Studijní text k projektu

Propojení teoretické a praktické přípravy budoucích pedagogických pracovníků na UP

UNIVERZITA PALACKÉHO V OLOMOUCI

Pedagogická fakulta

Rizika sociálních sítí

Mgr. Kamil Kopecký, Ph.D.

PhDr. René Szotkowski, Ph.D.

Olomouc 2015

Studijní text k projektu

Propojení teoretické a praktické přípravy budoucích pedagogických pracovníků na UP

Rizika sociálních sítí se specifickým zaměřením na sociální síť Facebook

Úvod do problematiky

Sociální sítě jsou specifické internetové služby, zaměřené primárně na získávání a udržování sociálních kontaktů s dalšími uživateli internetu. Mohou být zaměřeny univerzálně (Facebook, G+), nebo jsou zacíleny např. profesně (LinkedIn, Researchgate), na základě příslušnosti ke konkrétní třídě či studijní skupině (Spolužáci.cz) či podle dalších kritérií. Termín sociální sítě často splývá se termínem servery komunitních služeb.

Hranice mezi tím, co jsou a nejsou sociální sítě, jsou velmi neostré. Sociální sítě však mají řadu společných vlastností:

a) *obsah sociálních sítí vytvářejí sami uživatelé,*
b) *sociální sítě umožňují vytvářet sociální vazby (např. spojovat se s přáteli, followery atd.),*
c) *sociální sítě obsahují velké množství osobních a citlivých informací, které o sobě zveřejňují a šíří sami uživatelé,*
d) *sociální sítě podporují jednoduché a efektivní sdílení informací.*

Aby bylo možné sociální sítě hodnotit co nejvíce objektivně, je třeba uvědomit si, že mají vzhledem k jejich používání jak pozitiva, tak i negativa.

Pozitiva sociálních sítí

A. *Sociální sítě umožňují navazovat mezilidské kontakty.*

B. *Sociální sítě jsou nástrojem pro překonání sociální izolace.*

C. *Sociální sítě umožňují realizovat reklamu s přesným cílením na cílovou skupinu.*

D. *Sociální sítě jsou zdrojem poučení.*

E. *Sociální sítě jsou zdrojem zábavy.*

Negativa sociálních sítí

A. *Sociální sítě obsahují velké množství zneužitelných osobních údajů*

B. *Sociální sítě umožňují snadno, rychle a anonymně realizovat kyberšikanu, sexuální útoky na děti, kyberstalking apod.*

C. *Sociální sítě umožňují realizovat internetové podvody*

D. *Sociální sítě mají úzkou vazbu na majetkovou kriminalitu*

E. *Pro potřeby sociálních sítí často vznikají nebezpečné technologie, např. automatické označování obličejů na fotografiích (tzv. automatické tagování)*

F. *Sociální sítě se stávají terči internetových útoků vedoucích k úniku osobních údajů.*

Většina veřejných sociálních sítí obsahuje kontrolní mechanismy, které např. zpřístupňují přístup na sociální síť od určitého věku (např. od 13 let na sociální síti Facebook), případně obsahují jiné mechanismy kontroly uživatelů (např. kontrola pomocí institucionálního emailu). Většinu těchto kontrolních mechanismu však lze snadno "obejít", např. zadat jiné datum narození. V praxi je pak běžné, že sociální sítě masově využívají i uživatelé, kteří kritéria pro přístup do dané sociální sítě nesplňují – tedy i děti.

Děti v prostředí internetu sdílejí velké množství osobních a citlivých údajů, které umožňují jejich velmi přesnou identifikaci. Často si neuvědomují, jak jsou osobní údaje důležité a jak snadno je lze zneužít ke kybernetickému útoku.

Facebook – největší sociální síť světa

Facebook je největší světová sociální síť, která byla založena 1. února 2004 Markem Zuckerbergem, bývalým studentem Harvardu a jeho čtyřmi dalšími spolužáky. Zpočátku sociální síť sloužila pouze studentům Harvardu, později začala sloužit studentům Standordské univerzity a dalším univerzitám, postupně se otevřela celému světu. Facebooku celosvětově využívá více než 1,4 miliardy uživatelů ze všech kontinentů. Facebook je akciová společnost s více než 5000 zaměstnanci, její sídlo je umístěno v Kalifornii (od roku 2011 v Menlo Parku v Kalifornii), evropské ústředí Facebooku naleznete v Dublinu (Irsko). Hodnota Facebooku činí přibližně 104 miliard dolarů (údaje z června 2012).

