Trendy v podnikání - Business Trends (2019), 9(3), 4-12.
https://doi.org/10.24132/jbt.2019.9.3.4_12

BEZPEČNOST NA SOCIÁLNÍCH MÉDIÍCH
SAFETY ON SOCIAL MEDIA

Veronika Jánská[1], Michal Mičík[2]

[1] Bc. Veronika Jánská, Západočeská univerzita v Plzni, Fakulta ekonomická, vjanska@fek.zcu.cz
[2] Ing. Michal Mičík, Ph.D., Západočeská univerzita v Plzni, Fakulta ekonomická, micikm@kmo.zcu.cz

Abstract: Social media provide many benefits to its users, but with their use, people also face many risks. In this paper, the authors focus on these risks and, using two methods, a questionnaire survey and a focus group, research of the target group is conducted. The aim of this research is to learn whether the research participants feel safe on social media and whether they know the risks that may affect them or their close ones. At the end of the paper, there are recommendations and preventive measures that could help to minimize the exposure of users to these risks.

Keywords: Internet, risks, social media, safety, trust

JEL Classification: M30, L86

ÚVOD

V dnešní době už si většina studentů (a nejen oni) nedokáže svůj běžný den bez sociálních sítí představit. Staly se součástí každého z nás, pomocí sociálních sítí si uživatelé hledají informace, baví se s přáteli, sdílí s nimi jejich zážitky, svěřují se, nebo si prostřednictvím nich hledají práci. Někdo z nich ale netuší, že s těmito výhodami sociálních sítí jdou ruku v ruce také nevýhody. Tou nejhlavnější z nich je právě nebezpečnost a rizika spojená s užíváním sociálních médií. Spousta lidí si neuvědomuje, že na druhém konci počítače mnohdy nemusí sedět člověk, za kterého se na internetu někdo vydává a že může být vystaven nebezpečí. Mezi rizika, kterým je třeba věnovat pozornost, patří kyberšikana, phising, krádež identity, kybergrooming a poslední, v dnešní době stále více se objevující rizikové chování – sexting. Každé z těchto rizik je třeba zkoumat a eliminovat jeho dopady. V tomto článku jsou metody pro eliminaci těchto rizik popsány v poslední části.

1. SOCIÁLNÍ MÉDIA JAKO FENOMÉN 21. STOLETÍ

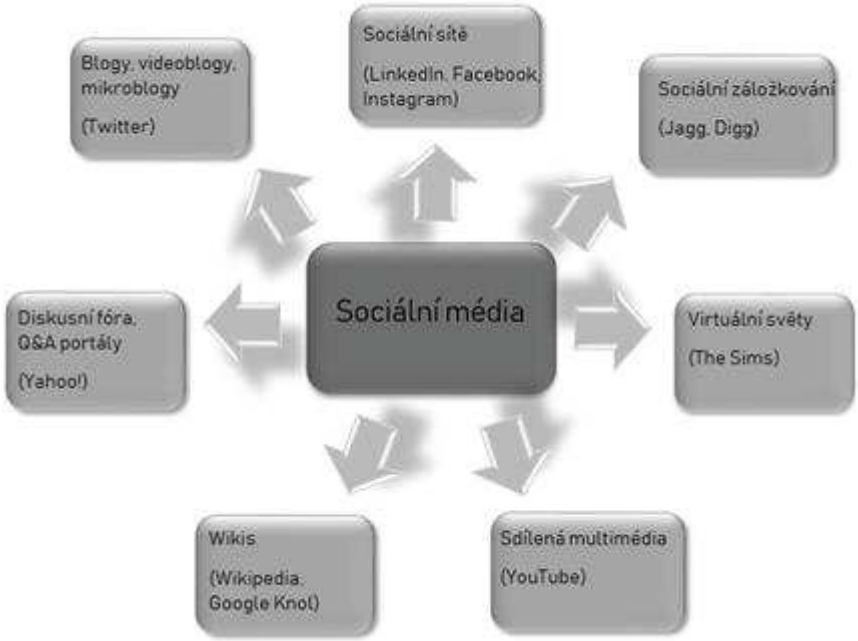
Ač se zdá, že sociální média jsou novým pojmem a fenoménem 21. století, lidé si mezi sebou předávají doporučení, myšlenky a názory už po staletí. V moderní historii k tomuto sdílení informací lidé používali diskuse z očí do očí, dopisy, telefon nebo nejvíce používaný email. Je zde ale spousta nových výhod a možností, co nám nabízejí sociální média, jak je známe dnes. Jsou to především jednoduchost, transparentnost a přístupnost (Smih, Wollan & Zhou, 2011).

