NDI
NATIONAL DEMOCRATIC INSTITUTE

Kiberbiztonsági kézikönyv

a következő számára:

Civil társadalmi szervezetek

Útmutató azoknak a civil társadalmi szervezeteknek, amelyek szeretnének elindítani egy kiberbiztonsági tervet

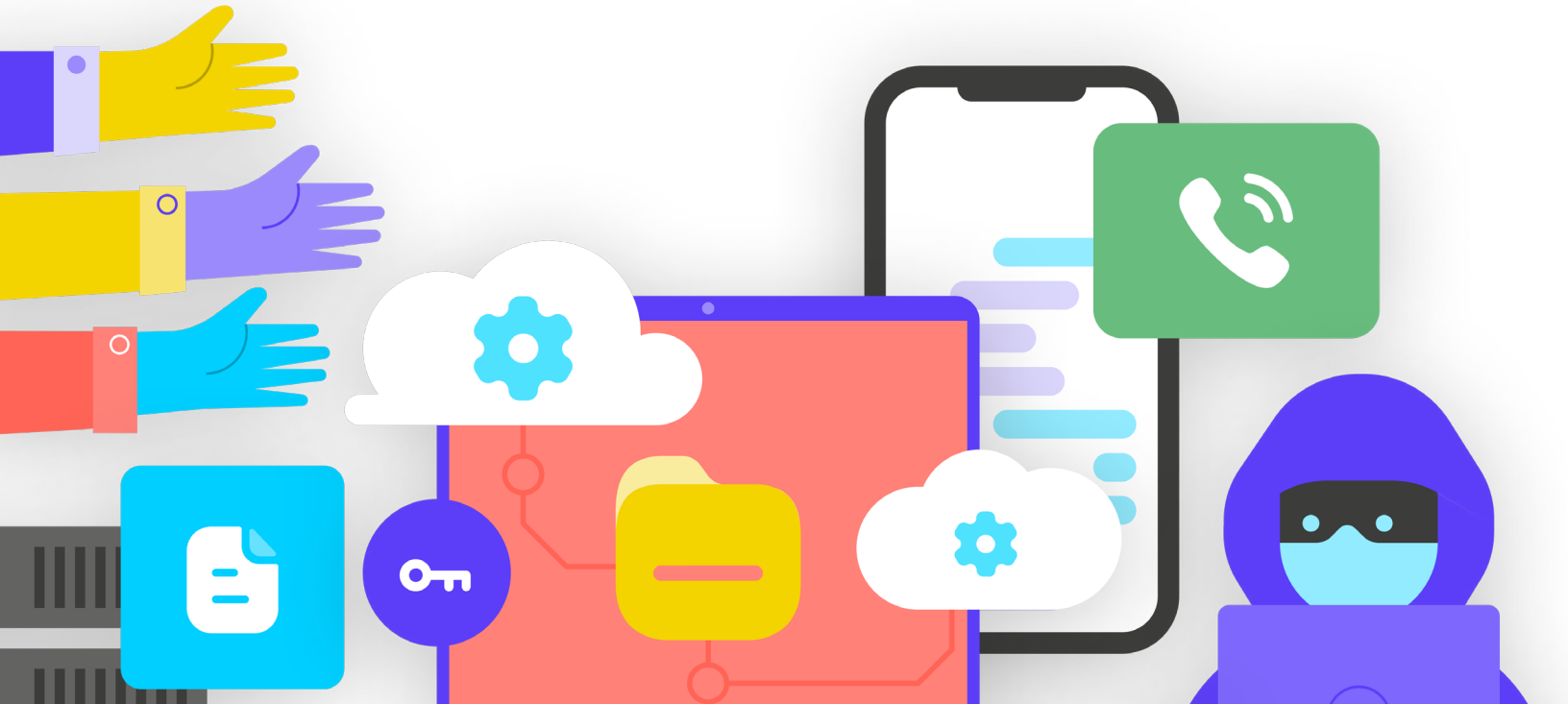
NDI
NATIONAL DEMOCRATIC INSTITUTE

Kiberbiztonsági kézikönyv

a következő számára:

Civil társadalmi szervezetek

Útmutató azoknak a civil társadalmi szervezeteknek,
amelyek szeretnének elindítani egy kiberbiztonsági tervet



Tartalomjegyzék

Vizuális jelmagyarázat

A Kézikönyvben a főszöveg mellett néhány különböző visszatérő, kiemelt elemet is talál. Íme egy rövid „jelmagyarázat”, amely segít megérteni az alapvető elemeket:

Esettanulmány

Esettanulmányokat jelöl, amelyek rávilágítanak egy adott téma valós hatására a civil társadalmi szervezetekre globálisan vagy egy adott országban.

Extra tippek

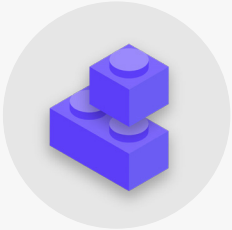
Kiemel néhány további tippet és információt, amelyekre a Kézikönyv olvasása közben figyelni kell.

Valós világ

Példákat hoz fel a „valós világban” használt kiberbiztonsági taktikai eszközökre, jókra és rosszakra egyaránt.

Speciális

Speciális témát jelöl – olyan információkat, amelyeket fontos figyelembe venni a szervezetének, de lehet, hogy kissé műszakibb vagy bonyolultabb.



Biztonsági terv építőelemei

A „Biztonsági terv építőelemeit” jelöli, amelyek a Kézikönyv egyes részeinek legfontosabb tudnivalói.

1

Biztonsági kultúra építése

2

Erős alapok: Fiókok és eszközök védelme

3

Adatok biztonságos kommunikációja és tárolása

4

Hogyan maradjon biztonságban az interneten

5

A fizikai biztonság védelme

6

Mi a teendő, ha a dolgok rosszul mennek

A Top 10

Ez a tíz elem kritikus fontosságú a szervezete biztonsági tervében. Ha valahol kezdeni szeretné, először nézze meg ezt.

1. **Rendszeresen tartson biztonsági képzést a szervezetén belül**
2. **Legyen óvatos az adathalászattal, és rendelkezzen jelentési rendszerrel**
3. **Használjon titkosítást minden kommunikációnál – a végpontok között, ha lehetséges**
4. **Erős jelszavakra van szükség, és a szervezeten belül vezessen be meg jelszókezelőt**
5. **Lehetőség szerint kéttényezős hitelesítés szükséges**
6. **Gondoskodjon arról, hogy a személyzet összes eszköze és szoftvere naprakész legyen**
7. **Használjon biztonságos felhőtárhelyet**
8. **Használjon HTTPS-t és adott esetben VPN-t az internet eléréséhez**
9. **Védje szervezete fizikai eszközeit**
10. **Készítsen szervezeti incidens-elhárítási tervet**

Szerzők és Köszönetnyilvánítás

Vezető szerző: **Evan Summers (NDI)**
Közreműködő szerzők: **Sarah Moulton (NDI); Chris Doten (NDI)**

A Kézikönyv kidolgozásához szeretnénk különösen köszönetet mondani szakértő külső lektorainknak, akik értékes visszajelzésekkel, szerkesztésekkel és javaslatokkal láttak el bennünket a tartalom összeállítása során, többek között:

Fiona Krakenburger, Open Technology Fund; Bill Budington és Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; and Whitney Pfeifer, NDI.

Ezúton is szeretnénk köszönetet mondani a Szervezetbiztonsági (OrgSec) Közösség által kifejlesztett és karbantartott fantasztikus kézikönyvekért, útmutatókért, munkafüzetekért, képzési modulokért és egyéb anyagokért. Ez a kézikönyv úgy készült, hogy kiegészítse ezeket a mélyrehatóbb anyagokat, és a kulcsfontosságú tanulságokat egyablakos, könnyen áttekinthető forrásban egyesítse azon civil társadalmi szervezetek számára, amelyek kiberbiztonsági tervet szeretnének kidolgozni.

Amellett, hogy közvetett ihletet merítettünk a közösség által összeállított számos csodálatos forrásból, e kézikönyvben, néhány meglévő forrásból is közvetlenül másoltunk hasznos információkat, különösen az Electronic Frontier Foundation Surveillance Self Defense Guide, Tactical Tech Holistic Security Manual dokumentumából, valamint egy sor magyarázatot a Center for Democracy and Technology és a Freedom of the Press Foundation forrásából. Az alábbi szakaszokban konkrét hivatkozásokat találhat ezekre a forrásokra, webes hivatkozásokra, szerzőkre és licencekre vonatkozó információkat az „A" függelékben.

Azt is nyomatékosan javasoljuk, hogy bárki, aki olvassa ezt a Kézikönyvet, használja az Open Technology Fund által összeállított és frissített digitális biztonsági útmutatók és források kiterjedt könyvtárát.

Kik vagyunk?

A Nemzetközi Ügyek Nemzeti Demokratikus Intézete (NDI) egy Washington DC-ben működő, nonprofit, pártoktól független szervezet, amely partnerségben dolgozik szerte a világon a demokratikus intézmények, folyamatok, normák és értékek megerősítése és védelme érdekében, hogy biztosítsa a jobb életminőséget mindenki számára.

Az NDI hiszi, hogy minden embernek joga van egy olyan világban élni, amely tiszteletben tartja a méltóságát, biztonságát és politikai jogait – és ez alól a digitális világ sem kivétel.

