Kapitola

[Informační tok a komunikace na internetu]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: bit schulungscenter
Poslední úprava: 14.08.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Informační tok a komunikace na internetu

Úvod

Internet značně ovlivnil způsob komunikace mezi lidmi. Pro většinu z nás je online komunikace běžnou každodenní záležitostí. Denně otevřeme, přepošleme a odpovíme na bezpočet e-mailů. Tímto způsobem lze informace předávat rychle, snadno a levně. A pokud Váš e-mailový klient z nějakého důvodu nefunguje? Stačí chvíli surfovat na internetu a za malý moment najdete fórum, kde uživatelé již podobný problém probírali a navzájem si sdělovali užitečné rady a tipy. Jak je vidět, není pochyb o tom, že komunikace na internetu nabízí plno výhod. Možnost užívat každý den komunikační technologie se však pro mnohé stává samozřejmostí, což má za následek neopatrnost a zpomalené či žádné reakce při rozpoznávání potenciálních rizik. Proto je velmi důležité dávat si při online komunikaci velký pozor a snížit tak pravděpodobnost ocitnutí se v nepříjemných situacích.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Se stále rostoucím užíváním internetu a různých elektronických komunikačních nástrojů, ať už v našem soukromém životě či v práci, přicházejí nové hrozby pro naše osobní údaje a soukromí. Je tedy velmi důležité znát aktuální rizika, abychom byli schopni rychle a správně jednat. V době rostoucí míry počítačové kriminality jsou znalost možných bezpečnostních problémů spojených s online komunikací a správné a bezpečné užívání e-mailu nezbytné pro každého uživatele.

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

1.Falešné e-maily a přílohy

E-mail je nejužívanějším komunikačním prostředkem na internetu. Otevírání a odesílání e-mailů je pro Vás nejspíš běžnou každodenní záležitostí. Ale právě díky vysoké oblibě e-mailové komunikace jsou i **falešné e-maily** zvýšenou hrozbou pro každého uživatele.

Definice
Falešným e-mailem rozumíme nežádoucí e-mail, který má za cíl oklamat Vás podvodnými informacemi nebo navést k provedení nějakého nevhodného činu. Často jsou prostřednictvím **příloh** těchto e-mailů rozesílány škodlivé programy.

Je tedy velmi důležité znát typické znaky škodlivých e-mailů. Předtím než otevřete přílohu, rozkliknete odkaz nebo odpovíte na e-mail, zeptejte se sami sebe:

1. Je mi nabízeno něco, co je **příliš dobré na to, aby to byla pravda**? Dávejte si pozor: pokud tomu tak je, s největší pravděpodobností se jedná o podvrh.

Příklad
Nejčastějším příkladem jsou e-maily od přitažlivých dam, které Vás "chtějí poznat", bezplatné dárky nebo oznámení o tom, že jste vyhráli nějakou cenu (přitom jste se nezúčastnili žádné soutěže nebo loterie).

2. Odpovídá **obsah** e-mailu údajnému **odesílateli**?

Příklad
Obdrželi jste e-mail od Vaší kamarádky Aničky. Píše Vám, že je v zahraničí na dovolené a že ji okradli. Naléhá na Vás, abyste jí ihned poslali peníze na účet, aby se mohla ještě tento týden vrátit domů. Takováto zpráva dává jasně najevo, že e-mailový účet Vaší kamarádky byl napaden hackery.

3. Obsahuje e-mail určitá **popudlivá slova** jako například "poslední výzva", "účet zablokován" a podobně? Žádá Vás odesílatel o sdělení přístupových údajů, hesel nebo jiných **důvěrných informací**?

Důležité
Kdykoli na Vás někdo naléhá nebo Vás žádá o sdělení důvěrných informací, měl by to pro Vás být červený vykřičník, že něco není v pořádku.

4. Přijde Vám na **odesílateli něco zvláštního** (např. obdrželi jste od německé firmy e-mail v angličtině)? Nebo se v e-mailu nachází plno **pravopisných či gramatických chyb** (nejspíš kvůli automatickému překladači)?

