DIGITAL ACCESS

DIGITAL SKILLS FOR PEOPLE LIVING IN THE 3RD AGE
Effective Digital Access to Public Services

Erasmus+

PROJEKT DIGITAL ACCESS

VZDĚLÁVACÍ MODUL

Středně pokročilá znalost online bezpečnosti

Vypracoval: AKLUB

Září 2018

Tento projekt je financován s podporou Evropské komise. Tato publikace odráží pouze názory autorů a Komise nemůže nést odpovědnost za jakékoli použití informací v ní obsažených.

Obsah

SHRNUTÍ....4
LEKCE 1- Zabezpečení připojení k internetu....6
Domácí bezdrátová síť....6
Krok 1. Změňte výchozí název domácí sítě....7
Krok 2. Ujistěte se, že jste pro zabezpečení bezdrátové sítě nastavili silné a jedinečné heslo....7
Krok 3. Zvyšte si zabezpečení WiFi aktivací síťového šifrování....8
Krok 4.Vypněte bezdrátovou domácí síť, když nejste doma....8
Krok 5. Kde máte doma router umístěný?....8
Krok 6. Pro zvýšení zabezpečení WiFi použijte silné heslo správce sítě....9
Krok 7. Změňte výchozí adresu IP v bezdrátovém routeru....9
Krok 8. Vypněte funkci DHCP na routeru....9
Krok 9. Vypněte vzdálený přístup....10
Krok 10. Udržujte software vašeho routeru vždy aktualizovaný....10
Krok 11. Firewall může pomoci zabezpečit vaši WiFi síť....10
Krok 12. Zvyšte ochranu zařízení nejčastěji připojených k domácí síti....10
Závěr....11
Instalujte si antivirový program....12
Vyhněte se podezřelým webovým stránkám....12
Nikdy neotvírejte přílohy e-mailů bez jejich screeningu....12
Nastavení automatického skenování....12
Sledujte, co stahujete 12
Aktualizujte, aktualizujte, aktualizujte!....13
Vždy mějte přehled....13
Vyhněte se cracknutému softwaru....13
Nainstalujte si firewall....13
Buďte připraveni....13
Ochrana proti malwaru....15
Instalujte si Anti-Spyware Software:....15
Jak vypadají skutečné malwarové emaily?....20

UČEBNÍ HODINY: [UČEBNÍ HODINY VŠECH LEKCÍ]
PRACOVNÍ VYTÍŽENÍ: [UČEBNÍ HODINY VŠECH LEKCÍ + CELKOVÝ ČAS NA CVIČENÍ]

SHRNUTÍ

Tento modul byl navržen tak, aby rozšířil základní znalosti uživatelů o online bezpečnosti, které by mohl použít nezasvěcený nebo začínající uživatel internetu. Hlavním cílem lekce je umožnit uživateli ochranu před počítačovými zločinci a udržet osobní údaje v bezpečí, což zajistí, že jeho online data a majetek nebudou ohroženy.

KLÍČOVÁ SLOVA

domácí bezdrátová síť, antivirový program, virus, malware, antispyware program, spyware

CÍLE MODULU

Činnosti /Dosažení		
Získání znalostí o internetové trestné činnosti zaměřené na jednotlivce a získání dovedností k identifikaci a vyhýbání se těmto činnostem.		
Znalosti	**Dovednosti**	**Kompetence**
Zabezpečení internetového připojení	Orientace v domácí bezdrátové síti Znalost jejího nastavení Znalost pravidel pro její bezpečnost	Schopnost nastavit a spravovat zabezpečení vaší domácí bezdrátové sítě
Antivirové programy	Znalost virů a potřeby antivirových programů Schopnost vybrat vhodný antivirový program Vědět, jak se vyhnout virům ve vašem počítači	Vědět, jak ochránit váš počítač před zavirováním

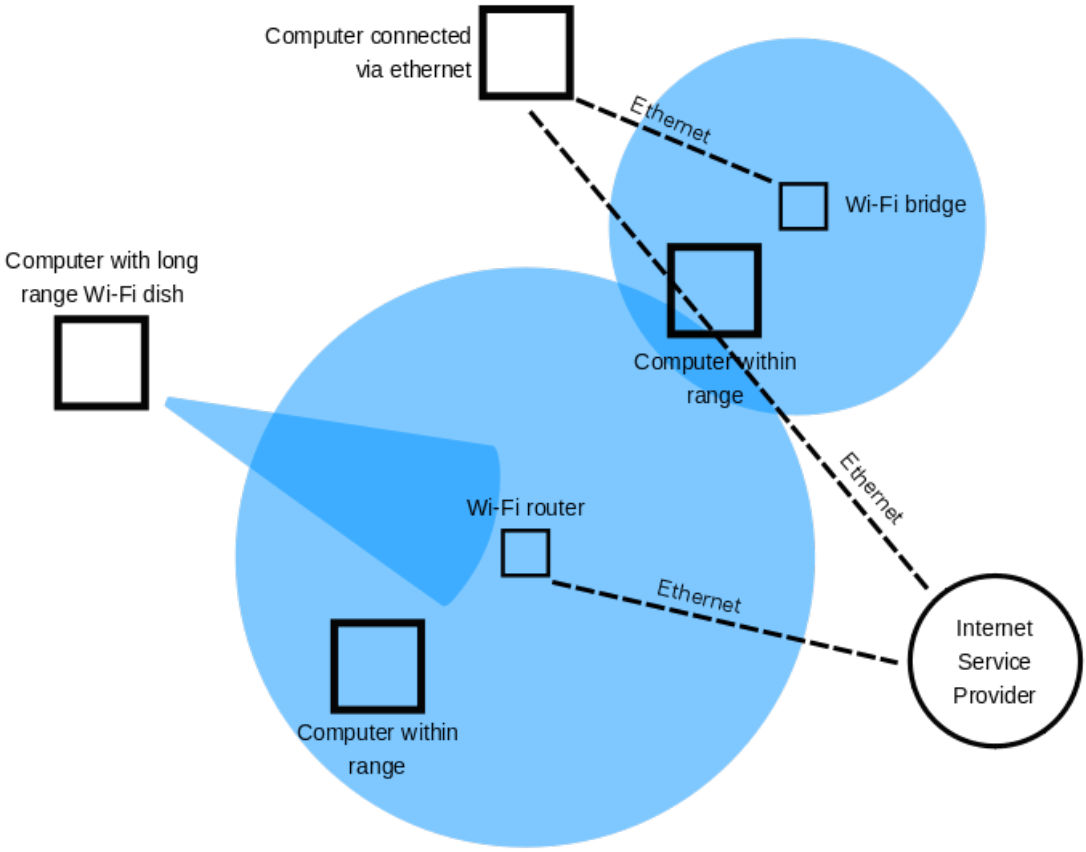
Malware	Pochopení malwaru a potřeby antimalwarových programů Být schopen vybrat si vhodný antimalwarový program Vědět, jak se vyhnout malwaru ve vašem počítači	Znalost toho, jak ochránit váš počítač vůči malwaru.