Az NDI-n belül a Demokrácia és Technológia csapata egy olyan globális digitális ökoszisztémát igyekszik előmozdítani, amelyben a demokratikus értékek védelmet élveznek, támogatják őket és virágozhatnak; a kormányok átláthatóbbak és befogadóbbak; és minden állampolgár fel van hatalmazva arra, hogy felelősségre vonja kormányát. Ezt a munkát a digitális ellenállás mellett elkötelezett aktivisták globális hálózatának támogatásával, valamint a partnerekkel az ehhez a kézikönyvhöz hasonló eszközök és erőforrások terén való együttműködés révén végezzük. Munkánkról többet megtudhat weboldalunkon, ha követ minket Twitteren, vagy közvetlenül a cyberhandbook@ndi.org címen. Mindig örömmel hallunk Öntől, és válaszolunk a csapatunkkal és a kiberbiztonsággal, technológiával és demokráciával kapcsolatos munkánkra vonatkozó kérdésekre.

Kinek szól ez a kézikönyv?

Ez a kézikönyv egy egyszerű célt szem előtt tartva íródott: hogy segítsen civil társadalmi szervezetének egy érthető és megvalósítható kiberbiztonsági tervet kidolgozni.

Ahogy a világ egyre inkább az internetre költözik, a kiberbiztonság nemcsak divatszó, hanem kritikus fogalom a szervezet sikere és a csapat biztonsága szempontjából. Különösen a demokrácia, az érdekképviselet, az elszámoltathatóság és az emberi jogi területek civil társadalmi szervezetei számára az információbiztonság (online és azon kívül is) olyan kihívás, amely összpontosítást, befektetést és éberséget igényel.

Szervezete valószínűleg kiberbiztonsági támadás célpontjává válik – ha még nem vált azzá. Ennek nem célja pánikkeltőnek lenni; ez még olyan szervezetek számára is valóság, amelyek nem tekintik magukat konkrét célpontnak.

Egy átlagos évben a Stratégiai és Nemzetközi Tanulmányok Központja, amely folyamatban lévő listát vezet az általuk „jelentős kiberincidensekről", több száz súlyos számítógépes támadást katalogizál, amelyek sokszor egyszerre több tucatnyi, ha nem többszáz szervezetet céloznak meg. Az ilyen bejelentett támadásokon kívül minden évben valószínűleg több száz kisebb támadásra is sor kerül, amelyek észrevétlenül vagy bejelentés nélkül maradnak, sokuk pedig a demokrácia, az elszámoltathatóság és az emberi jogok támogatásán dolgozó civil társadalmi szervezetek ellen irányul. A nőket vagy más marginalizált csoportokat képviselő szervezetek gyakran különösen célpontok.

Az ehhez hasonló kibertámadásoknak jelentős következményei vannak. Függetlenül attól, hogy a céljuk az Ön pénzének elvétele, hangjának elnyomása, szervezeti működésének megzavarása, hírnevének csorbítása, vagy akár olyan információk ellopása, amelyek pszichológiai vagy fizikai károsodáshoz vezethetnek partnereinél vagy munkatársainál, az ilyen fenyegetéseket komolyan kell venni. A jó dolog az, hogy nem kell kódolónak vagy technológusnak lennie ahhoz, hogy megvédje magát és szervezetét a gyakori fenyegetésekkel szemben. De fel kell készülnie arra, hogy némi erőfeszítést, energiát és időt fektessen egy erős szervezeti biztonsági terv kidolgozására és végrehajtására. Ha még soha nem gondolt a kiberbiztonságra a szervezetében, nem volt ideje rá koncentrálni, vagy ismer néhány alapvető dolgot a témával kapcsolatban, de úgy gondolja, hogy szervezete javíthatja kiberbiztonságát, akkor ez a kézikönyv Önnek szól. Függetlenül attól, hogy honnan érkezik, ennek a kézikönyvnek az a célja, hogy megadja szervezetének azokat az alapvető információkat, amelyekre egy erős biztonsági terv kidolgozásához szüksége van. Egy olyan tervhez, amely túlmutat a papírra vetett szavakon, és lehetővé teszi a bevált gyakorlatok megvalósítását.

Mi az a biztonsági terv, és miért kell a szervezetemnek rendelkeznie vele?

A biztonsági terv olyan írott irányelvek, eljárások és utasítások összessége, amelyekben a szervezet megállapodott, hogy elérje azt a biztonsági szintet, amelyet Ön és csapata megfelelőnek tart az emberek, partnerek és információk biztonságának megőrzéséhez.

Egy jól kidolgozott és frissített szervezeti biztonsági terv biztonságban tarthatja és hatékonyabbá teheti Önt azáltal, hogy nyugalmat biztosít a szervezete fontos napi munkájára való összpontosításhoz. Átfogó terv átgondolása nélkül nagyon könnyű vaknak lenni bizonyos típusú fenyegetésekkel szemben, túlságosan egy kockázatra összpontosítva vagy figyelmen kívül hagyva a kiberbiztonságot, amíg válság nem következik be. Amikor elkezdi a biztonsági terv kidolgozását, fel kell tennie magának néhány fontos kérdést, amelyek egy **kockázatértékelésnek** nevezett folyamatot alkotnak. A kérdések megválaszolása segít a szervezetnek megérteni azokat az egyedi fenyegetéseket, amelyekkel szembesül, és lehetővé teszi, hogy visszalépjen, és átfogóan átgondolja, mit kell megvédenie, és kitől kell megvédenie azt. A képzett értékelők, akiket olyan rendszerekkel támogatnak, mint az Interjúk SAFETAG auditálási keretrendszere, segíthetnek átvezetni a szervezetet egy ilyen folyamaton. Ha ilyen szintű szakmai tudáshoz jut hozzá, akkor megéri, de még ha nem is tud teljes körű felmérésen részt venni, akkor is érdemes megbeszélnie a szervezetével, hogy átgondolják ezeket a kulcsfontosságú kérdéseket:

1 Milyen eszközökkel rendelkezik a szervezete, és mit szeretne megvédeni?

Elkezdheti megválaszolni ezeket a kérdéseket, **ha létrehoz egy katalógust szervezete összes eszközéről**. Az olyan információk, mint az üzenetek, e-mailek, névjegyek, dokumentumok, naptárak és helyek, mind lehetséges eszközök. A telefonok, számítógépek és egyéb berendezések lehetnek eszközök. Az emberek és a kapcsolatok is értéket jelenthetnek. Készítsen **listát az eszközökről**, és próbálja katalogizálni azokat a szervezet számára fontosságuk, a tárolási helyük (esetleg több digitális vagy fizikai hely) szerint, és mi akadályozza meg, hogy mások hozzáférjenek, károsítsák vagy megzavarják őket. Ne feledje, hogy nem minden egyformán fontos. Ha a szervezet egyes adatai nyilvánosak, vagy olyan információk, amelyeket egyébként is közzétesz, akkor ezek nem titkok, amelyeket meg kell védenie.

2 Kik az ellenfelei, és mik a képességeik és motivációik?

Az „ellenfél" a szervezeti biztonságban általánosan használt kifejezés. Egyszerűen fogalmazva, az ellenfelek azok a szereplők (egyének vagy csoportok), akik érdekeltek abban, hogy megcélozzák az Ön szervezetét, megzavarják a munkáját, és hozzáférjenek az Ön információihoz vagy megsemmisítsék őket: a rosszfiúk. A lehetséges ellenfelek közé tartoznak például a pénzügyi csalók, versenytársak, helyi vagy nemzeti hatóságok vagy kormányok, vagy ideológiai vagy politikai indíttatású hackerek. Fontos, hogy listát készítsen az ellenfeleiről, és kritikusan gondolja át, kik akarnak negatívan hatni szervezetére és munkatársaira. Bár könnyű elképzelni a külső szereplőket (például egy külföldi kormányt vagy egy adott politikai csoportot) ellenfélként, ne feledje, hogy az ellenfelek lehetnek olyan emberek, akiket Ön ismer, például elégedetlen alkalmazottak, volt alkalmazottak, nem támogató családtagok vagy partnerek. A különböző ellenfelek különböző fenyegetéseket jelentenek, és eltérő erőforrásokkal és képességekkel rendelkeznek ahhoz, hogy megzavarják a műveleteket, és hozzáférjenek az Ön adataihoz vagy megsemmisítsék azokat.

Például a kormányok gyakran sok pénzzel és hatalmas befolyással rendelkeznek, beleértve az internet leállítását vagy a drága megfigyelési technológia használatát; a mobilhálózatok és az internetszolgáltatók valószínűleg hozzáférnek a hívási adataihoz és a böngészési előzményekhez; A nyilvános Wi-Fi hálózatokon képzett hackerek képesek a rosszul biztosított kommunikáció vagy pénzügyi tranzakciók lehallgatására. Akár saját maga ellenfele is lehet, ha például véletlenül töröl fontos fájlokat, vagy nem a megfelelő személynek küld privát üzenetet.

Az ellenfelek motívumai a képességeik, érdeklődési körük és stratégiáik függvényében valószínűleg különböznek. Érdekeltek a szervezet diszkreditálásában? Talán szándékukban áll elhallgatni az üzenetét? Vagy talán versenytársnak tekintik az Ön szervezetét, és előnyt akarnak szerezni? Fontos megérteni az ellenfél motivációját, mert ezzel segíthet a szervezetnek jobban felmérni az általa jelentett veszélyeket.