Minimální věk pro registraci na tuto sociální síť je 13 let, je však běžné, že mají na Facebooku své účty i děti mladší 13 let. Facebook obsahuje 250 miliard fotografií, denně se na tuto sociální síť nahraje 350 milionů fotografií. Průměrný počet fotografií na jednoho uživatele je 217.

Problematické licenční podmínky

Licenční podmínky používání Facebooku jsou podrobně popsány části Podmínky a zásady služby Facebook, je však běžné, že si uživatelé této sítě licenční podmínky nečtou. Podmínky používání jsou přeloženy rovněž do češtiny, není tedy problém je kdykoli prostudovat na stránce www.facebook.com/policies/. Pro potřeby tohoto kurzy si shrneme pouze ty nejdůležitější, které pro názornost zestručníme:

Vše, co nám dáte, můžeme použít

Facebook ve svých podmínkách zavádí kategorii tzv. IP obsahu (IP content), která označuje jakýkoli obsah, který na Facebook nahrajete ze své IP adresy. V praxi se jedná např. o obrázky, videa nebo text. Facebook ve svých podmínkách uvádí, že jakýkoli obsah, který na tuto sociální síť nahrajete, může použít pro své účely, dokonce jej i prodat dalším stranám.

Citujeme:
„Pro obsah chráněný právy k duševnímu vlastnictví, jako jsou fotografie a videa (obsah podléhající duševnímu vlastnictví, DV), nám výslovně udělujete následující oprávnění, v souladu s vaším nastavením soukromí a nastavením aplikací: udělujete nám nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího DV, který zveřejníte na Facebooku nebo v návaznosti na něj (Licence k DV). Tato licence k DV končí, jakmile svůj obsah podléhající DV odstraníte ze svého účtu, s výjimkou případů, kdy jste tento obsah sdíleli s ostatními (pokud jej také oni neodstranili). (www.facebook.com/legal/terms).“

Data si necháme i po jejich smazání

Další pravidlo Facebooku se zaměřuje na případy, kdy se uživatel rozhodne data, které na Facebook nahrál, smazat. V případě, že se rozhodnete svá data smazat, zůstávají na Facebooku i nadále po přiměřeně dlouhou dobu, nebudou však dostupná ostatním.

Citujeme:
„Jestliže obsah podléhající DV odstraníte, bude odstraněn obdobným způsobem, jako při přesunutí do Koše v počítači. Berete však na vědomí, že odebraný obsah může existovat v záložních kopiích po přiměřeně dlouhou dobu (nebude však dostupný ostatním).“

Uložíme si veškerou vaši komunikaci a historii hledání včetně GPS polohy

Facebook shromažďuje o svých uživatelích celou řadu informací, které jsou podrobně popsány na stránkách https://www.facebook.com/about/privacy/your-info. Facebook shromažďuje všechna data o vaší komunikaci, GPS polohu, IP adresy, vyhledávání apod. Facebook si například pamatuje, jaké produkty a služby vyhledáváte, informace ukládá a dále využívá.

Pokud nás chcete žalovat, musíte využít okresního soudu Spojených států pro okres Northern District of California

Je logické, že protože má Facebook sídlo v Kalifornii, případné žaloby musíte řešit se soudem v této oblasti. Nicméně v případě spáchání trestného činu v ČR s využitím sociální sítě Facebook samozřejmě můžete kontaktovat Policii ČR.

Citujeme:
„Veškeré žaloby, soudní nařízení nebo spory vůči nám vzešlé z tohoto prohlášení nebo používání služby Facebook budete vznášet výhradně u okresního soudu Spojených států pro okres Northern District of California nebo státního soudu kraje San Mateo. Souhlasíte s tím, že pro účely vedení veškerých takovýchto sporů se podřídíte jurisdikci daných soudů. Toto prohlášení a vaše případné žaloby na nás se řídí zákony státu Kalifornie, USA, bez ohledu na kolizi právních ustanovení.“

Sběr osobních údajů

Facebook stejně jako další sociální sítě o svých uživatelích sbírá a ukládá velké množství informací - osobních a citlivých údajů. Z velkého množství uživatelů a tedy i osobních údajů pak profituje – dokáže

je využít k přesně zacílené reklamě, prodává je dalším stranám, využívá je v rámci svých vlastních marketingových aktivit apod. Je poměrně běžné, že se fotografie a videa z uživatelských profilů prodávají třetím stranám (viz licenční podmínky), které tak mohou získat klientelu, kterou mohou oslovit reklamním sdělením.