LEKCE 1- Zabezpečení připojení k internetu

Domácí bezdrátová síť

V několika jednoduchých slovech znamená základní domácí bezdrátová síť připojení internetového přístupového bodu, jako například kabelu od poskytovatele služeb internetu až po (bezdrátový) router, aby bylo umožněno velmi rychlé připojení více zařízení k síti.

V mnoha případech je to tak, že jakmile bezdrátový směrovač nainstalujeme a najdeme pro něho místo, tak na něho zapomeneme. Stačí, že jsou všechna naše zařízení nastavena a připojena prostřednictvím sítě WiFi a je to vše, na čem záleží, ne? Špatně!



Mnozí z vás si to asi neuvědomují, ale internetový router je jedním z nejdůležitějších zařízení v naší domácnosti. Je to vstupní brána k našemu přístupu k internetu a je také náchylná ke zneužívání kybernetickými zločinci, kteří se mohou dostat do našich zařízení a získat přístup do našeho systému.

Jediné opatření, které většina lidí používá k ochraně své domácí sítě je, že si nastaví heslo, aby zabránili sousedům a ostatním lidem v převzetí kontroly nad jejich daty. Ale pokud jde

o bezpečnost, musíme být důraznější a udělat víc než jen nastavit jednoduché heslo. Vážným rizikem je, že online pachatel může využít vaše špatná WiFi bezpečnostní opatření a „odposlouchávat“ váš provoz, aby získal citlivé informace nebo využil vaší sítě ke spuštění škodlivých útoků, jako jsou například útoky typu „Man-in-the-Middle“, network sniffing nebo krádež dat.

WiFi sítě jsou sice poměrně snadno ovladatelné a přístupné, ale nejsou to vždy BEZPEČNÉ sítě. WiFi přináší spoustu bezpečnostních problémů a stojí za to připomenout si Krack zranitelnost zjištěnou v protokolu Wireless Protected Access II (WPA2), která ovlivnila všechna zařízení připojená přes WiFi.

Z tohoto důvodu je učení, jak zabezpečit bezdrátovou domácí síť proti kyberzločincům, moudrý a chytrý krok. Vzhledem k tomu, kolik zařízení z internetů věcí, můžete vlastnit, je dobré se ujistit, že vaše síť je extra bezpečná a unese ještě větší váhu, i když může být občas péče o vaši kybernetickou bezpečnost únavným, ale nezbytným úkolem.

V této lekci se dozvíte, jak můžete lépe zabezpečit domácí síť a snížit možnost ohrožení vašich cenných dat.

Krok 1. Změňte výchozí název domácí sítě

Pokud chcete lépe zabezpečit svou domácí síť, první věc, kterou byste měli udělat, je změnit název sítě WiFi, známé také jako SSID (Service Set Identifier).

Zatímco pojmenování vaší WiFi poněkud provokativním názvem, jako je „Nedá se hacknout“, může občas selhat, jiná jména jako „toto není wifi“ nebo „létánínawifi“ jsou naprosto přijatelné.

Změna výchozího názvu WiFi ztěžuje zákeřným útočníkům poznat, jaký typ routeru máte. Pokud kyberzločinec zná výrobní název vašeho routeru, bude vědět, jaká je zranitelnost tohoto modelu, a budete se snažit toho zneužít.

Důrazně doporučujeme, abyste svou domácí síť nenazývali podobně jako „Honzova WiFi“. Nechcete přece, aby na první pohled věděli, která bezdrátová síť je vaše, když jsou zde pravděpodobně tři nebo čtyři sousední WiFi.

Nezapomeňte také, že zveřejnění přílišného množství osobních informací v názvu bezdrátové sítě, vás může vystavit operaci krádeže identity.

Zde je postupný a jednoduchý průvodce, který vysvětluje, jak snadno změnit název bezdrátové sítě.