5. Byl e-mail automaticky přesunut do **složky spamu**?

Nejspíš si říkáte, proč byste si měli vůbec lámat hlavu se spamem. Plno poskytovatelů e-mailových klientů neustále vylepšuje své automatické monitorovací funkce a většina nežádoucích e-mailů automaticky skončí ve složce spamu. Problém je v tom, že některé e-maily mohou být nesprávně vyhodnoceny a jsou přesunuty do složky spamu, přestože jsou neškodné.

Příklad
Váš kamarád pořádá velkou narozeninovou oslavu. Všem svým kamarádům hromadně rozešle e-mailem pozvánky pomocí skryté kopie. Naneštěstí se může stát, že Vaše pozvánka skončí ve složce spamu, jelikož velké množství adres ve skryté kopii většinou značí spam.

6. Jste vyzváni k spuštění programu s podivným formátováním (např. složeniny známých formátů jako "jpg.vbs" nebo "gif.exe")?

Pokud Vaše odpověď na jednu nebo více z uvedených otázek zněla "ano" nebo pokud se Vám e-mail zdá podezřelý z jiných důvodů, **neměli byste ho otevírat** nebo klikat na soubory a odkazy, které obsahuje.

Zvláštní pozornost vyžadují takzvané phishingové e-maily.

Definice
Pojem **phishing** se skládá ze dvou slov — "password" (česky *heslo*) a "fishing" (česky *rybaření*). Phishing je snaha získat **cizí hesla** za pomoci falešných e-mailů.

Možná se Vám již někdy stalo, že Vám Vaše banka nebo obchod, který znáte, poslala podobný **neobvyklý e-mail**. Ve většině případů Vás e-mail informuje o tom, že údaje k Vašemu účtu byly

ztraceny, že Vám vypršela platnost hesla nebo že je z důvodu aktualizace naléhavě vyžadována nová identifikace. V e-mailu se také příhodně nachází **odkaz na webovou stránku společnosti.** Stránka se **velmi podobá** té skutečné, jedná se však o **podvrh**. Zadáním svých přístupových údajů poskytnete útočníkům přístup k Vašemu účtu a tím si způsobíte újmu.

Tip
Nikdy neodpovídejte na e-maily, které Vás žádají o sdělení přístupových údajů. Seriózní společnost by Vás o něco takového nikdy nežádala. Pokud si stále nejste jisti, zkuste údajného odesílatele kontaktovat po telefonu!

Následující opatření Vám mohou pomoci **snížit rizika** při e-mailové komunikaci:

- Zapněte si **zobrazení přípon souborů** (např. .docx, .exe). Tohle Vám pomůže lépe rozpoznat škodlivé programy zaslané v příloze e-mailu.
- Chcete-li zabránit spuštění aktivního obsahu v e-mailovém klientu, upravte si vhodně nastavení zabezpečení. Můžete tak například zamezit **nechtěnému malwaru**, aby se při otevření e-mailu spustil.
- **Než podezřelé přílohy otevřete, uložte si je** a zkontrolujte je pomocí antivirového programu.

1.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_01_01: Dokážete vysvětlit pojem falešný e-mail.

Zadání: Co znamená pojem "falešný e-mail"?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Falešné e-maily jsou nechtěné e-maily, které často obsahují v příloze malware.
- Falešné e-maily často obsahují nepravdivé nebo lživé informace.
- Falešné e-maily pravděpodobně nepocházejí od údajného odesílatele.
- Falešné e-maily jsou e-maily, které nemají žádný obsah. Tyto prázdné e-maily bývají zaslány buď úmyslně nebo omylem.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_01_02: Dokážete vyjmenovat znaky škodlivého e-mailu.

Zadání: Při kontrole doručené pošty si všimnete, že máte plno nových e-mailů. Který z následujících příkladů lze označit za falešný e-mail?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Je Vám slíbena velká odměna.
- Naléhavá žádost o změnu Vašich přístupových údajů.
- V e-mailu chybí předmět.
- V předmětu e-mailu se nachází "poslední výzva".
- E-mail obsahuje větší množství pravopisných chyb.
- E-mail byl automaticky přesunut do složky spamu.
- E-mail byl poslán v časných ranních hodinách.

