PROJEKT DIGITAL ACCESS

VZDĚLÁVACÍ MODUL

Základní 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, které může být učiněno z informací zde obsažených.

Obsah

UČEBNÍ HODINY: [UČEBNÍ HODINY VŠECH LEKCÍ]

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

SHRNUTÍ

Tento modul byl navržen tak, aby seznámil začínající uživatele internetu se základními uživatelskými znalostmi o online bezpečnosti. Hlavním cílem lekce je naučit uživatele, jak udržovat osobní údaje v bezpečí a zajistit, aby jejich online data a majetek nebyly ohroženy.

KLÍČOVÁ SLOVA

online bezpečnost, osobní informace, heslo, kyberstalking, trezor hesel

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**
Online bezpečnost	Porozumění online bezpečnosti Pochopení typů online rizik Porozumění základním klíčovým slovům	Pochopení, proč je online bezpečnost důležitá a jaká jsou online rizika.
Osobní informace	Jaké jsou mé osobní informace Zveřejnění osobních informací online Co se může stát, pokud budu své osobní informace sdílet online Jak mohu ochránit své osobní informace	Schopnost pochopit, co jsou osobní údaje, jaká jsou rizika v online prostředí a chránit svá osobní data.

Hesla	Výběr nejlepšího hesla Zacházení s vašimi hesly Činnosti, které je potřeba provést pro svou ochranu	Pochopení významu silných hesel. Vytváření a správa hesel a uživatelské účty.
Nastavení soukromí	Identifikace kyberstalkingu Strategie jeho zvládání Používání trezoru hesel Správa uživatelských účtů	Pochopení významu silných hesel. Vytváření a správa hesel a uživatelské účty.

LEKCE 1: Online bezpečnost

Výstup

Pochopení, proč je online bezpečnost důležitá a jaká jsou online rizika.

Úvod

10 základních pravidel online bezpečnosti

1. Zachovejte si osobní informace profesionální a limitované

Nikdo nemusí znát stav vašeho osobního vztahu nebo adresu domu. Potřebují vědět, jaké jsou vaše odborné znalosti a profesionální zázemí a jak se s vámi spojit. Nepodali byste čistě osobní informace individuálním cizincům - nedávejte je ani milionům lidí online.

2. Nechejte si zapnuté nastavení ochrany soukromí

Obchodníci se velmi rádi o vás dozvědí vše, a co teprve hackeři. Oba se mohou z vašeho prohlížení a používání sociálních médií hodně naučit. Ale o své informace se můžete postarat. Webové prohlížeče i mobilní operační systémy mají k dispozici nastavení, která chrání vaše soukromí online. Hlavní webové stránky, jako je Facebook, mají také nastavení, která zvyšují soukromí. Tato nastavení jsou někdy (záměrně) těžko dostupná, protože společnosti chtějí, aby vaše osobní údaje byly uváděny na trh. Ujistěte se, že jste aktivovali tato opatření pro ochranu soukromí a ponechali je aktivní.

3. Brouzdejte bezpečně

Asi byste se nerozhodli projít nebezpečnou čtvrtí - proto také nenavštěvujte nebezpečné čtvrti online. Kyberzločinci používají jako návnadu šokující obsah. Vědí, že lidi někdy pochybný obsah přitahuje a při jeho zkoumání mají svého strážce vypnutého. Internetový polosvět je naplněn těžko viditelnými nástrahami, kde by jedno neopatrné kliknutí mohlo odhalit osobní údaje nebo infikovat vaše zařízení malwarem. Tím, že odoláte nutkání, nedáte hackerům ani šanci.

4. Ujistěte se, že vaše internetové připojení je bezpečné

Pokud se připojujete na veřejném místě, například použitím veřejného Wi-Fi připojení, nemáte žádnou přímou kontrolu nad jeho zabezpečením. Odborníci na institucionální úrovni v oblasti kybernetické bezpečnosti se obávají „koncových bodů“ - míst, kde se soukromá síť připojuje k okolnímu světu. Váš ohrožený koncový bod je místní připojení k internetu. Než poskytnete

informace, jako např. číslo vašeho bankovního účtu, ujistěte se, že je vaše zařízení v bezpečí a v případě pochybností vyčkejte na lepší dobu (tj. dokud se nebudete moci připojit k bezpečné síti Wi-Fi). Více se dozvíte v modulu pro středně pokročilé.