Krok 2. Ujistěte se, že jste pro zabezpečení bezdrátové sítě nastavili silné a jedinečné heslo

Pravděpodobně víte, že každý bezdrátový router je přednastaven s výchozím uživatelským jménem a heslem, což je potřeba, abyste nejprve provedli instalaci a připojili se k routeru. Nejhorší na tom je že: pro hackery je snadné ho uhodnout, zejména pokud znají výrobce.

Proto obojí okamžitě změňte.

Dobré heslo pro bezdrátové připojení by mělo být nejméně 20 znaků dlouhé a musí obsahovat čísla, písmena a různé symboly.

Tento průvodce slouží k nastavení silného hesla pro vaši síť. Přátelé, kteří přijedou na návštěvu, si mohou stěžovat na neobvyklou délku vašeho hesla, což by je však mohlo odradit od zbytečné konzumace dat nudnými příspěvky na Facebooku nebo Instagramu.

Krok 3. Zvyšte si zabezpečení WiFi aktivací síťového šifrování

Bezdrátové sítě jsou dodávány s více jazyky šifrování, například WEP, WPA nebo WPA2.

Pro lepší porozumění této terminologii je WPA2 zkratkou pro WiFi Protected Access 2 a jedná se o bezpečnostní protokol a současný standard v oboru (sítě WPA2 jsou téměř všude) a šifruje provoz na sítích WiFi. Nahrazuje také starší a méně zabezpečené WEP (Wired Equivalent Privacy) a představuje upgrade původní technologie WPA (WiFi Protected Access). Od roku 2006 by všechny produkty certifikované WiFi měly používat zabezpečení WPA2.

WPA2 AES je také standardním bezpečnostním systémem, takže všechny bezdrátové sítě jsou s ním kompatibilní. Chcete-li v bezdrátovém směrovači povolit šifrování WPA2, použijte těchto šest kroků. Pokud používáte bezdrátový router TP-Link, zabezpečte si bezdrátovou síť.

Dobrou zprávou je, že WPA3 je již tady a nahradí WPA2. Aliance WiFi nedávno oznámila, že bude standardem bezdrátové sítě příští generace, jejímž cílem je vyřešit společný bezpečnostní problém: otevřené sítě WiFi. Dodává se s vylepšením zabezpečení a obsahuje sadu funkcí, které uživatelům a poskytovatelům služeb zjednodušují konfiguraci zabezpečení WiFi.

Krok 4.Vypněte bezdrátovou domácí síť, když nejste doma

Pro zabezpečení sítě doporučujeme v případě delšího období nepoužívání deaktivovat bezdrátovou domácí síť. Měli byste udělat totéž se všemi zařízeními, která používají kabely Ethernet nebo když nebudete doma.

Tímto způsobem zavíráte všechna okna příležitostí pro škodlivé hackery, kteří se k nim mohou pokusit získat přístup, když jste pryč.

Zde je několik výhod vypnutí bezdrátové sítě:

- **Bezpečnostní důvody - Vypnutí síťových zařízení minimalizuje šance, že se stanou terčem pro hackery.**
- **Přepěťová ochrana - Když vypnete síťové zařízení, snížíte také možnost poškození elektrickým proudem;**

• Redukce šumu - I když jsou moderní domácí sítě v těchto dnech mnohem tišší, deaktivace bezdrátové domácí sítě může vašemu domovu přinést klid.

Krok 5. Kde máte doma router umístěný?

Pravděpodobně jste na to v první chvíli nepomysleli, ale to, kde má WiFi místo ve vaší domácnosti může mít také dopad na vaši bezpečnost.

Bezdrátový router umístěte co nejblíže středu vašeho domu. Proč? Za prvé, bude poskytovat rovnocenný přístup k internetu ve všech místnostech vaší domácnosti. Zadruhé nechcete, aby dosah bezdrátového signálu dosahoval příliš daleko mimo váš domov, kde ho mohou snadno zachytit zákeřné osoby.

Z tohoto důvodu nedoporučujeme umístit bezdrátový směrovač do blízkosti okna, protože nic nebrání signálu, který jde mimo domov.

Krok 6. Pro zvýšení zabezpečení WiFi použijte silné heslo správce sítě

Chcete-li nastavit bezdrátový router, potřebujete obvykle vstoupit na online platformu nebo web, kde můžete provést několik změn nastavení sítě.

Většina routerů WiFi přichází s výchozími nastaveními, jako je „admin“ a „heslo“, které jsou pro zákeřné hackery tak snadné, že se do nich mohou dostat.

Věděli jste, že počet bezdrátových sítí za posledních 8 let dramaticky vzrostl? V roce 2010 bylo po celém světě 20 milionů WiFi sítí a za 8 let se tento počet zvýšil na 400 milionů.

Krok 7. Změňte výchozí adresu IP v bezdrátovém routeru

Změna výchozí IP adresy na méně běžnou je další věc, kterou byste měli zvážit, abyste lépe zabezpečili svou domácí síť a ztížili hackerům sledování.

Chcete-li změnit IP adresu routeru, postupujte takto:

1. Přihlaste se k routeru jako správce. Tyto základní kroky vás naučí, jak se snadno připojit k domácí síti jako správce. Typ adresního řádku obvykle vypadá jako http://192.168.1.1 nebo http://192.168.0.1

2. Jakmile jste tam, vložte na přihlašovací stránce uživatelské jméno a heslo;

3. Poté vyberte Síť> LAN, která je v menu na levé straně;

4. Změňte preferovanou adresu IP a klepněte na tlačítko Uložit.

Poznámka: Po změně adresy IP budete muset zadat novou adresu IP do panelu webového prohlížeče.