Cvičení /VÍCE MOŽNOSTÍ/

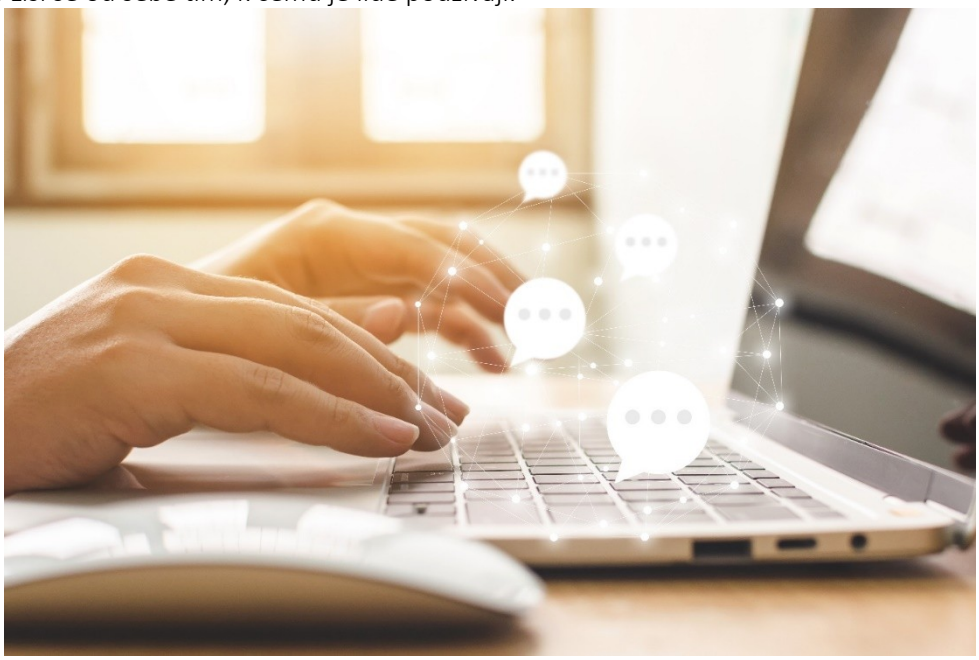
Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_01_03: Dokážete vyjmenovat opatření, která Vám mohou pomoci snížit rizika při e-mailové komunikace.

Zadání: Která opatření Vám mohou pomoci snížit rizika plynoucí z e-mailové komunikace.
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Zapněte si zobrazení přípon souborů (např. .docx, .exe).
- Vypněte si zobrazení přípon souborů.
- Vhodně si upravte nastavení zabezpečení, abyste zabránili spuštění aktivního obsahu v e-mailovém klientu.
- Zkontrolujte podezřelé přílohy pomocí antiviru.
- Své uživatelské údaje sdělujte pouze společnostem, které dobře znáte.

2.Fóra a chatovací místnosti

Fóra a **chatovací místnosti** jsou dalším oblíbeným způsobem komunikace a výměny informací na internetu. Liší se od sebe tím, k čemu je lidé používají.



Definice
Zatímco chatovací místnosti se zaměřují na komunikaci mezi lidmi **v reálném čase,** fóra jsou vhodnější pro **diskuze, při kterých nemusí být všichni zúčastnění online ve stejnou dobu.** Fóra jsou většinou lépe organizovaná a diskuze v nich jsou rozděleny do tzv. vláken, která jsou regulována moderátory.

Chatovací místnosti a fóra umožňují uživatelům výměnu textových zpráv a často i výměnu fotografií, videí, odkazů nebo souborů. Některé chatovací místnosti navíc podporují užití mikrofonu nebo webkamery ke komunikaci mezi uživateli.

