Kapitola

[Ochrana osobních údajů na sociálních sítích]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: EDIT VALUE®
Poslední úpravy: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Ochrana osobních údajů na sociálních sítích

Úvod

V roce 2010 natočila slavná americká komediální show *Saturday Night Live* scénku o sociálních sítích. V ní herec vystupující jako Julian Assange (zakladatel platformy WikiLeaks) radostně a sarkasticky prohlásil: „*Poskytuji zdarma tajné korporátní informace a jsem padouch. [Zakladatel Facebooku Mark] Zuckerberg poskytuje Vaše informace korporacím za peníze a je [podle časopisu Time] Mužem roku.*“ Vidíte souvislost mezi touto komediální scénkou a realitou? Jaký máte pocit z toho, že zdarma poskytujete společnostem své osobní údaje, zatímco oni na nich vydělávají? Jsou podle Vás Vaše osobní údaje při užívání sociálních sítí v bezpečí?

V dnešní době je ochrana osobních údajů na sociálních sítích velmi důležitou záležitostí. Užívání sociálních sítí prudce roste a je nezbytnou součástí každodenního života většiny lidí na světě. Od úředníků až po naši milovanou babičku, skoro každý používá sociální sítě k sdílení fotografií, videí, ke komunikaci s přáteli či rodinou a k celkovému zveřejňování osobních informací, což vytváří pocit důvěrnosti mezi Vámi a lidmi, kteří tento obsah vidí.

Přestože je užívání sociálních sítí hluboce zakotveno v našich zvyklostech jakožto jedinců i společnosti, většina lidí není dostatečně obeznámena s kyberbezpečností, což může mít vážné a dlouhodobé následky.

Kdo další má přístup k Vašim osobním údajům?

Z tohoto důvodu jsme pro Vás připravili velké množství užitečných informací o ochraně osobních údajů při užívání sociálních sítí, které na Vás v této kapitole netrpělivě čekají.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Prostudováním této kapitoly budete schopni rozeznat nejpodstatnější rizika, které užívání sociálních sítí přináší, a budete vědět, jak se před nimi náležitě ochránit.

Co-funded by the
Erasmus+ Programme
of the European Union

1.Ochrana osobních údajů na sociálních sítích

Definice
Sociální sítě jsou interaktivní počítačové technologie, které usnadňují lidem tvorbu a šíření informací, nápadů, kariérního zájmu a dalších způsobů osobního vyjádření v rámci virtuálních komunit nebo sítí. Hlavním cílem sociálních sítí je propojit a sdílet informace s kýmkoliv na Zemi nebo s co největším možným počtem lidí zároveň. Sociální sítě lze využít ke komunikaci s přáteli či rodinou nebo jako marketingový nástroj pro podnikatele. Pod pojem sociální sítě spadá jakýkoliv digitální nástroj, který umožňuje uživatelům rychle vytvořit a sdílet nějaký obsah s ostatními lidmi.

Výše v rámečku je uvedena obecná definice sociálních sítí. Ve skutečnosti se v dnešní době sociální sítě, které mají aktuálně 3,5 miliard aktivních uživatelů, dělí do různých kategorií podle zájmů a účelu. Níže je uvedeno 10 různých kategorií sociálních sítí podle toho, k čemu se používají:

	Účel	Příklad
Osobní sítě	Navazujte kontakty s lidmi (a obchodními značkami).	Facebook; Twitter; LinkedIN
Sítě zaměřené na sdílení obsahu	Sdílejte a objevujte fotografie, videa a přímé přenosy.	Instragram; Youtube; Tik Tok
Diskusní fóra	Objevujte, sdílejte a diskutujte o novinkách, vyměňujte si informace a názory.	Reddit; Quora
Sítě pro tvorbu obsahu	Objevujte, ukládejte, sdílejte a diskutujte o nových a aktuálních trendech.	Pinterest; Flipboard
Recenzní sítě	Najděte a sdílejte informace a recenze o značkách, produktech, službách, restauracích, destinacích na dovolenou atd.	Yelp; Zomato, Tripadvisor
Microblogging a sítě pro publikaci obsahu	Vytvářejte, objevujte a poskytujte zpětnou vazbu na sdílený obsah.	Wordpress; Tumblr
Sociální sítě pro nakupování	Sledujte trendy, značky, nakupujte a sdílejte své úlovky s ostatními.	Etsy
Zájmové sítě	Najděte uživatele s podobnými zájmy a koníčky.	Goodreads; Last.Fm
Sítě sdílené ekonomiky	Poskytujte, nakupujte, prodávejte a vyměňujte statky a služby.	

		Airbnb; Uber; Glovo
Anonymní sociální sítě	Drbejte, pomlouvejte a vyzpovídejte se.	Whisper; Ask.fm

Není pochyb o tom, že žijeme v době sociálních sítí. Z tohoto důvodu existuje několik právních problémů, které sdílením obsahu na sociálních sítích (Facebook, Instagram, Pinterest) vznikají. Nejdůležitější právní opatření na sociálních sítí se týkají toho, kdo je vlastníkem sdíleného obsahu, kdy a kde je sdílení jakého obsahu vhodné a jaké existují limity pro sdílení obsahu, což souvisí s porušováním práva z ochranné známky, porušováním autorských práv, marketingem na sociálních sítích, pracovními vztahy apod. Níže naleznete stručný seznam nejdůležitějších právních zásad na Instagramu, WhatsAppu, YouTube a Facebooku.