Můžete také změnit server DNS, který váš bezdrátový směrovač používá k filtrování internetového provozu, a tato lekce ukáže, jak to provést.

Krok 8. Vypněte funkci DHCP na routeru

Chcete-li zvýšit zabezpečení bezdrátové sítě, měli byste v routeru vypnout server DHCP (Dynamic Host Configuration Protocol), který je přiřazen každému zařízení v síti. Místo toho byste měli použít statickou adresu a zadat nastavení sítě.

To znamená, že byste měli vstoupit do zařízení a přiřadit mu adresu IP, která je vhodná pro router.

Krok 9. Vypněte vzdálený přístup

Většina routerů umožňuje přístup k jejich rozhraní pouze z připojeného zařízení. Některé z nich však umožňují přístup i ze vzdálených systémů.

Jakmile vzdálený přístup vypnete, nebudou se moci zákeřní hackeři dostat k nastavení soukromí routeru ze zařízení, které není připojeno k bezdrátové síti.

Chcete-li tuto změnu provést, otevřete webové rozhraní a vyhledejte „Vzdálený přístup“ nebo „Vzdálená správa“.

Krok 10. Udržujte software vašeho routeru vždy aktualizovaný

Software je nezbytnou součástí zabezpečení bezdrátové sítě. Firmware bezdrátového routeru, stejně jako jakýkoli jiný software, obsahuje chyby, které se mohou stát hlavními chybami zabezpečení a být bezohledně zneužívány hackery, jak by to nejedna nešťastná rodina zjistila.

Mnoho bezdrátových routerů bohužel nepřichází s možností automatické aktualizace softwaru, takže budete muset projít komplikacemi a provést to manuálně.

Dokonce i pro ty WiFi sítě, které se mohou automaticky aktualizovat, je stále nutné toto nastavení zapnout. Připomeňme si však, že je důležité, aby se software záplatoval a zanedbání tohoto, může nechat otevřené dveře pro kyberzločince, kteří mohou využívat různou zranitelnost. Přečtěte si, co bezpečnostní experti říkají o aktualizaci softwaru a proč je klíčem k online zabezpečení.

Krok 11. Firewall může pomoci zabezpečit vaši WiFi síť

Firewally nejsou jen softwarové programy používané na vašem PC, ale dodávají se také s různými typy hardwaru.

Hardwarová brána firewall má téměř stejnou funkci jako software, ale její největší výhodou je, že přidává další vrstvu zabezpečení.

Nejlepší na hardwarových firewallech je, že většina nejlepších bezdrátových routerů má vestavěnou bránu firewall, která by měla chránit vaši síť před potenciálními kybernetickými

útoky. Tato lekce vám pomůže zjistit, zda má router zabudovanou bránu firewall a jak ji můžete aktivovat. A důrazně doporučujeme ji zapnout, pokud to již není standardně ve výchozím nastavení jako extra vrstva ochrany.

Pokud ji váš router nemá, můžete do něho nainstalovat dobré firewall zařízení, abyste ochránili váš systém před zákeřnými hackerskými pokusy ve vaší domácí síti.

Krok 12. Zvyšte ochranu zařízení nejčastěji připojených k domácí síti

Důležité: Nenechávejte žádná nechráněná slabá místa pro online pachatele, na které by mohli mít spadeno!

I když jste zvýšili ochranu routeru a domácí sítě, musíte se ujistit, že nemáte žádné bezpečnostní díry, které mohou být zneužity online pachateli.

Doporučujeme vám udělat toto:

1. Nezapomeňte vždy udržovat zařízení v aktuálním stavu s nejnovějším dostupným softwarem;
2. Vždy používejte nejnovější bezpečnostní záplaty, abyste zajistili, že bezpečnostní díra nebude ponechána otevřená pro zle smýšlející hackery.
3. Zkontrolujte, která zařízení se nejčastěji připojují k vaší domácí síti, a ujistěte se, že mají nainstalován antivirový a / nebo antimalwarový bezpečnostní software. Pokud nevíte, který z nich byste si měli vybrat, bude tento průvodce velmi užitečný.
4. Zajistěte ochranu svých zařízení pomocí více bezpečnostních vrstev, které se skládají ze specializovaného bezpečnostního softwaru, například aktualizovaných antivirových programů a softwaru pro filtrování provozu. Můžete zvážit použití antimalware softwarového programu.

Závěr

Zabezpečení domácí sítě by mělo být nejvyšší prioritou pro každého z nás, kdo má zájem o bezpečné a spolehlivé uchovávání dat. Tyto kroky mohou být opravdu užitečné i pro netechnický typ člověka.

Nezapomeňte také, že zabezpečení bezdrátové sítě může být někdy slabé a náchylné ke zneužití. Téměř nezáleží na tom, jak silné je vaše heslo, nebo zda je váš software aktuální, pokud kyberzločinci mohou lehce ovládnout vaše WiFi data.

LEKCE 2: Antivirové programy

Výstup

Většina systémů potřebuje antivirový software. Zde je uvedeno, jaký si vybrat, jak jej nainstalovat a jak jej používat, abyste dodrželi bezpečnost

Viry

Všichni doufáme, že se tomu vyhneme, ale pravdou je, že se tomu nemůžeme vyhnout navždy. Někteří z nás jsou nešťastnými nabyvateli počítačových virů. Následující pravidla vám pomohou zvládnout minimalizaci rizik.