5. Buďte opatrní v tom, co stahujete

Hlavním cílem kyberzločinců je navést vás ke stažení malwaru - programů nebo aplikací, které nesou malware nebo se snaží ukrást informace. Tento malware může být maskovaný jako aplikace: cokoliv od populární hry k něčemu, co kontroluje dopravu nebo počasí. Nestahujte si aplikace, které vypadají podezřele nebo pocházejí z webu, kterému nedůvěřujete.

6. Vybírejte silná hesla

Hesla jsou jedním z největších slabých míst v celé internetové bezpečnostní struktuře, ale v současné době neexistuje jiné východisko. Problém s hesly spočívá v tom, že lidé mají sklon volit si snadno zapamatovatelná hesla (např. "Heslo" a "123456"), která jsou ovšem snadná i pro kyberzločince. Vybírejte si silná hesla, která jsou pro zločince těžší k rozkrytí. Software pro správu hesel vám může pomoci spravovat více hesel, abyste na ně nezapomněli. Silné heslo je takové, které je jedinečné a komplexní - nejméně 15 znaků dlouhé, směšující písmena, číslice a speciální znaky. Budeme o tom mluvit později v této lekci.

7. Online nákupy provádějte pouze ze zabezpečených webů

Kdykoliv provedete nákup online, musíte poskytnout informace o kreditní kartě nebo bankovním účtu - to je přesně to, po čem kyberzločinci nejvíce touží, aby se jim dostalo do rukou. Tyto informace poskytujte pouze webům, které mají zabezpečené šifrované připojení. Tyto zabezpečené weby můžete identifikovat vyhledáním adresy, která začíná https: (S znamená "secure" - zabezpečený), nikoli pouze http: Mohou být také označeny ikonou visacího zámku vedle adresního řádku.

8. Buďte obezřetní v tom, co zveřejňujete

Internet nemá klávesu Delete. Jakýkoli komentář nebo obrázek, který zveřejníte online, může zůstat navždy online, protože odstranění originálu (řekněme ze služby Twitter) neodstraní jakékoliv kopie, které provedli jiní lidé. Neexistuje žádný způsob, jak si „vzít zpět“ poznámku, kterou byste si přáli neudělat. Nedávejte online nic, co byste nechtěli, aby vaši příbuzní nebo jiní lidé viděli.

9. Buďte opatrní v tom, s kým se stýkáte online

Lidé, se kterými se setkáváte online, nejsou vždy těmi, za koho se prohlašují. V podstatě nemusí být ani skuteční. Falešné profily sociálních médií jsou pro hackery oblíbeným způsobem, jak chytit nepozorné uživatele webu a ukrást jim jejich kybernetické peněženky. Ve svém online společenském životě buďte stejně opatrní a vnímaví, jako ve svém osobním společenském životě.

10. Aktualizujte svůj antivirový program

Internetový bezpečnostní software nemůže chránit před každou hrozbou, ale odhalí a odstraní většinu malwaru - proto byste se měli ujistit, že je aktuální. Ujistěte se, že používáte aktuální aktualizace operačního systému a aktualizované aplikace. Poskytují životně důležitou úroveň zabezpečení.

Mějte na paměti těchto 10 základních pravidel bezpečnosti na internetu a vyhnete se mnoha nepříjemným překvapením, která číhají online na neopatrné uživatele. V dalších lekcích a modulech se budeme podrobněji učit, jak je aplikovat do praxe.

LEKCE 2: Osobní informace

Výstup

Být schopen pochopit, co jsou osobní údaje, jaká jsou rizika v online prostředí a schopnost ochránit své osobní údaje.

Jaké jsou moje osobní informace?

Vaše osobní informace mohou zahrnovat:

Celé jméno
Adresu
Telefonní čísla
Školu
Datum narození
Emailovou adresu
Uživatelské jméno a heslo
Bankovní detaily a detaily ke kreditní kartě.