Dalším způsobem, jak lze získat osobní údaje od konkrétních uživatelů, jsou online hry přístupné pomocí Facebooku. V současnosti online hry z Facebooku hrají stovky miliónů uživatelů, kteří vzájemně sdílí velké množství osobních a citlivých údajů, aniž by o tom věděli. Před vstupem do hry totiž souhlasí s tím, že se jejich osobní údaje budou šířit mezi další hráče a samozřejmě budou poskytnuty firmě, která danou počítačovou hru vytvořila.

Sledování komunikace uživatelů

Facebook stejně jako další sociální sítě monitoruje komunikaci uživatelů – ať již provoz na facebookových "zdech" nebo soukromou komunikaci (chat). Monitorování realizuje v zájmu ochrany uživatelů před trestnou činností, zejména před šířením dětské pornografie, sexuálními útočníky a terorismem. Ve většině případů komunikaci uživatelů sledují "automatičtí roboti", kteří podle konkrétních klíčových slov a identifikace vyhodnocují, jak moc je komunikace závažná a podezřelá. Kromě obsahu komunikace se rovněž sledují další varovné příznaky, jako je například příliš velký věkový rozdíl mezi komunikujícími.

Pokud automatizovaní roboti vyhodnotí komunikaci jako podezřelou, předávají podezřelé záznamy po ověření živými zaměstnanci Facebooku americké policii.

Monitorování komunikace samozřejmě probíhá i v prostředí českých sociálních sítí, kde kromě robotů komunikaci vyhodnocují také živí administrátoři.

Falešné profily

Facebook stejně jako další sociální sítě obsahuje velké množství falešných profilů, protože nekontroluje identitu svých uživatelů. Na Facebook se tedy může zaregistrovat kdokoli s funkční emailovou adresou, kdo při registraci do této sociální sítě zadá věk vyšší než 13 let.

Podle odhadů samotného Facebooku je na této sociální síti přibližně 5-10 % profilů falešných. To představuje přibližně 50 až 100 milionů účtů. Srovnáme-li tento počet např. se sociální sítí Lidé.cz, na té je řešeno přibližně 10 000 falešných profilů ročně.

Skrze falešné profily pak uživatelé provádějí útoky na ostatní uživatele, vydírají je, vyhrožují, vylákávají fotografie, manipulují, trollují atd.

Jak rozpoznat falešný profil?

Rozpoznat falešný profil od pravého je velmi obtížné, v praxi je to téměř nemožné. Existují však jistá vodítka, která jsou s falešnými profily spojena:

1. Příliš dokonalá fotografie.

Pokud se v profilu nachází mnoho velmi dokonalých fotografií (ideální ostření, žádné zrnění…) je pravděpodobné, že jsou stažené z veřejně dostupných databank.

2. Přehnaná přezdívka.

Vodítkem může být rovněž přehnaná přezdívka v profilu, dívky si zpravidla nedávají přehnané přezdívky jako např. *nadržená nymfomanka*, přehnané přezdívky jsou znakem falešných profilů.

3. Věci, předměty, které nejsou v ČR běžné.

Řada fotografií obsahuje předměty, které v České republice nejsou běžné. Typickým příkladem jsou např. kliky u dveří – většina českých domácností obsahuje běžné kliky u dveří, pokud se však na fotografii objeví klika kulatá, může to být znak toho, že fotografie pochází ze Spojených států či Velké Británie. Všímejte si vždy maličkostí.

4. Formální a obsahové chyby.

Dalším znakem falešného profilu jsou rovněž drobné pravopisné a obsahové chyby.

V prostředí internetu nalezneme celou řadu služeb, které nám umožní ověřit si, zda se konkrétní fotografie nevyskytuje i na jiných internetových stránkách. Jedná se o tzv. reverzní vyhledávače fotografií. Princip tohoto typu vyhledávání je jednoduchý – do reverzního vyhledávače nahrajete fotografii, kterou chcete na internetu nalézt, online služba poté porovná vaši fotografii s naindexovaným obsahem a zobrazí, na kterých internetových stránkách se vaše fotografie nachází.

