KAPITOLA 2

Kyberšikana

DETI MLÁDEŽ DOSPELÍ SENIOR

Šikana a jej online podoba – kyberšikana

Pod pojmom kyberšikana, ktorý sa stáva čoraz známejším, si môžete predstaviť niečo moderné a nové. Šikana zostala šikanou, iba vznikom nového priestoru sa presunula, a tak vznikla šikana virtuálna (tiež kybernetická, počítačová alebo, ak chcete - internetová). Kým za telocvičňou si vás po škole počkala banda chuligánov, dnes nemusí nikto nikde nikoho čakať. Najmä nie pred očami svedkov. Dnes si útok ktokoľvek nahrá na mobil a uploadne ho na YouTube v priebehu pár minút. Útočník sedí pohodlne doma v suchu na zadku, popíja ľadový čaj a presne vie, akým spôsobom vás pomaly trápiť. Nemusí to robiť po prvýkrát a určite nebudete ani jeho alebo jej posledné obete. Čas nie je prekážka, pretože e-mail môže odoslať aj o polnoci. Obetí môže mať viac. Sedieť môže na druhom konci vašej dediny, alebo sedí v hotelovom lobby bare niekde na zrejme nie príliš vydarenej dovolenke.

Kybernetická šikana je „modernejšia“ a čoraz viac aktuálnejšia, pretože:

1. Je bez svedkov a útočník alebo útočníčka môže presnejšie a nerušene plánovať.
2. Technológie a možnosti internetu mu alebo jej poskytujú mnoho nástrojov.
3. Nevyžaduje si konkrétne miesto, len pripojenie na internet alebo mobil.
4. Je anonymná a s tým je spojených aj menej výčitiek.
5. **Je trestne stíhateľná a zároveň je naivné, ak si páchateľ myslí, že je nepostihnuteľná.**

Čo je to tá „kyberšikana“?

Kybernetická šikana ako moderný pojem pomenúva rozsiahle formy útokov voči niekomu inému. Sú slovným napádaním, urážaním alebo rôznym iným poškodzovaním druhej osoby. Môže ísť o e-maily či odkazy, ktorými sa útočník akokoľvek vyhráža, oslovenú obeť zastrašuje a svojím konaním ohrozuje. Útočník sa nezamýšľa nad následkami. Online priestor je priam ideálny svojou anonymitou a tým, že útočník nemusí pozerať svojej obeti do tváre. Výčitky sa vtedy predierajú na svetlo oveľa ťažšie a svedomie pokojne odpočíva. Všetko si rozoberieme a kyberšikanu rozdelíme podľa technológie a typov útočníkov.

DETI MLÁDEŽ DOSPELÍ SENIOR

Rozdelenie kyberšikany podľa typov agresorov

Nasledovné rozdelenie typov útočníkov môže pôsobiť humorne, ironicky, ale pokojne aj neprofesionálne. Ich názvy však napovedajú, čo si o návštevníkoch možno myslieť.

1. Pán Správny alebo pani Správna

Najmenej nebezpečný typ agresora je *pán Správny* alebo v prípade ženy jej hovorme *pani Správna*. Ich prejav nie je pravidelný. Na zadku majú vyrážku, ktorú podráždi akýkoľvek falošný tón zaspievaný v ich obľúbenej skladbe. Aktivujete ich síce neúmyselne, ale hneď spoznáte, že tam sú. Za nesprávny názor sa stávate obeťou urážok a dehonestovania vašej existencie.

- **Poznávacie znamenia:** Nemusia byť anonymní, môžu vystupovať pod svojím menom. Vyprovokované urážky zväčša nepokračujú (pokiaľ neprechádzate do protiútoku). Ide zväčša o komentáre, sociálne siete a verejne prístupné miesta.
- **Riešenie:** *Hoďte ich za hlavu.*

2. Pán Papuľa alebo pani Papuľa

Tento typ agresora ovláda rozloženie znakov na klávesnici a žije v pocite, že ovláda aj výplň dutiny lebečnej. Papulí je mnoho medzi deťmi, žiakmi základných škôl aj medzi ľuďmi zo slabšej sociálnej vrstvy. Sú komentátormi udalostí, fotografií, statusov na sociálnych sieťach aj diania okolo seba, často bez reálnych vedomostí a skúseností. Radi hodnotia všetko a radi urážajú. Často nepoznajú hranicu kedy „dosť".

- **Poznávacie znamenia:** Vystupujú anonymne, tí odvážnejší pod svojím menom. Útoky môžu byť trvalejšie. Ideálne je ich nahlasovať a ignorovať. Agresor používa e-mail, telefonuje, píše SMS. Je odosielateľom textových odkazov.
- **Riešenie:** *Opakujúce sa útoky blokujte. Využite možnosti blokovania a ignorujte pisateľa. Ten menej nebezpečný prestane a nájde si inú zábavu.*

3. Pán Kyberkeliš alebo pani Kyberkelišová

Roznášajú klebety, ohovárajú, cielene si vymýšľajú a líšia sa najmä tým, že nie vždy ste to vy, komu píšu. Budú to vaši priatelia alebo ľudia mimo dosah, koho Kyberkelišová osloví. Horšie, ak ide o vašich učiteľov alebo kolegov a šéfov. Svojho času to bol Pokec a e-mail, dnes je to hlavne Facebook vďaka prístupu k vašim priateľom a prepojiteľnosti ľudí, ktorí vystupujú pod vlastnými menami.