Sociální média lze poznat podle některých typických prvků (Nations, 2019):

- Lze si na webu vytvořit uživatelský účet.
- Možnost přizpůsobení a nastavení profilu.
- Aktualizování informací.
- Možnost komentovat jiné příspěvky.
- Hodnocení nebo hlasování.

Sociální média se dělí na několik kategorií. Mnoho lidí zaměňuje pojem sociální média a sociální sítě. Sociální sítě jsou ale pouze podkategorií sociálních médií. Obrázek číslo 1 toto dělení znázorňuje.

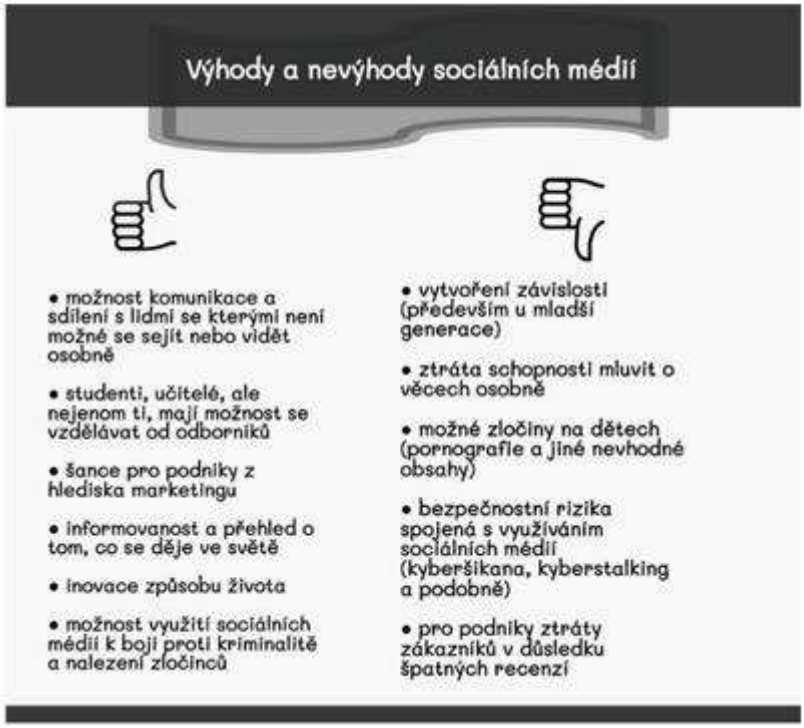
Obr. 1 – Dělení sociálních médií



Zdroj: Vlastní zpracování dle Janoucha, 2013

Jak již bylo v úvodu naznačeno, sociální média s sebou přináší řadu výhod, ale také nevýhod. Ty nejdůležitější z nich jsou popsány na následujícím obrázku:

Obr. 2 - Výhody a nevýhody sociálních médií



Zdroj: Vlastní zpracování, 2019

Mezi 15 nejpoužívanějších sociálních médií k lednu roku 2019 patří na prvním místě Facebook, dále YouTube, Twitter, Instagram, LinkedIn, Reddit, VK, Tumblr, Pinterest, Google+, Flickr, meetup, Ask.fm, LiveJournal, myspace (ebizmba.com, 2019).

V České republice mezi nejoblíbenější sociální média řadíme na prvním místě Facebook, dále YouTube, Instagram, LinkedIn, Twitter a Snapchat. Začínají se ale probouzet a získávat si stále větší popularitu sociální média jako Pinterest (s počtem něco kolem 200 tisíc uživatelů), nebo Tinder (Lorenc, 2017).