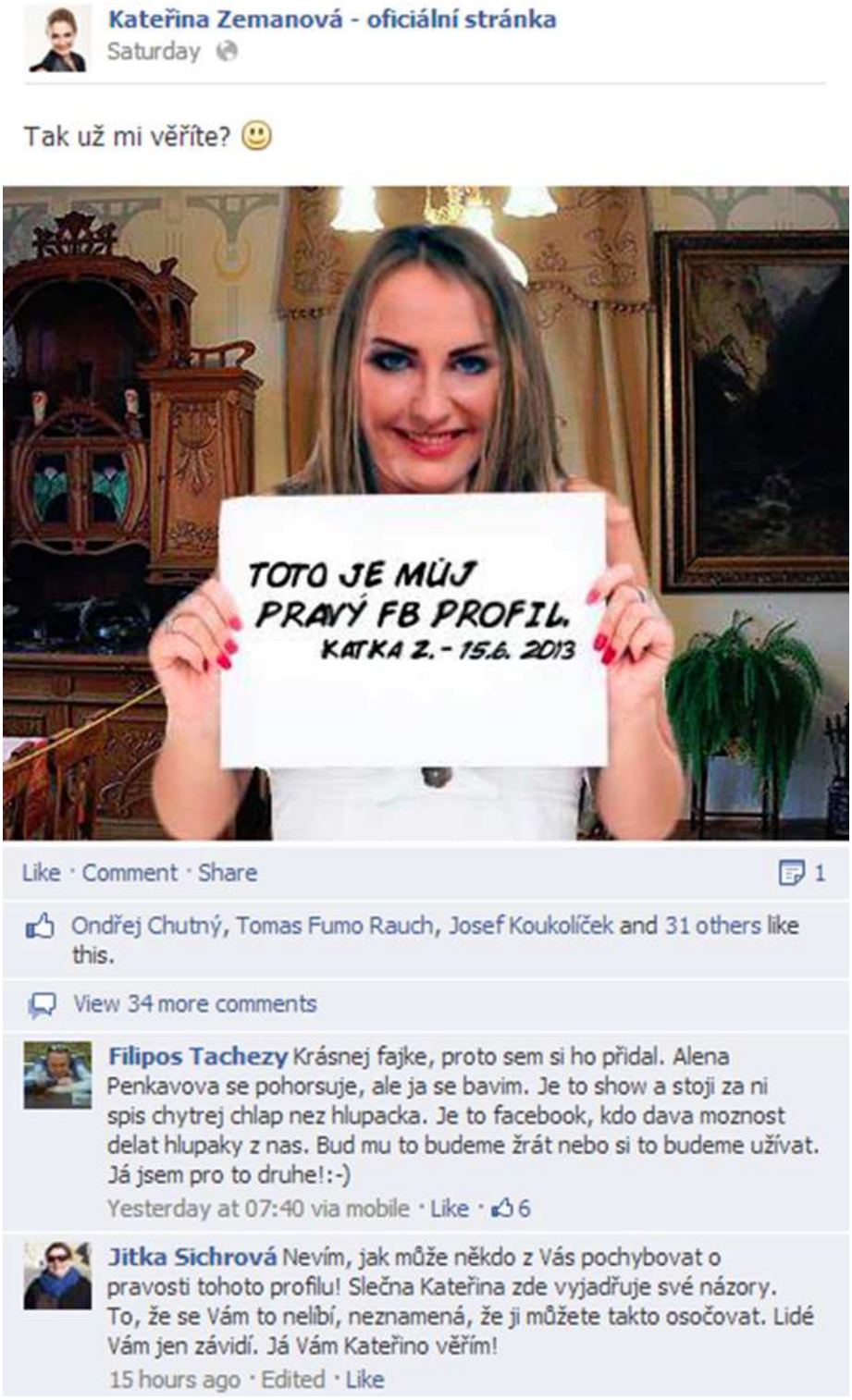
K neoblíbenějším službám tohoto druhu patří reverzní vyhledávací databáze **TinEye** (www.tineye.com), která má naindexováno přibližně cca 4.2 miliardy fotografií.

