SENIORI
BEZPEČNE
NA SOCIÁLNYCH SIEŤACH

Tento materiál je určený ako podklad na rozhovory o téme bezpečnosti na internete, v rámci diskusných stretnutí so seniormi. Hlavným zdrojom tohto materiálu boli kurzy o bezpečnosti na internete a dezinformáciách vytvorené spoločnosťou Safelab.

Materiál má za cieľ oboznámiť seniorov ako užívateľov rôznych sociálnych sieti s tým:

- ako nástroje komunikácie a propagandy fungujú;
- aké sú pozitíva, no najmä negatíva ich nekontrolovateľného používania;
- akým spôsobom tieto siete bezpečne používať;
- aké sú rizika zverejňovania niektorých faktov, údajov, materiálov;
- aké sú riziká vzájomnej komunikácie medzi užívateľmi sociálnych sietí;
- aké sú možnosti a spôsoby ochrany osobných údajov na internete, tvorba relatívne bezpečných hesiel.

Spracoval PaedDr. Ján Cangár a vznikol v rámci projektu „*Zvyšovanie odolnosti stredoeurópskych seniorov voči dezinformáciám*“, ktorý MEMO98 realizuje v spolupráci s Transitions (Česká republika), Független Médiaközpont – Center for Independent Journalism – (Maďarsko) Towarzystwo Inicjatyw Twórczych „ę“ (Poľsko).

Ďalšie materiály, venované tejto téme, sú uvedené v časti Pramene.

ÚVOD

Bezpečnosť na internete

Koncom 20. a začiatkom 21. storočia nastal obrovský rozmach digitálnych technológií. Internet, ktorého zrodenie sa datuje do roku 1983 (bol vytvorený nový komunikačný protokol, ktorý umožnil rôznym druhom počítačov v rôznych sieťach navzájom „komunikovať"), sa stal globálnym fenoménom. Internet sa v celosvetovom komunikačnom priestore udomácnil veľmi rýchlo: v roku 1993 sa ním prenášalo len 1 % informácií prúdiacich cez obojsmerné telekomunikačné siete, v roku 2000 už 51 % a v roku 2007 viac ako 97 % telekomunikačných informácií.

Súčasne internet sa stal aj sociálnym médiom, umožňuje realizovať globálnu komunikáciu v medzinárodnom kontexte. Stal sa prostriedkom resp. obrovským úložiskom informácií rôzneho typu, čo znamená, že priamo a nepriamo výrazne ovplyvňuje vzdelávací potenciál ľudstva. Globalizácia telekomunikačných sietí a masívny rozvoj a využívanie digitálnych technológií na prácu s internetom však prinášajú nielen pozitíva, ale znamenajú aj riziká.

Jedným z rizík pre užívateľom je sociálne inžinierstvo. Ide o premyslený postup ovplyvňovania čo najširšieho okruhu používateľov internetu prostredníctvom webových stránok, sociálnych sieti, inzertných a reklamných nástrojov. Zahŕňa široké spektrum oblasti obchodu a marketingu.

Sociálne inžinierstvo je aj účinným nástrojom internetových podvodov a hackerských útokov. Zneužívajú ho rôzni útočníci a hackeri, ktorí sa zameriavajú na užívateľov internetu a prostredníctvom klam-

stva, manipulácie alebo nátlaku sa snažia dosiahnuť svoj cieľ – informácie o finančných prostriedkoch, či citlivé osobné údaje využiť vo svoj prospech. Najpoužívanejšie formy útokov na používateľov internetu bývajú – emailový útok, útok cez sociálnu sieť, cez messaging aplikácie (Messanger, WhatsApp, Viber, Telegram), cez falošné webové stránky, telefonicky alebo cez klasické textové (SMS) alebo obrazové (MMS) správy. Útočníci a hackeri poznajú nástroje, umožňujúce prehľadávanie webových stránok, diskusií na sociálnych sieťach alebo inzertných portálov, vyhľadávajú zverejnené emailové adresy a nelegálne napádajú databázy emailových adries. Na internete sa nachádza aj množstvo podvodných stránok a formulárov, určených len na zber emailových adries.

Správcovia internetu, výrobcovia digitálnych technológií, vývojári aplikácií, alebo programátori sa snažia zdokonaľovaním ochrany citlivých dát a údajov minimalizovať negatívne dôsledky útokov na internetové stránky, kontá na sociálnych sieťach, či na mailové adresy. Preto pred väčšinou útokov môžu chrániť legálne certifikované operačné systémy, správne nastavený antivírový program (počítačový *program*, ktorého cieľom *je* identifikovať a eliminovať počítačové vírusy) a firewall (chráni siete a počítače pred neoprávnenými zásahmi zo strany potenciálne nebezpečných hackerov, ako aj pred útokmi prostredníctvom ktorých by mohli prevziať kontrolu nad zariadeniami a zneužiť ich na nekalé účely[1]).

Medzi vôbec najdôležitejšie prostriedky ochrany bezpečnosti na internete však patrí zodpovedne konanie samotných užívateľov internetu. To znamená, že je treba chrániť sa bezpečnými a spoľahlivými heslami, nezverejňovať citlivé osobné údaje, kópie alebo fotografie osobných dokladov, bankových kariet ani iných citlivých dokumentov. Takisto je treba vyhýbať sa podozrivým webovým stránkam, mailovým adresám, propagačným kampaniam, preverovať si informácie o neznámych stránkach, odosielateľoch mailových, telefonických SMS, či chatovacích správ, dôverovať iba kontaktom a ľuďom, ktorých poznáme alebo ktorých sme si preverili.

