dáte povolenie prehliadaču, aby si pamätal vaše heslá

Správna odpoveď: a

Ak používate rovnaké používateľské meno a heslo na viacerých stránkach (v rôznych účtoch alebo registráciách) a jedna z nich je ohrozená, môžu hackeri použiť vaše údaje na prihlásenie aj na iných stránkach. Odporúčanie: používajte pre každú službu jedinečné silné heslo. Prehliadač Chrome si môže pamätať rôzne heslá pre rôzne služby, ktoré používate a navyše aj znižuje riziko vystavenia phishingu.

3. Z nasledujúcich možností vyberte heslo, ktoré je podľa vášho názoru najbezpečnejšie:

a. Jakub1983

b. Qwerty321

c. J@Kub_839

Správna odpoveď: c

Čím je heslo dlhšie, tým ťažšie sa dá uhádnuť. Pridajte do hesla čísla, symboly a striedajte veľké a malé písmená. Kyberzločincom tým sťažíte cestu k získaniu prístupu do vášho účtu.

4. Experti odporúčajú používať pre najbezpečnejšie heslá tzv. prístupové frázy, čiže vety, ktoré si ľahko zapamätáte. Vyberte jednu z možností, ktorá je podľa vášho názoru takouto prístupovou frázou.

a. 2mrj1rz! – príslovie „Dvakrát meraj a raz rež!“, číslovky napísané príslušnou číslicou, vynechané medzery a samohlásky

b. Maria05081960 – meno a dátum narodenia vzdialeného príbuzného

c. AdamDurica – meno vášho obľúbeného speváka

Správna odpoveď: a

Prístupová fráza – gramaticky správna veta zložená zo slov a čísel, ktorá pomáha zapamätať si zložité heslo, ktoré je náročné prelomiť. Heslá typu (MenoPriezvisko), (dátum narodenia), (Mama1234) nie sú bezpečné. Nezabudnite, že dnes existuje mnoho programov, ktoré je možné použiť na prelomenie hesiel.

5. Čo je to „dvojstupňové overenie“?

a. Heslo, ktoré sa zadáva dvakrát za sebou

b. Heslo, ktoré je na získanie prístupu nutné overiť cez mobilný telefón

c. Heslo vyžadujúce odpoveď na doplňujúcu otázku

Správna odpoveď: b

Dvojstupňové overenie - spôsob zabezpečenia používateľského účtu, ktoré pre prístup vyžaduje okrem používateľského mena a hesla ešte zadanie špeciálneho kódu, ktorý používateľovi príde v SMS správe na jeho telefón vždy pri prihlasovaní do svojho účtu. Takýto postup poskytuje ďalšiu vrstvu ochrany. Dokonca, aj keď útočník získa vaše používateľské meno a heslo, nedostane sa tak k vášmu účtu bez vášho telefónu.

6. Ako chrániť deti pred nevhodným obsahom na internete?

a. Používať nástroje Bezpečného vyhľadávania pre deti vo svojom prehliadači a zapájať sa do ich online aktivít

b. Úplne im zakázať používať internet

c. Rozprávať deťom hrôzostrašné príbehy o zlých ľuďoch na internete

Správna odpoveď: a

Bezpečné vyhľadávanie umožňuje vo výsledkoch vyhľadávania zakázať zobrazovanie obsahu určeného len pre dospelých. Keď túto funkciu zapnete, bude nevhodný obsah blokovaný na všetkých zariadeniach, na ktorých ste prihlásení pod svojím účtom. Napríklad Bezpečné vyhľadávanie zapnete na svojom smartfóne alebo tablete nasledovne: navštívte stránku Nastavenia vyhľadávania, v sekcii "Filtre Bezpečného vyhľadávania" vyberte

možnosť "Filtrovať explicitné výsledky" a v dolnej časti stránky potvrďte voľbu kliknutím na "Uložiť". Popritom je, samozrejme, dôležité byť svojmu dieťaťu nablízku a učiť ho bezpečne používať internet.

7. Čo urobíte ako prvé, ak vám ukradnú telefón alebo tablet?

a. Idete na políciu ohlásiť krádež

b. Uzamknete zariadenie a všetko z neho vymažete pomocou vzdialenej správy zariadenia. Potom zájdete na políciu ohlásiť krádež

c. Kúpite si nový telefón a obnovíte pôvodné dáta

Správna odpoveď: b

Ak stratíte telefón so systémom Android alebo vám ho ukradnú, môžete pomocou Správcu zariadenia Android zistiť jeho približnú polohu na mape a čas, kedy bol naposledy použitý. Zariadenie môžete tiež na diaľku prezvoniť, uzamknúť ako aj vymazať všetko, čo je v ňom. Pre zariadenia od Applu použite program "Nájsť iPhone" - potom si svoje stratené zariadenie budete môcť zobraziť na mape, prehrať na ňom zvuk, ktorý vám ho pomôže nájsť, pomocou režimu straty ho uzamknúť a sledovať, prípadne z neho na diaľku vymazať všetky informácie.

8. Čo je to sociálne inžinierstvo?

a. Teória vytvárania sociálnej spoločnosti

b. Podvodné postupy, ako oklamať používateľa, aby zdieľal citlivé údaje, prípadne nevedomky stiahol škodlivý softvér

c. Krádež telefónu na verejných miestach s vysokou koncentráciou inžinierov

Správna odpoveď: b

Sociálne inžinierstvo - klamlivé praktiky, ktorých účelom je prinútiť používateľov vykonať na internete nevedomú aktivitu. Obvykle ste pripravení zadať svoje heslo alebo zavolať na číslo technickej podpory iba na oficiálnych stránkach, ktorým dôverujete. Pri útoku využívajúcom sociálne inžinierstvo sa preto ukazujú stránky, ktoré imitujú stránky dôveryhodných inštitúcií, napríklad bánk alebo štátnych inštitúcií, aby z vás vylákali vaše citlivé údaje alebo dokonca peniaze.