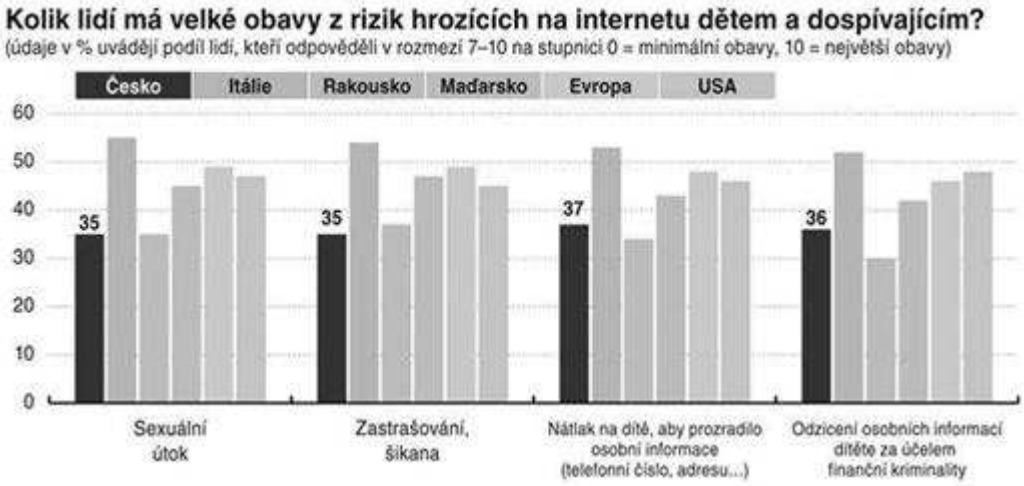
2. BEZPEČNOST A RIZIKA SPOJENÁ S UŽÍVÁNÍM SOCIÁLNÍCH MÉDIÍ

Internetová bezpečnost je relativně mladý pojem. Začala se řešit až na přelomu 80 a 90 let 20. století, i když k propojování počítačů docházelo již dříve. Doba kdy uživatelům hrozila ,,jen" zavirovaná disketa je bohužel už minulostí (Eckertová & Dočekal, 2013).

Nebezpečí na Internetu a sociálních médiích stále roste. Stále se objevuje více možností, jak si útočník může najít cestu k oběti. Největší chyba, které se uživatelé Internetu dopouštějí, je, že jsou přesvědčeni, že tohle se jim nikdy stát nemůže. Ale i člověk, který se snaží chovat na Internetu bezpečně, se tou obětí klidně může stát. Je proto třeba být opatrný a znát rizika, která uživatele mohou na Internetu a hlavně – na sociálních médiích – potkat, protože některá z nich do značné míry lze svým chováním ovlivnit a omezit nebo v opačném případě zvýšit pravděpodobnost jeho nastání.

Podle průzkumu Europ Assistance, kterého se zúčastnilo přes 7000 respondentů z Evropy a USA ukazuje, že Češi mají největší obavy z rizika, že bude vyvíjen nátlak na jejich dítě, aby prozradilo své osobní údaje. V porovnání s ostatními zeměmi - nejvíce se těchto rizik obávají Italové a nejméně Rakušané. Další rizika, kterých se Češi obávají, lze vidět na obrázku č. 3 (idnes.cz, 2019).

Obr. 3 - Obavy z rizik hrozících na Internetu



Zdroj: idnes.cz

Rizik, která uživatele na sociálních sítích mohou potkat, je spousta. Je potřeba je znát, umět na ně reagovat a především snažit se na sociálních médiích chovat tak, aby nedocházelo k jejich prohlubování.

3. METODOLOGIE

Pro výzkum byly použity dvě metody. První metodou bylo dotazníkové šetření, který byl zaměřený na studenty středních a vysokých škol. Dotazování probíhalo ve dvou formách – přes portál survio.com a v papírové podobě, která byla využita pro studenty středních škol. Dotazování probíhalo v elektronické podobě na sociální síti Facebook, byl umístěn na několika školních skupinách, soukromém profilu a probíhalo od 19. 2. 2019 do 19. 3. 2019. Vzhledem k tomu, že dotazníkové šetření vyplnilo celkem 150 studentů, nelze výsledky zobecňovat pro všechny studenty.

Cílem dotazníku bylo zjistit, zda se uživatelé Internetu cítí na sociálních mediích bezpečně a jestli znají rizika, která se jich nebo jejich blízkých mohou týkat, co nejčastěji na Internetu dělají, dále kolik času tráví na sociálních médiích, proč tyto média používají a zdali jim doba na nich přijde užitečná a v neposlední řadě také jestli je podle nich veřejnost obeznámena s nebezpečím, které jim může hrozit, jaká skupina je

dle nich nejvíce ohrožena a jestli znají alespoň nějaké projekty, které mají za cíl těmto rizikům předcházet nebo jejich obětem pomoc je řešit.
Bylo také zjišťováno, zda existuje vztah mezi důvěrou v informace uvedených na Facebooku a na internetové stránce, a zda existuje asociace mezi věkem respondenta a dobou strávenou na sociálních médiích. Byly taky formulovány dvě hypotézy:

H1: Existuje asociace mezi důvěrou v informace uvedených na Facebooku a na internetové stránce.
H2: Existuje asociace mezi věkem respondenta a dobou strávenou na sociálních médiích.