1. Oficiálním vlastníkem všech fotografií a videí, které se rozhodnete na Instagram přidat, jste Vy sami. Pokud chtějí jiní lidí Váš obsah použít, měli by Vám za něj zaplatit.
2. Při používání Instagramu jste zodpovědní za své chování a obsah, který přidáváte.
3. Instagram může shromažďovat, užívat nebo sdílet Vaše osobní informace s propojenými firmami. Za to, jaké informace na Instagram přidáváte, si zodpovídáte Vy sami.
4. Máte možnost kdykoliv svůj účet na Instagramu odstranit. Pokud tak učiníte, všechny fotografie, videa a informace z Vašeho účtu zmizí. Pokud však před smazáním někdo Váš obsah sdílel někam dál (např. na svůj účet), může se touto formou na Instagramu nadále vyskytovat.

1. Máte možnost si kdykoliv změnit svůj profilový obrázek, uživatelské jméno a status.
2. Kdokoliv, kdo je uživatelem WhatsAppu, má přístup k Vašemu telefonnímu číslu, uživatelskému jménu, profilovému obrázku, statusu a statusové zprávě Tuto možnost lze upravit v nastavení soukromí nebo zablokováním určitých osob.
3. Poté co jsou odeslané zprávy doručeny příjemci, jsou ze systému WhatsApp vymazány a uschovány pouze ve Vašem zařízení. Vaše zprávy jsou šifrovány, což znamená, že společnost vlastnící WhatsApp k nim nemá přístup.
4. Cizí společnosti nemají povoleno umisťovat na WhatsApp reklamy, pokud jim to sami nepovolíte.

1. Při založení účtu na YouTube jsou Vaše osobní údaje shromažďovány společností Google. V sekci "ovládací prvky aktivity" si můžete upravit, která nastavení budou ukládat data do Vašeho účtu Google. Společnost Google shromažďuje data bez Vašeho souhlasu.
2. Máte možnost požádat YouTube o poskytnutí informací, které o Vás nashromáždili, a požadovat jejich úpravu či smazání.
3. Chcete-li nahlásit, že jste se nechtěně objevili v něčím videu, zašlete YouTube příslušnou URL adresu videa a přesný čas, kdy jste se Vy nebo Vaše informace objevili.
4. Pokud si někdo stěžuje na video, které máte na svém kanálu, a YouTube s touto osobou souhlasí, budete upozorněni, že video musíte upravit nebo odstranit.

1. I přestože je váš profil na Facebooku soukromý, mějte na paměti, že lidé mohou vidět a sdílet informace, které o Vás zveřejňují druzí. Ostatní lidé si mohou také ukládat na své mobilní telefony a jiná zařízení informace, které jste o sobě zveřejnili.
2. Některé společnosti poskytují Facebooku získané informace o Vás a naopak.
3. Pokud souhlasíte s používáním aplikace na Facebooku, může tato aplikace používat, sdílet a uchovávat informace, které zveřejníte na Facebooku.
4. Pokud se rozhodnete odstranit svůj účet, informace, které jste o sobě zveřejnili, budou také odstraněny. Toto však neplatí pro obsah, který o Vás zveřejnil někdo jiný.

Zdroj: file:///C:/Users/joana.bastos/Desktop/Young%20people's%20rights%20on%20social%20media.pdf

1.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_01_01: Více, co znamená pojem sociální sítě a co všechno zahrnuje.

Zadání: Co znamená pojem sociální sítě?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Webové stránky a aplikace, které umožňují lidem posílat zprávy a fotografie.
- Forma elektronické komunikace.
- Webové stránky a počítačové programy, které umožňují lidem komunikovat a sdílet informace na internetu pomocí počítače nebo mobilního telefonu.
- Webové stránky a aplikace určené k rychlému sdílení obsahu.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_01_02: Znáte nejdůležitější práva spojená se sociálními sítěmi.

Zadání: Jaká práva na ochranu osobních údajů mají uživatelé WhatsAppu?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď není správně.

- Právo na šifrování zpráv tzn. WhatsApp nemůže číst zprávy, které odešlete druhým lidem.
- Máte právo smazat svůj účet na WhatsAppu. Zprávy, které byly doručeny druhým lidem, smazány nebudou.
- Smazáním aplikace z Vašeho telefonu nedojde ke smazání Vašeho účtu, a tedy ani ke smazání Vašich údajů.
- WhatsApp ukládá a uschovává údaje o Vás, nemůže je však nikde použít.

1. Nejčastější rizika na sociálních sítích

Co-funded by the
Erasmus+ Programme
of the European Union

V dnešní době je běžně známo, že sociální sítě propojují naše každodenní zájmy a aktivity. Sdílíme však stejné návyky a chování týkající se používání sociálních sítí? Abychom pochopili význam sociálních sítí v naší společnosti, je důležité mít na paměti těchto 10 statistik:

10 NEJDŮLEŽITĚJŠÍCH STATISTIK SOCIÁLNÍCH SÍTÍ

73 % marketingových pracovníků se domnívá, že marketing na sociálních sítích je velice efektivní pro jejich podnikání (Buffer, 2019)

Na světě je 3,5 miliard aktivních uživatelů sociálních sítí, což odpovídá 45 % celkové populace (Emarsysm, 2019)

Od ledna 2017 do ledna 2019 narostl počet denně aktivních uživatelů příběhů na Instagramu ze 150 milionů na 500 milionů. (Buffer, 2019)

