Počítačová bezpečnost, phishing a spam

Účastníci se seznámí s typy lidí, kteří mají v online prostředí nekalé úmysly a můžou se pokusit využít chyb zabezpečení k získání informací o lidech. Účastníci budou umět popsat rizika vyskytující se v online prostředí a naučí se, jak se chovat bezpečněji. Budou umět rozpoznat spam a vysvětlit, kdo může žádat o jejich heslo.

Materiály

- Podklady Spam

Rizika v online prostředí

1. část

Řekněte studentům

Při používání internetu na vás můžou číhat určitá rizika. Stačí, když navštívíte určitou webovou stránku, komunikujete online nebo si stahujete data. Když procházíte web, někdy se může stát, že navštívené webové stránky, lidé ve stejné síti nebo dokonce třetí strany odhalí vaši polohu nebo jiné informace o vás.

Zeptejte se studentů

Kdo může zneužít chyby v zabezpečení v online prostředí k tomu, aby si zobrazil vaše osobní údaje?

1. Může jít například o kyberzločince nebo vykonavatele vládního dohledu.

Řekněte studentům

Když procházíte web, kyberzločinci můžou data o vás sbírat stejným způsobem jako poskytovatelé internetu. Pokud chcete míru tohoto rizika snížit, musíte mezi vámi a navštěvovanými weby používat zabezpečené připojení. Spousta webů se snaží sledovat vaše vzorce používání napříč platformami, a to bez ohledu na připojení. Můžou sledovat váš prohlížeč, polohu a další vzorce používání, a vysledovat tak, kdo jste.

Zeptejte se studentů

Proč by se mohli kyberzločinci pokoušet o přístup k vašim informacím na internetu? O jaké informace lidem jde? Proč by web, ke kterému nejste přihlášení, chtěl zjistit, kdo jste?

1. Důvodem je možnost získání jakýchkoli osobních údajů a informací, které se dají prodat či zpeněžit.

Ví někdo z vás, co je to malware? A co vlastně dělá?

Řekněte studentům

Malware je škodlivý kód, který se vám tajně spustí v počítači. Některý malware může sbírat data z jakéhokoli místa ve vašem místním počítači – ať už z pevného disku, nebo z prohlížeče. Také může hackerům umožnit, aby převzali kontrolu nad vaším počítačem a používali ho ke svému prospěchu. Většinou ale malware pracuje na

jednodušším principu. Může jít třeba o weby vydávající se za bezpečné portály (například bankovní portál) nebo rozšíření, které vám v prohlížeči za účelem vydělávání peněz zobrazuje reklamy.

Zeptejte se studentů

Co můžete dělat, abyste se před malwarem, špehováním a sledováním ochránili?

Řekněte studentům

Buďte obezřetní při klikání na odkazy, reklamy nebo příspěvky na sociálních médiích. Odpovídá obsah na URL adrese tomu, co jste očekávali? Dostanete se na stejnou stránku, když její název znovu sami napíšete nebo zkusíte daný web vyhledat? Je vhodné, aby byla každá přihlašovací stránka důležitého účtu (jako je účet na Googlu, Facebooku nebo Twitteru či bankovní účet) chráněná protokolem SSL nebo TLS. Protokoly SSL a TLS hackerům působícím ve stejné síti znesnadňují, aby vám posílali falešné weby potom, co zadáte správnou URL adresu. Pokud nejsou tyto protokoly použity, je to pro hackera hračka.

Pokud se na platformách vyskytne chyba kódování, některé weby dokážou spustit kód, který jim umožní přístup k vašim osobním informacím nebo online účtům. Vaše účty pak můžou využít k posílání spamu dalším lidem.

Stahujte a instalujte jen software pocházející z důvěryhodných zdrojů. Buďte velmi obezřetní při stahování spustitelných souborů (soubory s příponou .exe, .pkg, .sh, .dll nebo .dmg). Spustitelné soubory jsou jakékoli soubory, které provedou určitou akci. Někdy se může jednat o nekalé akce. Někdo může například vytvořit spustitelný soubor, jehož cílem je vymazat něčí pevný disk nebo nainstalovat falešný prohlížeč. Právě proto byste měli instalovat jen obsah pocházející z důvěryhodných zdrojů.