1 Eset – Firewall ochrana.

ČO SÚ DIGITÁLNE SOCIÁLNE SIETE

Sociálne siete sú on-line prepojenia viacerých osôb (používateľov) na webe, ktoré fungujú pomocou špeciálneho, na to vytvoreného softvéru za rôznym účelom.

Nahrádzajú osobný kontakt medzi ľuďmi, ale sú aj veľmi dôležitým komunikačným, no zároveň marketingovým nástrojom, prostredníctvom ktorého je možné sprostredkovať širokej skupine ľudí veľké množstvo informácií rôzneho charakteru.

Sociálne siete fungujú na internete. Slúžia na nadväzovanie a udržiavanie kontaktov medzi ľuďmi. Ich používateľ si môže vytvoriť vlastný profil so základnými informáciami o sebe. Na základe profilov sa nadväzujú vzťahy medzi používateľmi. Používatelia sa môžu spájať do skupín. Ich prepojeniami vznikajú siete vzťahov. Rizikom sociálnych sietí je, že používatelia nemusia do svojho profilu vložiť pravdivé informácie a pravdivosť informácií sa často nedá zistiť.

Európska agentúra pre informačnú a sieťovú bezpečnosť za sociálnu sieť považuje on-line komunitu, ktorá pomocou vytvoreného profilu umožňuje používateľom stretávať ďalších členov siete, komunikovať s nimi, zostať s nimi v kontakte a zdieľať s nimi obrázky či videá v rámci zdieľaného priestoru.

Typy sociálnych sietí

Sociálne siete sú zväčša zložené z ľudí, ktorí hľadajú odpovede na každodenné udalosti, otázky a problémy. Často sú spojené s firmami, ktoré sú prostredníctvom sociálnych sietí spojené so svojimi zákazníkmi a komunikujú s nimi.

- **Profesijné siete** zamestnancom pomôžu v kariére alebo v odvetví alebo sa vytvárajú v podnikoch a slúžia na komunikáciu medzi zamestnancami a zamestnávateľom i medzi firmou a zákazníkmi.
- **Vzdelávacie siete** sú zoskupenia najmä študentov za účelom spolupráce na projektoch a výskume alebo komunikácie s profesormi a učiteľmi. Sú populárne v rámci vzdelávacieho systému.
- **Sociálne siete zamerané na záujmové hobby, či športové podujatia/kluby** patria medzi najpopulárnejšie, ich užívatelia často vykonávajú prieskum o koníčkoch, nadväzujú kontakty s ľuďmi z celého sveta.
- **Novinky –** druh sociálnej siete publikuje „komunitný obsah". Ide o webové stránky, na ktorých členovia publikujú novinové články, komentáre alebo iné materiály a dokumenty. Keď však obsah stránok nie je kontrolovaný, môže vytvoriť propagačný guláš reklám alebo aj hoaxov.

Európska agentúra pre informačnú a sieťovú bezpečnosť rozdelila sociálne siete z funkčného hľadiska do dvoch typov:
- **Univerzálne –** zamerané sú najmä na komunikáciu a interakciu medzi používateľmi, nemajú stanovené konkrétne záujmy. Sem patria Facebook, Twitter, Telegram, Pokec.
- **Špecializované – konkrétne orientované určitým smerom s vymedzenými témami.** Sem patrí LinkedIn (oblasť obchodu a podnikania), Odnoklassniki.ru/Classmates.com (zoznamovanie).

Podľa portálu digizen.org:
- **Profilovo zamerané** – orientované na používateľský profil, (Facebook, Instagram, TikTok).
- **Obsahovo zamerané –** priorita je obsah (Youtube – videá, Frickr – fotografie a Spotify – hudba, SoundCloud – podcasty,hudba).
- **Virtuálne –** výlučne on-line virtuálne prostredie, neprezentuje sa profil ale virtuálna postava. (hra World of Warcraft alebo Second Life).
- **Mikroblogovacie –** umožňujú publikovať krátke správy (Twitter).
- **White-label siete** – možnosť vytvorenia vlastnú verziu mini komunitu PeopleAggregator, Ning).

Okrem uvedených sociálnych sietí poznáme aj aplikácie určené na posielanie správ a multimediálnych obsahov (obrázkov či videí) ako Facebook Messenger, WhatsApp, Viber, Telegram či Signal.

Niektoré ďalšie sociálne siete a aplikácie sú:

Instagram, Snapchat, Pinterest, TikTok, WeChat, Viber, Minds.com, Hi5, netLog, Tagged, Twitter, GigaCast, Greenieplanet, Bebo, Habbo, SomTurista, Blindr, a iné.

REGISTRÁCIA DO SOCIÁLNEJ SIETE

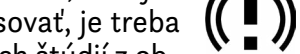
Do každej sociálnej siete je potrebné sa **zaregistrovať**. To znamená že je potrebné si vytvoriť **účet** resp. konto, zvyčajne **u administrátora** sociálnej siete. Registrácia spočíva v tom, že sa záujemca identifikuje určitými údajmi, predovšetkým **menom** a **heslom**. Súčasne administrátor zvyčajne vyžaduje v rámci registrácie aj kontakty na overenie údajov a komunikáciu s potenciálnym používateľom sociálnej siete – **emailovú adresu** a **mobilné telefónne číslo**. Tieto údaje administrátor nemôže zverejniť, pokiaľ používateľ k tomu nedá písomný súhlas, resp. pokiaľ ich používateľ sám nezverení vo svojom profile. Ako meno môže záujemca uviesť svoje **krstné meno, priezvisko, aj meno aj priezvisko**, ale môže uviesť aj **meno vymyslené** (pseudonym). Keďže členmi sociálnych sieti bývajú aj záujmové skupiny a rôzne iné kolektívy, firmy, združenia a podobne, tieto uvádzajú **názov skupiny**.