- **Poznávacie znamenia:** O ich činnosti nemusíte mať žiadne informácie. Dozviete sa ich vďaka pozornejším ľuďom alebo až v podobe následkov. Ide o priamu komunikáciu, ktorá môže prebiehať mimo vás. Prípadne ide o statusy, ktoré vás spomínajú, ohovárajú a poškodzujú.
- **Riešenie:** *Riešenie je ťažšie pre komplikovanejšie odhalenie a orientovanie sa v rozsahu poškodenia osoby. Kde nepomáha komunikácia a žiadosť, tam môže pomôcť autorita (vedenie školy, rodičia, v prípade vážneho poškodenia osoby aj polícia). Polícia je nástrojom riešenia v prípadoch poškodenia dobrého mena a trestného činu ohovárania.*

4. „Zábavný“ ignorant

„Zábavný“ ignorant ignoruje hranice medzi reálnym ohrozovaním druhého a zábavou. Stavia sa do úlohy zabávača. Otupený a zaslepený nevidí, že urážky namierené na spolužiaka alebo niekoho v jeho okolí už prekročili medze. Ignorantami sú neraz celé školské kolektívy, ktoré v rámci „srandy“ považujú (nech má obeť meno) Šimona za homosexuála. Jeho to ale znepokojuje a ničí. Ani tá kočka z vedľajšej triedy ho už nechce, lebo sa medzi babami šíria reči a ten chalan je predsa všetkým na smiech. Spolužiaci si všimnú jeho reakciu a považujú za zábavné, ako sa Šimon bráni a vykrúca. Pre spolužiakov zostáva „homosexuálom“ len preto, že je to „zábava“. Pre náramnú srandu sa však nikto nepozrie na vec Šimonovými očami. Outsider je v triede každý, čo nejde s ostatnými. Outsider je ten, kto sa kamaráti so Šimonom. Neustále zosmiešňovanie a hľadanie spojitostí, ktoré by ďalej a ďalej udržiavali zábavnú tému aktuálnou, môže na Šimona pôsobiť ako nutnosť neustáleho úteku pred zúrivým býkom. Raz ale môže prísť vyčerpanie. Šimon musí hľadať pomoc v prvom rade medzi priateľmi, doma a u triedneho učiteľa. Sme v dobe, keď by sa nemal stretnúť s nepochopením, ale mala by mu byť poskytnutá pomoc. Neriešená kyberšikana môže končiť aj tragicky.

- **Poznávacie znamenia:** Výsmech a ponižovanie zo strany konkrétneho jednotlivca alebo kolektívu v profile obete, e-mailovej schránke, pod príspevkami obete a pod. Obeť ako téma č. 1 nemusí byť menovaná skutočným menom. Stačí prezývka známa širšiemu publiku. Urážky majú rôznu podobu, no zábavné pre obeť určite nie sú. Aj fyzické útoky v reálnom svete sa po nakrútení dostávajú do sveta virtuálneho, kde sa takéto materiály ďalej zdieľajú a stávajú sa virálnymi. Ide aj o nevhodné fotografie v chúlostivej póze. Kolujú po triede, v e-mailoch a na sociálnych sieťach. Počítajú sa aj fotomontáže.
- **Riešenie:** *Šimon, žiak alebo študent, zároveň obeť kyberšikany, má niekoľko možností vlastnej ochrany. V jeho koži máte niekoľko možností a krokov, ktorými docieliť zmenu:*
  1. *Nájsť v triede spojencov, svedkov takejto šikany.*

2. *Zaznamenávajte si komunikáciu a prejavy šikany. Aj v spolupráci s priateľmi. Rovnako takto viete aj vy pomôcť inej obeti šikany. Nikdy nebuďte ticho a šikanu riešte bezodkladne.*
3. *Komunikujte s rodičmi a zdôverte sa im s aktuálnymi trápeniami. Rodič nesmie problém riešiť svojimi cestami s inými rodičmi ručnými ľudovými nástrojmi (nebudem konkretizovať). Spolu s rodičom oslovte triedneho učiteľa alebo iného učiteľa, s ktorým máte lepší vzťah a dokážete spolu komunikovať.*
4. *Požiadajte učiteľa o pomoc pri riešení tohto problému. Vaša škola môže byť tá, ktorej učitelia prešli školeniami a vedia, ako postupovať, alebo kde hľadať účinnú pomoc. Je vhodné rozlišovať na jednej strane* ***obranu pred nebezpečenstvom,*** *s ktorým si obeť nemá ako sama poradiť, a na druhej strane „žalovaním", ktoré je v kolektívoch vnímané ako neprípustné. Nejde o žalovanie, ak ide o nutnú obranu a ochranu.*
5. *V prípadoch fyzických útokov, ktoré sú nakrúcané na video, je ideálnym riešením získanie spojenca medzi priateľmi, ktorý video získa. Nevyhnutné je mať záznam na vlastnom zariadení nezávislý od pôvodného zdroja pre prípad zmazania zdrojom. Ak šikana nie je na videu, v mnohých prípadoch neexistuje a ťažko sa dokazuje.*