Instalujte si antivirový program

Ať už se připojujete k internetu nebo ne, měli byste jít cestou spolehlivé ochrany. Antivirové programy jsou minimální investicí a stojí za ty peníze, takže jakmile zapnete počítač, ujistěte se, že jste chráněni! V této lekci naleznete odkaz na recenze antivirového softwaru. Můžete si vybrat z bezplatných nebo placených nabídek, vybrat si nejvhodnější pro vás a snadno ho nainstalovat z původní webové stránky.

Vyhněte se podezřelým webovým stránkám

Mnohokrát vás webové stránky upozorní, pokud se chystáte vstoupit na webovou stránku, která se pokouší nainstalovat nebo spustit program na vašem počítači, ale ne vždy. Vyhněte se takovým webovým stránkám.

Nikdy neotevírejte přílohy e-mailů bez jejich screeningu

Nejběžnější způsob šíření virů zůstává prostřednictvím e-mailu. Ujistěte se, že máte poskytovatele e-mailu, který vyžaduje, aby všechny přílohy byly před otevřením zkontrolovány, aby se zajistilo, že počítač nedostane virus.

Nastavení automatického skenování

Nastavení skenování běžícího na vašem počítači denně nebo týdně je dobrý nápad, jak se zbavit virů. Udržuje to váš počítač v aktualizovaném a bezproblémovém stavu.

Sledujte, co stahujete

Chápeme, že stahování souborů z internetu, jako je hudba a filmy, je to, co mnozí z nás dělají, ale také to mnohé z nás dostává do nesnází. Zejména velké soubory jsou ty, které nás snadno dostanou do problémů, takže si buďte vědomi toho, co stahujete.

Aktualizujte, aktualizujte, aktualizujte!

„Kritická aktualizace“ systému Microsoft Windows je jedním z příkladů, jak zůstat popředu před všemi hackery. Kritická aktualizace je celá pobočka společnosti Microsoft, která je určena k udržování počítačů bez virů. Vždy udržujte svůj systém aktualizovaný.

Vždy mějte přehled

Ať už jste počítačový fanatik, nebo příležitostný uživatel, mějte vždy přehled, jaké jsou nejnovější viry a jak ovlivní váš počítač. Takto budete připraveni, když se něco stane, abyste mohli problém vyřešit co nejdříve.

Vyhněte se cracknutému softwaru

Každý ví, že si můžete stáhnout nelegální nebo „cracknutý“ online software, který se zdá být dostupnější pro peněženku, ale ve skutečnosti vám tyto programy ublíží. Vystaví váš počítač těžko rozpoznatelným chybám a nakonec způsobí více problémů.

Nainstalujte si firewall

Firewall je program, který provádí screening příchozího internetového a síťového provozu. Spolu s programem na ochranu proti virům může zabránit neoprávněnému přístupu k počítači.

Buďte připraveni

Máte-li obavy z viru, který proletí kolem jako ničivý požár, pak se ujistěte, že jste v režimu vysoké pohotovosti. Neakceptujte žádné soubory ke stažení a buďte opatrní při otevírání e-mailů a souborů. Tato lekce by vás měla připravit na jakékoli počítačové viry, které by vám mohly přijít do cesty. Při používání počítače nezapomeňte vždy být opatrní a chytří!

LEKCE 3: Malware

Výstup

Identifikace a řešení kyberstalkingu a způsoby, jak o něm informovat.

Malware

Malware, zkratka pro "škodlivý software", se týká typu počítačového programu, který je určen k infikování počítače legitimního uživatele a více způsoby ho poškozuje. Malware může infikovat počítače a zařízení několika způsoby a přichází v mnoha formách, z nichž některé obsahují viry, červy, trojské koně, spyware a další. Je důležité, aby všichni uživatelé věděli, jak ho rozpoznat a chránit se před škodlivým softwarem ve všech jeho formách.

Co je tedy malware? Přichází v ohromující rozmanitosti forem. Počítačové viry jsou pravděpodobně nejznámějším typem malwaru – jsou takto pojmenované, protože se šíří vytvářením kopií. Červi mají podobnou vlastnost. Ostatní typy škodlivého softwaru, například spyware, jsou pojmenovány podle toho, co dělají: V případě spywaru jde o přenášení osobních údajů, například čísel kreditních karet.

Ochrana počítače a osobních zařízení před škodlivým softwarem vyžaduje jak neustálou osobní ostražitost, tak pomoc profesionálních bezpečnostních společností. V současné době není malware zaměřen pouze na domácí počítače, ale také na mobilní zařízení, která vy a vaše rodina používáte. A problém je větší, než si myslíte.

Obětí útoku malwaru se můžete stát prostřednictvím webových prohlížečů, e-mailu, sociálních sítí, které používáte, rychlých zpráv a stažených souborů.

Vaše zařízení může být infikováno téměř jakýmkoli online procesem nebo dokonce z USB přítele, takže je důležité používat bezpečnostní program, který vám může poskytnout úplnou proaktivní ochranu, která vám pomůže před infikováním.

Po dotazu "Co je to malware?" tedy nastupují další logické otázky: "Kdo ho vytváří a proč?" Dny, kdy většina malwaru byla vytvořena žertíky dospívajících, jsou dávno pryč. Malware dnes je z velké části navržen pro profesionální zločince.

Tito pachatelé mohou využít různé sofistikované taktiky. V některých případech, jak poznamenává technologický web Public CIO, kyberzločinci dokonce "uzamkli" počítačová data - znepřístupnili informace - a pak požadovali výkupné od uživatelů, aby tato data dostali zpět.