Další účinný způsob vyhledávání obrázků představuje služba Google Obrázky (https://www.google.cz/imghp?hl=cs&tab=wi), do níž je reverzní vyhledávání fotografií integrováno. Službu spustíte kliknutím na symbol fotoaparátu ve vyhledávacím poli. Do následného formuláře pak nahrajete buď fotografii z disku, nebo URL odkaz na fotografii přímo na konkrétní webové stránce.

Obrázek č. 1: Vyhledávání Google Obrázky – reverzní vyhledávání

Mezi další reverzní vyhledávače patří např. **RevIMG** (http://www.revimg.net/), **SauceNAO** (http://saucenao.com/) atd.

Obrázek č. 2: Falešný profil dcery Miloše Zemana – Kateřiny Zemanové



Obrázek č. 3: Další část tohoto profilu – fotografie, která má dokladovat pravost, je to však podvrh

Studijní text k projektu

Propojení teoretické a praktické přípravy budoucích pedagogických pracovníků na UP

Blokace obsahu

V roce 2009 v rámci tzv. **Safer Internet Day** (dne bezpečnějšího internetu) uzavřelo 17 velkých firem, které poskytují internetové služby, dohodu o zvyšování bezpečnosti jejich služeb u osob mladších 18 let. Tuto dohodu uzavřeli zástupci firem/služeb Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo! Europe, a Zap.lu. Sociální sítě a služby, které tyto instituce provozují, pak byly vybaveny různými blokačními mechanismy, zejména blokačními tlačítky a systémy pro hlášení závadného obsahu. Blokační tlačítka tak nalezneme např. na Facebooku, YouTube a dalších službách.

Pokud tedy chceme na Facebooku blokovat konkrétní profil či diskusní skupinu, můžete použít blokační tlačítka. Těmi je vybavena každá stránka na Facebooku. Pokud však nemáte účet na Facebooku, nemůžete závadný obsah nahlásit – musíte využít registrovaného účtu.

Blokace se provádí centrálně – přímo v USA. Bohužel ne vždy proběhne blokace hladce, rozhodující je míra závadnosti obsahu (např. dětská pornografie a obecně pornografie je blokována dříve, než např. kyberšikana), zvolená klíčová slova a počet nahlášení. V praxi platí, že čím více uživatelů profil nahlásí, tím dříve blokace proběhne.

Video s návodem blokace obsahu naleznete pod níže uvedeným odkazem https://www.youtube.com/watch?v=cO38qnVDOFQ

Automatické označování obličejů

Facebook je od roku 2010 vybaven funkcí automatického rozpoznávání obličejů (automatické tagování obličejů, v českém překladu označování fotografií). V praxi tato funkce znamená, že při nahrávání fotografie Facebook podle zachycených obličejů rozpozná, kdo se na fotografii nachází, a nabídne propojení této fotografie a konkrétními profily na Facebooku. Informace z nahrávané fotografie porovnává zejména s profilovými fotografiemi.

Protože je tato funkce automatizovaná, automaticky tak dokáže rozpoznat obličej i na fotografii, na které nechcete být označeni. Označené fotografie se totiž připojují k vašemu profilu a mohou být snadno zneužity k vydírání.

V Evropě je funkce automatického rozpoznávání fotografií od roku 2012 zakázána, zákaz však platí pouze pro nové profily. Funkci lze samozřejmě v nastavení profilu vypnout, nicméně standardní nastavení této funkce je **ZAPNUTO**.

Řada komerčních firem, ale také státních institucí získává informace o svých zaměstnancích právě pomocí Facebooku – sleduje, zdali o nich nenaleznout např. diskriminující či ponižující informace, zdali např. potenciální zaměstnanci nekonzumují ve větší míře alkohol, zdali neholdují extrémismu apod.

GPS lokalizace uživatelů

Stejně jako další sociální sítě i Facebook sleduje GPS polohu svých uživatelů. Získaná data pak Facebooku umožňují přesněji zacílit reklamu (např. limitovat ji konkrétním regionem či jazykem) a rovněž získat detailní data o pohybu svých uživatelů.

Mazání účtu na Facebooku

V případě, že se rozhodnete účet na sociální síti Facebook smazat (nikoli pouze deaktivovat), využijte ke smazání adresu: **https://www.facebook.com/help/delete_account.** Do 14 dnů by mělo dojít k odstranění účtu včetně všech dat, nicméně Facebook v licenční podmínkách upozorňuje na právo ponechat si vaše data i po smazání vašeho uživatelského účtu po blíže neurčenou dobu.