5. Pán Hráč alebo pani Hráčka

Celkom iný level sú „hráči". Prichádzajú za vami, aby sa s vami pohrali. Je im jedno, čo všetko spôsobia. Chcú sa baviť. Zverejňujú chúlostivé informácie, videá, fotografie, čokoľvek, k čomu sa dostali z vášho telefónu alebo pri útoku do vášho účtu. Môže ísť pokojne o fotomontáž. Útočníkom je zväčša muž.

- **Poznávacie znamenia:** Využíva anonymitu cez falošný profil, prípadne skryté číslo. Chce sa baviť. Vy však určite nie. On určuje čas, spôsob, rozsah. V tom najhoršom prípade vy sami už neurčujete vôbec nič. Nevydiera. Jeho cieľom je ponížiť, zničiť alebo potrápiť. Môže ísť o priamu komunikáciu, zverejňovanie statusov, vytvorenie stránok s vaším menom, prípadne profilu s vašimi fotografiami a menom, avšak s falošnými príspevkami a názormi.

- **Riešenie:** *Konanie, ktoré nemá pre vás fatálne následky, je možné vždy nahlásiť konkrétnej službe. Kde nepomáha komunikácia a útok trvá, je nevyhnutné konať s použitím silnejších prostriedkov. Útoky, ktoré pokračujú, je nutné* ***oznámiť na polícii****. Utajené číslo na mobile nie je prekážkou, rovnako ako Hráčove anonymné e-maily. Pokiaľ ide o celú webovú stránku, majte ju celú zálohovanú v celej jej podobe vrátane URL adresy. Prejavy útokov si ukladajte (návod na vytvorenie screenshotu nájdete v časti NÁVODY na str. 273) a kontaktujte políciu s trestným oznámením. Pokojne nazývaj vec kyberšikanou, polícia tento pojem už pozná.*

6. Herci

Samostatným typom kyberšikany je vytváranie cudzej identity, jej zneužívanie, kopírovanie a manipulácia s ňou. Útočí na váš facebookový profil, prenikne doň a prevezme nad ním kontrolu. Vydáva sa za vás a vďaka tomu vás dokáže zničiť. Vo vašom mene zverejnené statusy sú prisúdené vám. Ak sa nedostal do vášho účtu, môže si z fotiek vyrobiť druhý. Vystupovanie takýchto hercov si nezaslúži Oscara. Skôr riešenie, podľa toho, akú veľkú škodu vám spôsobili alebo stále spôsobujú.

- **Poznávacie znamenia:** Nemáte kontrolu nad svojím profilom alebo e-mailovou schránkou. Prípadne pozeráte na seba, no nejde o váš profil. Prezradiť ho môže pozorný priateľ, ktorý si všimol podozrivý druhý účet skôr ako vy.
- **Riešenie:** *Prienik do vášho profilu znamená, že niekto má kontrolu nielen nad ním, ale aj nad všetkými vašimi správami a ich obsahom (fotografie, súkromné a chúlostivé informácie, videá). Aj preto mnoho služieb využíva dvojstupňovú ochranu (ochrana pred vstupom aj pomocou mobilu). Chrániť fotografie pred odcudzením je ťažšie. Ideálne je neposkytovať sociálnej sieti všetky snímky a v plnej kvalite. Falošný profil, ale aj jeho zneužitie, je možné oznámiť prevádzkovateľovi služby. Môžete sa pokúsiť vyžiadať „zabudnuté heslo" a opätovne prebrať nad účtom kontrolu.*

7. Vydierači

Vážnu kyberšikanu, ktorej následky dokážu poznačiť celý život detí a mládeže, budeme podrobnejšie rozoberať v časti venovanej zoznamkám a sociálnym sieťam. Vydierači sú mimoriadne nebezpeční. Pre konkrétne

pomenovanie a ďalšie delenie ich môžeme považovať za **pedofilov** ohrozujúcich deti viacerými spôsobmi (str. 273). Získajú fotografiu alebo video, no chcú viac. Využívajú na to slová, prosby, sľuby, rôzny nátlak, vyhrážky aj reálne skutky. Sú nimi aj **obchodníci**, ktorí chcú vaše peniaze alebo, nebodaj, ústupok v rozhodovaní. Vedia o vás niečo, čo by nemalo ísť von. Môžu sa vyhrážať ublížením rodine alebo iným útokom. Majú vaše nahé fotografie, obsah ukradnutého mobilu (téme sa venuje strana 195) či tajnú nahrávku z prokurátorovej kancelárie. Môže ním byť dokonca ex-priateľ, ktorý sa oháňa zverejnením súkromných záberov, ak nezíska hento-tamto, alebo ak mu nedáte „druhú šancu". Do tejto skupiny zaraďujeme aj **ransomware**, útočnú aplikáciu, ktorá vám zablokuje prístup do počítača a požaduje zaplatiť určitú sumu, aby sa prístup odomkol.