3 Milyen fenyegetésekkel néz szembe a szervezete? És ezek mennyire valószínűek és nagy hatásúak?

Ahogy azonosítja a lehetséges fenyegetéseket, valószínűleg hosszú listára bukkan, amely elsöprő lehet. Előfordulhat, hogy úgy érzi, minden erőfeszítés értelmetlen lenne, vagy nem tudja, hol kezdje. Annak érdekében, hogy szervezete képessé váljon a következő produktív lépések megtételére, hasznos az egyes fenyegetéseket két tényező alapján elemezni: a fenyegetés bekövetkezésének valószínűsége; és a hatása, ha bekövetkezik.

A fenyegetés valószínűségének mérésére (például „Alacsony, Közepes vagy Magas" annak alapján, hogy egy adott esemény nem valószínű, megtörténhet-e vagy gyakran megtörténik) felhasználhatja az ellenfelei kapacitásáról és motivációjáról ismert információkat, a múltbeli biztonsági incidensek elemzését, más hasonló szervezetek tapasztalatait, és természetesen a szervezete által bevezetett meglévő mérséklő stratégiák jelenlétét.

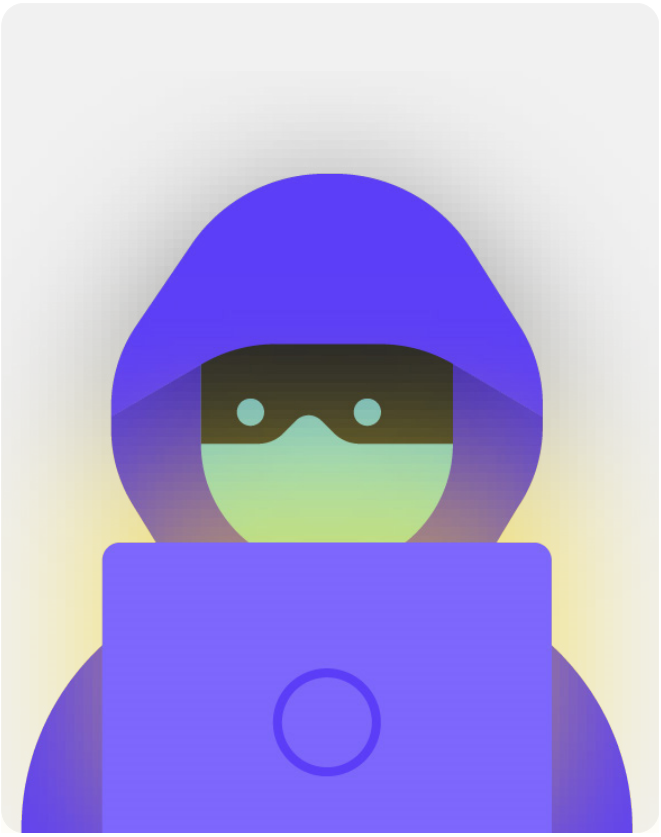
A fenyegetés hatásának méréséhez gondoljon arra, hogyan nézne ki a világa, ha a fenyegetés valóban megtörténne. Tegyen fel olyan kérdéseket, mint „hogyan ártott a fenyegetés nekünk, mint szervezetnek és az embereknek fizikailag és lelkileg?", „milyen hosszan tartó a hatása?", „teremt-e ez más káros helyzeteket?" és „hogyan hátráltat abban, hogy képesek legyünk elérni szervezeti céljainkat most és a jövőben?" Amikor válaszol ezekre a kérdésekre, gondolja át, hogy a fenyegetés alacsony, közepes vagy nagy hatású.

Miután a veszélyeket valószínűségük és hatásuk szerint kategorizálta, megkezdheti egy megalapozottabb cselekvési terv kidolgozását. Azokra a veszélyekre összpontosítva, amelyek a legvalószínűbbek

ÉS amelyeknek jelentős negatív hatásai lesznek, ott a korlátozott erőforrásait a lehető leghatékonyabb és legeredményesebb módon fogja átirányítani.

Az Ön célja mindig az, hogy a lehető legtöbb kockázatot csökkentse, de senki – sem a világ legjobb forrásaival rendelkező kormánya vagy vállalata – soha nem tudja teljesen kiküszöbölni a kockázatot. És ez így van rendjén: sokat tehet önmaga, kollégái és szervezete védelmében, ha gondoskodik a legnagyobb veszélyekről.

A kockázatértékelési folyamat kezelésének elősegítése érdekében fontolja meg az Electronic Frontier Foundation által kifejlesztett, ehhez hasonló munkalap használatát. Ne feledje, hogy a folyamat részeként kidolgozott információk (például az ellenfelek listája és az általuk jelentett fenyegetések) maguk is érzékenyek lehetnek. Ezért fontos, hogy biztonságban legyenek.



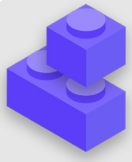
A Szervezeti kiberbiztonsági terv létrehozása

Bár a kockázatértékelés és a szervezeti dinamika alapján minden szervezet biztonsági terve egy kicsit másképp fog kinézni, bizonyos alapfogalmak szinte univerzálisak.

Ez a Kézikönyv ezekkel az alapvető fogalmakkal foglalkozik oly módon, hogy segítse szervezetét egy konkrét biztonsági terv felépítésében, amely gyakorlati megoldásokon és valós alkalmazásokon alapul.

Ez a kézikönyv arra törekszik, hogy ingyenes vagy nagyon alacsony költségű lehetőségeket és javaslatokat nyújtson. De ne feledje, hogy a hatékony biztonsági terv megvalósításának legjelentősebb költsége az idő, amikor Önnek és szervezetének meg kell beszélnie, megtanulnia és végrehajtania az új tervét. Tekintettel a kockázatokra, amelyekkel szervezete valószínűleg szembesül, ez a befektetés több mint megéri.

Minden szakaszban magyarázatot talál egy kulcsfontosságú témára, amellyel szervezetének és munkatársainak tisztában kell lenniük – mi ez és miért fontos. Mindegyik témakörhöz alapvető stratégiák, megközelítések és ajánlott eszközök párosulnak a kockázat csökkentésére, valamint tippek és hivatkozások további forrásokhoz, amelyek segíthetnek az ilyen ajánlások megvalósításában a szervezetében.



Biztonsági terv kezdőkészlet

Használja ezt a kezdőkészletet, hogy segítsen szervezetének feldolgozni a Kézikönyv leckéit, és valódi tervvé alakítani őket. A készletet kinyomtathatja, vagy digitálisan kitöltheti, miközben online olvassa a kézikönyvet. Miközben jegyzeteket készít, és elkezdi frissíteni vagy elkészíteni biztonsági tervét, feltétlenül hivatkozzon az egyes szakaszokban részletezett „Biztonsági terv építőelemeire” is. Egyetlen biztonsági terv sem teljes anélkül, hogy legalább ezekkel a lényeges elemekkel foglalkozna.

Használjon ki más forrásokat is, amelyek segíthetnek a terv elkészítésében és megvalósításában. Civil társadalmi szervezetként az ingyenes SOAP („Securing Organisations with Automated Policymaking”) alkalmazás segíthet leegyszerűsíteni és automatizálni a biztonsági terv létrehozását.

Használja az ingyenes képzési forrásokat is, mint például a Consumer Reports Security Planner, az Umbrella App a Security Firsttől, a Totem Project a Free Press Unlimitedtől és a Greenhost-tól, valamint a Global Cyber Alliance Cyber Hygiene for Mission Based-Organizations-jét, amelyek forrásokat tartalmaznak többre az ebben a kézikönyvben említett bevált gyakorlatok közül, valamint több tucat képzési eszközre mutató hivatkozásokat tartalmaznak, amelyek segítik az alapvető fontosságú alapok megvalósítását.

Biztonsági kultúra építése

A biztonság az emberekről szól, és szervezete védelme érdekében gondoskodnia kell arról, hogy minden érintett komolyan vegye a kiberbiztonságot. A kultúra megváltoztatása nehéz, de néhány egyszerű lépés és fontos beszélgetések sokat segíthetnek abban, hogy olyan légkört alakítsanak ki, amely növeli a személyzet és a szervezet ellenálló képességét a biztonsági fenyegetésekkel szemben. A szervezeti biztonsági kultúra felépítésének egyik legegyszerűbb, de legfontosabb lépése, hogy kommunikáljon erről a szervezeten belül, és hogy a vezetők mindig jó magatartást tanúsítsanak.

Integrálja a biztonságot normál működési struktúrájába

Amint azt a Tactical Tech holisztikus biztonsági útmutatója részletesen leírja, elengedhetetlen, hogy rendszeres, biztonságos tereket hozzunk létre, ahol a biztonság különböző aspektusairól beszélhetünk.