Administrátor môže pri registrácii požadovať aj ďalšie údaje, ktoré však bez súhlasu používateľa nemôže zverejniť.

Registrácia do sociálne siete býva ukončená zadaním hesla. Keď zadáte heslo a pošlete prostredníctvom tlačidla registráciu administrátorovi sociálnej siete, ten prostredníctvom emailu alebo telefónneho čísla potvrdí správnosť registrácie a vyzve vás, aby ste sa do sociálne siete **prihlásili**. To môžete urobiť zadaním **mena** a **hesla**.

HESLO

Heslo, ktoré vytvoríte a zadáte pri registrácii do akéhokoľvek digitálneho zariadenia (počítač, tablet, smartfón, iné), do akejkoľvek webovej aplikácie, účtu, konta, a teda aj sociálnej siete, je jeden z hlavných a najdôležitejších údajov zaručujúcich bezpečnosť vášho konta alebo účtu, a teda aj bezpečnú ochranu vašich osobných údajov.



Vytvoreniu správneho hesla, ktoré bude bezpečné, ktorým sa budete na svoj účet na sociálnej sieti prihlasovať, je treba venovať mimoriadnu pozornosť. Podľa odborných štúdií z oblasti IT, **bezpečné heslo** by nemalo pozostávať iba z písmen abecedy, ale **by malo byť kombináciou veľkých a malých písmen, číslice a iných znakov (+,, –!,?=*/%| §). Súčasne by malo obsahovať nie menej ako 10 znakov.**

Podľa informácií Safelab (Kurzy, TÉMA 2: Základy bezpečnosti na internete, časť Heslá) „Štvorpísmenové heslo má len necelých 500 000 kombinácií a bežný počítač si s ním poradí rádovo za sekundy... heslo dlhé 6 znakov z malých, veľkých písmen abecedy a číslic dokážu moderné počítače odhaliť za pár minút, ale odhaliť heslo dlhé 10 znakov by rovnakým počítačom trvalo roky.“

V takomto prípade sa bude jednať o pomerne bezpečné heslo. No keďže každý z nás je prihlásený do viacerých sociálnych sieti, na rôzne weby a stránky, má teda množstvo účtov, mal by mať aj každý účet samostatne heslo. To vytvára problém pamätania si všetkých hesiel. Slúžia na to napr. Aplikácie ako Kľúčenka Apple iOS, Password manager (správca hesiel).

Preto je vhodné vytvoriť si určitý **systém**, kde znaky v hesle môžu znamenať nejakú výpoveď, ktorej **obsah alebo zmysel môžete poznať a identifikovať iba vy**.

Príklady pre tvorbu bezpečných hesiel

- Školy, školské zariadenia ktoré ste navštevovali:
  ZšSnina96*04 (Základná škola Snina roky 1996-2004, (teda nedávať storočie, len desaťročie a rok)
  SVSTBlava(01-06) (Slovenská vysoká škola technická Bratislava 2001-2006)

- Vaše zamestnania:
  76Predavac+85
  ***MetodiK(94+99)**

- Vaši literárni autori:
  20 s.Kafka-Proces
  Homer7pml-Troja

- Vaše hudobné skupiny a speváci
  +GottKaja+20
  Chrobáci*62-+70

- Vaše turistické destinácie
  Bejrut:1969
  04:Stokholm!

- Vaše diagnózy:
  slepákX-984
  21-05:Kovid?

Aby ste si jednotlivé heslá pamätali, resp. si ich niekde zapísali, stačí potom uviesť:

Facebook korona
Google Trójska vojna
Twitter základná škola
Mobil Libanon
VUB Beatles

Tieto heslá môžete mať napísané v **dokumente Word** alebo **Excel** v prehľadnej **tabuľke**, pričom tento dokument máte uložený buď na nejakom **externom zariadení** – disk, USB kľúč, alebo na disku vášho počítača a tento **dokument si zabezpečte kódom, resp. heslom** vytvoreným podobne ako iné heslá, ktoré bude ľahko zapamätateľné.

PROFIL NA SOCIÁLNEJ SIETI

Profil na sociálnej sieti je kvázi životopis, akési curriculum vitae. Nie všetky sociálne siete ho vyžadujú, pričom aj ponuka množstva údajov býva rôzna. Súčasťou profilu na sociálnej sieti bývajú osobné údaje, emailové adresy, čísla telefónov, webové linky (www), rodinné vzťahy, vzdelanie, zamestnanie, pracovné pozície, politická orientácia, náboženstvo, zdravotný stav, záľuby, koníčky, prezentácia a výstupy z realizácie študijných a pracovných aktivít, výrobky, a ďalšie informácie. Je nutné dodať, že iba niektoré základné identifikačné kategórie sú povinné a poskytnutie väčšieho rozsahu osobných informácií je dobrovoľné – je dobré naozaj zvážiť čo všetko chcete, aby o Vás svet vedel.

Konkrétne a všeobecné údaje z hľadiska bezpečnosti

Pri kreovaní a tvorbe vášho profilu na sociálnej sieti sa riaďte zásadou **„čím menej, tým bezpečnejšie“**.