POZNÁMKA: Takzvaný **sexting** je komunikácia, ktorá na začiatku môže vyzerať nevinne a zvrtne sa hneď, ako útočník získa do rúk nástroj (chúlostivé informácie v textovej komunikácii, nahé fotografie, videá, hlasový záznam). Môže ísť o komunikáciu, ktorá od počiatku môže byť obeti nepríjemná a zo strachu inej hrozby v nej pokračuje. Vždy však ide o nepríjemnú komunikáciu so sexuálnou tematikou, ktorá vedie k zneužitiu obete, vylákaniu ďalších materiálov alebo k vydieraniu.

- **Poznávacie znamenia:** Využívajú takmer vždy anonymitu. V takom prípade chcú úhradu online kreditným systémom, čísla z karty alebo BitCoin. Len riskujúci útočník vás vydiera a pošle svoje číslo účtu. Nechce sa s vami hrať. Chce získať to, kvôli čomu sa rozhodol vás vydierať. Ak ide o ransomware, požaduje úhradu, inak prídete o svoje dáta v počítači (hoci, občas môže ísť len o falošné tvrdenie a dáta v skutočnosti neboli zablokované).
- **Riešenie:** *Akýkoľvek typ vydierania je nevyhnutné riešiť s políciou. Napriek zaužívanej nedôvere a strachu z riešenia vlastných nahých fotiek v neznámom policajnom prostredí ide o najúčinnejší nástroj, ktorý nesie najmenej následkov. V súčasnosti a v našom štáte iné nástroje, ktoré môžu mať účinok, neexistujú. Riešenie útokov ransomwaru je možné riešiť vyhľadávaním problému a sledovaním konkrétneho prípadu.*

8. Kyberstalkeri

Ďalšia nebezpečná forma kyberšikany je stalking. Obeťou stalkera môžete byť určitý čas aj bez toho, aby ste o tom vedeli. Sociálne siete im priniesli priam neuveriteľné možnosti, ako svoje obete sledovať, spoznávať a následne s nazbieranými informáciami tiež operovať. Zistiť o vás môžu čokoľvek, sledovať všetky vaše kliknutia, ale prechádzať môžu z virtuálneho sveta aj do toho reálneho. Kyberstalkerom môže byť muž aj žena.

- **Poznávacie znamenia:** Neznámi narábajú s podrobnosťami o vašom živote. Čelíte e-mailom, esemeskám, neprestávajúcim hovorom, správam a žiadostiam. Ste pod drobnohľadom odoberateľov každého príspevku a komentára. Neustále sa prejavujú, až máte z nich strach. Kontakt môže prechádzať až do reálneho stretnutia a sledovania.
- **Riešenie:** *Stalking v reálnom svete je nebezpečný a je nevyhnutné kontaktovať políciu. Kyberstalker o sebe zachováva oveľa viac stôp než stalker mimo internet. Preto ponúka ešte presnejšie nástroje na identifikáciu a zaistenie konkrétneho páchateľa. Polícii poskytnite všetky záznamy o jeho prejavoch, dátumy, názvy služieb, mená, pod ktorými vystupuje.*

9. Pán alebo pani Šoumanovci

Celkom osobitná kategória ľudí, ktorí šikanujú svoje okolie a spadajú pod všeobecné definície kyberšikany, sú útoční prankeri a autori videí typu „happy slapping“. Voľný preklad je „facka zo srandy“ alebo „úsmevná fackovačka“. Akokoľvek pojem preložíte, ten ironický podtón mu zostane. Cieľom je úspech v podobe uznania kamošov v kruhu blízkych alebo sledovanosť na YouTube. Iným cieľom je dostať vás na video, vašu reakciu, rozhorčenie, hnev, prekvapený pohľad. Na Slovensku to ešte nie je také bežné, aké je to bežné vo svete, v Južnej Amerike, v Británii, v USA, v Thajsku a v ďalších kútoch sveta.

- **Poznávacie znamenia:** Ste obeťou nelogického fyzického útoku, ktorý nepokračuje a nerozumiete mu. Celý útok logiku nemá. Ide o zábavu a sledovanosť.

KAPITOLA 3

Sociálne siete

VŠETCI

Sociálne siete

Sociálne siete boli vytvorené na to, aby zarobili obrovské peniaze. Ani jedna sociálna sieť v skutočnosti nie je udržiavaná za účelom pomoci ľuďom alebo za účelom ich spájania. Je to zisk z reklamy, ktorá je cielená na konkrétneho človeka. Z obchodného hľadiska je totiž sociálna sieť výnimočný nástroj, v ktorom každý o sebe uvedie všetko a dobrovoľne. Preto elektrikárovi Jánovi, ktorý má rád rockovú hudbu, nebudú zverejňovať reklamy na kabelky, ale skôr na gitaru, nové izolované kombinačky a pod. Pohľad užívateľský je ten náš. Sociálna sieť je pre užívateľa priestorom, v ktorom sa dokáže spájať s inými ľuďmi, komunikovať s nimi, vytvárať vzťahy – „socializovať sa".