Na základě charakteru dat byla pro zkoumání asociací vybrána neparametrická statistická metoda Kendallovo Tau,. Tento koeficient se používá pro měření síly vztahu dvou proměnných a je používán pro pořadová data (Hendl, 2015).
Druhou metodou použitou pro výzkum byla metoda focus group (např. Bryman, 2016; Hyman & Sierra, 2010). Jedná se o metodu, kdy se s několika respondenty vede diskuse na dané téma a měla by trvat přibližně jednu hodinu. Diskuse byla provedena se studenty střední školy v Rakovníku, z Masarykovy obchodní akademie, konkrétně studenty 3. ročníku. Studenti byli rozděleni na dvě skupiny po 8 a obě pohlaví byla zastoupena ve stejném poměru. Nejdříve byly probírané doplňující otázky k dotazníku, který studenti dostali k vyplnění a poté otázky, které byly rozděleny do čtyř oblastí – závislost na sociálních médiích, Facebook, obsah na síti a důvěra v přátele, které na sociální síti mají. Cílem této diskuse bylo doplnit otázky z dotazníku, seznámit studenty s problematikou bezpečnosti na sociálních médiích a zachytit jejich názory a domněnky vůči tomuto tématu.

4. VÝSLEDKY VÝZKUMU

4.1 Výsledky focus groups

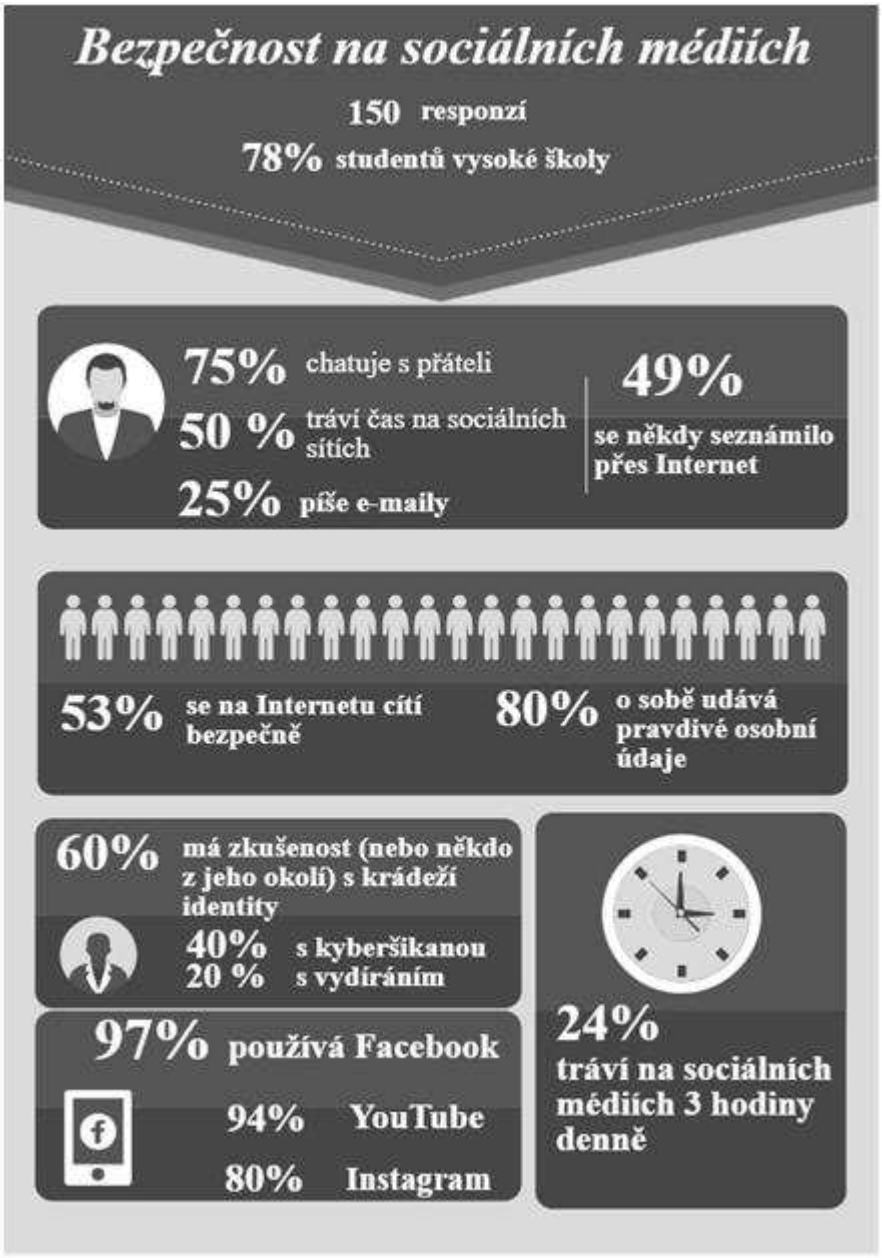
Studenti nejčastěji na internetu tráví čas na sociálních médiích, čtou zprávy, novinky ze světa a sledují on-line seriály. Téměř polovina z nich uvedla, že nejčastěji sledují dění ve sportu a vyhledávají si informace pro vzdělávání. Důvěru ale v sociální sítě nemají, informace uvedené na Facebooku jsou pro ně nedůvěryhodné, vnímají je spíše jako marketingový tah nebo hoax a věří spíše informacím, které jsou uvedené na internetové stránce. Jedna studentka jako příklad uvedla, že se jí ne jednou stalo, že na facebookové stránce obchodu byly rozdílné ceny, než na internetové. Informace, které nejčastěji na Internetu vyhledávají, jsou informace o počasí, informace do školy, nebo o cestování. Studenti většinou tráví na sítích déle než tři hodiny a to hlavně proto, že sledují videa na YouTube, ale záleží na dni, o víkendu je to déle než o všední dny. Doba strávená na sociálních médiích jim ale užitečná nepřijde – většinou spíše prokrastinují a některým z respondentů to přijde jako ztráta času. Na otázku, co užitečnějšího by místo toho mohli dělat, odpověděli učení, sportování, nebo osobní setkání s člověkem, se kterým si na síti píší.
Z průzkumu také vyplývá, že sociální média pro většinu respondentů mají více výhod, než nevýhod. Jsou mezi nimi rychlost, možnost plánování akcí, sledování událostí co se dějí v okolí, možnost zhlédnutí seriálu zadarmo, nebo sportovní informace. Mezi nevýhodami se objevil fakt, že si o Vás může kdokoli cokoli zjistit a bezpečnostní rizika z toho plynoucí.
Studenti na sítě o sobě většinou uvádějí pravdivé osobní údaje, ale údaj, který by na sociální média nikdy nedali, je pravý věk, bydliště, nebo telefonní číslo. Své vztahy na sociálních sítích také nezveřejňují a to hlavně pro to, že je to zásah do jejich soukromí. Přes internet se ale seznamují, dokonce někteří z nich uvedli, že si díky nim našli partnera. Mají kolem sebe také lidi, kteří zcela běžně využívají portály pro seznamování – většinou badoo nebo tinder, oni sami ale tento způsob seznamování nevyužili.
Nejvíce ohrožená věková skupina je 15 a méně, je to dáno tím, že takto mladí uživatelé sociálních sítí se na nich nedokáží tak orientovat, snáze uvěří, jsou naivnější a mají skony k tomu odpovídat cizím lidem.
Rizika, se kterými se na sociálních sítích nejvíce setkávají, jsou krádež identity, většinou na Instagramu a kyberšikana, Většinou se tato rizika dají ovlivnit svým chováním například tím, že uživatelé nebudou na svůj profil uvádět fotografie a odepisovat cizím lidem.