Facebook nadále zůstává nejužívanější sociální sítí. (Pewinternet, 2018)

91 % uživatelů navštěvuje sociální sítě prostřednictvím mobilního telefonu. (Buffer, 2019)

71 % spotřebitelů si přeje, aby značky tlačily na sociální sítě pro lepší zabezpečení jejich osobních údajů. (Edelman, 2008)

91 % uživatelů navštěvuje sociální sítě prostřednictvím mobilního telefonu. (Buffer, 2019)

Co-funded by the
Erasmus+ Programme
of the European Union

Průměrně spotřebitelé tráví posíláním zpráv a užíváním sociálních sítí 3 hodiny denně. (Globalwebindex, 2018)

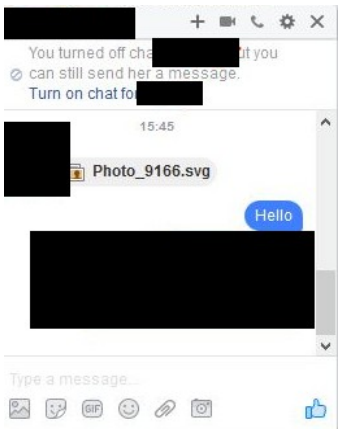
81 % malých a středně velkých podnikatelů používá v současné době sociální sítě pro podporu růstu svého podnikání a 9 % je plánuje využít v budoucnosti. (LinkedIN, 2014)

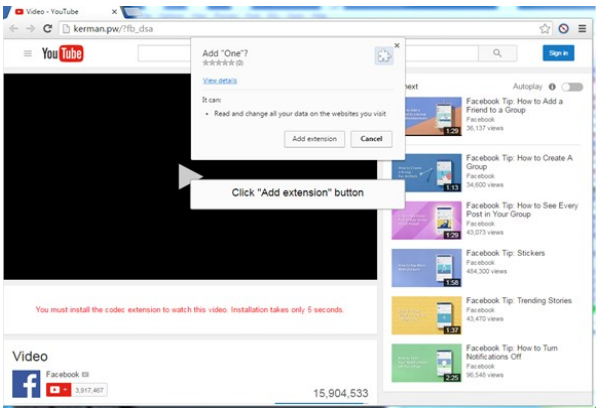
V průměru mají lidé 7,6 účtů na sociálních sítích. (Clement, 2019)

Po prohlédnutí těchto statistik není divu, že se sociální sítě stávají jednou z nejproslulejších platforem pro shromažďování uživatelských dat, ať už legálně poskytovatelem služby nebo hackery se zákeřnými úmysly.
Největší riziko představuje pro uživatele sociálních sítí malware, který může značně ohrozit všechna jejich data. Existují různé druhy malwaru, které se liší podle svého účelu:

1. Ransomware – software, který pomocí šifrování odepře uživateli přístup k jeho datům (fotografiím, dokumentům), dokud nezaplatí výkupné. Tento druh malwaru je aktivován při rozkliknutí odkazu, který byl zveřejněn na sociální síti, nebo obrázku, který následně uživatele přesměruje na externí web, který škodlivý kód šíří.

Příklad ransomwaru
Chatovací aplikace jako WhatsApp nebo Facebook Messenger jsou běžnými prostředky pro útok ransomwaru. Na obrázku vidíte příklad, kdy útočníci rozeslali prostřednictvím Facebook Messengeru podvodné zprávy obsahující SVG obrázky. Uživatelé, kteří na obrázek klikli, se ocitli na stránce, která je pomocí vyskakovacího okna donutila ke stažení rozšíření nebo doplňku pro spuštění videa. Poté, co škodlivý kód nakazil systém uživatele, se objevilo další vyskakovací okno požadující platbu výměnou za odemknutí souborů uživatele.





2. Trojský kůň – Druh malwaru, který na první pohled vypadá věrohodně, ale dokáže převzít kontrolu nad Vaším počítačem. Účelem trojského koně je krást údaje (přihlašovací údaje, finanční data, dokonce i elektronické peníze), instalovat další malware, upravovat soubory, sledovat činnost uživatele (sledování obrazovky, keylogging atd.), využít počítač k botnetům a anonymizovat internetové aktivity útočníka. Trojský kůň se chová jako věrohodná aplikace nebo soubor a oklame Vás k stažení a instalaci malwaru. Po instalaci může trojský kůň provést činnost, pro kterou byl původně navržen.
   Obvykle je trojský kůň skryt pod falešnou reklamou nebo zaslán uživateli prostřednictvím nějakého messengeru.

3. Počítačový vir – Druh malwaru, který se dokáže kopírováním sám množit a šířit na další počítače. Viry se většinou šíří tak, že se připojí k jiným programům a vypustí škodlivý kód, když uživatel poškozený program spustí. Dále se viry šíří prostřednictvím skriptových souborů, dokumentů a využitím bezpečnostních chyb ve skriptech stránek. Viry se používají ke krádeži informací, poškození hostitelských počítačů a sítí, vytváření botnetů, krádeži peněz a dalším účelům.

4. Greyware – Tento druh nepředstavuje fyzickou hrozbu pro Vaše data, jedná se spíše o protivný a otravný malware, jako je adware nebo spyware. Vyskytuje se převážně na sociálních sítích ve formě "click baitu" – většinou se jedná o nějaký lákavý či zajímavý článek, který Vás přesměruje na stránku, která po Vás chce, abyste si nainstalovali falešný plugin na sociální sítě nebo vyplnili krátký online průzkum, než Vám umožní přístup k obsahu. Tyto informace jsou následně shromažďovány a prodány jiným kyberzločincům a mohou být použity k získání přístupu k Vašim osobním účtům.