Vzťahy sa na sociálnej sieti tvoria už len tým, že ste s inými ľuďmi fanúšikom rovnakého záujmového miesta, stránok, komentujete rovnaké príspevky s cudzími ľuďmi, dochádza k spojeniam, lajkovaniu a pod. O skutočnej socializácii (čiže prispôsobovaniu sa okolitej spoločnosti) nemôže byť ani reč.

Dojem bežného človeka je, že sociálna sieť je tu pre neho a nič sa mu nemôže stať. Opak je pravdou. Ľudia sú tu pre sociálnu sieť. Je riešená tak, aby nebolo možné len nahliadnuť a stránku vypnúť. Miliónové investície do jej prvkov neraz siahnu aj po psychológoch a odborníkoch v takzvanej UX oblasti. Oni vyhodnocujú, ako umiestnené tlačidlo, prvok, klik a vypínanie má tie najlepšie výsledky. Sociálne siete investovali milióny dolárov do toho, aby dokázali návštevníka zachytiť a už nepustiť. Dôvod je jednoduchý. Ak vďaka tomu udržia 10 miliónov návštevníkov na sociálnej sieti dlhšie o jedi-

né zobrazenie reklamy, už to je astronomicky vysoký zisk násobený každou ďalšou návštevou, dňom, týždňom, mesiacom, rokom... [1]

Je nástrojom na komunikáciu s priateľmi, nástrojom na zdieľanie akcií a propagáciu vlastného podnikania, aj nástrojom na zábavu. Stále však môže ísť aj o nebezpečný nástroj a novodobú závislosť, ktorú ak nediagnostikuje bežný lekár počas preventívnej prehliadky, nepovažujeme ju za problém. Na internet a jeho riziká nie je prirodzene pripravený absolútne nikto. Ani polícia, ani lekári, ani samotní používatelia, no tvárime sa, že je všetko v poriadku. Nasledovné riadky vás nechcú presvedčiť, že Facebook či Twitter je zlý alebo nebezpečný. Zlí a nebezpeční sú ľudia, ktorí sú pripravení zbierať o vás všetky súkromné údaje, a aj tí, ktorí sa zaregistrovali a prihlásili presne tak ako vy.

Chráňte sa, má to zmysel!

DETI MLÁDEŽ DOSPELÍ SENIOR

Neprezrádzajte o sebe priveľa

Čím viac toho o sebe dáte na internet, tým viac o vás vedia druhí a vy o nich pritom stále neviete absolútne nič. To je nevyrovnané, nemyslíte? Vlastne, čím viac toho o sebe prezradíte sociálnej sieti, tým viac vie samotná sociálna sieť všetko využiť na bombardovanie ideálnou reklamou. Nepriatelia to môžu zneužiť pri hľadaní zbraní proti vám a ktokoľvek nebezpečný vďaka tomu má ľahšiu cestu vás oklamať, okradnúť alebo aj zneužiť. Na sociálne siete nie je dnes vhodné nahrávať fotografie vo veľkej kvalite, ktoré zachytávajú celú tvár alebo dokonca doklady, diplomy či iné osobné údaje, napríklad na dokumentoch. Veľké fotografie dnes dokážu zneužiť technológie na rozpoznávanie tváre, no pre zahmlené pravdy-nepravdy o pozadí sociálnych sietí a kontrole zahraničnými bezpečnostnými agentúrami je otázne, či vôbec nahrávať osobné fotografie napríklad aj do osobnej komunikácie. Ove-

1 SPITZER, M. Digitálna demencia, Bratislava: Citadella, 2018. 304 s. ISBN: 9788081820885

ľa častejšie sa však vaše fotografie môžu ocitnúť v rukách cudzích ľudí, ktorí s nimi môžu vytvárať pokojne aj celkom nové falošné profily. Aj fotografie odoslané v Messengeri pred rokmi môžu znamenať problém. V prípade, ak ste posielali akékoľvek fotografie, dokumenty, osobné údaje alebo chúlostivé fotografie cez Messenger, skúste ich dohľadať a pokúste sa ich zmazať. Samotný Facebook mi už v minulosti opakovane dokázal, že nahraté fotografie nezmaže a sám si ich uchováva. Odkazy na balíčky fotografií na vlastnom serveri sa Facebook pokúšal opakovane stiahnuť v čase, keď boli zmazané. Správu som pritom poslal sám sebe niekoľko mesiacov skôr. Facebook si komunikácie prechádza a odkazované ZIP súbory snaží stiahnuť? Zvláštne, no ako informácia cenné zistenie. Ďakujem Facebooku, že mi jeho kalifornská IP adresa odhalila, že ani v súkromnej komunikácii nie je nič súkromné.