Zveřejnění osobních informací online

Mnoho online služeb vyžaduje, aby uživatelé poskytovali některé osobní informace, aby mohli využívat své služby. Před poskytnutím osobních údajů byste měli přemýšlet o tom, co lze s vašimi osobními údaji udělat, a posoudit, zda tyto údaje opravdu rádi předáte. Kromě nevhodného nebo nezákonného použití informací může zveřejnění osobních informací online ovlivnit vaši digitální pověst.
Existuje několik online aktivit, kterých byste si měli být vědomi a které mohou vyžadovat úroveň zpřístupnění osobních údajů. Tyto zahrnují:

Nakupování: ověření totožnosti kupujícího, zpracování plateb nebo dodání zboží.

Přihlášení nebo registrace: jméno nebo uživatelské jméno a e-mailová adresa jsou často minimální požadavky, ale další požadované informace mohou zahrnovat: věk, pohlaví, adresu, fotografie a osobní preference (červená hvězdička (*) obecně označuje povinná pole, která jsou potřebná k zaregistrování se).

Soutěže, ceny a odměny: často vyžadují, aby uživatelé poskytovali rozsáhlá osobní data, včetně osobních zájmů a demografických detailů - obvykle je používají obchodníci k propagaci produktů a služeb.

Online hry a virtuální světy: mohou vyžadovat, aby se uživatelé zaregistrovali dříve, než začnou hrát.

Co se může stát, když sdílím své osobní informace online?

Spam, scam, krádeže identity a podvody jsou jen některé z vážnějších problémů, s nimiž se můžete setkat, pokud sdílíte osobní údaje online.

Jak mohu ochránit své osobní informace

Je důležité pochopit, jak jsou osobní údaje používány online a jak chránit vaše informace a digitální pověst.

Následující tipy jsou skvělým základem pro ochranu vašich osobních údajů online:

Finanční informace poskytujte pouze na zabezpečených webových stránkách. Hledejte adresu začínající znakem https: // a symbolem uzamčeného zámku ve spodní části obrazovky, který označuje, že data jsou šifrována.

Pokud máte pochybnosti o legitimitě webové stránky, zavolejte organizaci, kterou zastupuje. Webové stránky SCAMwatch poskytují další rady, jak identifikovat a nahlásit potenciální podvody.

Bankovní instituce nikdy nebudou posílat jednotlivcům email s žádostí o jejich uživatelské jméno nebo heslo. Pokud obdržíte email od organizace, která prohlašuje, že zastupuje bankovní instituci, oznamte tuto emailovou zprávu bance a společnosti SCAMwatch. Neodpovídejte a neklikejte na žádné odkazy.

Přečtěte si uživatelské smlouvy a zásady ochrany soukromí. Mnoho organizací využívá informace pro marketingové účely a může je prodávat jiným marketingovým firmám. Pokud jsou informace zveřejněny na webových stránkách, které prodávají informace obchodníkům, jednotlivci mohou obdržet propagační spamové emaily, u kterých může být obtížné je zastavit.

Redukujte spam ochranou svých detailů. Spam může být redukován:

limitováním poskytování emailových adres a mobilních čísel

instalací a používáním softwaru pro filtrování spamu

zkontrolováním podmínek při nákupu produktů, vstupu do soutěží nebo registrací do služeb a přihlášením k emailovému odběru newsletterů

nepovolením použití kontaktních údajů pro marketingové účely (ujistěte se, že jste zaškrtli políčko pro odhlášení)

posílením online bezpečnosti k redukci spamu

Je potřeba si uvědomit, že informace sdílené online mohou být permanentní – uživatelé nemusí mít kontrolu nad tím, kdo bude vidět a kdo bude mít přístup k jejich osobním informacím.

Hesla vybírejte pečlivě. Při vytváření hesel existují určitá doporučení, co dělat a nedělat:

Co dělat

používat osm a více znaků

používat kombinaci slov, která nejsou předvídatelná

používat dvoufázové ověření na účtech obsahujících osobní informace.