Příklad greyware

V průběhu let útočníci využili jak opravdová, tak falešná úmrtí celebrit, aby zaujali pozornost uživatelů a vymámili z nich informace.
Jeden takový případ se stal po smrti herce Robina Williamse v roce 2014. Pouhých 48 hodin po jeho smrti, začal po Facebooku kolovat odkaz, který měl údajně obsahovat jeho video na rozloučenou. Uživatelé byli po rozkliknutí přesměrováni na falešnou stránku BBC News. Poté jim bylo řečeno, že než si budou video moci pustit, musí jej nejdříve sdílet na Facebooku. Následně se objevila druhá falešná stránka, která po nich požadovala vyplnění krátkého online průzkumu. Tímto způsobem byly

posbírány osobní údaje velkého počtu lidí a následně prodány internetovým obchodníkům.

5. Počítačový červ – Červi jsou jedním z nejčastějších typů malwaru. Dokážou upravovat a mazat soubory, krást data nebo nainstalovat tzv. zadní vrátka, která umožní hackerovi získat kontrolu nad počítačem a jeho systémovým nastavením. Mohou dokonce do počítače vložit další infikovaný software. Počítačoví červi mohou být přenášeni prostřednictvím slabých míst v softwaru nebo v přílohách nevyžádaných e-mailů či rychlých zpráv. Po otevření Vás mohou tyto soubory přesměrovat na škodlivou stránku nebo automaticky stáhnout červa do počítače. Po nainstalování červ nenápadně nakazí počítač bez vědomí uživatele. Často se červi šíří pomocí hromadného rozesílání rychlých zpráv s kontaminovanou přílohou všem kontaktům uživatele.

Jak jste si mohli všimnout, všechny druhy malwaru používají pro nalákání uživatele stejnou strategii, zejména phishingové podvody nebo útoky. Phishingové útoky používají škodlivé zdroje ke shromažďování osobních údajů a finančních dat nebo k infikaci počítače uživatele malwarem.

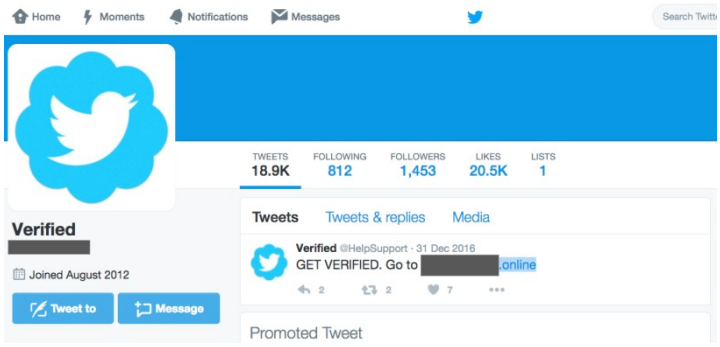
Co-funded by the
Erasmus+ Programme
of the European Union

První krok phishingového útoku je vždy stejný: Na Vaší zdi na sociální síti nebo v aplikaci pro rychlé posílání zpráv se objeví odkaz, fotografie, video, článek nebo reklama. Zdrojem může být kdokoliv – novinové zpravodajství, celebrita, podnik, samotná sociální síť nebo dokonce i důvěryhodná osoba. Ve většině případů se tyto zdroje pouze vydávají za skutečné účty nebo jde o uživatele, jejichž účet byl napaden nebo jejichž identita byla ukradena.

Příklad napodobování skutečného účtu

Twitter má nástroj, pomocí kterého ověřuje účty s cílem snížit podvodné aktivity, který se nazývá "Twitter Verified". Níže můžete vidět opravdový ověřený účet:

Netrvalo dlouho, než se objevil falešný účet napodobující ten skutečný, který uživatele přesměrovával na všemožné škodlivé odkazy požadující platby.



Phishing na sociálních sítích cílí na Vaše základní emoce a potřeby, jako jsou důvěra, bezpečnost, zármutek, strach ze ztráty peněz, touha dostat věci zadarmo nebo najít výhodné koupě, touha najít lásku nebo získat popularitu/postavení. Také obvykle uvádí nebo naznačuje, že je potřeba jednat rychle, abyste se vyhnuli problému nebo nezmeškali výhodnou nabídku.

Příklad phishingového podvodu

OMG! Už jste viděli tuto Vaši fotografii?
Tajné podrobnosti o úmrtí Michaela Jacksona!
Pouze 1 % lidí dokáže tento problém rozlousknout! Vyzkoušejte si kvíz hned teď!
Adidas zdarma rozdává 3000 párů bot při příležitosti 93. výročí! Získejte boty zdarma nyní!

Všechny tyto příklady patří mezi velmi časté způsoby phishingových podvodů – obsahují otázku, celebritu, značku nebo nějakou skutečnost, která zaujme pozornost uživatele, který je následně

přesměrován na falešnou přihlašovací stránku. Cílem je získat jeho přihlašovací údaje nebo automaticky nainstalovat malware do počítače.