V súkromnej správe sa môže nachádzať všeličo. Aj medzi partnermi vymenené nahé fotografie, čo býva jeden z najčastejších problémov. Ak by sa raz niekto dostal k vášmu mobilu, uloženým heslám a vôbec do konta Facebooku, čo by tam našiel? Fotografie a dáta nezmazané vami sú viditeľné aj pre páchateľa, ktorý by prenikol do vášho konta.

Súkromie je oveľa cennejšie

Prečo práve vy? Pokiaľ sa vám ešte nič zlé na internete nestalo, odpovedať na túto otázku vám bude pripadať smiešne. Facebook sa v plnej sile začal na Slovensku prejavovať v roku 2008 až 2009. Odvtedy ubehol nejaký čas a aj samotný Facebook či Twitter sa neustále vyvíjajú. Dokonca aj známa slovenská zoznamka Pokec sa svojho času snažila podobať na sociálnu sieť, čiže do určitej miery je dnes sociálnou sieťou aj ona. Zdá sa byť zábavou vypĺňať všetky tie okienka. Ak niektoré vynecháte, služba na to po čase upozorní. Sociálna sieť chce vedieť všetko. Na princípe zbierania údajov pracujú mnohé spoločnosti. Informácie totiž majú hodnotu. Kto pozná svojich používateľov, ten je schopný zarobiť milióny alebo miliardy dolárov. Ako je to možné? Jednoducho. Zisk prináša reklama a vám, ak ste dievča z Popradu a máte rada kone, predsa nebudú zverejňovať reklamu o pneuservise z Dunajskej Stredy. Čím menej toho o vás vie sociálna sieť, tým menej toho vie aj niekto vonku. Je pritom celkom jedno, ako vyzeráte a odkiaľ ste. Kto je ľahkou obeťou a zraniteľnou, ten je ihneď na rane.

DETI MLÁDEŽ DOSPELÍ

Neznámi „priatelia“

Medzi priateľov patria len priatelia. Nepochybne ste už získali žiadosti o priateľstvo od neznámych. Hľadáte aspoň jeden dôvod, prečo si takého človeka pridať? Neexistuje žiaden. Akceptovať ich žiadosť len preto, aby narástol počet priateľov je nezmysel. Na súčasných základných školách panuje názor, že čím viac priateľov, tým „coolovejšia baba“. Pritom ktokoľvek s nepotrebnými piatimi eurami si môže kúpiť 500 falošných priateľov v inzeráte na webe. Súťaž v počte priateľov je hlúposť. Naopak, existujú dôvody, prečo si neznámych ľudí nepridať. Vždy totiž predstavujú riziko, či veľké množstvo viacerých rizík naraz. Môže to byť omyl, kedy niekto naozaj požiadal o priateľstvo omylom. Skrátka, hrubý prst na telefóne. Za ten sa ešte nestrieľa. No niektoré falošné profily sa prejavujú ako trójske kone. Áno, to je niečo z dejepisu. Profil sa dostane medzi priateľov a prejaví sa v nestráženej chvíli. Je to napríklad stalker, ktorý je odrazu oveľa bližšie k sledovanej obeti. Alebo ukrivdený bývalý tajný ctiteľ či nebezpečný hráč. Mnoho falošných účtov funguje aj pre obchodné účely. Chcú mať priateľov, lebo taký účet sa lepšie predá na ilegálne činnosti. Účet bez priateľov predsa nikto nekúpi. Takých môže mať ktokoľvek koľkokoľvek. Vo všeobecnosti sú to však často účty špionážne. Vytvorené len preto, aby vás sledovali a podávali informácie či analyzovali správanie. Zneužívali na marketing alebo cielené útoky. Napríklad aj priamu kyberšikanu (viac o kyberšikane od strany 65).

Novinkou je podstrčený profil. Pri ňom nemusíte prijať žiadosť o priateľstvo, no profil veľmi dobre vie, že vás bude motivovať kliknúť si a pozrieť na jeho nástenku a vlastnosti. Môže to byť atraktívne dievča, ktoré žiada o priateľstvo mladých mužov. Samozrejme, že funguje zvedavosť. Profil si otvoria a jediným obsahom je klik na video, článok odkazujúci na nahotu alebo neprístupný film. Tlačidlo „PLAY“ je však často súčasťou obrázku, čo je podozrivé. V skutočnosti ide o klik na nebezpečné stránky.

TIP: Ak ste zvedaví, kto je neznámy žiadateľ o priateľstvo, nikdy neprijmite žiadosť a potom sa pýtajte. Kontaktovať s otázkou môžete žiadateľa skôr, ako prijmete priateľstvo.