V druhé části focus group otázky spadaly do 4 okruhů, jak již bylo zmíněno – závislost na sociálních médiích, Facebook, důvěru a obsah na síti.
Většina studentů je na sociálních sítích závislá a nedokáže si bez nich svůj běžný den představit. Zrušit by si ho ale dokázali, někteří o tom i uvažovali, ale nakonec se rozhodli pro používání, hlavně pro to, že by nebyli schopni sledovat dění ve skupinách ve kterých jsou členy (například skupina jejich ročníku). Studenti také uvedli, že by se cítili mimo hru, pozvánky na akce a domlouvání se na ně probíhá většinou právě přes sociální sítě a tak by o tyto informace byly ochuzeny. Pokud nemají delší dobu připojení, nervózní se ale necítí, možná jen mají starost, jestli jim někdo nepsal. Na otázku, které komunikaci dávají přednost, zda-li osobní, nebo na sociálních médiích, odpověděli, že záleží na tom s kým. S důležitými lidmi, kamarády a partnery se raději setkávají osobně.
Další okruh byl věnován Facebooku. Facebook je podle většiny respondentů nejrozšířenější sociální síť. Všichni jí mají a běžně používají, i když Facebook podle nich bude brzo nahrazen jinou platformou (Instagramem). Důvodem proč se tak může stát, uvádějí větší přehlednost instagramu a nedostatky, které Facebook má. Hlavním důvodem proč Facebook používají je možnost komunikace, sledování událostí a skupiny, do kterých se mohou přidávat. Na Facebook si většinou přidávají lidi, které osobně znají, nebo znají od vidění (například studenty z vyšších ročníků). Hlavní výhodu Facebooku vidí v možnosti komunikace a možnosti sestavit si vlastní plán akcí (událostí).
Co se týče obsahu, který na sociální sítě přidávají, většinou se jedná o aktualizaci profilové fotky, kterou mění v průměru jednou za měsíc, dále sdílení videí z youtube, většinou písničky, nebo zprávy ze světa (novinky). Nejvíce obsahu přidávají na Instagram a to na insta story, většinou denně. Přímo na profil pak fotky přidávají 1x týdně.
Posledním podtématem, o kterém se hovořilo, byla důvěra v lidi, které na sociálních médiích respondenti mají. Ať už jejich přátelům, nebo followerům, studenti spíše věří. Profilům, kterým ale nedůvěřují, jsou profily, které nemají profilovou fotku, nebo které na profilu mají jen jednu, nebo dvě fotografie. Uvádějí, že takové profily jim přijdou nedůvěryhodné, nebo falešné. Na sociálních médiích přesto, že svým přátelům důvěřují, se ale veřejně na profilu nesvěřují, jen pár z nich po chatu, pokud je to neodkladné a důležité.