Druhým krokem útoku je přesměrování uživatele na webovou stránku, která požaduje zadání důvěrných informací nebo která nakazí Váš počítač či mobilní telefon malwarem. K instalaci může dojít automaticky nebo po požadavku ke stažení programu, aplikace nebo doplňku prohlížeče.
Případně Vám příspěvek, tweet nebo zpráva může nařídit, abyste zavolali na uvedené číslo. To může mít za následek buď požadavek o zadání důvěrných informací nebo vysokou částku za účet za telefon.

2. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_02_01: Znáte nejdůležitější statistiky spojené s užíváním sociálních sítí.

Zadání: Která z uvedených možností není pravdivá?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správně.

- Sociální sítě jsou efektivním marketingovým nástrojem pro podnikatele.
- Facebook je nejpoužívanější sociální sítí.
- Většina uživatelů navštěvuje sociální sítě prostřednictvím mobilního telefonu.
- Malé a středně velké podniky využívají sociální sítě k podpoře růstu svého podnikání.
- Uživatelé mají tendenci si vybrat pouze jednu sociální síť, kterou používají každý den.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_02_02: Znáte nejčastější rizika sociálních sítí.

Zadání: Procházíte svou zeď na Facebooku a narazíte na toto oznámení:

Co uděláte?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

- "Super! Dneska je můj šťastný den!" Kliknete na "POKRAČOVAT" a zadáte všechny požadované informace, abyste výhru získali. Potom tuto ojedinělou příležitost budete sdílet, aby ji viděli všichni Vaši přátelé.

- Na získání výhry máte pouze 2 minuty – rychle kliknete na "POKRAČOVAT" a zadáte všechny potřebné údaje. Když přijde na řadu zadávání bankovních údajů, vzdáte to – je to pro Vás příliš mnoho práce.
- Jste zvědaví a kliknete na "POKRAČOVAT". Když zjistíte, že je potřeba zadat osobní údaje, stránku opustíte. Jedná se nejspíš o podvrh.
- Na oznámení nekliknete. Není možné, abyste vyhráli soutěž, které jste se neúčastnili! Příspěvek označíte jako podvod.

2.Tipy, jak bezpečně používat sociální sítě

Nyní, když jste se seznámili s různými druhy rizik při užívání sociálních sítí, si nemyslete, že jediným možným řešením, jak ochránit svoje soukromí, je smazání všech Vašich účtů. Trik je v tom, používat sociální sítě a zároveň znát všechny možné hrozby a vědět, jak se zachovat, pokud na ně narazíte.
Existují časté způsoby chování podvodníků a hackerů, které Vás mohou upozornit na případný phishingový podvod. Při prohlížení svých oblíbených sociálních sítí si dávejte pozor na tato varovná znamení:

Varovné znamení č. 1: Žádosti o přátelství od cizích lidí

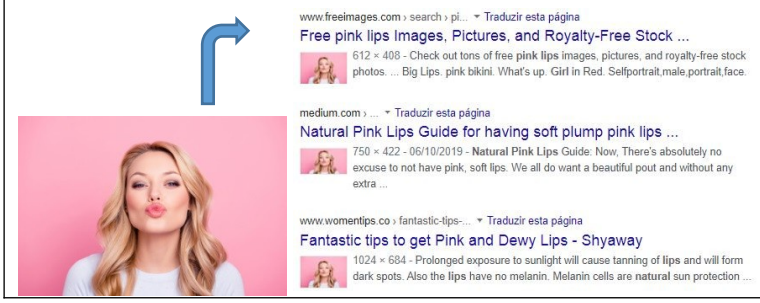
Obdrželi jste žádost o přátelství od někoho, koho neznáte? Někdo cizí Vám poslal soukromou zprávu? Podnik nebo veřejná osobnost Vás žádá o sledování?

Co-funded by the
Erasmus+ Programme
of the European Union

Facebook, Twitter, Instagram a podobné platformy jsou plné falešných profilů vytvořených za účelem phishingu. Nepřijímejte žádné žádosti o přátelství, aniž byste si profil ověřili. Pokud Vás někdo obtěžuje, je dobré takový účet nahlásit a zablokovat.

Rychlý tip

Proveďte kontrolu profilového obrázku pomocí **zpětného hledání** na Googlu. Hackeři a podvodníci většinu času totiž používají stock fotografie. Pokud se při zpětném hledání fotografie objeví na několika webových stránkách, jedná se o falešný účet.



Rychlý tip

Všimli jste si někdy na sociálních sítích modré "fajfky" vedle jména vysoce postavených osob nebo podniků? Vypadá nějak takto:

Twitter: **Stephen King**
Facebook: **adidas**
Instagram: **cristiano**

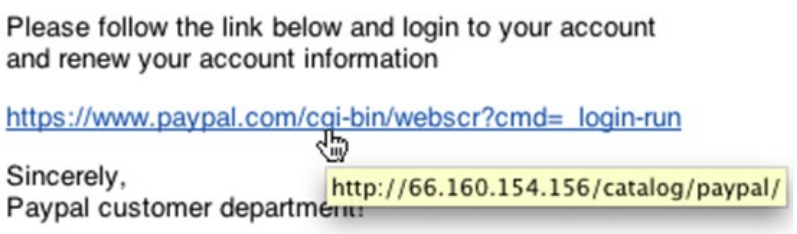
Tento odznáček je dostupný téměř na každé sociální síti a upozorňuje na to, že je **účet ověřený** – tedy že skutečně patří celebritě nebo nějakému vedoucímu představiteli v oboru.
Pokud například obdržíte zprávu od účtu "Twitter Verified", který toto ověření nemá, jedná se s největší pravděpodobností o podvrh!