Abyste se mohli aktivně účastnit komunikace na fóru nebo v chatovací místnosti, je potřeba **zaregistrovat se za pomoci platné e-mailové adresy**. Tím lze například předejít spamu. Kromě toho mají i moderátoři možnost vyloučit nebo zablokovat uživatele, pokud se chovají nevhodně. Užití těchto komunikačních médií však může vést k různým rizikům a hrozbám, jako jsou například:

- **Malware nebo odkazy na phishingové stránky:** Se všemi soubory a odkazy zveřejněnými na fórech by se tedy mělo zacházet opatrně.
- Hackování účtů nebo předstírání identity: tímto způsobem Vás mohou lidé snadno oklamat – za **účtem se může skrývat někdo úplně jiný**, než za koho se vydává.
- Komunikace na fórech a v chatovacích místnostech je většinou **nešifrovaná**, takže vše, co se rozhodnete napsat a sdílet s ostatními, si může kdokoliv přečíst. Profesionálním hackerům navíc nedělá žádný problém se dostat i k Vašim soukromým zprávám.

Nedokážete se bez fór a chatovacích místností obejít a zajímá Vás, co můžete udělat, abyste se vyhnuli bezpečnostním rizikům? Mějte na paměti následující body:

- Neotevírejte bezmyšlenkovitě všechny soubory, které Vám někdo zaslal.
- Nikdy nesdělujte osobní a citlivé údaje osobám, které neznáte.
- **Nikdy nikomu nepovolujte přístup k Vašemu počítači**

Příklad
Máte problém s počítačem a hledáte radu od odborníka v nějakému chatu nebo na fóru. Ozve se Vám údajný odborník a chce od Vás, abyste mu poskytli vzdálený přístup k Vašemu počítači.

- Přečtěte si **obecné zásady a podmínky** a **obecná nařízení o ochraně osobních údajů** (GDPR) komunikační služby, kterou používáte, a obeznamte se s tím, co se stane s Vašimi údaji a informacemi – zda jsou prodány, skladovány nebo šifrovány.
- **Blokujte si uživatele,** které neznáte nebo kteří Vás obtěžují. Případné urážky, sexuální obtěžování, vydírání nebo výhrůžky nahlaste policii.
- Mějte na paměti **autorské právo:** neměli byste bez souhlasu autora rozesílat obrázky nebo soubory, které jste sami nevytvořili.
- Při **randění s neznámým člověkem**, kterého znáte pouze z fóra nebo chatu, **buďte** vždy **opatrní**. Nikdy si nemůžete být stoprocentně jisti, že danou osobu znáte – poskytnuté informace mohou být falešné nebo vymyšlené.

2.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_02_01: Dokážete vysvětlit, co je to fórum a chatovací místnost a jak se od sebe liší.

Zadání: Co si představíte pod pojmem chatovací místnost a co pod pojmem fórum? Jak se tyto dva komunikační nástroje od sebe liší?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Chatovací místnosti jsou vhodnější pro diskuze, při kterých nemusí být všichni zúčastnění online ve stejnou dobu.
- Fóra jsou pro komunikaci v reálném čase vhodnější než chatovací místnosti.

- Textové zprávy lze posílat jak v chatovacích místnostech, tak na fórech. Dále je často možné posílat si navzájem fotografie, videa, odkazy nebo soubory.
- Chatovací místnosti jsou pro komunikaci v reálném čase vhodnější než fóra.
- Na rozdíl od fór, kde musíte uvést své pravé jméno, v chatovacích místnostech lze komunikovat anonymně nebo pod pseudonymem.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_02_02: Dokážete vyjmenovat možná rizika komunikace prostřednictvím fór a chatovacích místností.

Zadání: Fóra a chatovací místnosti jsou oblíbeným způsobem komunikace na internetu. Jaká rizika však z jejich užívání plynou?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Napadení škodlivým softwarem po otevření souboru, který někdo sdílel na fóru nebo v chatovací místnosti.
- Přesměrování na phishingovou stránku po rozkliknutí sdíleného odkazu.
- Komunikace na fórech je nákladná.
- Někdo se Vás pokusí oklamat falešnou identitou.
- Ke zprávám, které pošlete, má tajně přístup třetí strana.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_02_03: Dokážete vyjmenovat opatření, která Vám mohou pomoci snížit rizika při komunikaci na fórech a v chatovacích místnostech.

