Bezpečnost na internetu

Internet se stal klíčovou součástí našich životů. Je to neocenitelný nástroj, který však s sebou nese i řadu rizik. Již jste se pravděpodobně setkali s tím, že se útočníci snaží zmocnit vašich účtů, úřady se pokoušejí sledovat vaši online aktivitu nebo vás na sociálních sítích obtěžují trollové. Většina uživatelů internetu se musí vypořádat s kombinací všech tří možností.

Tento průvodce vám pomůže zabezpečit vaše online účty, zařízení a soukromé údaje.

Uživatelské účty

Používejte silná a jedinečná hesla

Pravděpodobně máte desítky účtů, které k přihlášení vyžadují uživatelské jméno a heslo. E-mail, sociální sítě atd. Všechny tyto účty je třeba chránit silnými a jedinečnými hesly. To znamená, že by měla být dlouhá - alespoň 16 znaků - a neměla by obsahovat nic předvídatelného, jako je vaše jméno nebo datum narození.
Proč? Protože pokud dojde ke kompromitaci jedné služby a vaše heslo unikne na internet, přinejmenším jeden z útočníků pravděpodobně zkontroluje, zda ho může použít k přístupu k vašim dalším účtům.

Používejte dvoufaktorové ověřování (2FA) všude, kde je to možné.

Ověřování pomocí 2FA ještě více ztěžuje útočníkům přístup k vašim účtům. Řekněme, že se někomu podařilo zjistit nebo uhodnout jedno z vašich hesel. Pokud by se pokusil přihlásit k vašemu účtu, služba by po něm požadovala 2FA kód.
Tento systém vás ochrání, protože útočník pravděpodobně nebude mít přístup jak k vašemu heslu, tak k zařízení, kde získáváte dočasné 2FA kódy.

Používejte náhodná uživatelská jména pro účty.

Mnoho uživatelů chce mít jedno rozpoznatelné uživatelské jméno pro všechny své účty na sociálních sítích, jako je Twitter, Instagram, TikTok a YouTube. Proč? Protože to pomáhá lidem najít a sledovat vaši práci. Budování osobní značky může být také rozhodující pro zvýšení vašeho profilu, přilákání pracovních nabídek apod.
Pro všechny ostatní účty byste si však měli vytvořit náhodná, jedinečná uživatelská jména. Pokud budete pro všechny účty používat stejné, bude to o jednu informaci méně, kterou musí útočník zjistit, aby se dostal k vašim účtům. Možná chcete mít stejné uživatelské jméno pro účty na sociálních sítích, ale to neznamená, že byste se jím měli přihlašovat i k bankovnímu účtu.

Bezpečné sdílení hesel

Pravděpodobně máte alespoň jedno heslo, které musíte čas od času sdílet. Může to být heslo k Wi-Fi

ve vaší práci, předplatné nebo přihlašovací údaje k účtu na Twitteru.

Spoléhat se na lístečky, textové zprávy, e-maily, tabulky nebo náhodné textové dokumenty je riskantní - používejte raději správce hesel. Pomocí např. aplikací 1Password Teams a 1Password Business můžete vytvářet vlastní trezory a řídit, kteří kolegové k nim mají přístup. Kromě toho můžete bezpečně sdílet kopie hesel a dalších položek uložených v 1Password s kýmkoli - i když nepoužívá 1Password - pomocí sdílení položek.

Ochrana hesel a dalších digitálních důvěrných informací na cestách

Co dělat, když vás na celnici náhle požádají, abyste odemkli svůj telefon, tablet nebo notebook? Vaše zařízení pravděpodobně obsahují nejrůznější hesla a další důvěrné digitální údaje.

Tomuto potenciálnímu problému se můžete vyhnout tím, že si svá zařízení před každou cestou pečlivě připravíte. Například aplikace 1Password má „Travel Mode“, který vám umožní dočasně odstranit některé trezory ze zařízení. Jakmile bezpečně dorazíte na místo určení, můžete režim vypnout a normálně prohlížet, upravovat a automaticky vyplňovat uložená data.