Ily módon, ha a csapattagoknak aggályaik vannak a biztonsággal kapcsolatban, kevésbé aggódnak, hogy paranoiásnak tűnnek, vagy mások idejét pazarolják. **A biztonságról szóló rendszeres beszélgetések ütemezése** normalizálja a biztonsággal kapcsolatos kérdésekről való interakció és gondolkodás gyakoriságát is, így a problémák nem merülnek feledésbe, és a csapat tagjai nagyobb valószínűséggel vesznek fel legalább passzív biztonsági tudatosságot a folyamatban lévő munkájukhoz. Nem kell minden héten, de legyen ismétlődő emlékeztető. Ezeknek a megbeszéléseknek nem csak a műszaki biztonság témaköreinek kell teret hagyniuk, hanem olyan kérdéseknek is, amelyek befolyásolják a személyzet kényelmét és biztonságát, mint például a közösségi konfliktusok, az online (és offline) zaklatás vagy a digitális eszközök használatával és bevezetésével kapcsolatos problémák. A beszélgetések olyan témákat is tartalmazhatnak, mint az offline információmegosztási szokások és az, hogy az alkalmazottak hogyan biztosítják vagy sem az információkat a munkahelyükön kívül. Végül is fontos észben tartani, hogy egy szervezet biztonsága csak annyira erős, amennyire a leggyengébb láncszeme. A következetes elkötelezettség megvalósításának egyik módja az, ha a rendszeres értekezletek napirendjét a biztonsággal egészítik ki. Forgathatja is a biztonságról szóló megbeszélések megszervezésének és elősegítésének felelősségét is a szervezet tagjai között, ami elősegítheti azt az elképzelést, hogy a biztonság mindenki felelőssége, nem csak néhány kiválasztotté. Ahogy elkezdi formalizálni a biztonsággal kapcsolatos megbeszéléseket, a személyzet valószínűleg kényelmesebben fogja megvitatni ezeket a fontos kérdéseket egymás között, és kevésbé formális környezetben is.

Az is fontos, hogy a biztonsági elemeket beépítsék a szervezet normál működésébe, például az alkalmazottak bevonása során – és gondoljanak arra, hogy csökkentsék az off-boardinghoz való hozzáférést. A biztonság nem lehet valami „extra dolog”, ami miatt aggódni kell, hanem inkább a ***stratégiájának és működésének szerves része.***

Ne feledje, hogy minden biztonsági tervet élő dokumentumnak kell tekinteni, és rendszeresen újra kell értékelni és meg kell vitatni, különösen akkor, ha új alkalmazottak vagy önkéntesek csatlakoznak a szervezethez, vagy ha megváltozik a biztonsági környezet.

Tervezze meg, hogy felülvizsgálja stratégiáját, és évente frissítéseket hajt végre, vagy ha jelentős változások következnek be a stratégiában, az eszközökben vagy az Ön előtt álló fenyegetésekben.

Szervezeti felvásárlás

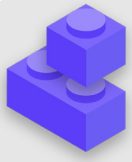
A sikeres biztonsági kultúra része az is, hogy biztosítsa a szervezeten belüli részvételt a biztonsági tervben.

Ennek döntően erős, hangos támogatást és útmutatást kell tartalmaznia a szervezeti vezetés részéről, akik sok esetben meghozzák a végső döntést az idő, az erőforrások és az energia beosztásáról egy hatékony biztonsági terv kidolgozására és végrehajtására. Ha ők nem veszik komolyan, senki más nem fogja. Ahhoz, hogy a szervezeten belül elérje ezt a részvételt, alaposan gondolja át, mikor és hogyan vezeti be a tervét, tegye ezt világosan, győződjön meg arról, hogy a vezetés megerősíti az üzeneteket, és mindenkit végigvezet a terv minden elemén és lépésén, hogy nincs rejtély vagy zűrzavar azzal kapcsolatban, hogy mit próbál elérni. Sok adományozó manapság megköveteli a támogatottaktól az erős biztonság fenntartását, így ennek hangsúlyozása az alkalmazottaknak jó módja lehet a szervezeti felvásárlás mélyebbé tételének. Ha a biztonságról beszél, kerülje az ijesztgetési taktikákat. Néha a fenyegetések, amelyekkel szervezete és munkatársai szembesülnek, ijesztőek lehetnek, de próbáljon meg a tények megosztására összpontosítani, és nyugodt teret teremtsen a kérdések és aggályok megvitatására. Ha túlságosan fenyegetőnek tűnnek a veszélyek, az arra késztetheti az embereket, hogy szenzációhajhásznak minősítsék Önt, vagy egyszerűen feladják, azt gondolva, hogy semmi sem számít, amit csinálnak – és semmi sem állhat távolabb az igazságtól.

Készítsen képzési tervet

Miután elkészítette és elkötelezte magát egy terv mellett, gondolja át, hogyan fogja az összes alkalmazottat (és önkénteseket) kiképezni ezekre az új bevált gyakorlatokra.

Hasznos taktika lehet a rendszeres képzés megkövetelése – és a képzésen való részvétel kötelezővé tétele, valamint az alkalmazottak teljesítményértékelésének értékelési pontja. Kerülje el, hogy kemény, negatív következményekkel járjon a biztonsági koncepciókkal küszködő személyzet számára. Ne feledje, hogy bizonyos alkalmazottak másként alkalmazkodhatnak a technológiához, és másként tanulhatnak a technológiáról, mint mások, a digitális eszközök és az internet különböző szintű ismeretében. A kudarctól való félelem csak tovább riasztja el az alkalmazottakat attól, hogy jelentsék a problémákat vagy segítséget kérjenek. A pozitív elszámoltathatóság és a sikeres képzésért és az irányelvek elfogadásáért járó jutalom megteremtése azonban elősegítheti a fejlődést az egész szervezetben. További értékes támogatást találhat a helyi vagy nemzetközi digitális biztonsági képzési hálózatokon és ingyenes képzési forrásokon keresztül, mint például az Umbrella App a Security Firsttől, a Totem Project a Free Press Unlimitedtől és a Greenhosttól, valamint a Global Cyber Alliance oktatási portálja.



Biztonsági kultúra építése

- **Rendszeres beszélgetések és képzések ütemezése a biztonságról és a biztonsági tervről.**
- **Vonjon be mindenkit – ossza meg a biztonsági terv végrehajtásával kapcsolatos felelősséget az egész szervezetben.**
- **Gondoskodjon arról, hogy a vezetés jó biztonsági magatartást és a terve iránti elkötelezettséget modellezzen.**
- **Kerülje el a félelem taktikáját vagy a büntetést – jutalmazza a fejlődést, és hozzon létre kényelmes teret a személyzet számára, hogy jelentse a problémákat és segítséget kérjen.**
- **Frissítse biztonsági tervét évente vagy a szervezetben bekövetkezett jelentős változások után.**

Erős alapok: Fiókok és eszközök védelme

Miért a fiókokra és az eszközökre kell összpontosítani? Mert ezek képezik az alapját mindannak, amit szervezete digitálisan csinál.

Szinte biztosan hozzáfér érzékeny információkhoz, belső és külső kommunikációt folytat, és személyes információkat ment el rajtuk. Ha nem biztonságosak, akkor mindezek és még sok más dolog veszélybe kerülhet. Például, ha hackerek figyelik a billentyűleütéseket vagy hallgatják le a mikrofonját, akkor a beszélgetései rögzítésre kerülnek, függetlenül attól, hogy mennyire biztonságosak az üzenetküldő alkalmazásai. Vagy ha egy ellenfél hozzáfér a szervezet közösségimédia-fiókjaihoz, könnyen árthat az Ön hírnevének és hitelességének, ami aláásható munkája sikerét. Ezért alapvető fontosságú, hogy szervezetként mindenki tegyen néhány egyszerű, de hatékony lépést eszközei és fiókjai biztonságának megőrzése érdekében. Fontos megjegyezni, hogy ezek az ajánlások magukban foglalják a személyes fiókokat és eszközöket is, mivel ezek gyakran könnyű célpontok az ellenfelek számára. A hackerek szívesen keresik a legegyszerűbb célpontot, és betörnek egy személyes fiókba vagy otthoni számítógépbe, ha csapata ezeket használja kommunikációra és fontos információk elérésére.

Biztonságos fiókok és civil társadalom

A 2020 végén feltárt, széles körben nyilvánosságra hozott SolarWinds feltörés, amely több mint 250 szervezetet veszélyeztetett, köztük a legtöbb amerikai kormányhivatalt, technológiai szállítókat, például a Microsoftot és a Cisco-t, valamint a civil szervezeteket, részben annak a következménye, hogy a hackerek gyenge jelszavakat találtak ki, amelyeket fontos rendszergazdai fiókokhoz használtak. Összességében a hackeléssel kapcsolatos jogsértések körülbelül 80%-a gyenge vagy újrafelhasznált jelszavak miatt következik be.

Az ehhez hasonló jelszavak megsértésének növekvő elterjedésével és a könnyebb hozzáféréssel a kifinomult jelszófeltörő eszközökhöz a különböző ellenfelek számára a kéttényezős hitelesítés elengedhetetlen biztonsági követelmény a civil társadalmi szervezetek számára. A Facebook 2020-ban beszámolt arról, hogy civil társadalmi fiókokat támadtak meg.

Beszámolójuk szerint a bangladesi hackercsoportok a helyi civil társadalmi aktivisták, újságírók és vallási kisebbségek beszámolóit vették célba. Sajnos a hackereknek sikerült feltörniük néhány ilyen Facebook-fiókot, köztük egy helyi csoport Facebook-oldalának az adminisztrátoráét. Az adminisztrátori fiókhoz való hozzáféréssel a hackerek eltávolították a fennmaradó adminisztrátorokat, átvették és letiltották az oldalt, megakadályozva, hogy a csoport megosszon kulcsfontosságú információkat és kommunikáljon a közönségével. A Facebook vizsgálata során kiderült, hogy a fiókokat valószínűleg különféle eszközökkel, többek között a fiók-helyreállítási folyamattal való visszaélésekkel is feltörték. Ha az összes fiók kéttényezős hitelesítést használt volna, az ilyen támadásokat sokkal nehezebb lett volna hatékonyan végrehajtani a hackerek számára.