Zadání: Která z následujících opatření Vám mohou pomoci snížit rizika, kterým jste vystaveni na fórech nebo v chatovacích místnostech?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Seznamte se s obecnými podmínkami a zásadami a s obecným nařízením o ochraně osobních údajů.
- Zablokujte si uživatele, které neznáte.
- Sdílejte pouze fotografie a soubory, které jste nevytvořili.
- Přístup k Vašemu počítači povolte pouze osobám, které mají důvěryhodné uživatelské jméno a profilový obrázek.
- Neotevírejte bezmyšlenkovitě všechny soubory, které obdržíte.

3. Komunikace na sociálních sítích

Navozený pocit anonymity při užívání sociálních sítí může vést k lehkomyslnému zacházení s údaji a informacemi. To má za následek větší zranitelnosti sociálních sítí a jejich uživatelů a oblibu útočníků se na ně zaměřovat.

Při užívání sociálních sítí byste měli brát v úvahu následující body:

- Nikdy nerozebírejte osobní či důvěrné informace na veřejných místech na internetu. Zveřejnění bezohledného či neprokazatelného tvrzení pro Vás může mít právní následky.
- Každá sociální síť umožňuje upravit nastavení soukromí pomocí filtrů tak, aby jen určitá skupina lidí měla přístup k Vašim osobním údajům. Úprava nastavení Vám nezabere více než pár minut, a navíc nikdy nebudete muset řešit situaci, kdy na Vaši soukromou narozeninovou oslavu dorazí stovky nezvaných hostů.
- Chcete mít v přátelích na sociálních sítích co nejvíce lidí? Buďte obezřetní a mějte na paměti staré dobré přísloví: „Představ mi své přátele a já ti řeknu, kdo jsi". **Nekritické přijímání žádostí o přátelství může mít neblahý dopad na Váš život**, například v případě, že hledáte zaměstnání. Spousta zaměstnavatelů si prověřuje uchazeče na sociálních sítích a na základě zjištěných skutečností se rozhodne o jejich přijetí či nepřijetí.
- Vždy zkontrolujte nastavení soukromí na sociálních sítích.
- Mějte na paměti, že se na sociálních sítích vystavujete velkému **riziku oklamání**. Pachatelé záměrně poskytují svým obětem zavádějící nebo potenciálně nebezpečné informace ve snaze oklamat je nebo manipulovat s nimi.

Důležité
Pokud se setkáte s nevhodným užíváním sociálních sítí nebo nevhodným chováním na nich, můžete a měli byste tento nález nahlásit poskytovateli služby nebo jiným příslušným orgánům.

3.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_03_01: Dokážete popsat, na co si při komunikaci na sociálních sítích dávat pozor a vyvarovat se tak nechtěným následkům.

Zadání: Na co byste si měli při užívání sociálních sítí dávat pozor, abyste se vyhnuli nežádoucím důsledkům?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Více přátel na sociální sítí znamená větší oblíbenost a popularitu.
- Vždy zkontrolujte nastavení soukromí na sociálních sítích.
- Nevěřte všemu, co se na sociálních sítích dozvíte.
- Chcete o někom, koho nemáte rádi, napsat nějaký nehezký komentář? Dejte si pozor, abyste tak neučinili pod svým skutečným jménem, zvláště pokud chcete použít sprostá slova. Takto zůstanete anonymní a nemusíte se obávat žádných následků.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Informační tok a komunikace na internetu_03_02: Dokážete vysvětlit, jak se zachovat, pokud se stanete svědkem přestupku či zneužití na sociálních sítích.