Před spouštěním malwaru vás může ochránit antivirový software. Někdy může být antivirový software už předinstalovaný v počítači (například Microsoft Security Essentials pro Windows). Některé operační systémy (třeba systémy na počítačích Apple) disponují nastavením zabezpečení, které blokuje instalaci softwaru pocházejícího z nedůvěryhodných zdrojů. Pokud chcete toto nastavení vypnout, dobře si to rozmyslete.

Také můžete použít rozšíření prohlížeče, která můžou zajišťovat například blokování pluginů usnadňujících webům rozpoznání a sledování vaší osoby. Stejný plugin ale může blokovat rovněž určité funkce webů (například možnost sledování videí). Je jen na vás, jestli se rozhodnete rozšíření prohlížeče nainstalovat. Pokud ho používat nechcete, je třeba dobře zvážit rizika online zabezpečení, která z tohoto rozhodnutí plynou. Možná vám hlavou běží tyto otázky: Jak moc je nevhodné, aby někdo sledoval moji aktivitu? Jakou hodnotu má moje soukromí? Opravdu musím tento obsah vidět (například v případě, že rozšíření prohlížeče zablokuje plugin vykreslující video)?

Nástroje pro zabezpečení

1. část

Interakce ve třídě

Poznámka: Část obsahu v rámci této aktivity už byla probraná v aktivitě číslo 1 s názvem Rizika v online prostředí. Pokud už máte za sebou aktivitu číslo 1, je čistě na vás, jestli budete chtít tento materiál projít znovu, nebo jestli ho přeskočíte.

Zeptejte se studentů

Víte, jestli jste při používání internetu v bezpečí?

Řekněte studentům

Bez přijetí preventivních opatření je obtížné (ne-li nemožné) se před riziky v online prostředí popsanými v předchozí části úspěšně chránit.

Navíc je třeba mít na paměti, že se na internetu neustále objevují nová rizika, před kterými byste se měli mít na pozoru.

Zeptejte se studentů

Co může někdo udělat, když vás přesvědčí, že je jeho web jedním z webů, které jsou pro vás důležité?

Existují nástroje, které vám můžou pomoct těmto rizikům předcházet nebo je zmírnit. Znáte některé?

Řekněte studentům

HTTPS je standardní protokol, který používají weby k šifrování dat přenášených přes internet. Šifrování může zabránit tomu, aby si data z vašeho připojení zobrazila třetí strana. Poskytuje další vrstvu zabezpečení a dá se použít v jakémkoli prohlížeči. Stačí před příslušnou URL adresu přidat “https://” (například https://www.mojestránka.com). Ovšem ne všechny weby protokol HTTPS podporují.

1. Citlivé informace (jako třeba hesla, údaje o platebních kartách apod.) byste měli zadávat jenom na weby s předponou HTTPS://.

2. Můžete použít softwarové nástroje, které zajistí, abyste používali protokol HTTPS, kdykoli je to možné.

3. Většina hlavních prohlížečů má bezpečnostní indikátor vedle adresního řádku. Má podobu symbolu zámku a označuje, že se jedná o zabezpečené připojení

HTTPS.

4. Ovšem bohužel ani protokol HTTPS nezaručuje bezpečnost, protože ho podporují i některé škodlivé weby. Protokol HTTPS zabezpečuje připojení samotné, ale nemůže zaručit, že se jedná o poctivý web.

Technologie s názvem Secure Sockets Layer (SSL) a Transport Layer Security (TLS) poskytují zabezpečení HTTPS. Protokoly SSL a TLS používají digitální šifrovací klíče, které fungují podobně jako skutečné klíče. Pokud byste kamarádovi napsali na papír nějaké tajemství, mohl by si ho přečíst každý, kdo papír najde. Představte si, že místo toho kamarádovi osobně předáte kopii klíče a potom své tajemství pošlete v zamčené krabici, která se dá tímto klíčem odemknout. Pokud by se krabice dostala do rukou někomu jinému, bylo by pro daného člověka těžké se k tajemství dostat, protože by neměl klíč. A pokud by se někdo pokusil vaši krabici vyměnit za podobnou, všimli byste si, že není vaše, protože by do ní nepasoval váš klíč. Protokoly SSL a TLS fungují na stejném principu, ale na webu.