Biztonságos fiókok: Jelszavak és kétfaktoros hitelesítés

A mai világban valószínű, hogy az Ön szervezete és munkatársai több tucat, ha nem több száz fiókkal rendelkeznek, amelyek feltörése érzékeny információkhoz vezethet, vagy akár a veszélyeztetett egyének sérülését is okozhatja.

Gondoljon az egyes alkalmazottak és a szervezet egészének különböző fiókjaira: e-mailek, csevegőalkalmazások, közösségi média, online banki szolgáltatások, felhőalapú adattárolás… és ruhaüzletek, helyi pizzéria, újságok és bármely más weboldalak vagy alkalmazások, amelyekbe bejelentkezik. A jó biztonság a mai világban szorgalmas megközelítést igényel az ezen fiókok támadásokkal szembeni védelméhez. Ez a jó jelszóhigiéniával és a kétfaktoros hitelesítés használatával kezdődik az egész szervezetben.

MITŐL LESZ JÓ EGY JELSZÓ?

A jó, erős jelszónak három kulcsa van: hossz, véletlenszerűség és egyediség.

HOSSZ

Minél hosszabb a jelszó, annál nehezebb az ellenfélnek kitalálnia. Manapság a legtöbb jelszófeltörést számítógépes programok hajtanak végre, és ezeknek az aljas programoknak nem tart sokáig egy rövid jelszó feltörése. Emiatt elengedhetetlen, hogy jelszavai legalább 16 karakterből, vagy legalább 5 szóból álljanak, de lehetőleg hosszabbak legyenek.

VÉLETLENSZERŰSÉG

Még ha egy jelszó hosszú is, nem túl jó, ha olyasmiről van szó, amit az ellenfél könnyen kitalál Önről. Kerülje az olyan információk megadását, mint a születésnapja, szülővárosa, kedvenc tevékenységei vagy egyéb olyan tények, amelyeket valaki egy gyors internetes kereséssel megtudhat Önről.

EGYEDISÉG

Talán a legelterjedtebb „legrosszabb gyakorlat” az ugyanazon jelszó használata több weboldalon. A jelszavak ismétlése nagy probléma, mert ez azt jelenti, hogy ha csak az egyik fiókot feltörték, az ugyanazt a jelszót használó többi fiók is sebezhetővé válik. Ha ugyanazt a jelszót több weboldalon használja, az nagymértékben növelheti egyetlen hiba vagy adatszivárgás hatását. Bár lehet, hogy nem törődik a helyi könyvtár jelszavával, ha azt feltörik, és ugyanazt a jelszót használja egy érzékenyebb fiókban, fontos információkat lophatnak el.

A hossz, véletlenszerűség és egyediség céljainak elérésének egyik egyszerű módja, ha kiválasztunk három vagy négy gyakori, de véletlenszerű szót. Jelszava például lehet „virághagyma zöld medve", amelyet könnyű megjegyezni, de nehéz kitalálni. Vessen egy pillantást **erre a weboldalra** a Better Buys-tól, hogy megtudja, milyen gyorsan lehet feltörni a rossz jelszavakat.

HASZNÁLJON JELSZÓKEZELŐT SEGÍTSÉGKÉNT

Tudja tehát, hogy a szervezet minden tagja számára fontos, hogy hosszú, véletlenszerű és eltérő jelszót használjon minden személyes és szervezeti fiókjához, de hogyan teheti ezt meg valójában? Több tucat (ha nem több száz) fiókhoz lehetetlen jó jelszót megjegyezni, ezért mindenkinek csalnia kell. Ennek rossz módja a jelszavak újrafelhasználása. Szerencsére ehelyett a digitális jelszókezelőkhöz fordulhatunk, hogy sokkal könnyebbé tegyük életünket (és jelszavaink biztonságosabbá tételét). Ezek az alkalmazások, amelyek közül sok számítógépről vagy mobileszközről is elérhető, jelszavakat hozhatnak létre, tárolhatnak és kezelhetnek az Ön és az egész szervezete számára. A biztonságos jelszókezelő alkalmazása azt jelenti, hogy mindig csak egy nagyon erős, hosszú jelszót kell megjegyeznie, amelyet elsődleges jelszónak (vagy „fő" jelszónak) neveznek, miközben kihasználhatja a jó, egyedi jelszavak használatának biztonsági előnyeit az összes fiókjában. Ezt az elsődleges jelszót (és esetleg egy második hitelesítési tényezőt (2FA), amelyet a következő részben tárgyalunk) fogja használni a jelszókezelő megnyitásához és az összes többi jelszavához való hozzáférés feloldásához. A jelszókezelők több fiók között is megoszthatók a biztonságos jelszómegosztás megkönnyítése érdekében az egész szervezeten belül.

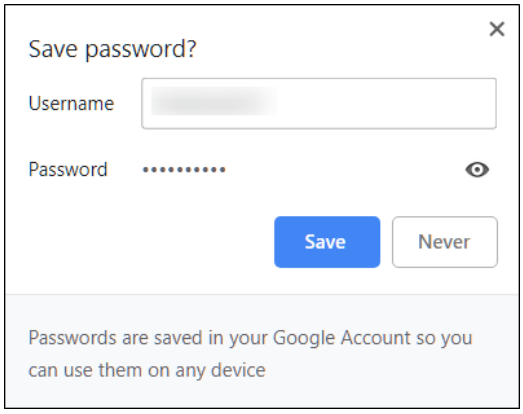
Miért kell valami újat használnunk? Nem írhatjuk le csak papírra vagy egy táblázatba a számítógépen?

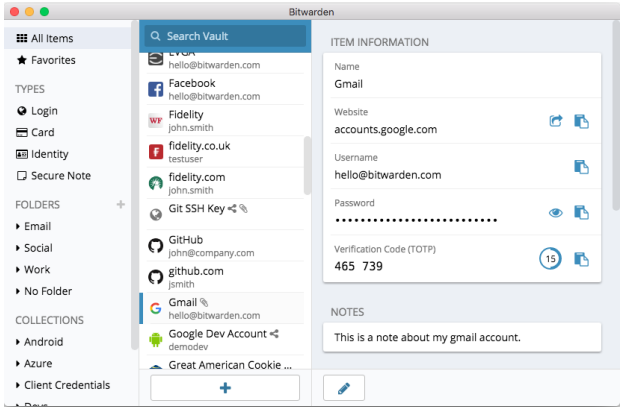
Sajnos sok elterjedt módszer létezik a nem biztonságos jelszavak kezelésére. Ha papírlapokon tárolja a jelszavakat (hacsak nem tartja őket széfben elzárva), fizikai lopásnak, kíváncsi tekintetnek, valamint könnyű elvesztésnek és sérülésnek teheti ki őket. Ha elmenti a jelszavakat egy dokumentumba a számítógépén, a hacker sokkal könnyebben hozzáférhet – vagy ha valaki ellopja a számítógépét, akkor nemcsak az eszközéhez, hanem az összes fiókjához is hozzáférhet. Egy jó jelszókezelő használata ugyanolyan egyszerű, mint a dokumentum, de sokkal biztonságosabb.

Miért bízzunk meg a jelszókezelőben?

A minőségi jelszókezelők rendkívüli erőfeszítéseket tesznek (és kiváló biztonsági csapatokat alkalmaznak), hogy rendszereiket biztonságban tartsák. A jó jelszókezelő alkalmazások (az alábbiakban néhány ajánlott) szintén úgy vannak beállítva, hogy ne tudják „feloldani" a fiókokat. Ez azt jelenti, hogy a legtöbb esetben még ha feltörték is őket, vagy jogilag kényszerítenék őket információ átadására, akkor sem veszíthetnék el vagy adhatnák fel jelszavait. Azt is fontos megjegyezni, hogy végtelenül valószínűbb, hogy egy ellenfél kitalálja valamelyik gyenge vagy ismétlődő jelszavát, vagy talál egyet **nyilvános adatvédelmi incidensben**, mint annak, hogy egy jó jelszókezelőnek hiányosak a biztonsági rendszerei. Fontos, hogy szkeptikusak legyünk, és semmiképpen sem szabad vakon megbízni minden szoftverben és alkalmazásban, de a jó hírű jelszókezelők minden megfelelő ösztönzést megkapnak a helyes cselekvésre.

Ahelyett, hogy böngészőjét (például a bal oldalon látható Chrome-ot) használná a jelszavak mentésére, használjon dedikált Jelszókezelőt (például a jobb oldalon látható Bitwarden-t). A Jelszókezelők olyan funkciókkal rendelkeznek, amelyek biztonságosabbá és kényelmesebbé teszik szervezete életét.





Mi a helyzet a jelszó tárolásával a böngészőben?

A jelszavak böngészőben való mentése nem egyenlő a biztonságos jelszókezelő használatával. Röviden: ne használjon Chrome-ot, Firefoxot, Safarit vagy bármilyen más böngészőt jelszókezelőként. Bár határozottan előrelépést jelent a papírra íráshoz vagy a táblázatba mentéshez képest, a webböngésző alapvető jelszómentési funkciói hagynak némi kívánnivalót maga után biztonsági szempontból. Ezek a hiányosságok megfosztják attól a kényelemtől is, amelyet egy jó jelszókezelő nyújt a szervezet számára. Ennek a kényelemnek az elvesztésével valószínűbb, hogy az emberek a szervezetben továbbra is rossz jelszó létrehozási és megosztási gyakorlatokat fognak folytatni.