Vo svojom profile by ste samozrejme nemali uvádzať citlivé osobné informácie, predovšetkým napríklad rodné číslo, banku, v ktorej máte konto, údaje z kreditnej karty, ale ani súkromné telefónne číslo alebo presnú a úplnú adresu bydliska. Zneužitý môže byť napríklad aj celý dátum narodenia (potenciálny útočník vie pomocou rôznych programov vygenerovať rodné číslo). Ak chcete dať svojím priateľom a známym resp. ďalším čitateľom najavo, kedy budete mať narodeniny, uveďte len deň a mesiac narodenia.

Neuvádzajte tiež presne údaje o vašom sobáši, rodine, – počet a mená detí, meno manžela/manželky/partnera, podrobné a presne údaje o vzdelávacích inštitúciách, kde ste nadobudli školské vzdelanie. Neuvádzajte ani presné adresy a názvy vašich zamestnávateľov, ani zamestnávateľov vašich rodinných príslušníkov a príbuzných, ani vzdelávacie inštitúcie, ktoré navštevujú. Neuvádzajte tiež podrobností o svojom zdravotnom stave – diagnózy, ktorými trpíte, ochorenia, ktoré ste prekonali, operácie a podobne. Neodporúčame tiež uvádzať vaše náboženské vyznanie, ani členstvo v politickej strane. Buďte tiež opatrný/á pri uvádzaní vašich koníčkov a záľub, pokiaľ možno uvádzajte iba všeobecné údaje, nie konkrétnosti a podrobnosti.

FOTOGRAFIE

Profilová fotografia

Ak nemusíte, neuvádzajte resp. nezverejňujte na svojom účte alebo profile v rámci registrácie svoju fotografiu. Ak sa vyžaduje fotografia, pričom nie je určené, že musí byť fotografia aktuálna, môžete použiť akúkoľvek fotografiu buď z detstva alebo fotografiu skupiny. Takéto fotografie sa potenciálnymi útočníkmi v rámci krádeže identity dajú zneužiť omnoho ťažšie.

Albumy fotografií

Súčasťou konta na sociálnych sieťach bývajú aj albumy fotografií. Dávajte si pozor pri tom, čo na sociálnej sieti zverejníte.

Zvážte zverejňovanie fotografii Vašich rodinných príslušníkov, najmä detí, ktoré by mohli evokovať útočníkov možne sexuálnej aktivity. Zvážte tiež zverejňovanie obrázkov svojej nehnuteľnosti a pokiaľ sa chcete pochváliť obrázkami z turistických destinácií, odporúčame zverejňovať také fotografie, kde je problém vašej identifikácie potenciálnym útočníkom či podvodníkom, zverejňujte iba rôzne zábery na prírodu, historické pamiatky, koláže, a podobne.

KONTAKTY – OKRUH PRIATEĽOV, SKUPINY

Po založení účtu na sociálnej sieti a vytvorený profilu si môžete kreovať okruh Vašich potenciálnych priateľov resp. záujemcov.

Pri tvorbe okruhu priateľov existujú dva spôsoby:

1. Ako majiteľ účtu vyhľadávate osoby na základe určitých kritérií,
2. Na základe Vášho profilu sa Vám ponúknu za priateľov iní ľudia.

V oboch prípadoch buďte opatrný/á a obozretný/á.

Najprv si podrobne preštudujte všetky dostupné informácie o človeku, ktorého oslovíte za priateľa, resp. ktorý sa Vám za priateľa ponúkne:

- Pozrite si jeho profil.
- Zistíte odkedy ma založený účet na sociálnej sieti.
- Ak je to osoba verejne známa (poznáte ju buď osobne, z verejného, kultúrneho, športového alebo iného života), pravdepodobne môžete takejto osobe dôverovať.
- Preverte si, kto patrí do okruhu priateľov danej osoby. Ak sú to ľudia, ktorí patria do okruhu aj Vašich priateľov, môžete takejto osobe dôverovať.
- Prezrite si históriu statusov tejto osoby. Z nej sa dozviete viac o záujmoch, názoroch, úrovni komunikácie takejto osoby.

Častokrát sa stáva, že sa vám objaví notifikácia, že záujem o priateľstvo s Vami ma iná osoba.

- Keď si kliknete na jej účet, a zistíte, že konto bolo založené pred pár dňami alebo týždňami, že v profile nemá uvedené absolútne nič (alebo veľmi málo), že nemá zverejnené takmer žiadne statusy, alebo že jediná činnosť v rámci statusov je prezentácia vlastnej profilovej fotografie, môže ísť o falošnú identitu. A aj keď takýto človek má zaradených medzi priateľmi veľa ľudí z okruhu Vašich priateľov, radšej takéhoto človeka medzi priateľov nezaraďujte, resp. si ho pred akceptovaním pozvánky na priateľstvo inak overte.
- Ďalej sa môže stať, že uchádzač o priateľstvo má vo svojom profile uvedených veľmi veľa podrobných údajov. Napríklad presné adresy zamestnávateľských organizácií. V takomto prípade, pokiaľ sú takéto adresy verejne dostupné, je možné si ich overiť prostredníctvom Google. Môže sa stať, že daná osoba uvedie, že ako lekár je zamestnancom nejakého zdravotníckeho zariadenia. Prostredníctvom Google sa dá zistiť či daný lekár naozaj v uvádzanom zariadení pracuje.
- Stalo sa tiež napríklad, že na Facebooku bol aktívny človek, ktorého konto znelo na meno významného politika, bola tam uvedená jeho emailová adresa, nielen jeho profilová fotografia, ale rôzne iné osobné fotografie, aj ďalšie údaje, ktoré zneli veľmi dôveryhodne. Podozrivé na tomto profile a na tomto účte bolo to, že na svojom statuse daná osoba propagovala webovú stránku, v rámci ktorej mal byť záujemca resp. čitateľ tohto statusu zapojený do nejakej súťaže, prostredníctvom ktorej mohol vraj vyhrať nemalé sumy eur. Podmienkou však bolo zaregistrovať sa na danej webovej adrese a zaplatiť registračný poplatok.
- Z takýchto statusov sa dá jednoznačne identifikovať, že sa jedna o falošný status resp. ukradnutú identitu, pretože je nepravdepodobné, že by vyššie uvedené webové stránky propagoval daný politik. Okrem toho bolo tiež podozrivé, že podmienkou zapojenia do súťaže o peniaze bolo zaplatenie registračného poplatku. Takéto falošné profily je možné nahlásiť ako podozrivé administrátorovi sociálnej siete.