Zadání: Projíždíte si zeď na svém účtu na sociální síti. S hrůzou zjistíte, že někdo přidal video, ve kterém skupina teenagerů psychicky i fyzicky týrá mladou dívku. Co uděláte?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Svůj nález nahlásíte poskytovateli služby (např. Facebooku).
- Bohužel neexistuje nic, co byste mohli udělat. Je možné, že video ani není skutečné. Raději ho ignorujte, abyste neohrozili sami sebe.
- Svůj nález nahlásíte policii.
- Neznáte ani oběť ani útočníky, takže nejste schopni poskytnout příslušným osobám žádná jména. Tedy nemá smysl, abyste zasahovali.

Zdroje

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/chat/

onlinesicherheit.gv.at: https://www.onlinesicherheit.gv.at/gefahren_im_netz/soziale_medien/gefahren/250080.html

securitymetrics.com: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

ftc.gov: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

smallbusiness.com: https://smallbusiness.chron.com/differences-between-chat-rooms-forums-71296.html

socialnomics.net: https://socialnomics.net/2017/11/08/chatting-online-risks-the-tips-to-stay-safe/

getsafeonline.org: https://www.getsafeonline.org/social-networking/chatrooms/

cybersecurity.edu: https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/social-media

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

Zapamatujte si

Shrnutí

E-mail je nejužívanějším komunikačním prostředkem na internetu, což bohužel také poskytuje široký prostor pro **podvodné a falešné e-maily**. Falešným e-mailem rozumíme nežádoucí e-mail, který obsahuje škodlivé, nepravdivé nebo zavádějící informace. Často je například **v přílohách** těchto e-mailů skryt **malware**.

Abyste těmto falešným e-mailům nenaletěli, je **nutná ostražitost**. S e-maily, které Vám slibují velkou výhru nebo Vás žádají o sdělení důvěrných informací, byste měli zacházet opatrně. To stejné platí pro e-maily obsahující popudlivé výrazy jako "Váš bankovní účet byl zablokován" nebo e-maily s velkým množstvím pravopisných či gramatických chyb.
Zvlášť obezřetní byste měli být, pokud přijdete do styku s **phishingovým e-mailem.** Jedná se o falešný e-mail, který má za úkol získat Vaše hesla. Abyste se těmto rizikům vyhnuli, stáhněte si podezřelé přílohy, než je otevřete, a zkontrolujte je pomocí antivirového programu.

Ani užívání **fór nebo chatovacích místností** není stoprocentně bezpečné. Při jejich používání se vystavujete riziku zamoření Vašeho počítače malwarem nebo nechtěnému přesměrování na phishingovou stránku bezmyšlenkovitým rozkliknutím odkazu či souboru, který někdo sdílel. Dále se můžete setkat s osobami s falešnou identitou nebo nechtěným čtením Vašich zpráv třetí stranou. Důležité je důkladně se **seznámit s nařízením o ochraně osobních údajů** při komunikaci na internetu a nikdy **nesdělovat osobní či citlivé informace** v chatovacích místnostech nebo na fórech.

Vše výše zmíněné platí i pro užívání **sociálních sítí**. Zvláště rizika jako oklamání falešnou identitou nebo vědomé či nevědomé šíření **nepravdivých informací** jsou velmi častá. Pokud se setkáte s nevhodným užíváním sociálních sítí nebo nevhodným chováním na nich, **můžete a měli byste tento nález nahlásit** poskytovateli služby nebo jiným příslušným orgánům.

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

Správné odpovědi

Zadání: Co znamená pojem "falešný e-mail"?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Falešné e-maily jsou nechtěné e-maily, které často obsahují v příloze malware.**
- **Falešné e-maily často obsahují nepravdivé nebo lživé informace.**
- **Falešné e-maily pravděpodobně nepocházejí od údajného odesílatele.**
- Falešné e-maily jsou e-maily, které nemají žádný obsah. Tyto prázdné e-maily bývají zaslány buď úmyslně nebo omylem.

Zadání: Při kontrole doručené pošty si všimnete, že máte plno nových e-mailů. Který z následujících příkladů lze označit za falešný e-mail?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Je Vám slíbena velká odměna.**
- **Naléhavá žádost o změnu Vašich přístupových údajů.**
- V e-mailu chybí předmět.
- **V předmětu e-mailu se nachází "poslední výzva".**
- **E-mail obsahuje větší množství pravopisných chyb.**
- **E-mail byl automaticky přesunut do složky spamu.**
- E-mail byl poslán v časných ranních hodinách.