4.2 Výsledky dotazníkového šetření

Formulované hypotézy H1 a H2 byly testovány s pomocí software Statistica. Na základě p-hodnoty, která v případě H1 vyšla 0,000001 lze konstatovat, že mezi proměnnými (důvěra v informace uvedené na Facebooku a na internetové stránce) existuje statisticky signifikantní asociace, jejíž hodnota je 0,438. **H1 je tak přijata.**
Na základě p-hodnoty, která v případě H2 vyšla 0,805 lze konstatovat, že mezi zkoumanými proměnnými (věk a doba strávená na sociálních médiích) není statisticky významný vztah. **H2 není přijata.**
Dále byl pro přehlednou interpretaci dotazníkového šetření vytvořen report, ve kterém jsou shrnuty výsledky šetření. Procenta jsou pro větší přehlednost zaokrouhlena.

Obr. 4 - Výsledky dotazníkového šetření



Zdroj: Vlastní zpracování, 2019

5. DOPORUČENÍ A PREVENTIVNÍ OPATŘENÍ

Na základě provedeného výzkumu byla formulována následující doporučení a preventivní opatření.

Uchovávat si své soukromí

První a zároveň jedna z nejdůležitějších věcí, je uchovávat si své soukromí. Je třeba si svůj profil nastavit tak, aby vyhovoval požadavkům uživatele a cítil se bezpečně. Upravit si své osobní údaje a zveřejňovat jen ty, které chce, aby viděli jeho přátelé. Také je důležité si své profily nastavit jako soukromé, nehrozí tak, aby údaje viděli cizí lidé. Je vhodné, udávat o sobě jen informace, jaké si dané sociální médium žádá, většinou je to jméno, email a věk. Svou adresu, rodinný stav, nebo telefonní číslo většinou není nutné udávat – a pokud ano, lze je nastavit soukromě, ovšem nedávnému problému s únikem dat, se kterým se potýkal Facebook, by se dalo předejít jedině tím, Facebook si vůbec nezakládat.

Nesdílet svou polohu
Ať už sdílení polohy přes sociální média soukromě (messenger) nebo veřejně (instastory) může být nebezpečné a pokud má uživatel veřejný profil a jeho příběhy může vidět tedy kdokoliv, je lepší svou polohu raději vůbec nesdílet. Je to nejsnadnější způsob jak si stalker může najít cestu k oběti. Instagram ale umožňuje nastavení příběhů pouze pro blízké přátele, do kterých je možné si zvolit jen lidi, které uživatel chce, aby příběh viděli a proto v případě sdílení polohy je rozumné využít právě tuto funkci.

Psát si jen s důvěryhodnými osobami
Dalším, velmi důležitým bodem, je psát si s lidmi, ke kterým uživatel chová důvěru. Jak je ve výsledcích focus group psáno – lidé nejčastěji nevěří profilům, které mají v albu jen jednu fotografii. Je třeba si na tyto lidi dávat pozor, protože většinou se jedná o profily falešné. Tento profil se snaží vždy tuto domněnku vyvrátit, ale pokud má uživatel potřebu si s ním psát, může ho poprosit o fotku se specifickou věcí (např. s ovladačem v ruce nebo s datem, na které je dobře vidět) aby dokázal, že je to opravdu on. Pokud se jedná o osobu, která již profil má, tak je dobré ho nahlásit – jedná se totiž o krádež identity. Častým případem to teď bývá právě na Instagramu.

Být obezřetní při schůzce naslepo
Na Internetu je možné setkat se se spoustou lidí, mezi kterými se bohužel mohou objevit podvodníci nebo útočníci. V situaci, kdy osoba, se kterou uživatel udržuje virtuální kontakt a se kterou si nějaký čas píše a která poté požaduje osobní setkání, je dobré být na pozoru. Nikdy není jisté, kdo za počítačem na druhé straně sedí a co po dotyčné osobě opravdu požaduje. Pokud má na schůzce zájem i druhá strana, určitě je třeba sejít se na veřejném místě, ideálně ve dne a ještě s někým ,,při ruce“, kdyby se cokoliv stalo. Určitě je dobré o této schůzce říct kamarádům, nebo rodičům.