STATUSY: ČO PUBLIKOVAŤ, ČO NIE, ZDIEĽANIE, LAJKY, KOMENTÁRE, DISKUSIE

Pri komunikácii na sociálnej sieti môžete vytvárať vlastné statusy, ktorými reagujete na to, čo sa deje v spoločnosti, aké máte názory na rôzne udalosti, čo si myslíte o určitých veciach. Tvorením statusov sa dá identifikovať to, aké sú Vaše názory, princípy, zásady, aké hodnoty zdieľate. Je samozrejmé, že ak uverejníte nejaký status, môže vyvolať rôznorodé reakcie. V prípade toho, že v rámci statusu reagujete na určitú udalosť na základe vášho presvedčenia a životnej filozofie, ktorú vyznávate, môžete očakávať nielen pozitívne ohlasy na tento status, ale aj množstvo negatívnych, zamietavých a často až agresívnych reakcií.

- Buďte obozretný/á najmä pri komentovaní takýchto reakcií, pretože sa vám môže stať, že sa zapletiete do často siahodlhej kontraproduktívnej a nezmyselnej diskusie s ľuďmi, ktorých cieľom fungovania na sociálnych sieťach je provokovať, vyvolávať rozbroje, podnecovať agresivitu a nenávisť. Častokrát ide o hoaxy, ktorých cieľom je podnecovať vášne.
- Takisto buďte opatrný/á pri zdieľaní príspevkov, ktoré môžu šíriť nepodložené a neoverené informácie. Ak sa jedná o informácie, ktoré uvádzajú podozrivé tvrdenia a údaje, predtým ako sa takýto príspevok rozhodnete šíriť, je potrebné si overiť, či sa uvedené tvrdenia a údaje opierajú o relevantné informačné zdroje. Seriózni prispievatelia na sociálnych sieťach pri svojich statusoch uvádzajú aj adresy zdrojov, z ktorých čerpali svoje informácie.
- Takisto zvážte zdieľanie príspevkov, ktoré propagujú rôzne formy ľahkého získania finančných prostriedkov prostredníctvom rozmanitých súťaži, statusy, ktoré zdieľajú kontakty na podozrivé webové stránky, ktoré ponúkajú výhodné nákupy rôznych výrobkov nielen

z oblasti informačných technológií, ale napríklad aj nehnuteľností, automobilov, ale aj liekov, potravín, a podobne.

- Podozrivé sú tiež statusy, ktoré ponúkajú rôzne formy zoznámenia, pracovné príležitosti, ubytovania, turistických destinácií. Všetky podobné informácie uvedené v podozrivých statusoch, je treba preverovať.

Nikdy neklikajte na neoverené webové adresy, rôzne typy tlačidiel, nikdy neposkytujte vaše osobné údaje, najmä nie rodné číslo, číslo občianskeho preukazu alebo pasu, nikdy neplaťte žiadne registračné a iné poplatky dopredu.

BLOKOVANIE, NAHLÁSENIE PRÍSPEVKU, UKLADANIE

Každý status na sociálnej sieti môžete skúsiť zablokovať, resp. nahlásiť administrátorovi ako podozrivý. Niekto, kto má záujem zneužiť Vaše osobné údaje, môže používať falošné alebo ukradnuté kontá a profily, napríklad pod menami Vašich priateľov.

Pokiaľ Vám pošle priateľ status zameraný na propagáciu nejakej webovej stránky, propagáciu rôznych podozrivých súťaži, hier, nákupov alebo iných akcií, ak je to možné, radšej sa skontaktujte s týmto priateľom a overte si u neho, či je autorom zdieľania tohto statusu, resp. či to, čo status uverejňuje a propaguje, si Váš priateľ overil a či je to bezpečné.

UKRADNUTÁ IDENTITA, FALOŠNÉ ÚČTY A PROFILY A ICH ZNEUŽITIE

Často sa stáva, že v rámci komunikácie na sociálnej sieti buď s niektorým z Vašich rodinných príslušníkov alebo priateľov vediete nezáväznú konverzáciu, ktorá môže obsahovať rôzne konkrétne osobné údaje, týkajúce sa Vašej rodiny, partnerov, aktivít, finančných alebo zdravotných problémov, atď.

Ak uvádzate príliš veľa podrobností a priateľ/kolega, s ktorým komunikujete, tiež reaguje uvádzaním ďalších podrobností, niekto, kto má záujem zneužiť Vaše osobné údaje, môže na základe informácií, ktoré Vy a Váš komunikačný priateľ uvádzate v profiloch a na základe uvedenej konverzácie pomerne jednoducho identifikovať rôzne podrobnosti o Vašej osobe, Vašej rodine či Vašich priateľoch.