Video s návodem mazání účtu na Facebooku naleznete pod níže uvedeným odkazem https://www.youtube.com/watch?v=gahpcBvqrps

Facebook a majetková kriminalita

V posledních letech je Facebook stále více využíván jako nástroj pro získání informací pro osoby páchající majetkovou kriminalitu (tzv. bytaře). Řada uživatelů Facebooku totiž na svých profilech a "zdech" zveřejňují informace, které pomáhají pachatelům zjistit:

a) počet obyvatel bytu,

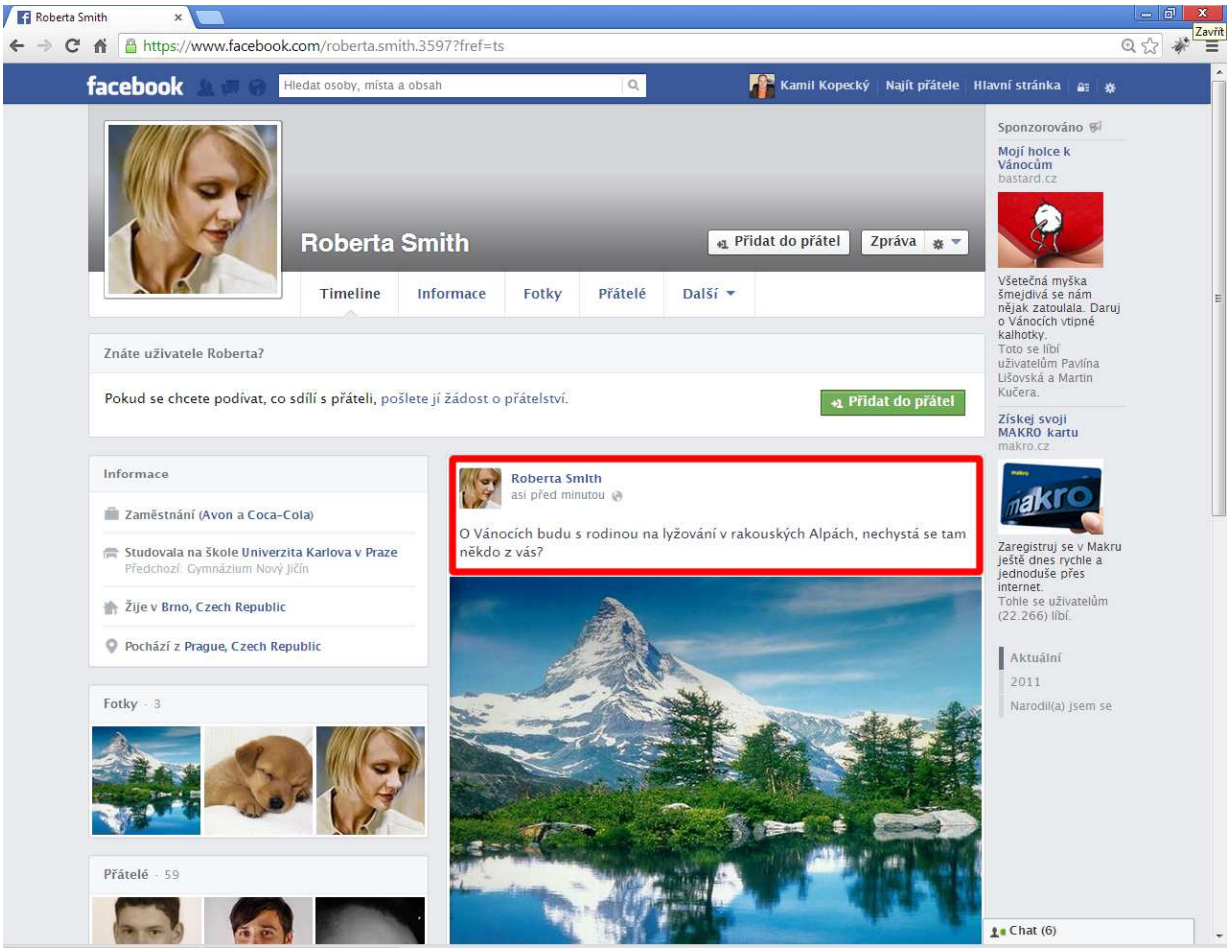
b) zdali mají obyvatelé bytu domácího mazlíčka (psa apod.),

c) adresu bytu, patro, ve kterém se nachází,

d) informace o době, kdy je byt prázdný (práce, škola, dovolená),

e) vybavení domácnosti.