Ale hlavní riziko, které kybernetičtí zločinci představují pro velké uživatele počítačů, je krádež online bankovních informací, jako jsou bankovní a kreditní karty a hesla. Kriminální hackeři, kteří ukradnou tyto informace, je pak mohou použít k odčerpání vašeho účtu nebo k podvodným platbám z karty na vaše jméno. Nebo mohou prodávat informace o vašem účtu na černém trhu, kde tyto důvěrné informace mají dobrou cenu.

Ochrana proti malwaru

Takže teď jsme u největší otázky ze všech: "Jak se ujistím, že počítač nebo síť je bez malwaru?"

Odpověď má dvě části: osobní bdělost a ochranné nástroje. Jedním z nejpopulárnějších způsobů šíření malwaru je e-mail, který může být zamaskovaný, aby vypadal, jako by pocházel z důvěrně známé společnosti, jako je banka nebo osobní e-mail od přítele.

Dejte si pozor na e-maily, které vás požádají o zadání hesel. Nebo e-maily, které se zdají být od přátel, ale obsahují jen zprávu, jako je "podívejte se na tuto skvělou webovou stránku!", následovanou odkazem. Osobní ostražitost je první vrstvou ochrany proti malwaru, ale pouhá opatrnost nestačí. Protože obchodní bezpečnost není dokonalá, i stahování z legitimních stránek může někdy obsahovat malware. Což znamená, že i nejopatrnější uživatel je ohrožen, pokud nepřijme další opatření.

Instalujte si Anti-Spyware Software:

Spyware je softwarový program, který shromažďuje osobní informace nebo informace o organizaci bez jejich souhlasu. Tyto informace jsou přesměrovány na webové stránky třetích stran. Spyware je navržen tak, aby se nedal snadno odstranit. Anti-Spyware software je určen výhradně pro boj proti spywaru. Podobně jako antivirový software nabízí anti-spyware software ochranu v reálném čase. Kontroluje všechny příchozí informace a pomáhá při blokování hrozby, jakmile je jednou odhalena.

Doporučený anti spyware software najdete na konci lekce. Můžete si ho projít a vybrat si pro vás ten nejvhodnější.

Žádná ochrana není absolutní. Ale kombinace osobního povědomí a dobře navržených ochranných nástrojů zajistí, že váš počítač bude bezpečný.

CVIČENÍ

Cvičení 1: Mějte nad svým routerem kontrolu prostřednictvím jedinečného hesla:

Krok 1: Přihlaste se ke svému bezdrátovému routeru.

Otevřete Internet Explorer a napište adresu http://192.168.0.1 nebo http://192.168.1.1 (Podle výchozího nastavení bude mít většina routerů **192.168**.0.1
nebo **192.168**.**1.1** jako výchozí IP adresu routeru. To je adresa, kterou zadáte do adresního řádku prohlížeče pro přístup ke konfigurační stránce routeru.)

Nyní se přihlaste k routeru. Cože??. Nemáte uživatelské jméno a heslo ??. Nebojte se. Mám vaše přihlašovací údaje (pokud jste je nezměnili dříve)

Vaše uživatelské jméno a heslo by mělo být:

Pět
znaků. Všechno malým. 1. písmeno abecedy pak 4. písmeno abecedy pak 13. písmeno abecedy pak 12.písmeno abecedy pak 14. písmeno abecedy

Aby to pro vás bylo snazší:

Uživatelské jméno:admin

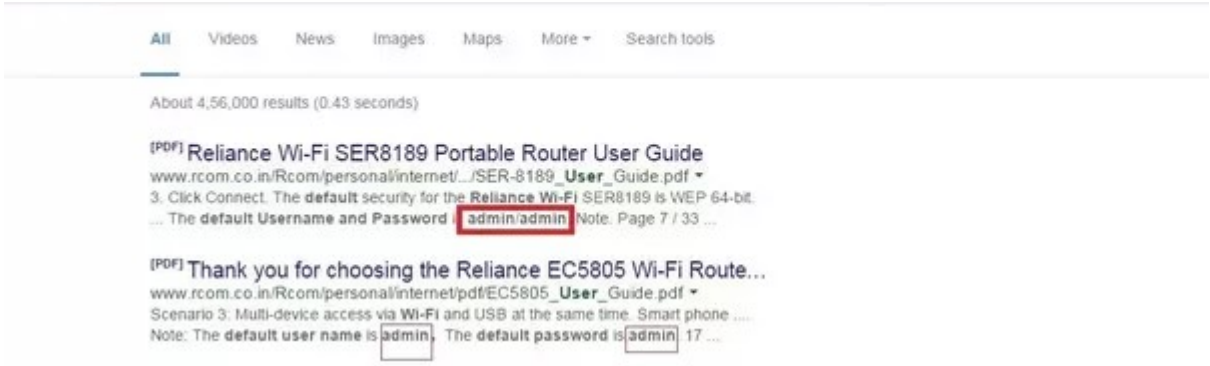
Heslo:admin

NEBO

Uživatelské jméno:admin

Heslo(prázdné):

Pokud to u vás nefunguje, prosím, použijte Google pro výchozí uživatelské jméno / heslo pro váš router/ poskytovatele služeb.