Medzi najnebezpečnejšie aktivity podvodníkov na sociálnych sieťach patrí aktivita založená na ukradnutej identite. Na internete existujú takzvané trhoviská, na ktorých ponúkajú ukradnuté identifikačné údaje jednak z rôznych inštitúcií, ale aj z úradov a súkromných osôb, ktoré boli odcudzené z nedostatočne zabezpečených počítačov a počítačových serverov. Mnohokrát ide aj o údaje získané prostredníctvom neopatrne preposielaných identifikačných kariet – občianskych preukazov, pasov, platobných kariet, zdravotných preukazov skenovaných a preposielaných prostredníctvom mailov, aplikácií určených na posielanie správ a multimediálnych obsahov (Messenger, WhatsApp, Viber, Telegram, Signal), sociálnych sieti a podobne. Podvodník si práve na základe údajov z takto získaných identifikačných kariet vytvorí na sociálnej sieti falošný účet, na ukradnuté meno založí ma-

ilový účet resp. aj telefónne číslo. Prostredníctvom takéhoto účtu na sociálnej sieti môže zasielať a tvoriť rôzne statusy, propagovať rôzne falošné weby na vylákanie finančných prostriedkov od dôverčivých užívateľov sociálnych sieti.

Ďalšou formou napádania na sociálnych sieťach je vytvorenie falošných profilov, prezentujúcich rôzne typy kompetencií a aktivít, ktorých cieľom je nalákať a okradnúť dôverčivých užívateľov sociálnych sieti. Podvodník má napr. na profile uvedené, že je lekár a lieči určité diagnózy spojené s bolesťou chrbtice. Ak nájde na sociálnej sieti človeka, ktorý buď v profile alebo vo svojom statuse uvádza, že má problémy s chrbticou, takýto útočník nadviaže komunikáciu s týmto človekom a v podstate ho donúti (dotknutý človek sám bude považovať za nutnosť), aby využil jeho ponúkané služby. Za ponúkané služby bude nutné sa buď dopredu zaregistrovať a zaplatiť registračný poplatok, alebo zaplatiť zálohu za liečebné úkony alebo iné vymyslené poplatky. Takýto podvodník je schopný aj na svojom profile presne uviesť adresu, kde dané služby poskytuje. Ak si záujemca nepreverí túto adresu napríklad pomocou Google Maps, a vyberie sa za takýmto podvodníkom resp. liečiteľom, môže zistiť že na danej adrese sa nachádza nejaká polo-zbúraná budova resp. úplne iné zariadenie. Ak sa takémuto podvodníkovi podarí oklamať viacero záujemcov, svoje konto na sociálnej sieti zruší a ľudia, ktorí mu poslali peniaze, sa k nim už nikdy nedostanú.

Podobne môže podvodník na osobnom profile uvádzať napr. že je členom skupiny prominentných fanúšikov futbalového klubu. Zase prostredníctvom zisťovania profilov a komunikácie na sociálnych sieťach môže ľuďom, ktorí uvádzajú, že majú radi daný futbalový klub, ponúknuť službu zaobstarania vstupeniek na nejaký významný futbalový zápas. Samozrejme, za takúto vstupenku je potrebné zaplatiť dopredu. Dôverčivý človek, ktorý si nepreverí údaje, príde o peniaze.

Podozrivé informácie, hoaxy, rôzne údaje, či webové stránky môžu vo svojich statusoch okrem podvodníkov s falošnou identitou a profilom zdieľať aj bežní užívatelia sociálnych sietí. Môže sa to diať tak, že človek patriaci do okruhu Vašich priateľov na sociálnej sieti zdieľa nejakú webovú stránku, ktorá ponúka prostredníctvom zakúpenia aktivity okamžité a veľmi výhodné zbohatnutie a získanie finančných

prostriedkov. Tento Váš priateľ túto stránku mohol dostať buď od svojho priateľa alebo od niekoho s falošným účtom alebo identitou.

Preto vždy, skôr, než začnete s takouto zdieľanou stránkou alebo adresou nejakým spôsobom narábať, overte si údaje o tejto stránke, a to prostredníctvom prehliadačov, ako je napr. Google. Radšej neklikajte na uvedenú adresu webovej stránky ani na nejaký odkaz alebo tlačidlo, pokiaľ o tejto stránke nezískate relevantné a dôveryhodné informácie.

PRÁVNICKÉ OSOBY NA SOCIÁLNYCH SIEŤACH

Na sociálnych sieťach majú svoje účty aj rôzne inštitúcie, úrady, firmy, neziskové organizácie, ekonomické subjekty, kultúrne inštitúcie, školy, športové kluby a podobne. Drvivá väčšina týchto inštitúcií resp. účty a profily týchto inštitúcií sú dôveryhodné a relevantné, to znamená, že nie sú rizikové. Treba si však zistiť prostredníctvom webovej stránky danej inštitúcie alebo subjektu, či má na danej sociálnej sieti účet naozaj vytvorený. Zvyčajne sa to dá zistiť tak, že tieto subjekty majú na svojej úvodnej stránke webu ikonu danej sociálne siete, na ktorú keď kliknete, otvorí sa vám účet tohto subjektu na danej sociálnej sieti.

• Na sociálnych sieťach však majú otvorené účty aj falošné subjekty. Tieto však tiež môžu mať zaregistrovanú aj vlastnú webovú stránku a na nej odkaz na danú sociálnu sieť.