Például a dedikált jelszókezelőkkel ellentétben a böngészők beépített „jelszó mentése” vagy „emlékezzen erre a jelszóra” funkciói nem biztosítanak egyszerű mobilkompatibilitást, böngészők közötti funkcionalitást, valamint erős jelszógeneráló és -auditáló eszközöket. Ezek a funkciók nagy részét képezik annak, ami a dedikált jelszókezelőt olyan hasznossá és előnyössé teszi a szervezet biztonsága szempontjából.

A jelszókezelők szervezetspecifikus szolgáltatásokat is tartalmaznak (például a jelszómegosztást), amelyek nemcsak az egyénnek, hanem a szervezet egésze számára is biztonsági értéket jelentenek. Ha a böngészővel mentett jelszavakat (szándékosan vagy véletlenül), szánjon egy percet azok eltávolítására.

Milyen jelszókezelőt használjunk?

Sok jó jelszókezelő eszköz létezik, amelyek kevesebb mint harminc perc alatt beállíthatók. Ha megbízható online lehetőséget keres szervezete számára, amelyhez az emberek bármikor több eszközről is hozzáférhetnek, akkor a 1Password (2,99 USD/felhasználó/hó) vagy az ingyenes, nyílt forráskódú BitWarden jól támogatott és ajánlott. Egy olyan online lehetőség, mint a BitWarden, nagyszerű lehet a biztonság és a kényelem szempontjából. A BitWarden például segít erős egyedi jelszavak létrehozásában, és a böngészőbővítményeken és egy mobilalkalmazáson keresztül több eszközről is elérheti a jelszavakat. A fizetős verzióval (10 dollár egy teljes évre) a BitWarden az újrafelhasznált, gyenge és esetleg feltört

jelszavakról is jelentéseket készít, hogy segítsen a dolgokkal kapcsolatban naprakésznek maradni. Miután beállította elsődleges jelszavát (amelyet fő jelszónak neveznek), be kell kapcsolnia a kétfényezős hitelesítést is, hogy a jelszókezelő tárolója a lehető legnagyobb biztonságban legyen.

A jelszókezelő használatakor is elengedhetetlen a jó biztonság gyakorlása. Például, ha a jelszókezelő böngészőbővítményét használja, vagy bejelentkezik a BitWardenbe (vagy bármely más jelszókezelőbe) egy eszközön, ne felejtsen el kijelentkezni használat után, ha megosztja az eszközt, vagy úgy gondolja, hogy felfokozott fizikai eszközlopás veszélye áll fenn. Ez magában foglalja a jelszókezelőből való kijelentkezést, ha felügyelet nélkül hagyja a számítógépet vagy mobileszközt. Ha a szervezeten belül megosztja a jelszavakat, feltétlenül vonja vissza a jelszavakhoz való hozzáférést (és módosítsa magukat a jelszavakat), amikor az emberek elhagyják a szervezetet. Nem szeretné például, hogy egy korábbi alkalmazott továbbra is hozzáférjen szervezete Facebook-jelszavához.

Mi van, ha valaki elfelejti az elsődleges jelszavát?

Fontos, hogy emlékezzen az elsődleges jelszóra. A fent javasolthoz hasonló jó jelszókezelő rendszerek nem emlékeznek az elsődleges jelszavára, és nem teszik lehetővé annak közvetlen visszaállítását e-mailben, ahogyan azt weboldalak esetében megteheti. Ez egy jó biztonsági funkció, de elengedhetetlenné teszi az elsődleges jelszó tárolását a jelszókezelő első beállításakor. Ennek elősegítése érdekében fontolja meg egy napi emlékeztető beállítását, amely emlékezteti elsődleges jelszavára, amikor először hoz létre jelszókezelő fiókot.

Jelszókezelő használata a szervezeténél

Megerősítheti a teljes szervezet jelszóhasználati gyakorlatát, és biztosíthatja, hogy minden alkalmazott hozzáférjen (és használjon) jelszókezelőt, ha bevezet egyet az egész szervezetre kiterjedően. Ahelyett, hogy minden egyes alkalmazott saját maga állítaná be a sajátját, fontolja meg az egy „csapat” vagy „üzleti” tervbe való befektetést. Például a BitWarden **„csapatszervezési” terve** felhasználónként havonta 3 dollárba kerül. Ezzel (vagy a jelszókezelők más csapatterveivel, mint például a 1Password) képes kezelni az összes megosztott jelszót a szervezeten belül. Az egész szervezetre kiterjedő jelszókezelő szolgáltatásai nemcsak nagyobb biztonságot, hanem kényelmet is nyújtanak a személyzet számára. A hitelesítő adatokat a jelszókezelőn belül biztonságosan megoszthatja különböző felhasználói fiókokkal. A BitWarden például egy kényelmes, végpontok közötti titkosított szöveg- és fájlmegosztó funkciót is biztosít, „BitWarden Send” néven a csapattervén belül. Mindkét funkció segítségével szervezete jobban szabályozhatja, hogy ki láthatja és oszthatja meg a jelszavakat, és biztonságosabb lehetőséget kínál a csoportszintű vagy csoportos fiókok hitelesítő adatainak megosztására. Ha beállít egy szervezetszintű jelszókezelőt, győződjön meg arról, hogy valaki kifejezetten felelős a személyzeti fiókok eltávolításáért és a megosztott jelszavak megváltoztatásáért, amikor valaki elhagyja a csapatot.

MI AZ A KÉTTÉNYEZŐS HITELESÍTÉS?

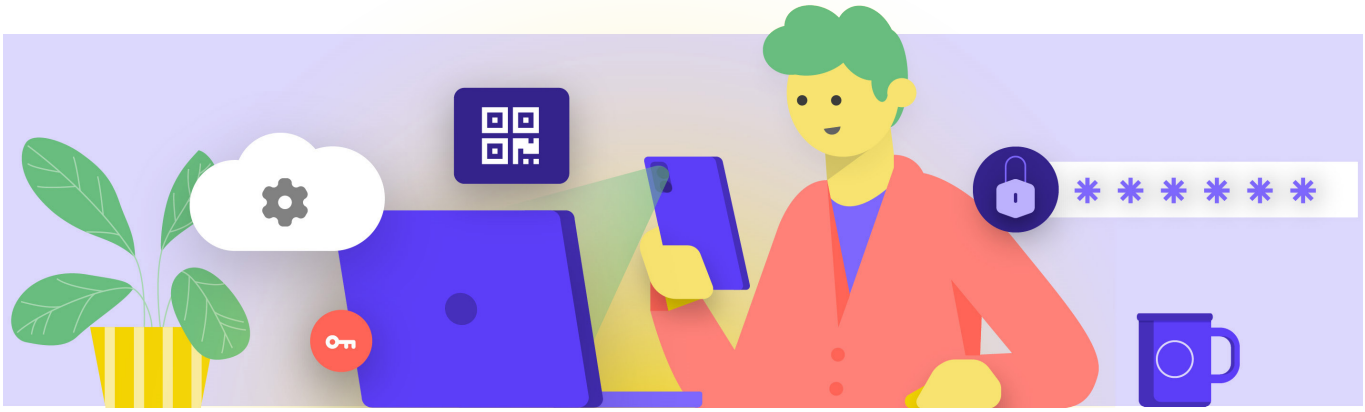
Bármilyen jó is a jelszóhigiénia, túlságosan gyakori, hogy a hackerek kitalálják a jelszavakat. Ahhoz, hogy fiókjait biztonságban tartsa a mai világban gyakori fenyegetésekkel szemben, egy másik védelmi szintre van szükség. Itt jön képbe a többtényezős vagy kéttényezős hitelesítés – ezt 2FA-nak nevezik. Számos nagyszerű útmutató és forrás magyarázza a kéttényezős hitelesítést, köztük Martin Shelton Kéttényezős hitelesítés kezdőknek cikke és a Demokrácia és Technológiai Központ Election Cybersecurity 101 Field Guide-ja. Ez a rész mindkét forrásból nagymértékben kölcsönöz, hogy elmagyarázza, miért olyan fontos a 2FA alkalmazása az egész szervezetben. Röviden, a 2FA erősíti a fiók biztonságát azáltal, hogy egy második információra is szükség van – ami több, mint egy jelszó – a hozzáféréshez. A második információ általában az Ön birtokában lévő információ, például a telefonon lévő alkalmazásból származó kód vagy egy fizikai token vagy kulcs. Ez a második információ a védelem második rétegeként működik. Ha egy hacker ellopja az Ön jelszavát, vagy egy jelentős adatvédelmi incidens során jelszóhalmazon keresztül hozzáfér, a hatékony 2FA megakadályozhatja, hogy hozzáférjen a fiókjához (és ezáltal távol maradjon a személyes és bizalmas információktól). Rendkívül fontos annak biztosítása, hogy a szervezetben mindenki 2FA-t helyezzen el a fiókjában.

HOGYAN ÁLLÍTHATJUK BE A 2FA-t?

A 2FA-nál három általános módszer létezik: biztonsági kulcsok, hitelesítési alkalmazások és egyszeri SMS-kódok.