Varovné znamení č. 2: Klikněte na odkaz!

Cílem phishingového útoku je ve většině případů donutit Vás ke stažení přílohy (např. fotografie poslané v soukromém chatu) nebo otevření odkazu. Někdy se zločinci vydávají za důvěryhodné zdroje, aby Vás donutili kliknout na odkaz nebo stáhnout aplikaci, která obsahuje malware. To, co se na první pohled zdá být věrohodný odkaz, může být ve skutečnosti odkaz na nelegální stránku.
Z tohoto důvodu je dobré neklikat na žádný odkaz, který Vás má přesměrovat na jinou webovou stránku. Místo toho jděte přímo ke zdroji (na webovou stránku značky, banky atd.) a ujistěte se, zda to, co jste obdrželi, je opravdové oznámení či reklama.

Rychlý tip

Rychlý způsob, jak si ověřit, zda Vás odkaz přesměruje na důvěryhodnou stránku, je najetí myší na hypertextový odkaz. Měla by se Vám ukázat úplná URL adresa, pomocí které zjistíte, zda stránce věřit.



Co-funded by the
Erasmus+ Programme
of the European Union

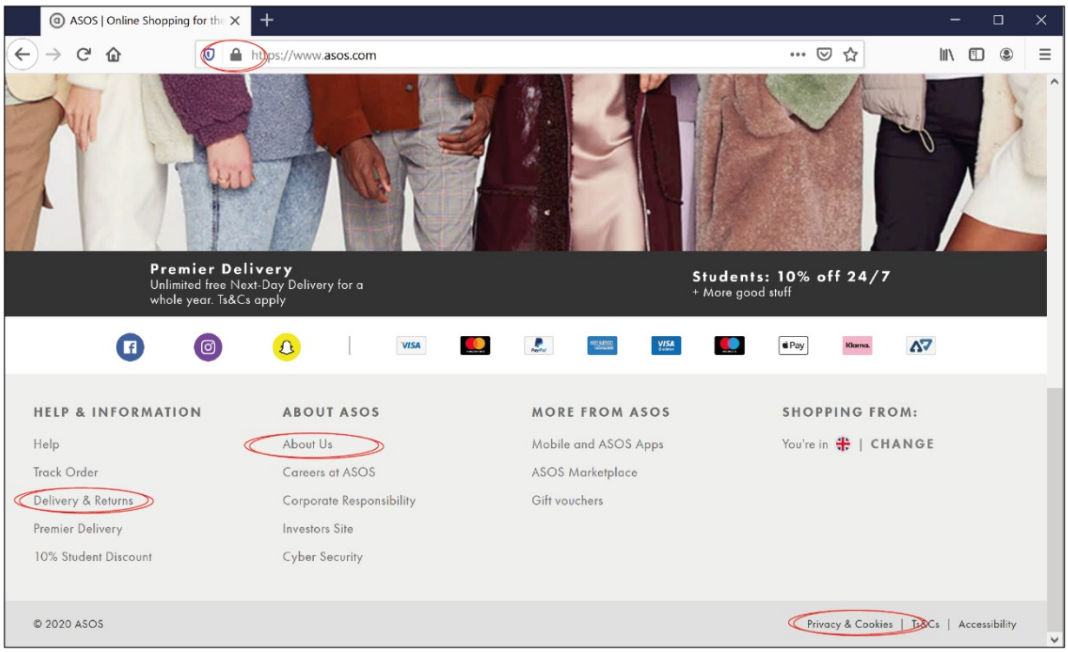
Na co si při kontrole URL dávat pozor?
Věnujte pozornost začátku URL adresy: bezpečné URL adresy mají na začátku "https" místo "http", což znamená, že jsou šifrované. "S" v "https" znamená secure (bezpečný).
Tímto ověřením zjistíte, že odkaz na obrázku je podvodný.

Rychlý tip

Co když na odkaz přece jen kliknete? Jak se zachovat?
Pokud Vás odkaz přesměruje na jinou webovou stránku, existuje několik vodítek, která Vám pomohou rozeznat, zda se jedná o skutečnou společnost či nikoliv.
Předtím, než začnete někam zadávat svoje přihlašovací údaje nebo kliknete na tlačítko stahovat, ověřte si bezpečnost stránky pomocí těchto jednoduchých kroků:

- Pokud se v adresním řádku nachází "https" nebo obrázek visacího zámku, znamená to, že je **stránka zabezpečená.**
- **Zkontrolujte internetovou doménu** – kyberzločinci jsou velmi prozíraví. Většinou jsou falešné domény velmi podobné těm reálným, např. "as0s.com" nebo "asos.net" místo "asos.com".
- **Na webové stránce se nacházejí kontaktní informace jako poštovní adresa a telefonní číslo** – seriózní společnosti uvádějí na svých stránkách tyto informace, abyste měli možnost je v případě problému kontaktovat.
- **Reklamační řád** – společnosti by měly uvádět podmínky vrácení zboží a informace o dopravě.
- **Prohlášení o ochraně osobních údajů** – věrohodné weby by Vás měly informovat o tom, co dělají pro to, aby ochránily Vaše údaje a zda je poskytují třetím stranám.

Co-funded by the
Erasmus+ Programme
of the European Union



Varovné znamení č. 3: Propagační akce a soutěže, které se zdají být příliš výhodné!