Krok 2: Změňte si ihned své uživatelské jméno a heslo

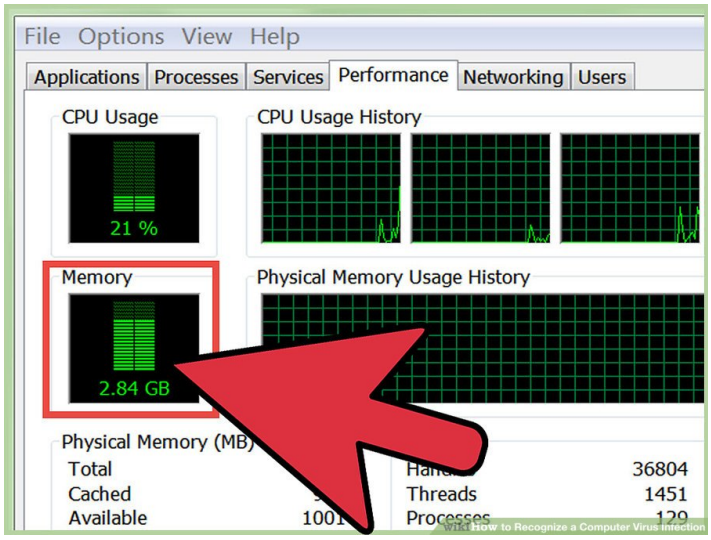
-Běžte na nastavení

-Uživatelská nastavení

-Aktualizujte si své nové údaje

Cvičení 2: Rozpoznání viru ve vašem počítači

1. Zkontrolujte činnost pevného disku. Pokud nemáte spuštěné žádné programy a světlo pevného disku se neustále zapíná a vypíná, nebo pokud slyšíte, že pevný disk pracuje, můžete mít virus, který pracuje v pozadí.



2. Sledujte, jak dlouho trvá spuštění počítače. Pokud začnete pozorovat, že zapnutí vašeho počítače trvá podstatně více času, než je obvyklé, může zpomalovat proces spouštění virus.

Pokud se nemůžete přihlásit do systému Windows, a to ani se správnými přihlašovacími údaji, virus s největší pravděpodobností převzal proces přihlášení.

3. Podívejte se na světla vašeho modemu. Nemáte-li žádné programy spuštěné a modemová přenosová světla neustále blikají, může se stát, že máte virus, který přenáší data po síti.

Cvičení 3: Rozpoznání malwarového emailu

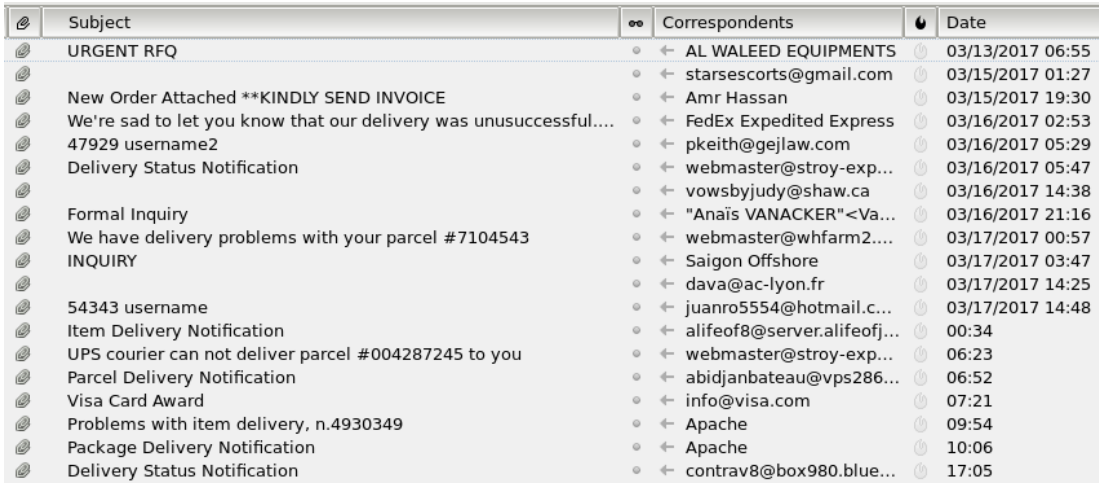
1. **Emailová adresa odesílatele**. Pokud je adresa odesílatele neznámá nebo neodpovídá očekávané adrese společnosti, jedná se pravděpodobně o e-mail s malwarem. Většina e-mailů s malwarem se jeví jako oznámení o doručení balíku, faktury, faxu/skenu nebo soudní oznámení. Zdá se, že tyto e-maily zřídka pocházejí z příslušné adresy, například e-maily, které prohlašují, že jsou z DHL nebo UPS, jsou pravděpodobně škodlivé v případě, že neodpovídají ups.com nebo dhl.com.
2. **Předmět emailu nebo příloha obsahují uživatelské jméno.** E-mail s malwarem může obsahovat vaše uživatelské jméno v předmětu nebo název souboru přílohy nebo pole Předmět může být prázdné. Oproti normálním e-mailům, které téměř vždy mají předmět a zřídka zmiňují vaše e-mailové uživatelské jméno.
3. **Lákadlo k otevření přílohy.** Mnoho e-mailů, které obsahují malware, vás vyzve k otevření přílohy. Mnoho příloh může být stále škodlivých, i když používáte antivirový program. Emaily o problémech s doručováním balíčků nemají žádný důvod k tomu, aby po vás vyžadovaly otevření přílohy; pokud by vám posílali email o legitimním problému s doručením, mohli by vás pouze informovat v hlavní části e-mailu.
4. **Lákadlo k následování odkazu.** Některé e-maily se škodlivým softwarem jsou podobné phishingovým e-mailům, kde vám doporučují sledovat webový odkaz. Tento webový odkaz by mohl vést k malwaru, proto prosím nejprve zvažte všechny tipy.
5. **Ověření informací.** Pokud vás e-mail žádá o potvrzení, kontrolu, přezkoumání nebo poskytnutí informací pomocí přílohy, může se jednat o přílohu s malwarem. Znovu zvažte, zda se to zdá bezpečné a v případě pochybností se obraťte na podporu. Otevření přílohy nemusí být bezpečné.
6. **Varování před problémem, hrozba nebo naléhavost.** Malwarové e-maily se často snaží podněcovat váš strach, obavy nebo pocit naléhavosti. Pokud vás e-mail vyzve, abyste problém vyřešili otevřením přílohy, měli byste být velmi opatrní. Některé e-maily se zdají být druhou odpovědí, která vás požádá o následnou kontrolu. Mezi příklady patří řešení problémů s doručováním balíků, informace o falešných soudních jednáních nebo falešné faktury od subjektů, se kterými pravděpodobně neobchodujete.
7. **Nezveřejnění příjemci / neuvedení příjemci.** Pokud seznam příjemců e-mailů zobrazuje nezveřejněné příjemce / neuvedené příjemce nebo jinou e-mailovou adresu než vaši, může se jednat o malware.