Co nedělat

používat jména domácích mazlíčků, data narození, jména rodinných příslušníků a přátel

používat předvídatelné kombinace slov (např. ''milujituristiku“), a obsahově specifická slova (např. „google“) nebo opakované sekvenční znaky (např. „aaaaaa“ nebo „123456“)

sdílet hesla s ostatními, ani s přáteli

ukládejte je do svého zařízení, pokud to není prostřednictvím správce hesel, který je ukládá v zašifrované databázi. Mezi zastrašovací a vydírající podvody patří „ransomware“, „malware“ a „hit man“. Podvody s ransomware a malware mohou zahrnovat škodlivý software umístěný na vašem počítači. To může zločincům umožnit přístup k vašim osobním informacím, což může mít za následek ztrátu dat nebo zabránění přístupu k vašim programům a souborům. Podvodníci pak požadují platbu předem, než vám umožní opětovný přístup k počítači.

LEKCE 3: Hesla

Výstup

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

Úvod

Vaše hesla jsou nejběžnějším způsobem, jak prokázat svou totožnost při používání webových stránek, e-mailových účtů a samotného počítače (prostřednictvím uživatelských účtů). Používání silných hesel je proto nezbytné pro ochranu vaší bezpečnosti a identity. Nejlepší bezpečnost na světě je k ničemu, pokud osoba se zlými úmysly vlastní legitimní uživatelské jméno a heslo.

Hesla se běžně používají ve spojení s vaším uživatelským jménem. Na zabezpečených stránkách však mohou být také použity spolu s jinými metodami identifikace, jako je samostatný PIN a / nebo zapamatovatelné informace. V některých případech budete také vyzváni k zadání pouze určitých znaků vašeho hesla pro další zabezpečení.

Riziko používání slabého hesla a neexistence samostatného hesla pro váš e-mailový účet

Činnosti osob, které zneužívají vaši osobu k podvodům a dalším kriminálním činům zahrnují:

- Přístup k vašemu bankovnímu účtu
- Nákup zboží online vašimi penězi
- Vydávání se za vaši osobu na sociálních sítích a seznamkách
- Odesílání e-mailů vaším jménem
- Přístup k soukromým informacím uloženým v počítači

Výběr nejlepšího hesla

Co dělat:

Vždy použijte heslo.

Používejte silné, samostatné heslo pro váš emailový účet.

Chcete-li vytvořit silné heslo, jednoduše vyberte tři náhodná slova. Čísla, symboly a kombinace velkých a malých písmen lze použít, pokud máte pocit, že potřebujete vytvořit silnější heslo, nebo účet, ke kterému vytváříte heslo, vyžaduje více než jen písmena.

Existují alternativy, které nemají pevně stanovená pravidla, ale můžete zvážit následující návrhy:

Zvolte heslo s nejméně osmi znaky (a více, pokud můžete, protože delší hesla jsou pro pachatele těžší k uhodnutí nebo prolomení), kombinace velkých a malých písmen, čísel a symbolů klávesnice, jako je @ # $% ^ & * ( ) _ +. (například SP1D3Rm @ n - variace slova spiderman s písmeny, čísly, velkými a malými písmeny). Uvědomte si však, že některé z těchto interpunkčních znamének může být obtížné zadat na zahraničních klávesnicích. Také pamatujte na to, že změna písmen na čísla (například E na 3 a i na 1) jsou techniky, které jsou pachatelům dobře známy.

Řádek písně, kterou by si s vámi lidé nespojili.

Rodné jméno matky někoho jiného (ne rodné jméno vaší vlastní matky).

Vyberte si frázi, která je vám známa, například „Trampi jako my, děti narozené k běhu“ a vyberte první znak z každého slova, abyste dostali „tjm, “dnkb"

Co nedělat:

Používat následující jako hesla:

Vaše uživatelské jméno, aktuální jméno nebo obchodní jméno.

Jména členů rodiny nebo domácích mazlíčků.

Vaše datum narození a data členů rodiny.

Oblíbený fotbalový nebo F1 tým nebo další slova, na které lze lehce přijít s určitými malými znalostmi prostředí.

Slovo „heslo“.

Číselnou sekvenci.

Jediné běžné slovníkové slovo, které by mohlo být odhaleno běžnými programy na hackování.

Při volbě číselných kódů nebo PIN nepoužívejte vzestupná nebo sestupná čísla (například 4321 nebo 12345), duplicitní čísla (například 1111) nebo snadno rozpoznatelné vzory klávesnice (například 14789 nebo 2580).

Zacházení s vašimi hesly

Nikdy nezveřejňujte svá hesla nikomu jinému. Pokud si myslíte, že vaše heslo zná někdo jiný, okamžitě jej změňte.