- Preto ak Vám nejaký takýto subjekt bude prostredníctvom sociálnej siete ponúkať nejaké služby resp. vám bude chcieť niečo predať, vyhľadajte takýto subjekt prostredníctvom Google na internete a overte si údaje, ktoré sa ho týkajú a ktoré by mal mať ako zaregistrovaný subjekt zaevidované v rôznych typoch registrov.

- Odporúčame na webovej stránke takéhoto subjektu preveriť údaje o danom subjekte – mailovú adresu, telefónne čísla, ak ide o právnické osoby, dá sa overiť aj IČO a podobne.

SKUPINY NA SOCIÁLNYCH SIEŤACH

Svoje účty na sociálnych sieťach majú aj alebo si vytvárajú aj rôzne záujmové skupiny. Môžu to byť skupiny, vznikajúce na základe určitých profesných kompetencií, koníčkov, zdieľania určitých rovnakých názorov, alebo na základe poskytovania určitých sociálnych, kultúrnych, športových, spoločenských služieb, a podobne. Ak sa chcete stať členom takejto skupiny, v prvom rade si pozrite jej profil, zistite počet členov a prečítajte si statusy, ktoré táto skupina zdieľa. Ak má skupina relevantné množstvo členov, niekoľkoročnú existenciu a obsah statusov korešponduje s tým, prečo sa chcete aj vy stať členom skupiny resp. aké informácie chcete získať, môžete sa do takejto skupiny prihlásiť.

Dôveryhodné skupiny záujem o členstvo často preverujú, to znamená, že sa členom skupiny nestanete automaticky, ale Vám najprv príde notifikácia, že relevantné zodpovedné osoby Vaše členstvo v skupine preverili a odsúhlasili. Výhodou takýchto skupín je, že sa od členov týchto skupín môžete dozvedieť dôveryhodné a pre Vás potrebné informácie, na ktoré sa môžete spoľahnúť. Ak máte napríklad nejaké problémy s Vaším počítačom, vlastnou webovou stránkou, klubovým členským a podobne, prostredníctvom týchto skupín môžete takéto problémy vyriešiť, pretože členovia týchto skupín vám poradia.

RIZIKOVÉ AKTIVITY NA SOCIÁLNYCH SIEŤACH

Digitalizácia spoločnosti v súčasnej dobe umožňuje vytvoriť obrovský priestor pre ekonomické a marketingové aktivity. Sociálne siete v súčasnosti používajú miliardy ľudí, milióny firiem, organizácií, inštitúcií a iných subjektov. Sociálne siete nevytvárajú priestor len pre komunikáciu medzi súkromnými osobami, ale vytvárajú možnosti pre rôzne typy najrôznejších spoločenských (ekonomických, sociálnych, kultúrnych, športových a iných) aktivít. Na sociálnych sieťach právnické aj fyzické osoby propagujú svoju činnosť, ponúkajú svoje produkty, poskytujú služby, poradenskú činnosť, vytvárajú priestor pre rôzne typy súťaženia, investovania prostriedkov, atď. Myslíme si, že je možné konštatovať, že drvivá väčšina všetkých subjektov zapojených na sociálnych sieťach sú spoľahlivé subjekty a seriózni partneri a užívatelia. No je zároveň samozrejmé, že tento obrovský priestor poskytuje možnosť aj pre páchanie nekalej, až trestnej činnosti vo všetkých oblastiach, ktoré sa na sociálnych sieťach vyskytujú.

A tak môžeme vidieť, že sociálne siete sa hemžia rôznymi reklamnými kampaňami, že sa na nich prezentujú rôzne webové stránky, organizujú rôzne súťaže, ankety, že množstvo užívateľov na sociálnych stránkach zverejňuje inzeráty rôzneho typu, že sa ponúkajú možnosti na investovanie peňazí, že na sociálnej sieti je možné získať pôžičku, že tu fungujú rôzne typy zoznamovacích služieb alebo sa tu prezentujú rôzne charitatívne aktivity. Preto ak chceme nejakým spôsobom komunikovať či zapojiť sa do niektorej z týchto aktivít, musíme sa mať na pozore, musíme byť ostražití a musíme každú jednu aktivitu, do ktorej sa zapojíme, preveriť z hľadiska pravdivosti, relevantnosti i bezpečnosti.