Indikátory zabezpečení prohlížeče budou také poskytovat informace o certifikátu rozšířeného ověření (EV). EV certifikáty dostanou weby, které svoji identitu ověří u certifikační autority. V prohlížečích má někdy indikátor rozšířeného ověření podobu názvu webu nebo registrujícího subjektu a najdeme ho vedle adresního řádku prohlížeče. EV certifikáty dostanou weby, které svoji identitu ověří u certifikační autority. V prohlížečích má někdy indikátor rozšířeného ověření podobu názvu webu nebo registrujícího subjektu a najdeme ho vedle adresního řádku prohlížeče. Pokud nemáte důvěru k obsahu určitého webu, můžete zkontrolovat, jestli URL adresa v certifikátu odpovídá URL adrese v prohlížeči. Stačí kliknout na tlačítko „Zobrazit certifikát“. (Může být užitečné ukázat na projekčním plátně, jak možnost „Zobrazit certifikát“ najít.) Jak se k této možnosti dostanete, závisí na tom, jaký prohlížeč používáte. Například v prohlížeči Chrome u možnosti „Zobrazit“ klikněte na „Vývojář“ a pak na „Nástroje pro vývojáře“. V části „Nástroje pro vývojáře“ klikněte na kartu „Zabezpečení“ a pak na „Zobrazit certifikát“.

Jedním z pravidel je nespouštět software z nedůvěryhodných zdrojů. V návštěvě nedůvěryhodných stránek a stahování malwaru vám může zabránit také antivirový software.

K phishingovým útokům dochází především přes e-mail. Odesilatel takových e-mailů se vydává za věrohodný subjekt. V e-mailu vás útočník požádá o vaše heslo, které máte buď poslat e-mailem, nebo ho zadat na falešném webu. Filtry nevyžádané pošty můžou zařídit, aby se vám některé tyto e-maily vůbec nezobrazily v doručené poště. Filtry nevyžádané pošty můžete sami zlepšovat. Stačí, abyste veškeré podezřelé e-maily v doručené poště označovali jako spam.

Zeptejte se studentů

Jak můžete předejít neúmyslnému stahování souborů, které jsou pro váš počítač

škodlivé?

Řekněte studentům

Vždycky důkladně zkontrolujte, jestli se pokoušíte stáhnout soubory z důvěryhodných webů. Pokud narazíte na neznámé e-mailové přílohy nebo vyskakovací okna a chybové zprávy, buďte mimořádně opatrní a kliknutí na ně si opravdu důkladně promyslete. Také se vyplatí nainstalovat si na počítač ověřený antimalwarový program.

Sdílení hesel

1. část

Zeptejte se studentů

Kdy je podle vás sdílení hesla s dalšími lidmi v pořádku?

1. Mezi možné odpovědi patří sdílené účty (například ve službě Netflix).

Jaká rizika plynou ze sdílení hesla?

1. Pokud vaše heslo získá člověk s nekalými úmysly, může napadnout váš účet. Když budete heslo sdílet, zvýší se pravděpodobnost, že se někdo k vašemu účtu dostane. Pokud stejné heslo používáte i na dalších webech, může útočník získat přístup také k nim.

Řekněte studentům

Obecně platí, že byste svá hesla neměli s nikým sdílet. Heslo zadávejte jen v aplikaci, do které se chcete přihlásit. Jak už jsme si říkali, cílem phishingu je lstí vás přimět ke sdílení hesla.

Někdy vás ale můžou určití lidé ke sdílení hesla přímo vyzvat. Odůvodní to tak, že se potřebují dostat k vašemu účtu, protože může být ohrožen. Někteří z nich můžou mít dobré úmysly. Může třeba jít o vašeho přítele, který vám chce pomoct vyřešit nějaký problém s účtem. Přesto ale není moudré s někým své heslo sdílet. Obzvlášť to platí v případě, že stejné heslo používáte pro víc účtů. Pokud se chystáte heslo sdílet, ujistěte se, že ho nepoužíváte nikde jinde. Ke sdílení přístupu pomocí hesla použijte správce hesel.