Nezadávejte své heslo, když ostatní vidí, co píšete.

Rutinní změna hesel se nedoporučuje, pouze pokud účty, na které se vztahují, byly napadeny, v takovém případě by měly být okamžitě změněny. To platí i v případě, že byl napaden jiný účet nebo webová stránka, pro kterou používáte stejné přihlašovací údaje.

Pro každou webovou stránku použijte jiné heslo. Pokud máte pouze jedno heslo, zločinec ho musí prolomit, aby získal přístup ke všemu.

Nezadávejte hesla (například heslo2, heslo3).

Pokud si musíte zapisovat hesla, abyste si je mohli zapamatovat, zašifrujte je způsobem, který je znám vám, ale tak, aby je ostatní nerozluštili.

Alternativou k zapisování hesel je použití online úschovny hesel nebo trezoru. Vyhledejte si doporučení a ujistěte se, že ta, kterou si vyberete, bude bezpečná a seriózní.

Heslo neposílejte e-mailem.

Skutečnost, že byste měli používat různá hesla pro každý z vašich účtů, je může činit velmi obtížně zapamatovatelná. Zvažte použití jednoho z mnoha trezorů hesel dostupných na internetu, ale přečtěte si recenze a získejte doporučení.

Trezor hesel/Sejfy

Existuje několik trezorů hesel (jinak známých jako sejfy s hesly nebo možná i další termíny), které jsou k dispozici pro vaše použití - některé jsou placené, některé zdarma. To vám umožní ukládat všechna vaše hesla na jednom snadno přístupném místě, takže si je nemusíte pamatovat všechny nebo si je zapisovat. Stačí si jen zapamatovat jednu sadu přihlašovacích údajů.

Před vložením hesla do trezoru hesel byste si měli přečíst recenze nebo získat osobní doporučení. Ať si vyberete cokoliv, naším doporučením je, aby byl vybaven dvoufaktorovou autentizací (2FA) - jinými slovy, odešle kód do vašeho mobilního telefonu nebo jiného zařízení, který potřebujete zadat pro vstup do trezoru hesel k získání přístupu, podobně jako když potvrdíte online bankovní platbu.

Správa uživatelských účtů

Každému, kdo používá počítač, by měl být přidělen vlastní uživatelský účet, aby k jeho souborům a programům měl přístup pouze on. Každý uživatelský účet by měl být přístupný pouze zadáním uživatelského jména a hesla, aby bylo zajištěno soukromí uživatelů.

Nepoužívejte účet s oprávněními správce pro každodenní použití, protože malware může převzít práva správce. I když jste jediným uživatelem, nastavte účet správce, který chcete použít, když potřebujete provádět úkoly, jako je instalace programů nebo změna konfigurace systému, a další „standardní uživatelský účet“ jako běžný účet. Pokud nejste přihlášeni jako správce, budete při instalaci nového ovladače zařízení nebo programu vyzváni k zadání hesla správce.

LEKCE 4: Nastavení soukromí

Výstup

Pomoc uživateli při identifikaci, řešení a ohlašování kyberšikany.

Počítačové soukromí

Podívejte se na nastavení ochrany osobních údajů nabízená ve vašem prohlížeči (obvykle se nacházejí v nabídce Nástroje), abyste zjistili, zda ho můžete doladit tak, aby se zachovalo to dobré a blokovalo špatné. Když jste online, webové stránky instalují do vašeho počítače soubory cookie, které sledují vaše pohyby. Některé soubory cookie mohou být prospěšné, například ty, které si pamatují vaše přihlašovací jména nebo položky v nákupním košíku online. Některé soubory cookie jsou však navrženy tak, aby si zapamatovaly vše, co děláte online, vytvoří profil vašich osobních informací a zvyků a tyto informace se prodávají inzerentům a dalším společnostem.

Příklad nastavení v Internet Exploreru

Chcete-li chránit počítač před vniknutím nebo viry, které by mohly poškodit váš systém, musíte vědět, jak změnit nastavení ochrany osobních údajů v aplikaci Internet Explorer. Změnou nastavení ochrany osobních údajů se rozhodnete, jaké druhy webů může aplikace Internet Explorer otvírat a proti jakým druhům stránek chcete váš počítač chránit.