8. **Podezřelá příloha.** Pokud má e-mail neočekávanou přílohu, například soubor s příponami .doc, .zip, .xls, .js, .pdf, .ace, .arj, .wsh, .scr, .exe, .com, .bat, nebo jiné typy souborů Microsoft Office, pak to může být malware. Zvažte, že někdy je přípona souboru skrytá nebo obsah je odlišný od uvedeného.
9. **Obyčejný text / absence log.** Většina legitimních e-mailových zpráv bývá napsána ve formátu HTML a může obsahovat kombinaci textu a obrázků. Malwarové e-maily mají zřídka obrázky a mají sklon k obyčejnému formátování.
10. **Obecný pozdrav.** Pokud je e-mail adresován obecnou frází jako „Vážený zákazníku“, může se jednat o malware nebo phishingový pokus.

11. **Neočekávaný obsah přílohy.** Pokud nakonec otevřete přílohu a obsah je prázdný nebo se velmi liší od toho, co jste očekávali, může se jednat o malware. Obraťte se prosím okamžitě na podporu. Podpora může být schopna omezit škody nebo pomoci k obnově.

Jak vypadají skutečné malwarové emaily?

Zde je skutečný screenshot mailboxu obsahující 19 malwerových e-mailů:



Subject	Correspondents	Date
URGENT RFQ	AL WALEED EQUIPMENTS	03/13/2017 06:55
	starsescorts@gmail.com	03/15/2017 01:27
New Order Attached **KINDLY SEND INVOICE	Amr Hassan	03/15/2017 19:30
We're sad to let you know that our delivery was unusuccessful....	FedEx Expedited Express	03/16/2017 02:53
47929 username2	pkeith@gejlaw.com	03/16/2017 05:29
Delivery Status Notification	webmaster@stroy-exp...	03/16/2017 05:47
	vowsbyjudy@shaw.ca	03/16/2017 14:38
Formal Inquiry	"Anaïs VANACKER"<Va...	03/16/2017 21:16
We have delivery problems with your parcel #7104543	webmaster@whfarm2....	03/17/2017 00:57
INQUIRY	Saigon Offshore	03/17/2017 03:47
	dava@ac-lyon.fr	03/17/2017 14:25
54343 username	juanro5554@hotmail.c...	03/17/2017 14:48
Item Delivery Notification	alifeof8@server.alifeofj...	00:34
UPS courier can not deliver parcel #004287245 to you	webmaster@stroy-exp...	06:23
Parcel Delivery Notification	abidjanbateau@vps286...	06:52
Visa Card Award	info@visa.com	07:21
Problems with item delivery, n.4930349	Apache	09:54
Package Delivery Notification	Apache	10:06
Delivery Status Notification	contrav8@box980.blue...	17:05

Cvičení 4: Online bezpečnostní kvíz

Udělejte si tento online kvíz a podívejte se, jak dopadnete.

https://www.proprofs.com/quiz-school/story.php?title=esafety-quiz

DALŠÍ ČTENÍ A ZDROJE

Pojmy, které byste měli znát

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Plánování internetové bezpečnosti pro seniory (PDF ke stažení)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReqQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Hlavní tipy pro internetovou bezpečnost (PDF ke stažení)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC&url=https%3A%2F%2Fquery.prod.cms.rt.microsoft.com%2Fcms%2Fapi%2Fam%2Fbinary%2FRE1ImTu&usg=AOvVaw0QyXRMv5RLg-kAS0tIaUvz

Jak se ochránit před malwarem – Youtube video

https://www.youtube.com/watch?

v=uJRqZTNMCMo

Nejlepší antivirové služby pro rok 2018

https://www.itproportal.com/guides/best-antivirus-services-for-2018/

Nejlepší antimalwarový software pro rok 2018

https://www.techradar.com/news/best-free-anti-malware-software

Ochrana vašich dat

https://youtu.be/BL7WJM342Uc

Online bezpečnost pro seniory

https://www.connectsafely.org/seniors/

Další informace k online bezpečnosti

https://www.protectseniorsonline.com/resources/

Jak zkontrolovat, zda váš počítač obsahuje virus

https://www.youtube.com/watch?v=4i_cCPhewu4