Pozor na fotografie
Když uživatelé vkládají fotografie na svůj profil, měli by u toho být opatrní. Pokud není na fotografii sám, měl by se nejdřív zeptat, jestli osoba, která se s ním na fotce nachází, s uveřejněním souhlasí. Je také samozřejmé, že fotografie, na kterých je uživatel jen v plavkách, nebo které působí vyzývavě, akorát zvyšují riziko, že je někdo zneužije, takže je lepší, takové fotografie vůbec nepřidávat. Posílat je někomu soukromě do chatu – jen pokud toho člověka uživatel opravdu zná, avšak ani tady se riziko dalšího rozesílání nevylučuje. Pokud uživatel dá na Internet fotografii, kterou po nějaké době (může to být týden, měsíc, rok..) vyhodnotí jako nevhodnou, nebo kterou na svém profilu dále nechce mít, může ji smazat, ale nebude mít záruku, že se nešíří dále po Internetu. Existuje na to ale služba TinEye, do které lze nahrát tuto fotografii a tato služba najde, kde se daná fotografie ještě nachází. Také existuje podobná služba přímo od Google, kde jdou místo textu nahrát obrázky a stejně jako TinEye Google vyhledá, na jakých webových stránkách se tato fotografie nachází.

Myslet na to, že obsah přidaný na Internet je většinou nevratný
Vše, co na Internet uživatel přidá, mnohdy nelze vrátit. Lze sice tento obsah smazat, nebo upravit ale nikdy není jistota, že to někdo jiný nevyfotil, nebo neuložil a v budoucnu nepoužije proti osobě, která příspěvek napsala. Proto je třeba promýšlet co na Internet sdílet a co ne. Někdy si uživatelé neuvědomují, že informace, které o sobě na sociálních médiích uvádějí, mohou vidět i subjekty, o kterých vůbec nepřemýšleli, že by se k nim mohli dostat. Většinou jde o zaměstnavatele, kteří si o svých zaměstnancích stále více zjišťují informace na sociálních médiích a je to v praxi stále více běžnější metodou, jak si získat o potenciálním uchazeči co nejvíce informací.

Rodič jako vzor
Při prevenci je třeba také myslet na aktéry těchto bezpečnostních rizik, ne jen na jeho oběti. Velkou roli hraje v těchto případech rodič, který by měl být pro své dítě vzorem – pozitivním vzorem. Měl by s ním především komunikovat a snažit se aby měl o těchto rizicích povědomí. Také by měly být děti poučeny, že není správné ubližovat jiným lidem a když něco takového uvidí u jiných, aby to rychle nahlásili a nebyli přihlížejícími (toto platí především pro věkovou skupinu 15 a méně).

Preventivní semináře a interaktivní cvičení na základních školách
Z dotazníkového šetření vyplývá, že nejvíce ohroženou skupinou na Internetu bývají žáci základních škol (15 let a méně). Proto by se na základních školách měly konat preventivní opatření v rámci seminářů jak pro žáky, tak pro rodiče. Na českých základních školách probíhá těchto projektů spousty, avšak při provádění focus group někteří studenti uvedli, že to byla „jen" hodinová přednáška, kterou si poslechli a nic moc si z ní neodnesli. Proto by bylo vodné dělat na škole pravidelné projekty, které se této problematiky týkají a zapojit do nich samotné žáky prostřednictvím interaktivních cvičení. Z dotazníkového šetření také vychází, že studenti (nebo někdo z jejich okolí) se nejvíce setkávají s kyberšikanou a krádeží identity, proto by bylo vhodné zaměřit tyto cvičení především na tyto rizika a věnovat jim větší pozornost.

Být obezřetný k informacím na sociálních médiích
Ne vše, co se na Internetu píše, je pravdivé, jak už bylo popsáno v teoretické části. Proto je třeba si informace ověřovat z více zdrojů, znát dezinformační weby a znát také projekty, které na tyto weby a dezinformace upozorňují. Je vhodné si na vše udělat vlastní názor a posoudit, zdali je informace věrohodná a nešířit hoaxy dál.