Informace samozřejmě nejsou na facebookovských virtuálních zdech či profilech takto jednoduše umístěny a seřazeny, jsou fragmentovány. Vzhledem k tomu, že však Facebook umožňuje snadno přistupovat i ke starším záznamům (historie, timeline), složení využitelné informace je otázkou několika hodin procházení profilem.



Obrázek č. 4: Pozvánka pro zloděje

Ve vztahu k majetkové trestné činnosti stále panuje celá řada mýtů:

1. **Mýtus o sousedech** – více než polovina pachatelů tvrdí, že sousedé pro ně nepředstavují žádnou překážku. Více než 1/4 pachatelů spoléhá na to, že sousedé budou předstírat, že si ničeho nevšimli, než aby volali policii.

2. **Mýtus o tom, kam ukrýt klíče od objektu** – celá řada vlastníků domů či bytů věří, že je bezpečné schovávat klíče po rohožku či do květináče, umístěného v okolí hlavního vchodu do objektu. Přitom statisticky platí, že si 90 % pachatelů prohlédne nejdříve rohožku a květináče, jestli pod nimi nejsou klíče. Řada z obyvatel bytů či domů si rovněž klíče od automobilu poměrně lehkomyslně věší na věšáčky v předsíni, což je místo, které prohledá téměř 100 % zlodějů.

O co mají zloději největší zájem? O mobilní elektroniku – notebooky, mobily, LCD televize (pokud nejsou napevno připevněny např. ke zdi), šperky a cennosti (umístěné zejména na dně šatní skříně či na/v nočním stolku), peníze (často uschované např. v kuchyňských šuplících), hodinky (volně položené např. na policích) atd.

Jaké místo v bytě je nejbezpečnější? Je to lednice – pouze 4 % pachatelů prohlíží chladničku či mrazničku, je to tedy jedno z nejvíce bezpečných míst v domácnosti. Pozor, nepoužívejte však lednici jako "trezor" pro notebooky či jinou elektroniku! Dobrou obranou je rovněž domácí zvíře, nejlépe pes. Většina pachatelů uvádí, že se domu či bytu se psem raději vyhnou.

Literatura

E-bezpečí [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.e-bezpeci.cz/

České děti a Facebook 2015. *E-bezpečí* [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.e-bezpeci.cz/facebook2015/

Jít či nejít. *E-bezpečí* [online]. 2013 [cit. 2015-09-16]. Dostupné z: http://www.e-bezpeci.cz/jitcinejit

Seznam se bezpečně! [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.seznamsebezpecne.cz/

Prevence kriminality v České republice [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.prevencekriminality.cz

Sexting [online]. 2013 [cit. 2015-09-16]. Dostupné z: http://www.sexting.cz/

Dítě v ohrožení [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://esynergie.upol.cz/ditevohrozeni/

Podmínky a zásady služby Facebook. *Facebook* [online]. 2015 [cit. 2015-09-16]. Dostupné z: https://www.facebook.com/policies/

Zásady používání dat. *Facebook* [online]. 2015 [cit. 2015-09-16]. Dostupné z: https://www.facebook.com/about/privacy/your-info

Prohlášení o právech a povinnostech. *Facebook* [online]. 2015 [cit. 2015-09-16]. Dostupné z: https://www.facebook.com/legal/terms

TinEye [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.tineye.com/

Google obrázky. *Google* [online]. 2015 [cit. 2015-09-16]. Dostupné z: https://www.google.cz/imghp?hl=cs&tab=wi

RevIMG [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://www.revimg.com/

SauceNAO [online]. 2015 [cit. 2015-09-16]. Dostupné z: http://saucenao.com/

Blokace obsahu na Facebooku. *YouTube* [online]. 2013 [cit. 2015-09-16]. Dostupné z: https://www.youtube.com/watch?v=cO38qnVDOFQ

Jak smazat účet na Facebooku. *YouTube* [online]. 2013 [cit. 2015-09-16]. Dostupné z: https://www.youtube.com/watch?v=gahpcBvqrps