Jedná se o velmi častý druh phishingového podvodu. Útočníci Vás pomocí nízkých cen, nabízením neodolatelných výher nebo rozdáváním slev donutí k poskytnutí soukromých údajů.

Rychlý tip
Jak rozpoznat podvodnou soutěž? • Jejich stránka na sociální síti má nízký počet sledujících; • Špatná gramatika a pravopis; • Velmi osobní otázky, jako například jméno matky, první mazlíček, zda máte děti apod. Tyto informace jim mají pomoct zjistit Vaše heslo! • Neodbytnost podvodníků. Jejich cílem je u Vás vyvolat pocit naléhavosti.

Jak jste již mohli usoudit, existují způsoby, jak odhalit phishingové podvody na sociálních sítích a nestát se tak obětí kybernetického útoku, který může ohrozit Vaše osobní data. Ale dobrá pozornost nestačí. Nejlepší obranou před kybernetickými útoky je prevence. Co tedy můžete udělat, abyste byli vždy o krok napřed před kyberzločinci?

Co-funded by the
Erasmus+ Programme
of the European Union

Pro zabezpečení soukromí na sociálních sítích zkontrolujte možnosti nastavení Vašeho účtu.

nevyžádanou

Co-funded by the
Erasmus+ Programme
of the European Union

3. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_03_01: Znáte různá opatření, která Vám pomohou bezpečně užívat sociální sítě.
DVC_Ochrana osobních údajů na sociálních sítích_03_02: Dokážete vyjmenovat tipy pro bezpečné užívání sociálních sítí.

Zadání: Podle kterých znaků lze poznat, že se jedná o phishingový podvod?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Chyby v gramatice a pravopisu oznámení.
- Přítomnost hypertextových odkazů: Pouze důvěryhodné zdroje mohou publikovat odkaz na své webové stránky.
- Hypertextový odkaz neodpovídá adrese URL.
- Pokud mi dobrý přítel zašle fotografii ke stažení, mohu mít jistotu, že se nejedná o žádné nebezpečí.
- Známá společnost nemá ověřený účet na sociální síti.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Ochrana osobních údajů na sociálních sítích_03_02: Dokážete vyjmenovat tipy pro bezpečné užívání sociálních sítí.

Co-funded by the
Erasmus+ Programme
of the European Union

Zadání: Co můžete udělat pro to, abyste se ujistili, že používáte sociální sítě bezpečným způsobem?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Bezpečnější je používat stejné heslo na všechny vaše účty, protože ho jen tak snadno nezapomenete.
- Předtím než někomu potvrdíte žádost o přátelství, ověřte si věrohodnost jejich profilového obrázku a celého účtu.
- Nikdy byste neměli prozrazovat na svém účtu podrobnosti o tom, kam jste jeli na dovolenou, kde nakupujete nebo kam jedete a stejně tak ani informace o tom, kdy odjíždíte a kdy se vracíte domů.
- Je v pořádku používat počítač s internetovým připojením bez nainstalovaného anti-malwaru a antivirového programu.
- Abyste měli přehled o všech aktivitách svých přátel na internetu, musíte být neustále přihlášeni ke svému účtu.

Zdroje

-
- Akilawala, T. (August 16, 2014) *Fake Robin Williams goodbye video on Facebook is a scam.* Retrieved from https://www.bgr.in/news/fake-robin-williams-goodbye-video-on-facebook-is-a-scam-321750/
- Crowdstrike (October 15, 2019) *The 11 most common types of malware*. Retrieved from https://www.crowdstrike.com/epp-101/types-of-malware/
- Constanza, T. (August 19, 2019) *Scam on Facebook exploits Robin Williams' suicide.* Retrieved from https://www.siliconrepublic.com/enterprise/scam-on-facebook-exploits-robin-williams-suicide
- DuPaul, N. (October 12, 2012) *Common Malware Types: Cybersecurity 101.* Retrieved from https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
- Foreman, C. (June 20, 2017) *10 Types of Social Media and How Each Can Benefit Your Business*. Retrieved from https://blog.hootsuite.com/types-of-social-media/
- Get Safe Online (n. d.) *Social Media Phishing. https://www.getsafeonline.org/social-networking/social-media-phishing/*
- GMA News Online (August 15, 2014) *Beware of Robin Williams goodbye video scam.* Retrieved from https://www.gmanetwork.com/news/hashtag/content/375009/beware-of-robin-williams-goodbye-video-scam/story/
- Kietzmann, J. H. and Hermkens, K. (2011) *Social media? Get serious! Understanding the functional building blocks of social media*. Business Horizons (Submitted manuscript). 54 (3): 241–251. doi:10.1016/j.bushor.2011.01.005.
- Mohsin, M. (Febrauary 7, 2020) *10 Social Media Statistics You Need to Know in 2020 [Infographic].* Retrieved from https://www.oberlo.com/blog/social-media-marketing-statistics
- NortonLifeLock (n. d.) *What is a Trojan? Is it a virus or is it malware?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
- NortonLifeLock (n. d.) *What is a computer worm, and how does it work?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Zapamatujte si

Co-funded by the
Erasmus+ Programme
of the European Union

Shrnutí

Žijeme ve světe globalizace, ve kterém nám internet umožňuje komunikovat s kýmkoliv a kdekoliv. Sociální sítě se staly **neoddělitelnou součástí našich životů** a představují skvělý způsob, jak zůstat propojeni se světem.