Použití náhodných odpovědí na bezpečnostní otázky

Při vytváření účtu online budete často vyzváni k nastavení několika bezpečnostních otázek a odpovědí. Mnohé z těchto otázek vyžadují osobní údaje, které si každý snadno najde na internetu, například dívčí jméno vaší matky, základní školu nebo oblíbenou knihu.

Ale: odpovědi, které uvedete, nemusí být věcně správné. Stačí, když znáte a na výzvu napíšete odpověď, kterou jste původně zvolili. (Např. pokud dostanete otázku „Jaké je vaše oblíbené město?“, nezáleží na tom, zda zvolíte „Londýn“ nebo „Paříž“ - musíte se jen ujistit, že pokaždé, když se vás na to někdo zeptá, odpovíte stejně).

Kontrola upozornění na neobvyklé pokusy o přihlášení

Mnoho služeb vám pošle e-mail nebo push oznámení, pokud zjistí podezřelý pokus o přihlášení. Tato upozornění jsou obvykle falešným poplachem. Například je často obdržíte, když změníte zařízení, stáhnete nový prohlížeč nebo odcestujete do jiné lokality.

Těmto upozorněním byste však měli věnovat pozornost, protože jednoho dne mohou upozornit na škodlivý pokus o přihlášení. Otevřením upozornění na důvěryhodném zařízení obvykle získáte možnost útok zablokovat, čímž zůstanou váš účet a související data v bezpečí. Heslo k účtu pak budete moci změnit dříve, než se útočník pokusí znovu získat přístup.

Komunikace

Šifrování e-mailů pomocí PGP

Téměř každý uživatel používá e-mail ke komunikaci se spolupracovníky. Pokud chcete, aby vaše

zprávy zůstaly soukromé, měli byste zvážit jejich šifrování. Existuje více způsobů, jak to udělat, ale nejoblíbenější je PGP neboli Pretty Good Privacy. Je zdarma a funguje ve všech hlavních operačních systémech včetně Mac, iOS, Windows, Android a Linux.

Zvažte přechod k poskytovateli e-mailu zaměřenému na ochranu soukromí

Nechcete se zabývat PGP? To nevadí! Stále existuje několik kroků, které můžete podniknout, abyste svou schránku trochu zabezpečili. Můžete například přejít k poskytovateli e-mailu, který upřednostňuje soukromí uživatelů. Např. švýcarská firma ProtonMail.

Používání aplikací pro zasílání zpráv a videohovory, které podporují šifrování end-to-end

Jednoduchým způsobem bezpečné komunikace je používání aplikací, které podporují koncové šifrování. Obvykle vyžadují jen velmi málo nastavení - stačí stáhnout aplikaci do zařízení, vytvořit si účet a pak zkontrolovat, že pro aktivaci koncového šifrování nemusíte v nastavení nic přepínat. (Pro mnohé je to mnohem rychlejší než nastavení PGP v e-mailu.)

Pomocí těchto aplikací můžete komunikovat s kýmkoli, včetně důvěrných zdrojů, spolupracovníků a lidí z vašeho osobního života, jako jsou přátelé a rodina. Mnoho bezpečnostních expertů doporučuje aplikaci Signal pro zasílání zpráv a videohovory, protože je založena na open-source protokolu Signal a ve výchozím nastavení nabízí šifrování end-to-end. Viz Signal - private messenger.

Odesílání zpráv, které po uplynutí nastavené doby zmizí

Mnoho aplikací nabízí možnost odesílat samodestruktivní zprávy např. Signal. (Tato funkce se někdy nazývá mizející zprávy.) Po uplynutí nastavené doby se tak odstraní každá odeslaná a přijatá zpráva. Pokud vám tak někdo vezme telefon, tablet nebo počítač - ať už je to útočník nebo státní úředník - nebude si moci přečíst vaše soukromé zprávy, i když bude vědět, jak zařízení odemknout a otevřít aplikace pro zasílání zpráv.