Lidé, kteří od vás požadují heslo, můžou být dospělí, které znáte a důvěřujete jim (třeba rodiče, učitelé nebo zaměstnavatel). I když tyto lidi dobře znáte a důvěřujete jim, pro obě strany bude nejlepší, když spolu proberete, proč vaše heslo chtějí a co s ním hodlají dělat. Hlavně dospělých lidí, které nepatří do vašeho rodinného kruhu, byste se měli přímo zeptat, jestli se jejich žádost o poskytnutí hesla zakládá na nějakém zákoně nebo předpisu.

Obzvlášť v případě, že vás o heslo žádá dospělý, která není vaším příbuzným a neznáte ho osobně (například pracovník bezpečnostních složek), byste se měli daného člověka slušně a napřímo zeptat, na jakém zákoně nebo předpisu se jeho žádost zakládá. Pokud vás o vaše hesla pro sociální média požádá příslušník policie nebo státní úředník, zůstaňte v klidu a chovejte se zdvořile. Zeptejte se daného člověka, proč vás o heslo žádá a na základě kterého zákona nebo předpisu má

podle svého mínění právo po vás takovou informaci požadovat.

V závislosti na okolnostech žádosti ze strany rodiče nebo opatrovníka, učitele, zaměstnavatele, pracovníka bezpečnostních složek, státního úředníka nebo jiného dospělého se může stát, že budete muset své heslo sdělit. Mezi okolnosti, kdy se na vás může vztahovat povinnost svá hesla sdělit, patří situace, kdy vám tuto povinnost ukládá zákon nebo předpis. Můžete se také řídit vlastním úsudkem, který vám může říkat, že výhody plynoucí z poskytnuté pomoci převažují nad riziky souvisejícími ze sdílení hesla.

Pokud vás někdo dospělý požádá o vaše hesla, ale tato žádost je pro vás z jakéhokoli důvodu nepříjemná, obraťte se nejlépe ještě předtím, než odpovíte, na rodiče, opatrovníka nebo jiného dospělého člověka, kterému důvěřujete.

Zeptejte se studentů

Za jakých okolností byste heslo na internetu měli sdílet?

1. Jen v případě, že vás k zadání hesla vyzve web, k němuž se chcete přihlásit. Nikdy své heslo nesdílejte nikde jinde. Neposílejte ho ani e-mailem, protože tento způsob komunikace většinou není šifrovaný ani zabezpečený.

Zadání

Podklady

Zadání

Rozdělte účastníky do skupin po dvou až třech. Rozdejte účastníkům podklady s názvem Spam. Pak nechte jednotlivé účastníky vypracovat vývojový diagram, pomocí něhož ostatním ukážou, jak rozpoznat spam a jestli by měli s konkrétními jedinci nebo skupinami lidí sdílet určité informace.

Řekněte studentům

Přečtěte jednotlivé scénáře a rozviňte diskuzi o tom, jestli jsou jednotlivé zprávy spam a jestli by měl uživatel s daným člověkem nebo skupinou lidí sdílet požadované informace.

Interakce ve třídě

Dejte účastníkům na práci deset minut. Potom skupiny požádejte, aby své poznatky sdílely s ostatními.

Zeptejte se studentů

Kdy byste měli své heslo sdílet prostřednictvím e-mailu?

Řekněte studentům

Obecně platí, že weby ani společnosti po uživatelích nepožadují, aby jim e-mailem posílali heslo. Své heslo byste takto nikdy nikomu neměli předávat, a to ani v případě, že vám zdroj připadá věrohodný. E-mailová komunikace není ve většině případů bezpečná.

2. část

Zadání

Vyzvěte účastníky, aby rozpustili vytvořené skupiny. Následující cvičení je totiž určené pro jednotlivce.

Dejte účastníkům na vytvoření vývojového diagramu patnáct minut.

Řekněte studentům

Na list papíru nakreslete vývojový diagram. Ukažte na něm účastníkům, jak identifikovat spam a jestli by měli s ostatními sdílet určité informace. Vývojový

diagram můžete podpořit konkrétní situací. Můžete použít buď některý ze scénářů z podkladů (pokud se rozhodnete některý z nich použít, napište jeho číslo nad vývojový diagram), nebo si vymyslet úplně nový. Pokud chcete použít vlastní scénář, stručně ho popište nad vývojovým grafem.

Dejte účastníkům na vytvoření vývojového diagramu patnáct minut.