Zadání: Která opatření Vám mohou pomoci snížit rizika plynoucí z e-mailové komunikace.
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Zapněte si zobrazení přípon souborů (např. .docx, .exe).**
- Vypněte si zobrazení přípon souborů.
- **Vhodně si upravte nastavení zabezpečení, abyste zabránili spuštění aktivního obsahu v e-mailovém klientu.**
- **Zkontrolujte podezřelé přílohy pomocí antiviru.**
- Své uživatelské údaje sdělujte pouze společnostem, které dobře znáte.

Zadání: Co si představíte pod pojmem chatovací místnost a co pod pojmem fórum? Jak se tyto dva komunikační nástroje od sebe liší?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Chatovací místnosti jsou vhodnější pro diskuze, při kterých nemusí být všichni zúčastnění online ve stejnou dobu.
- Fóra jsou pro komunikaci v reálném čase vhodnější než chatovací místnosti.
- **Textové zprávy lze posílat jak v chatovacích místnostech, tak na fórech. Dále je často možné posílat si navzájem fotografie, videa, odkazy nebo soubory.**
- **Chatovací místnosti jsou pro komunikaci v reálném čase vhodnější než fóra.**

- Na rozdíl od fór, kde musíte uvést své pravé jméno, v chatovacích místnostech lze komunikovat anonymně nebo pod pseudonymem.

Zadání: Fóra a chatovací místnosti jsou oblíbeným způsobem komunikace na internetu. Jaká rizika však z jejich užívání plynou?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Napadení škodlivým softwarem po otevření souboru, který někdo sdílel na fóru nebo v chatovací místnosti.**
- **Přesměrování na phishingovou stránku po rozkliknutí sdíleného odkazu.**
- Komunikace na fórech je nákladná.
- **Někdo se Vás pokusí oklamat falešnou identitou.**
- **Ke zprávám, které pošlete, má tajně přístup třetí strana.**

Zadání: Která z následujících opatření Vám mohou pomoci snížit rizika, kterým jste vystaveni na fórech nebo v chatovacích místnostech?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Seznamte se s obecnými podmínkami a zásadami a s obecným nařízením o ochraně osobních údajů.**
- **Zablokujte si uživatele, které neznáte.**
- Sdílejte pouze fotografie a soubory, které jste nevytvořili.
- Přístup k Vašemu počítači povolte pouze osobám, které mají důvěryhodné uživatelské jméno a profilový obrázek.
- **Neotevírejte bezmyšlenkovitě všechny soubory, které obdržíte.**

Zadání: Na co byste si měli při užívání sociálních sítí dávat pozor, abyste se vyhnuli nežádoucím důsledkům?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Více přátel na sociální síti znamená větší oblíbenost a popularitu.
- **Vždy zkontrolujte nastavení soukromí na sociálních sítích.**
- **Nevěřte všemu, co se na sociálních sítích dozvíte.**
- Chcete o někom, koho nemáte rádi, napsat nějaký nehezký komentář? Dejte si pozor, abyste tak neučinili pod svým skutečným jménem, zvláště pokud chcete použít sprostá slova. Takto zůstanete anonymní a nemusíte se obávat žádných následků.

Zadání: Projíždíte si zeď na svém účtu na sociální síti. S hrůzou zjistíte, že někdo přidal video, ve kterém skupina teenagerů psychicky i fyzicky týrá mladou dívku. Co uděláte?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Svůj nález nahlásíte poskytovateli služby (např. Facebooku).**

- Bohužel neexistuje nic, co byste mohli udělat. Je možné, že video ani není skutečné. Raději ho ignorujte, abyste neohrozili sami sebe.
- Svůj nález nahlásíte policii.
- Neznáte ani oběť ani útočníky, takže nejste schopni poskytnout příslušným osobám žádná jména. Tedy nemá smysl, abyste zasahovali.