Mizející zprávy představují bezpečný a pohodlný způsob chatování s důvěrnými zdroji. Nejsou sice dokonalé - příjemce si může před zmizením vašich zpráv udělat screenshot obrazovky, ale jsou cennou obranou proti nechtěným odposlechům.

Naučte se rozpoznat phishingové e-maily

Dostali jste někdy e-mail, který na první pohled vypadá jako skutečný, ale ve skutečnosti je od zločince, který se vydává za seriózní osobu nebo společnost? Nejde jen o spam, ale o phishingový útok. Tyto zprávy vás často vyzývají ke kliknutí na odkaz, který se zdá být legitimní, ale ve skutečnosti vás pošle na škodlivou stránku určenou ke krádeži vašich soukromých informací.

Pro člověka může být lákavé kliknout na odkaz z anonymního zdroje, který tvrdí, že má pro vás něco důležitého. Musíte se však mít na pozoru. Zkontrolujte e-mailovou adresu odesílatele (zdá se být legitimní?), zkontrolujte, zda ve zprávě nejsou překlepy, a věnujte velkou pozornost zvláštním výrazům a formulacím v textu. Pokud se vám něco nezdá, zastavte se a vyhodnoťte to. Pokuste se

ověřit totožnost odesílatele nebo ho požádejte, aby své informace poslal jiným, bezpečnějším způsobem.

Webový prohlížeč

Používejte protokol HTTPS všude, kde to jde

Přejděte do adresního řádku prohlížeče a vyberte malý symbol visacího zámku vedle adresy URL tohoto článku. Pravděpodobně uvidíte zkratku „HTTPS“. Je to webový protokol, který využívá typ šifrování zvané SSL nebo TLS. Protokol HTTPS má velký podíl na zajištění bezpečnosti všech uživatelů webu.

Použití prohlížeče Tor pro citlivé projekty

Bezplatný prohlížeč Tor je skvělý způsob, jak zvýšit své soukromí a zajistit, aby nikdo, včetně vašeho poskytovatele internetových služeb, nemohl sledovat stránky, které navštěvujete. Tor (což je zkratka pro The Onion Routing) zabezpečuje váš provoz tím, že jej předává přes několik serverů. Jak vysvětluje webová stránka Tor, v současné době existují tisíce relay po celém světě, které pomáhají zakrýt skutečné IP adresy uživatelů.

Prohlížeč Tor se pro některé účely může zdát jako přehnaný. Vyplatí se však nastavit si ho v počítači pro případ, že byste někdy cestovali do země s extrémní úrovní vládního dohledu nebo náhle potřebovali zjistit něco, co vyžaduje vyšší úroveň opatrnosti a soukromí.

Buďte opatrní na veřejných Wi-Fi

Když jste v terénu a potřebujete něco nahrát - ať už jde o text, fotografii nebo videozáznam - může být lákavé připojit se k první veřejné síti Wi-Fi, která se ve vašem zařízení objeví. Buďte však opatrní, protože ne všechny jsou bezpečné. Útočníci mohou zneužít špatně zabezpečené sítě Wi-Fi k odposlouchávání vašeho webového provozu a využít tyto informace k řadě nepěkných věcí, jako je krádež účtu nebo krádež identity.

To však neznamená, že byste nikdy neměli používat veřejnou síť Wi-Fi. Můžete zůstat v bezpečí tím, že se budete vyhýbat sítím Wi-Fi s podezřelými názvy, budete udržovat software svých zařízení aktualizovaný a budete se držet webových stránek, které používají protokol HTTPS (prohlížeče o tom obvykle informují ikonou visacího zámku v adresním řádku). Můžete také po připojení na Wi-Fi spustit VPN šifrovaný tunel.