TIP: Vytvoril si niekto z vašich fotografií profil a obťažuje vašich blízkych? Akýkoľvek profil, ktorý používa vaše fotografie a meno, máte právo nahlásiť aj bez toho, aby sa akokoľvek prejavil. Je teda jedno, či niekomu taký profil píše alebo je nečinný. Mnohé činnosti sa nemusia prejavovať navonok. Žiadať Facebook, aby odstránil profil, ktorý zneužíva vašu identitu a biometriu – fotografie, je nevyhnutné okamžite. Postup nahlásenia je uvedený v kapitole NÁSTROJE. Ide o formu kyberšikany, ktorá ak prerastá do útokov vyzerajúcich, akoby ste boli útočníkom vy, mala by zakročiť polícia. Jeho útok je totiž pripisovaný vašej osobe.

FAKT: Neodporúčam sťahovať niekoho fotografie a vytvárať falošný profil. Môže sa vám to celé zvrtnúť a stačí drobnosť, ktorá vyvolá reťazovú reakciu.

Profil môže mať ktokoľvek a pod ním sa môže skrývať ešte väčšie tajomstvo

Nie je nič nové, že vytvoriť profil zvládne aj malé dieťa. Pri 40 opýtaných ľudí vo veku 16 až 35 rokov mi v anonymnom dotazníku priznalo až 15 z nich, že majú viac ako jeden profil na Facebooku. Zväčša kvôli biznisu alebo súťažiam. Čudujem sa prečo, ak je zo 100 súťaží na Facebook podvodných 98. Na Facebooku nájdete mnoho profilov známych osobností, politikov či športovcov. Herci a herečky si neraz dávajú iné mená, namiesto priezviska použijú prezývku. Ani na fotografii sa zväčša nenachádza priamo tvár. Politici radi používajú svoje skutočné mená. Mimo skutočné profily sa objavujú aj mnohé falošné. Fico by vedel hovoriť. Vytvorené sú z rôznych dôvodov, pre zábavu, pre slovné útoky aj pre vysmievanie sa na iných miestach pod menom politika. Zopár účtov má aj Pablo Picasso. Nič na tom nemení fakt, že zomrel už dávno a Facebook nezažil.

DETI MLÁDEŽ DOSPELÍ

Deti na sociálnych sieťach

Deti, nie ako narážka na slabú úroveň znalostí ľudí všetkých vekových kategórií. Myslím deti. Čiže ľudí od prvých rokov, od ktorých si dokážu s pomocou kohokoľvek vytvoriť svoj vlastný profil na sociálnej sieti, až po 13, 14 alebo 15-ročných tínedžerov. Aj oni sú súčasťou, hoci niektoré portály umožňujú vstup až od určitého veku. Prostredie stránok sa deťom prispôsobuje jedine ak na YouTube v rozrhaní YouTube Kids, a aj to len po zásahu rodiča. Ostatné služby majú rozhranie rovnaké pre všetkých. Čiže ak chcete smerovať podvodnú reklamu na dvojzmyselne ukryté erotické fórum, ide to. Ale nerobte to. Administrátori Facebooku (sediaci v zahraničí) si to nemusia preložiť správne. Stačí, ak pri schvaľovaní kampaň smeruje na nevinný odkaz a po schválení sa presmeruje na druhý. Deti sú obeťami presne cielených reklamných kampaní a rodičom sa takáto reklama nezobrazí. Pochopiteľne, nemajú nastavený vek 13 rokov. S takýmto problémom som sa stretol skôr v minulosti. Na jednej strane, môžeme byť radi, že deti sú dnes vyspelé, dokážu sa orientovať na internete a predbiehajú dobu. Na druhej strane, je to len zdanie. To nepoznané preskakujú a málokedy chcú vedieť viac, pretože im ujde nejaký status či nejaký dôležitý podcast. Ak im teda odrazu blikne správa a tam zhovorčivý človek, ktorý im pripadá zaujímavý, tak prečo neodpovedať? Tento záujem priláka dotyčná osoba rôznym spôsobom. V rámci prípadov, s ktorými som sa stretol, ide hlavne o:

Neznámy pisateľ a spôsob, ako sa prihovoriť dieťaťu

- Ponuka darčeka, akéhokoľvek, napríklad aj peňazí (uspokojenie potreby a zaslepenie odmenou)
- Odpoveď na otázku dieťaťa, ktorú zverejnilo verejne (vyriešenie problému)
- Reakcia na nejakú tému a stret rovnakého názoru (spoločná reč)
- Pochvala alebo pozdvihnutie sebavedomia (psychologický efekt)
- Zneužitá bezradnosť či smútok, ťažšia situácia pre dieťa (efekt záchrancu)
- Hra na náhodu alebo náhodný prieskum, otázka a pod.

POZNÁMKA: Bez toho, aby som spresňoval spôsoby ohrozenia, akýkoľvek kontakt neznámeho dospelého človeka, ktorý je smerovaný na deti, je dôvodom na pozornosť. Ak neznámy starší od detí čokoľvek žiada, do niečoho ich núti a akokoľvek ohrozuje, ide o dôvod, kedy by mal spozornieť rodič a posúdiť nutnosť privolania polície. V každej rodine by medzi deťmi aj rodičmi malo existovať povedomie o tom, že niektoré druhy správ dospelých je potrebné ignorovať a nereagovať na ne, prípadne nahlasovať. Takéto poučenie by malo existovať už na základnej škole s oveľa väčším dôrazom, ako sa to deje, respektíve nedeje dnes. Je priam neuveriteľné, že na stredných školách sa žiaci prihlasujú do svojich účtov na Facebooku a Pokec a už v školskom prostredí si čítajú správy od rôznych pisateľov zvonka s aj nevhodným obsahom.