Sociální sítě jako Facebook, Instagram nebo YouTube jsou oblíbené napříč všemi věkovými kategoriemi a neustále hledají inovativní způsoby, jak do svých platforem začlenit nové trendy a nalákat nové uživatele.

Nicméně, navzdory všem těmto výhodám, uživatelé čelí na sociálních sítí velkému množství **bezpečnostních rizik a hrozeb** útočících na jejich soukromí, které souvisí s neustálým a lehkovážným užíváním těchto médií. Útočníci rádi zneužívají chování a návyky uživatelů sociálních sítí, aby je nalákali na **phishingové podvody a útoky**, které ohrožují jejich zařízení a data. Proto by si měl každý uvědomovat svou odpovědnost za udržování **bezpečného prostředí na internetu** a zároveň chápat rizika, která přítomnost ve virtuálním světě přináší. **Obezřetnost, silné heslo a antivirový program** jsou základní opatření, která musí uživatelé začlenit do svého každodenního brouzdání po internetu, aby mohli získat kontrolu nad svou bezpečností při užívání sociálních sítí.

Svět se postupně vyvíjí k jednotnému digitálnímu trhu, a je tady důležité, aby si všichni byli vědomi zákonů uplatňovaných na ochranu osobních údajů, jako jsou **GDPR**, a jak je lze uplatnit na různé scénáře.

Na závěr je důležité si uvědomit, že **vláda, společnost a koncoví uživatelé musí spolupracovat na ochraně soukromí a zabezpečení osobních údajů na sociálních sítích.**

Co-funded by the
Erasmus+ Programme
of the European Union

Správné odpovědi

Zadání: Co znamená pojem sociální sítě?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Webové stránky a aplikace, které umožňují lidem posílat zprávy a fotografie.
- Forma elektronické komunikace.
- Webové stránky a počítačové programy, které umožňují lidem komunikovat a sdílet informace na internetu pomocí počítače nebo mobilního telefonu.
- Webové stránky a aplikace určené k rychlému sdílení obsahu.

Zadání: Jaká práva na ochranu osobních údajů mají uživatelé WhatsAppu?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď není správně.

- Právo na šifrování zpráv tzn. WhatsApp nemůže číst zprávy, které odešlete druhým lidem.
- Máte právo smazat svůj účet na WhatsAppu. Zprávy, které byly doručeny druhým lidem, smazány nebudou.
- Smazáním aplikace z Vašeho telefonu nedojde ke smazání Vašeho účtu, a tedy ani ke smazání Vašich údajů.
- WhatsApp ukládá a uschovává údaje o Vás, nemůže je však nikde použít.

Zadání: Která z uvedených možností není pravdivá?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správně.

- Sociální sítě jsou efektivním marketingovým nástrojem pro podnikatele.
- Facebook je nejpoužívanější sociální sítí.
- Většina uživatelů navštěvuje sociální sítě prostřednictvím mobilního telefonu.
- Malé a středně velké podniky využívají sociální sítě k podpoře růstu svého podnikání.
- Uživatelé mají tendenci si vybrat pouze jednu sociální síť, kterou používají každý den.

Zadání: Procházíte svou zeď na Facebooku a narazíte na toto oznámení:

Co-funded by the
Erasmus+ Programme
of the European Union

Co uděláte?
Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

- "Super! Dneska je můj šťastný den!" Kliknete na "POKRAČOVAT" a zadáte všechny požadované informace, abyste výhru získali. Potom tuto ojedinělou příležitost budete sdílet, aby ji viděli všichni Vaši přátelé.
- Na získání výhry máte pouze 2 minuty – rychle kliknete na "POKRAČOVAT" a zadáte všechny potřebné údaje. Když přijde na řadu zadávání bankovních údajů, vzdáte to – je to pro Vás příliš mnoho práce.
- Jste zvědaví a kliknete na "POKRAČOVAT". Když zjistíte, že je potřeba zadat osobní údaje, stránku opustíte. Jedná se nejspíš o podvrh.
- Na oznámení nekliknete. Není možné, abyste vyhráli soutěž, které jste se neúčastnili! Příspěvek označíte jako podvod.

Zadání: Podle kterých znaků lze poznat, že se jedná o phishingový podvod?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Chyby v gramatice a pravopisu oznámení.
- Přítomnost hypertextových odkazů: Pouze důvěryhodné zdroje mohou publikovat odkaz na své webové stránky.
- Hypertextový odkaz neodpovídá adrese URL.
- Pokud mi dobrý přítel zašle fotografii ke stažení, mohu mít jistotu, že se nejedná o žádné nebezpečí.
- Známá společnost nemá ověřený účet na sociální síti.

Zadání: Co můžete udělat pro to, abyste se ujistili, že používáte sociální sítě bezpečným způsobem?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Bezpečnější je používat stejné heslo na všechny vaše účty, protože ho jen tak snadno nezapomenete.
- Předtím než někomu potvrdíte žádost o přátelství, ověřte si věrohodnost jejich profilového obrázku a celého účtu.

Co-funded by the
Erasmus+ Programme
of the European Union

- Nikdy byste neměli prozrazovat na svém účtu podrobnosti o tom, kam jste jeli na dovolenou, kde nakupujete nebo kam jedete a stejně tak ani informace o tom, kdy odjíždíte a kdy se vracíte domů.
- Je v pořádku používat počítač s internetovým připojením bez nainstalovaného anti-malwaru a antivirového programu.
- Abyste měli přehled o všech aktivitách svých přátel na internetu, musíte být neustále přihlášeni ke svému účtu.