Biztonsági kulcsok

A biztonsági kulcsok a legjobb megoldás, részben azért, mert szinte teljesen adathalászat-biztosak. Ezek a „kulcsok" hardveres tokenek (gondoljunk csak a mini USB-meghajtókra), amelyek a kulcstartóhoz csatlakozhatnak (vagy a számítógépben maradhatnak) a könnyű hozzáférés és a biztonságos tárolás érdekében. Ha eljött az ideje, hogy a kulccsal feloldja egy adott fiók zárolását, egyszerűen helyezze be a készülékbe, és fizikailag érintse meg, amikor a rendszer kéri a bejelentkezés során. A modellek széles skáláját vásárolhatja meg online (20-50 USD), beleértve a Yubikeys-t vagy a Google Titan kulcsait. A New York Times Wirecutter egy hasznos útmutatót jelentetett meg, amely ajánlásokat tartalmaz a kulcsok megvásárlására vonatkozóan. Ne feledje, hogy ugyanaz a biztonsági kulcs tetszőleges számú fiókhoz használható. Míg a biztonsági kulcsok sok szervezet számára költségesek, az olyan kezdeményezések, mint a Google Speciális védelmi programja vagy a Microsoft AccountGuard, ingyenesen biztosítják ezeket a kulcsokat bizonyos kockázati csoportok számára. Lépjen kapcsolatba azokkal az emberekkel, akik a Kézikönyvet adták Önnek, és nézze meg, hogy összekapcsolhatják-e Önt ilyen programokkal, vagy lépjen kapcsolatba a cyberhandbook@ndi.org címen.



Hitelesítési alkalmazások

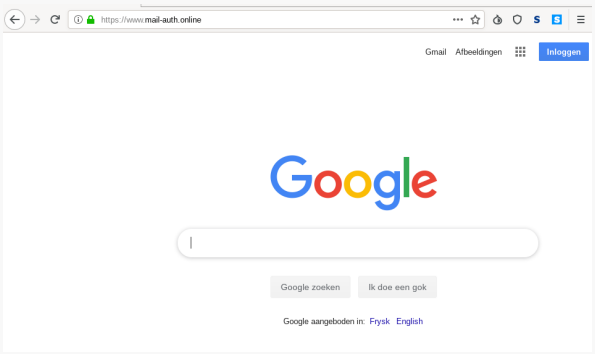
A **2FA második legjobb módja a hitelesítő alkalmazások.** Ezek a szolgáltatások lehetővé teszik, hogy ideiglenes kétfényezős bejelentkezési kódot kapjon mobilalkalmazáson keresztül vagy push értesítésként okostelefonján. Néhány népszerű és megbízható lehetőség közé tartozik a Google Authenticator, az Authy és a Duo Mobile. A Hitelesítő alkalmazások azért is nagyszerűek, mert akkor működnek, amikor nem fér hozzá a mobilhálózathoz, és ingyenesen használhatók egyének számára. A hitelesítő alkalmazások azonban jobban ki vannak téve az adathalászatnak, mint a biztonsági kulcsok, mivel a felhasználókat rávehetik arra, hogy biztonsági kódokat írjanak be egy hitelesítő alkalmazásból egy hamis weboldalra. Ügyeljen arra, hogy a bejelentkezési kódokat csak legitim weboldalakon adja meg. És ne „fogadja el" a bejelentkezési push értesítéseket, hacsak nem biztos abban, hogy Ön kérte a bejelentkezést. Az is elengedhetetlen, ha hitelesítő alkalmazást használ, hogy készüljön fel biztonsági kódokkal (lásd alább) arra az esetre, ha telefonja elveszne vagy ellopnák.

Kódok SMS-ben

A 2FA legkevésbé biztonságos, de sajnos még mindig leggyakoribb formája az SMS-ben küldött kódok. Mivel az SMS-ek lehallgathatók, a telefonszámok pedig hamisíthatók vagy feltörhetők a mobilszolgáltatón keresztül, az SMS sok kívánnivalót hagy maga után a 2FA-kódok kérésének módjaként. Ez jobb, mint a jelszó használata, de a hitelesítő alkalmazások vagy a fizikai biztonsági kulcs használata javasolt, ha egyáltalán lehetséges. Egy elszánt ellenfél hozzáférhet az SMS 2FA kódokhoz, általában csak felhívja a telefontársaságot és kicseréli a SIM-kártyáját. Ha készen áll arra, hogy engedélyezze a 2FA-t szervezete összes különböző fiókjában, használja ezt a weboldalt: (https://2fa.directory/), ahol gyorsan megkeresheti az információkat és utasításokat bizonyos szolgáltatásokhoz (például Gmail, Office 365, Facebook, Twitter stb.), és megtudhatja, hogy mely szolgáltatások milyen típusú 2FA-t tesznek lehetővé.

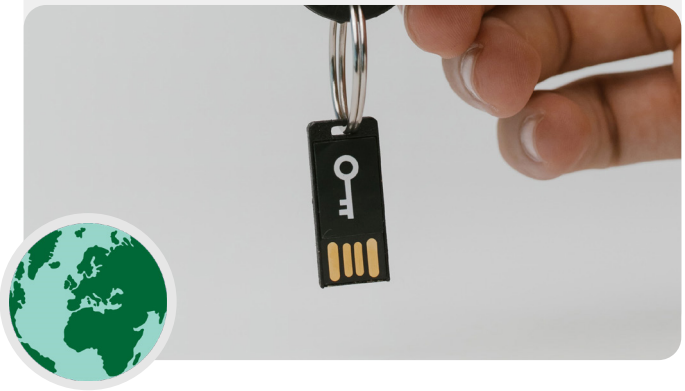
2FA és a civil társadalom

Az Amnesty International közelmúltbeli jelentése szerint az üzbegisztáni emberi jogi jogvédőket megcélzó hackerek adathalász támadásokkal verték át a felhasználókat, hogy hamis Gmail bejelentkezési oldalakon jelszavaikat *és* kétfaktoros hitelesítési kódokat osszák meg e-mail fiókjaikkal. Az ilyen támadások egyre gyakoribb módja a kétfaktoros hitelesítés „megkerülésének". Fontos – még akkor is, ha a 2FA a helyén van –, hogy ügyeljen arra, hogy hova írja be a kódokat. Még jobb, ha fizikai biztonsági kulcsok elfogadásával kiküszöbölheti ezt a kockázatot.



Biztonsági kulcsok a való világban

Azáltal, hogy fizikai biztonsági kulcsokat biztosított a kétfaktoros hitelesítéshez mind a 85 000+ alkalmazottja számára, a Google (egy nagyon magas kockázatú, célzott szervezet) hatékonyan kiküszöbölte a szervezet elleni sikeres adathalász támadásokat. Ez az eset megmutatja, milyen hatékonyak lehetnek a biztonsági kulcsok még a leginkább veszélyeztetett szervezetek számára is.



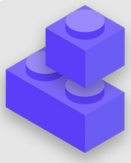
MI VAN, HA VALAKI ELVESZÍT EGY 2FA-KÉSZÜLÉKET?

Ha biztonsági kulcsot használ, kezelje ugyanúgy, mint háza vagy lakása kulcsát, ha rendelkezik ilyennel. Röviden: ne veszítse el. Csakúgy, mint a házkulcsok, mindig jó ötlet egy tartalék kulcsot regisztrálni a fiókjába, amely biztonságos helyen (például otthoni széfben vagy széfben) elzárva marad, ha elveszik vagy ellopják. Alternatív megoldásként (azoknál a fiókoknál, amelyek ezt lehetővé teszik) biztonsági kódokat kell létrehoznia. Ezeket a kódokat nagyon biztonságos helyen kell tárolnia, például a jelszókezelőben vagy egy fizikai széfben. Az ilyen biztonsági kódok a legtöbb weboldal 2FA-beállításaiban generálhatók (azon a helyen, ahol először engedélyezi a 2FA-t), és vészhelyzet esetén biztonsági kulcsként működhetnek. A leggyakoribb 2FA hiba akkor fordul elő, amikor az emberek kicserélik vagy elvesztik a hitelesítési alkalmazásokhoz használt telefonjukat. Ha a Google Hitelesítőt használja, nem jár szerencsével, ha telefonját ellopják, hacsak nem menti el azokat a biztonsági kódokat, amelyeket a fióknak a Google Hitelesítőhöz való csatlakoztatásakor generált. Ezért, ha a Google Hitelesítőt 2FA-alkalmazásként használja, ügyeljen arra, hogy biztonságos helyen mentse el az összes csatlakoztatott fiók biztonsági kódját. Az Authy vagy a Duo használata esetén mindkét alkalmazás rendelkezik beépített biztonsági mentési funkciókkal, erős biztonsági beállításokkal, amelyeket engedélyezhet. Ha valamelyik alkalmazást választja, konfigurálhatja ezeket a biztonsági mentési beállításokat az eszköz törése, elvesztése vagy ellopása esetén. Tekintse meg az Authy utasításait itt, a Duo utasításait pedig itt. Győződjön meg arról, hogy a szervezet minden tagja tisztában van ezekkel a lépésekkel, amikor elkezdi engedélyezni a 2FA-t az összes fiókjában.

A 2FA érvényesítése az egész szervezetben

Ha szervezete e-mail fiókokat biztosít minden alkalmazottnak a Google Workspace (korábbi nevén GSuite) vagy a Microsoft 365 szolgáltatáson keresztül a saját tartományán (például @ ndi.org) keresztül, akkor minden fiókra érvényesítheti a 2FA és erős biztonsági beállításokat. Az ilyen betartatás nemcsak segít megvédeni ezeket a fiókokat, hanem a 2FA bevezetésének és normalizálásának módja is az alkalmazottak számára, hogy kényelmesebben alkalmazzák azt a személyes fiókokhoz is. Google Workspace-adminisztrátorként ezeket az utasításokat követve érvényesítheti a 2FA-t a tartományában. Hasonló műveleteket hajthat végre a Microsoft 365 rendszerben ezeket a lépéseket követve tartományi rendszergazdaként.