1. Otevřete Internet Explorer, vyberte Nástroje→Možnosti internetu, a klikněte na kartu Zabezpečení.
2. Posunutím jezdce nahoru a dolů zobrazíte různé úrovně nastavení zabezpečení.

Na každé úrovni vám aplikace Internet Explorer poskytne informace o tomto konkrétním nastavení zabezpečení.

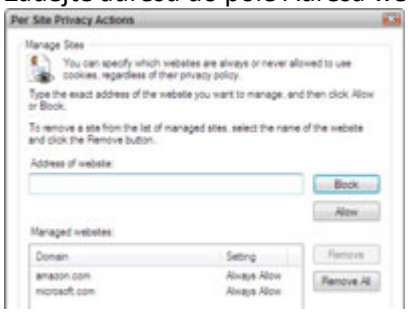
3. Přečtěte si volby a vyberte nastavení, které vám vyhovuje.

Pokud nevíte, co si vybrat, středně vysoké je dobrým místem, kde začít. Pokud to nevypadá na dostatečnou blokaci, úroveň zabezpečení můžete vždy zvýšit.

4. Kliknutím na tlačítko Weby určete weby, které by měly vždy nebo neměly nikdy používat soubory cookie.

Otevře se dialogové okno Akce na stránce Ochrana osobních údajů, která umožňuje přepsat obecné nastavení zvolené posuvníkem.

Zadejte adresu do pole Adresa webu a klepněte na položku Blokovat nebo Povolit.



Klepněte na tlačítko Povolit pro weby, o kterých víte, že jim můžete vždy důvěřovat, a klepněte na položku Blokovat pro weby, o nichž víte, že jim nikdy nemůžete věřit (např. www.ComputerDemolishingDownloads.com).

5. Klikněte na OK pro uložení vašich nových nastavení.

Vraťte se do dialogového okna Možnosti internetu.

6. Upravte blokování automaticky otevíraných oken a po dokončení klikněte na tlačítko OK.

Blokování automaticky otevíraných oken můžete zapnout a vypnout a můžete povolit vyskakovací okna určitých webů prostřednictvím blokátoru klepnutím na tlačítko Nastavení. Zde přidáváte weby stejným způsobem, jakým jste přidali weby v dialogovém okně Akce na základě soukromí na webu.

Soukromí na smartphonu

Nastavení na chytrých telefonech se liší, ale s těmito opatřeními můžete zpřísnit soukromí:

Vypněte si lokalizační služby. Zabrání to aplikacím, aby detekovali vaše umístění.

Nedovolte aplikacím sdílet vaše data. Některé aplikace chtějí použít informace uchované ve vašem telefonu (váš seznam kontaktů, například). Řekněte ne.

Povolte nastavení ochrany osobních údajů v aplikacích, které stahujete. Ujistěte se, že používáte přísná nastavení soukromí na služby, jako je Instagram a Facebook.

Dávejte pozor na přihlášení ze sociálních sítí. Když se přihlásíte na stránky se svým Facebookovým nebo Google uživatelským jménem a heslem, můžete této aplikaci povolit přístup k určitým informacím z vašeho profilu. Přečtěte si i drobné písmo, abyste věděli, co sdílíte.

CVIČENÍ

Jaké je vaše IQ soukromí? Udělejte si náš kvíz a zjistěte to!

https://blog.avast.com/2014/01/27/what-is-your-privacy-iq-take-our-quiz-and-find-out-2/

Online hra pro kybernetickou bezpečnost

NOVA spojila své síly s odborníky na kybernetickou bezpečnost a vytvořila svou laboratoř Cybersecurity Lab. Jedná se o hru, ve které hráči zjistí, jak mohou udržet svůj digitální život v bezpečí. Hra pomáhá hráčům rozvíjet porozumění běžným kybernetickým hrozbám, které existují online a jejich obraně.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Seznam nejhorších hesel

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

Internetová bezpečnostní pravidla

https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

Jak zachovat online bezpečnost pro seniory –

Youtube video https://www.youtube.com/watch?v=HGHxRNT6PjU

Online bezpečnost pro seniory

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

Více informací k online bezpečnosti

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