MLÁDEŽ DOSPELÍ

Ochrana detí na sociálnych sieťach

Zásah rodiča do komunikácie dieťaťa je niečo, čo netreba preháňať. Jasné. Rodič si vyžiada heslo, aby si prečítal diskusiu. Dosiahne tým vyššiu bezpečnosť? Dosiahne len to, že dieťa bude odteraz históriu komunikácie mazať, alebo si vytvorí náhradný profil. Rodič vezme dieťaťu telefón? Dieťa nadšené nebude, no v škole mu prvý dobrý kamoš pomôže a prihlási sa cez jeho zariadenie. Rodič bude dieťa sledovať tajne? Ako bude narábať so zisteniami, ktoré dieťa neohrozovali, ale môžu sa rodičia ich poznaním prezradiť? Deti nie sú hlúpe. Okrem toho, zistenie, že sa rodič dostáva do účtu, aby dieťa sledoval, naštrbí dôveru. Ako rodič chcete, aby vám dieťa verilo, no ono samo vie, že nemôže veriť svojim rodičom. Dosť na nič. Patová situácia, ktorá nemá zdanlivé riešenie. Kontrolu dieťaťa je nutné prispôsobiť veku, využívať aplikácie na stráženie činnosti v mobile. Vyžaduje si to však niečo mimoriadne náročné. V prvom rade vedieť obsluhovať svoj vlastný telefón, ak má rodič vedieť ovládať a zabezpečiť telefón dieťaťa.

TIP: Pre počítače aj mobilné zariadenia sú vhodné ESET Parental Control, Kaspersky Safe Kids, KidLogger, Norton Family parental control, Qustodio Parental Control a ďalšie fungujúce na rovnakom princípe. Ideálna cesta pri ich hľadaní je sledovať reálne skúsenosti rodičov, články skúsených redaktorov a vynechať cielené vyhľadávanie a sťahovanie z neznámych stránok. Aplikácie pri platených verziách poskytujú možnosti ako nahrávanie hovorov, sledovanie písanej komunikácie, používané aplikácie a navštívené stránky. Bezplatná aplikácia Google Family Link je taktiež obľúbenou alternatívou. Určená je však len pre systém Android. Skladá sa z dvoch rôznych aplikácií. Aplikáciu s názvom Google Family Link pre rodičov preto rodič inštaluje sebe a aplikáciu Google Family Link pre deti a tínedžerov inštaluje do telefónu dieťaťa. Google môže pri zadávaní kódu a vytváraní účtu požadovať číslo karty, no nepôjde o úhrady, ale o spôsob overenia.

Problém má riešenie, len je náročné a vyžaduje si „rodiča – priateľa". Šlo by to?

Za najdôležitejšie považujem vzdelávanie detí. Osvedčilo sa mi vysvetľovať na vyučovaní deťom možné riziká spôsobom, aby to nebrali ako povinnosť. Fádne reči znudeného učiteľa nebudú deti brať vážne. Dokonca si zmysel výkladu neuvedomia plne ani vtedy, keď je pri tom uvedené „*Bude to v písomke*!". Sú aj nenásilné riešenia, ktoré sa dajú využiť v bežnej slovenskej domácnosti. Ak už sme ako rodičia a moderní ľudia dopustili, aby boli naše deti a mládež online, nesme následky... alebo ešte lepšie – počítajme s prevenciou. Obetujme čas pre jeden z dvoch nasledovných nástrojov. Oba sú predstavené ako súčasť hry, s ktorou bude dieťa o štipku celej veci rozumieť viac ako pri teoretickom popise a ostrých príkazoch, čo má robiť a čo nie.

Tomáš Šalmon
(Ne)bezpečný internet
Sprievodca pre používateľov internetu od 10 do 99 rokov

Prvé slovenské vydanie
Vydalo vydavateľstvo Lindeni v roku 2021
v spoločnosti Albatros Media Slovakia, s. r. o.,
so sídlom Mickiewiczova 9, Bratislava, Slovenská republika.
Číslo publikácie 2 283
Zodpovedný redaktor Tomáš Krejčiřík

Jazyková korektúra Michaela Kobidová
Sadzba Petr Klíma
Obálka slaavo

Tlač NOVOPRINT SLOVENSKO, s. r. o., Zlaté Moravce

Cena uvedená výrobcom predstavuje nezáväznú odporúčanú spotrebiteľskú cenu.

Objednávky kníh:
www.albatrosmedia.sk
eshop@albatrosmedia.sk
tel.: 02/4445 2046

ALBATROS MEDIA