1. *Vždy musíme preveriť, kto je majiteľom účtu a identity na sociálnej sieti, ktorá prezentuje danú aktivitu. To znamená, že ak je majiteľom účtu/identity nejaká právnická osoba, mali by sme prostredníctvom napr. Google zistiť, či má webovú stránku a zverejnené dôveryhodné kontaktné údaje, podrobne posúdiť profil a ďalšie náležitosti. Podobne je to treba urobiť aj prípade, ak rôzne typy aktivít ponúkajú súkromné osoby. Tam by sme tiež mali zistiť, či má kontaktné údaje (e-mailovú adresu, telefónne číslo, adresu), alebo či je možné túto osobu relevantne kontaktovať, resp. či má aj webovú stránku.*
2. *Takisto by sme mali posúdiť údaje majiteľa účtu zverejnené v profile na sociálnych sieťach. Ak sa tam nachádza málo informácií a majiteľ účtu má webovú stránku, je treba zistiť relevantné informácie z tejto webovej stránky. Medzi relevantné a dôležité informácie každej takejto webovej stránky resp. každého, kto ponúka nejaké aktivity alebo služby, musí byť dostupná emailová adresa, telefónne kontakty, adresa, alebo iné možnosti komunikovania resp. spätnej väzby s daným subjektom.*
3. *Súčasne každý subjekt ponúkajúci na sociálnych sieťach rôzne typy ekonomických, marketingových alebo iných aktivít by mal mať vytvorené určité pravidlá opierajúce sa o relevantnú legislatívu. To znamená, že by mal mať napríklad stanovené obchodné podmienky, reklamačný poriadok, resp. pravidlá súťaženia, pri investovaní finančných prostriedkov aj podrobne portfólia pre investovanie.*
4. *Pri zapájaní sa do takýchto aktivít by si mal každý, kto sa chce do nejakej takejto aktivity zapojiť, podrobne prečítať podmienky registrácie. Ak vyžadujú od účastníka tejto aktivity zaplatenie nejakého typu registračného poplatku, je treba zvýšiť pozornosť. Ak sa chceme zaregistrovať do nejakej súťaže alebo kampane, ktorej výsledkom by malo byť získanie nejakého benefitu, napríklad finančnej výhry, vecné ceny alebo podobne, je nelogické, aby organizátor tejto aktivity požadoval od účastníka, ktorý sa jej chce zúčastniť, vopred zaplatenie registračného poplatku. Takisto pri nákupoch rôznych tovarov, služieb a podobne, je treba preveriť spôsob platby za takéto služby a tovary. Poskytovateľ takejto aktivity musí umožniť platenie poplatkov za nákup služby alebo tovaru nielen prostredníctvom bankovej karty, ale aj v hotovosti alebo na dobierku, resp. inak. V opačnom prípade sa jedna zrejme o podvodníka.*

Zásadné a základné pravidlo pri zapájanie sa do aktivít ekonomického a marketingového typu na sociálnych sieťach:

Skôr, než sa začnete registrovať do danej aktivity, kliknete na link webovej stránky alebo na nejaké tlačidlo na profilovej stránke alebo statuse subjektu, ktorý tieto aktivity ponúka, preverte si všetky možné údaje a tvrdenia zverejnené v tomto statuse či profile. Až potom, keď zistíte, že sa jedna o bezpečnú a relevantnú aktivitu, môžete konať.

PRAMENE

SafeLab:
https://safelab.sk/internetova-bezpecnost/online-kurzy-pre-dospelych

Wikipedia:
https://sk.wikipedia.org/wiki/Soci%C3%A1lna_sie%C5%A5_(internet)

Iné zdroje:
https://www.blueinfo.sk/co-je-to-socialna-siet-a-na-co-sluzi/
https://blogit.sk/co-su-socialne-siete-definicia/
https://eduworld.sk/cd/jaroslava-konickova/1557/socialne-siete-nam-ublizuju-stale-viac
https://itlib.cvtisr.sk/%c4%8 cl%c3%a1nky/clanek645/

OBSAH

SENIORI BEZPEČNE NA SOCIÁLNYCH SIEŤACH

Spracoval: PaedDr. Ján Cangár
V rámci projektu „Zvyšovanie odolnosti stredoeurópskych seniorov voči dezinformáciám“ vydalo MEMO98 v roku 2022.

DESATORO O BEZPEČNOSTI NA SOCIÁLNYCH SIEŤACH

1. Nemusíte byť zaregistrovaný/á vo všetkých existujúcich sociálnych sieťach a komunikačných službách, preto zvážte výber podľa vašej osobnej potreby, zamestnania, záujmov alebo obsahu, profilu, spôsobu a formy komunikácie.
2. Pri registrácii nemusíte ako identifikačné meno, ktoré bude verejne dostupné, uvádzať svoje celé meno a priezvisko, môžete použiť aj pseudonym. Nikdy ako meno neuvádzajte svoju emailovú adresu.
3. Pre každý účet si zvoľte iné heslo, ktoré by malo mať minimálne 10 znakov v zložení veľké a malé písmena, čísla, znaky, kompatibilné minimálne medzi anglickou a slovenskou klávesnicou.
4. Vo svojom profile neuvádzajte konkrétne údaje o sebe ani svojich príbuzných – celý dátum narodenia, rodné číslo, telefónne číslo, emailovú adresu, adresu bydliska a údaje platobných kariet.
5. Profilové fotografie a fotografie v albumoch by mali byť čo naj všeobecnejšie, skupinové, aby sa nedali jednoducho zneužiť.
6. Dôsledne preverujte všetky kontakty, priateľov a skupín, s ktorými chcete komunikovať. Nie je cieľom mať čo najviac priateľov: čím viac kontaktov, priateľov a skupín, tým väčšie riziko zneužitia vašich údajov a informácií.
7. Nezverejňujte statusy, ani iné informácie, ktoré budú obsahovať konkrétne údaje a fakty o osobnom živote Vás, resp. o životy Vašich príbuzných, ani statusy znevažujúce ľudské práva a dôstojnosť, provokujúce a vyvolávajúce nenávisť, aroganciu a agresívne reakcie.
8. Vždy zvažujte, aké statusy a informácie budete zdieľať komentovať lajkovať. Nedajte sa vyprovokovať do komunikácie s agresívnymi či manipulatívnymi užívateľmi sociálnej siete.
9. Podozrivé statusy a informácie môžete zablokovať, resp. ich aj nahlásiť administrátorovi. Nesnažte sa prečítať všetky zaujímavé statusy naraz, ale si ich uložte a prečítajte neskôr.
10. Veľmi opatrne reagujte a preverujte si podozrivé informácie a aktivity – statusy, profily, kontakty, emailové adresy, telefónne čísla, reklamy, inzeráty, ktoré môžu predstavovať bezpečnostné riziko.