Sociální média

Udržujte své osobní účty v soukromí

Vaše online účty by měly patřit do jedné ze dvou kategorií: veřejné a soukromé. Řekněme, že Twitter používáte k propagaci své práce, ke komunikaci s ostatními kolegy. To je veřejný účet. Ale vaše

osobní stránka na Facebooku? Nebo sekundární účet na Twitteru, kam rádi zveřejňujete neformálnější informace? Ty je nejlepší nechat soukromé.

Většina platforem sociálních médií nabízí spoustu nástrojů, které vám umožňují kontrolovat úroveň soukromí kolem vašeho účtu (účtů). Můžete mít například zcela soukromou stránku na Twitteru, ke které budou mít přístup pouze schválení sledující. Pokud máte veřejnou stránku na Instagramu, můžete si ještě zvolit, zda bude příběh viditelný pro všechny, kteří vás sledují, nebo pouze pro lidi, které jste si vybrali jako blízké přátele.

Pravidelně používejte možnosti "kontroly zabezpečení"

Mnoho služeb nabízí „kontrolu zabezpečení“, která vás provede nejdůležitějšími nastaveními ochrany osobních údajů. Je to pohodlný způsob, jak si rychle udělat přehled o svých účtech a rozhodnout se, zda je třeba nějaké nastavení upravit. A nepoužívejte je jen jednou - vytvořte si opakující se položku v kalendáři, která vám připomene, abyste si nastavení zabezpečení zkontrolovali např. každých 12 měsíců.

Dávejte si pozor na to, co sdílíte

Přemýšlejte, než něco napíšete. To platí pro osobní i pracovní účty. Možná máte nějaké „veřejné“ stránky na sociálních sítích, ale to neznamená, že byste na nich měli sdílet celý svůj život. Zvažte, co by z vašich veřejně přístupných stránek a příspěvků mohl vyčíst nějaký útočník. Například:

- Je opravdu nutné, abyste na své stránce na Twitteru sdíleli své narozeniny?
- Co je vidět na veřejně sdílených fotografiích a videích? Mohl by z nich někdo zjistit vaši aktuální polohu nebo místo, kde žijete?
- Sdílíte někde údaje o poloze? Mohou se například cizí lidé podívat na váš profil na Stravě a zjistit, kde každé ráno běháte?

Hardwarové vybavení

Šifrování citlivých dat

Citlivá data v počítači je dobré zašifrovat pro případ, že by je někdo ztratil, ukradl nebo zabavil. Pomocí služby FileVault společnosti Apple a šifrování zařízení společnosti Microsoft nebo služby BitLocker můžete zašifrovat pevný disk a zabránit tomu, aby související soubory viděla nebo zkopírovala osoba, která k tomu nedostala povolení.

Existují také nástroje třetích stran, jako je Veracrypt, který umožňuje šifrovat jakýkoli pevný disk, soubory a složky, a Boxcryptor, který chrání soubory uložené v cloudových platformách, jako jsou OneDrive, Dropbox a Disk Google.

Zvažte použití druhého zařízení, které je trvale offline

Jako další opatření můžete použít druhý počítač, který je vždy v režimu offline. Aby to fungovalo,

museli byste přenášet všechna data prostřednictvím externího úložiště, například USB flash disku nebo SD karty. Po dokončení práce by bylo třeba ji podobným způsobem přenést z počítače.

Proč se tím vším zabývat? Pokud je zařízení offline, bylo by pro útočníka mnohem těžší získat vzdálený přístup nebo vás podvodem přimět ke stažení škodlivého softwaru. Je to časově náročné nastavení, nicméně pokud pracujete s citlivými daty, které vyžadují mimořádnou péči a opatrnost, měli byste tuto možnost zvážit.

From:
https://navody.asuch.cas.cz/ -

Permanent link:
https://navody.asuch.cas.cz/doku.php/security?rev=1655288010

Last update: **2022/06/15 10:13**