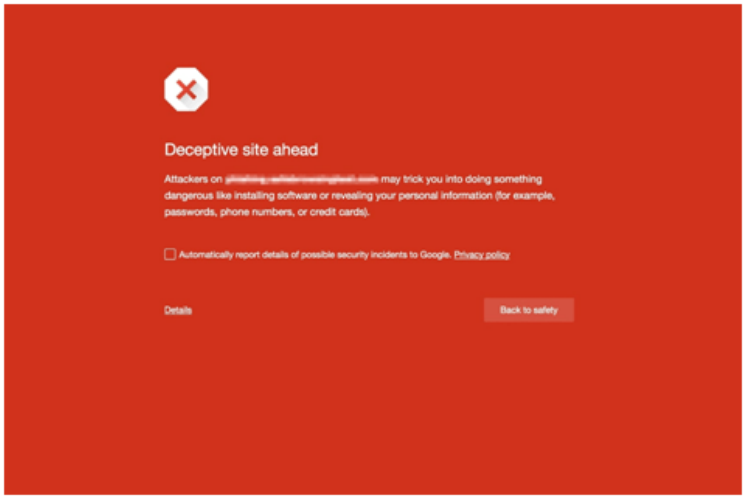
9. Ktorá z nasledujúcich situácií je príkladom sociálneho inžinierstva?

a. Dostali ste e-mail zo Singapuru alebo Nigérie (a nemáte tam žiadnych známych), ktorý vás odkazuje na stránky, ktoré nepoznáte

b. Na stránke sa vám zobrazí upozornenie na problém, zároveň obsahuje telefónne číslo na podporu Google alebo iné známe spoločnosti

c. Na vašom mobilnom zariadení sa objavila správa, že je potrebné obnoviť systém
d. Všetky možnosti sú správne
Správna odpoveď: d

10. Prešli ste na stránku, ktorá vykazuje znaky sociálneho inžinierstva. Na displeji sa objavilo varovanie. Čo urobíte?



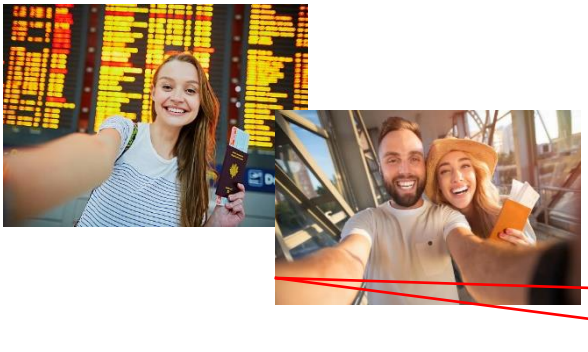
a. Pokračujete na zvolenú stránku
b. Kliknete na možnosť „Späť do bezpečia“
c. Odpojíte internetový kábel od počítača a počkáte, kým pominie nebezpečenstvo
Správna odpoveď: b
Ak sa používateľovi zobrazí takéto oznámenie, znamená to, že stránka môže byť kompromitovaná aktivitami sociálneho inžinierstva a je potrebné vrátiť sa do bezpečia. Ak si myslíte, že je daná stránka označená ako sociálno inžinierska omylom, upozornite na to bezpečnostný tím Googlu.

Príloha č.2


This traffic ugh


Osobné
údaje!!!


GET IN
VIP
Ticketmaster Presents
Music Festival
1000 Music Festival Landing
Fri Jun 10, 2016


Kedy áno,
kedy nie???

Príloha č. 3

BEZPEČNOSTNÉ DESATORO:

1. **Buďte obozretní!**
2. **Nepodľahnite spamu a phishingu!**
3. **Dávajte pozor kam dávate svoje údaje!**
4. **Používajte aktualizovanú ochranu pred škodlivým softvérom!**
5. **Pozor na sťahované súbory!**
6. **Používajte silné a unikátne heslo!**
7. **Majte povolenia pre mobilné zariadenia pod kontrolou!**
8. **Dbajte na bezpečné online nákupy!**
9. **Vyvarujte sa cudzích zariadení!**
10. **Zálohujte... zálohujte... Zálohujte!**

Príloha č. 4

Čo všetko je kiberšikana?

1. Publikovanie ponižujúcich záznamov alebo fotografií (napr. v rámci webových stránok,MMS správ).
2. Ponižovanie a ohováranie v rámci sociálnych sietí, blogov, alebo na iných webových stránkach.
3. Krádež identity, zneužitie cudzej identity ku kyberšikane alebo ďalšiemu sociálne patologickému jednaniu (napr. krádež elektronického účtu).
4. Strápňovanie pomocou falošných profilov (napr. v rámci sociálnych sietí, blogov alebo iných webových stránok).
5. Provokovanie a napádanie užívateľov v on-line komunikácii (predovšetkým v rámci verejných chatov a diskusií).
6. Zverejňovanie cudzích tajomstiev s cieľom poškodiť obeť.
7. Vylúčenie z virtuálnej komunity (napr. zo skupiny priateľov v rámci sociálnej siete).
8. Obťažovanie (napr. opakovaným prezváňaním, volaním nebo písaním SMS správ, mailov).