Vytvářet silná hesla
Dalším velmi důležitým bodem jsou silná hesla. Je potřeba si svůj učet dobře zabezpečit a nastavit si takové heslo, které nelze snadno uhádnout. Mezi nevhodná hesla, která se nedoporučují používat, se řadí jména svých domácích mazlíčků, poštovní směrovací číslo, nebo jména svých blízkých. Je třeba si nastavit heslo, které bude přiměřené dlouhé a bude obsahovat všechny možné znaky od velkých písmen přes číslice až po písmena s háčky. Také by heslo nemělo být stejné na více účtech a už vůbec by se nemělo nikomu prozrazovat a zvyšovat tak riziko jeho zneužití. Na Internetu jsou některé generátory, které dokáží vytvořit silné a náhodné heslo, které si zároveň lze zapamatovat. Je jím například stránka Xkpaswd.net.

Odhlašovat se z účtů a 2-faktorová autentifikace
Při používání sociálních médií na jiném počítači než na zařízení uživatele je důležité dbát na odhlašování se ze všech účtů, na kterých se při užívání jiného zařízení uživatel přihlásil. Eliminuje se tak riziko jejich zneužití. Kromě hesla je důležité také myslet na 2-faktorovou autentifikaci a při přihlašování nepoužívat jen heslo, ale například nechat si poslat SMS s kódem, které ověřují, že jde opravdu o majitele účtu.
Signifikanci významnosti vlivu dítěte na kupní rozhodování podle pohlaví rodiče autoři testovali pomocí Cramerova V a kontingenčního koeficientu, jak je uvedeno v Tab. 1. Statistická významnost pohlaví rodiče při působení dětmi na kupní rozhodnutí byla potvrzena.

ZÁVĚR

Cílem příspěvku bylo pomocí vhodných metod zjistit, zdali se uživatelé Internetu cítí na sociálních médiích bezpečně, zdali jsou obeznámeni s riziky, která je na sociálních médiích mohou potkat a na základě toho navrhnout opatření a doporučení, jak se těmto rizikům vyvarovat.
Jak bylo zjištěno z dotazníkového šetření, přestože většina respondentů uvedla, že se na internetu cítí bezpečně, respondenti ale spíše nejsou obeznámeni s nebezpečím, jaké je může na Internetu potkat. V rámci testovaných hypotéz se potvrdil vztah mezi důvěrou v informace uvedených na sociálních médiích a na internetu, naopak vztah mezi věkem respondentů a dobou strávenou na sociálních médiích se nepotvrdil. Metoda focus group napomohla doplnit a zpřesnit některé výsledky dotazníkového šetření a tím zlepšit navrhovaná opatření. Ta jsou, spolu s dalšími doporučeními, poslední částí tohoto příspěvku a mohly by napomoct k tomu, aby se uživatelé vystavovali rizikům co nejméně. Především věková skupina 16 let a méně (podle respondentů nejohroženější skupina) by tato opatření měla dodržovat. Mezi navržená doporučení se např. řadilo vytváření silných hesel, dvoufázové přihlašování, uchovávání soukromých informací, nezveřejňování intimních fotografií, psaní si jen s lidmi, kterým studenti věří a uskutečňování preventivních seminářů a cvičení na školách. Na prevenci je potřebné myslet jak z pohledu uživatele sociálních médií, rodiče (v případě nižší věkové skupiny), tak i školy.

ZDROJE

Bryman, A. (2016). *Social Research Methods*. Oxford: Oxford University Press
Hyman, M. R., & Sierra, J. J. (2010). *Marketing Research Kit for Dummies*. Hoboken: Wiley Publishing.
Ebizmba. (2019). *Top 15 Most Popular Social Networking Sites*. Retrieved March 15, 2019, from: <http://www.ebizmba.com/articles/social-networking-websites>.
Eckertová, L., & Dočekal, D. (2013). *Bezpečnost dětí na internetu: Rádce zodpovědného rodiče*. Brno: Computer Press.
Hendl, J. (2015). *Přehled statistických metod: Analýza a metaanalýza dat*. Praha: Portál.
Idnes.cz. (2019) *Důvěřují a neprověřují. Čechům bezpečnost na internetu moc neříká*. Retrieved March, 15, 2019, from: <https://www.idnes.cz/ekonomika/domaci/internet-bezpecnost-cesi-pruzkum-zneuziti.A190213_457221_ekonomika_rts>.
Janouch, V. (2013*). Internetový marketing: Prosaďte se na webu a sociálních sítích*. Brno: Computer Press.
Lorenc, J. (2017). *Jak se daří jednotlivým sociálním sítí v České republice?* Retrieved March, 10, 2019, from: <https://www.linkedin.com/pulse/jak-se-daří-jednotlivým-sociálním-sítí-v-české-republice-jakub-lorenc/>.
Nations, D. (2019). *What Is Social Media?* Retrieved March, 14, 2019, from: <https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616>.
Smith, N., Wollan, Ro., & Zhou, C. (2011). *The Social Media Management Handbook*. New Jersey: John Wiley & Sons.