Fontolja meg szervezete fiókjainak regisztrálását a Speciális védelmi programba (Google) vagy az AccountGuardba (Microsoft), hogy további biztonsági ellenőrzéseket hajtson végre, és fizikai biztonsági kulcsokat igényeljen a kétfaktoros hitelesítéshez.



Biztonságos fiókok

- **Erős jelszavak megkövetelése minden szervezeti fiókhoz; ösztönözze ugyanezt a személyzet és az önkéntesek személyes fiókjai esetében is.**
- **Megbízható jelszókezelő bevezetése a szervezet számára (és ösztönözze annak használatát a személyzet személyes életében is).**
  - Minden jelszókezelő fiókhoz erős elsődleges jelszót és 2FA-t kell megkövetelni.
  - Emlékeztessen mindenkit, hogy jelentkezzen ki a jelszókezelőből megosztott eszközökön, vagy ha nagyobb az eszköz ellopásának vagy elkobzásának kockázata.
- **Módosítsa a megosztott jelszavakat, amikor az alkalmazottak elhagyják a szervezetet.**
- **A jelszavakat csak biztonságosan ossza meg, például szervezete jelszókezelőjén vagy végpontok közötti titkosított alkalmazásokon keresztül.**
- **Követelje meg a 2FA-t minden szervezeti fiókban, és ösztönözze a személyzetet, hogy minden személyes fiókban állítsanak be 2FA-t.**
  - Ha lehetséges, adjon fizikai biztonsági kulcsot minden alkalmazottnak.
  - Ha a biztonsági kulcsok nem szerepelnek a költségvetésben, ösztönözze a hitelesítő alkalmazások használatát az SMS-ek vagy a 2FA telefonhívások helyett.
- **Tartson rendszeres képzést annak biztosítására, hogy az alkalmazottak tisztában legyenek a jelszavakkal és a 2FA bevált gyakorlataival, beleértve azt is, hogy mitől erős a jelszó, és annak fontosságával, hogy soha ne használják fel újra a jelszavakat, csak jogos 2FA-kéréseket fogadjanak el, és biztonsági 2FA-kódokat hozzanak létre.**

Biztonságos eszközök

A fiókok mellett elengedhetetlen az összes eszköz – számítógépek, telefonok, USB-k, külső merevlemezek stb. – megfelelő védelme.

Az ilyen védelem azzal kezdődik, hogy körültekintően kell eljárni azzal kapcsolatban, hogy szervezete és munkatársai milyen típusú eszközöket vásárolnak és használnak. A kiválasztott szállítóknak vagy gyártóknak bizonyítottan be kell tartaniuk a hardvereszközök (például telefonok és számítógépek) biztonságos fejlesztésére vonatkozó globális szabványokat. Az Ön által beszerzett eszközöket megbízható vállalatoknak kell gyártaniuk, amelyeknek nincs késztetésük arra, hogy adatokat és információkat adjanak át egy potenciális ellenfélnek. Fontos megjegyezni, hogy a kínai kormány megköveteli a kínai vállalatoktól, hogy adatokat szolgáltassanak a központi kormányzatnak. Tehát annak ellenére, hogy az okostelefonok, például a Huawei vagy a ZTE mindenütt megtalálhatók és olcsók, kerülni kell őket. Bár az olcsó hardver ára nagyon vonzó lehet egy szervezet számára, a demokráciát, az emberi jogokat vagy az elszámoltathatóságot hirdető szervezetek potenciális biztonsági kockázatai más eszközlehetőségek felé terelhetik Önt, mivel ez az adatokhoz való hozzáférés elősegítette a kínai és más kormányokat, hogy bizonyos személyeket és közösségeket céloznak meg. Ellenfelei veszélyeztethetik eszközeinek biztonságát – és mindazt, amit ezeken az eszközökön csinál – azáltal, hogy fizikai vagy „távoli” hozzáférést kapnak az eszközhöz.

Eszközbiztonság és civil társadalom

A világ legfejlettebb rosszindulatú programjai közül néhányat a civil társadalmi szervezetek és az emberi jogok védelmezői céljára fejlesztettek ki és helyeztek el szerte a világon. Indiában például az Amnesty International jelentette, hogy 2020-ban legalább kilenc emberi jogi jogvédőt kémprogrammal (rosszindulatú szoftverek egy fajtája) vettek célba mobileszközeiket és számítógépeiket. A kémprogramokat adathalász e-mailek sorozatán keresztül szállították, amelyek a Firefox Senden (azóta megszűnt fájlmegosztó program) keresztül megosztott fertőzött fájlokra mutató hivatkozásokat tartalmaztak. Azoknál a célpontoknál, akik megnyitották a fájlokat, az eszközök megfertőződtek olyan szoftverrel, amely hangot rögzített, billentyűleütéseket és üzeneteket fogott el, és gyakorlatilag a támadók teljes felügyelete alá helyezték őket. Az ilyen támadások, amelyek gyakran a civil társadalmi csoportok és egyéni munkatársaik ellen irányulnak, sajnos gyakori módját képezik annak, hogy a támadók „távolról” hozzáférjenek egy eszközhöz.

FIZIKAI ESZKÖZ HOZZÁFÉRÉSE ELVESZTÉS VAGY LOPÁS MIATT

A fizikai kompromittálás elkerülése érdekében elengedhetetlen, hogy az eszközöket fizikailag biztonságban tartsa. Röviden: ne könnyítse meg az ellenfél számára, hogy ellopja, vagy akár ideiglenesen is elvegye Öntől az eszközt. Tartsa zárva az eszközöket, ha otthon vagy az irodában hagyja őket. Vagy ha úgy gondolja, hogy biztonságosabb, tartsa magánál. Ez természetesen azt jelenti, hogy az eszközbiztonság része a munkahelyek fizikai biztonsága (akár irodai környezetben, akár otthon). Előfordulhat, hogy erős zárakat, biztonsági kamerákat vagy egyéb megfigyelőrendszereket kell telepítenie – különösen, ha szervezete nagy kockázatnak van kitéve. Emlékeztesse a személyzetet, hogy úgy bánjanak az eszközökkel, mint egy nagy halom készpénzzel – ne hagyják őket felügyelet vagy védelem nélkül heverni.

Mi van, ha egy készüléket ellopnak?

Az eszközlopás hatásának korlátozására – vagy még akkor is, ha csak rövid időre férnek hozzá – mindenképpen **kötelezzen mindenkit erős jelszavak vagy biztonsági kódok használatára mindenki számítógépén és telefonján**. A kézikönyv Jelszavak részében található jelszótippek érvényesek a számítógép vagy laptop megfelelő jelszavára. Amikor a telefon zárolásáról van szó, használjon legalább hat-nyolc számjegyű kódokat, és kerülje a „csúsztatási minták” használatát a képernyő feloldásához. A képernyőzárakkal kapcsolatos további tippekért tekintse meg a Tactical Tech Data Detox készletét. A jó jelszavak használata megnehezíti az ellenfél számára, hogy gyorsan hozzáférjen az eszközön lévő információkhoz lopás vagy elkobzás esetén. Erős jelkóddal az Arcazonosítás vagy az ujjlenyomat-feloldás aktiválása megfelelő lehet, de mindenképpen deaktiválja azt (miközben az erős jelszót érvényben hagyja), mielőtt bármilyen kockázatos tevékenységet, például tiltakozást vagy határátlépést hajtana végre, ha Ön és munkatársai aggódnak amiatt, hogy a hatóságok elkobozzák az eszközöket. Ha a szervezet által kibocsátott bármely eszköz rendelkezik „Készülékkereső” funkcióval, például az iPhone-on az iPhone keresése és az Androidon az Eszközkereső funkció, fontolja meg annak az aktiválásának a megkövetelését a személyzet részéről. Ösztönözze a személyzetet, hogy ezeket a funkciókat személyes eszközökön is használják. Ha ezek a funkciók be vannak kapcsolva, az eszköz tulajdonosa (vagy egy megbízható kapcsolattartó) megkeresheti az eszközt, vagy távolról törölheti annak tartalmát, ha ellopják, elveszik vagy elkobozzák. iPhone-ok esetén beállíthatja az eszközt úgy is, hogy több sikertelen bejelentkezési kísérlet után is automatikusan törlődjön. Az ilyen eszközkezelési funkciók rendkívül fontossá válnak egy szervezet számára, ha egy érzékeny információkat tartalmazó eszköz elveszik vagy rossz kezekbe kerül.

Mi a helyzet az eszköztitkosítással?

Fontos, hogy minden eszközön – különösen számítógépen és okostelefonon – használjon titkosítást, az adatok titkosítását, hogy azok olvashatatlanok és használhatatlanok legyenek. Ha lehetséges, a szervezet összes eszközét a teljes lemezes titkosítással kell beállítani. A teljes lemezes titkosítás azt jelenti, hogy az eszköz egésze titkosítva van, így az ellenfél, ha fizikailag ellopná, nem tudja kibontani az eszköz tartalmát anélkül, hogy ismerné a titkosításhoz használt jelszót vagy kulcsot. Sok modern okostelefon és számítógép teljes lemezes titkosítást kínál. Az Apple-eszközök, például az iPhone-ok és az iPadek, meglehetősen kényelmesen bekapcsolják a teljes lemez titkosítását, amikor beállítja az eszköz normál jelszavát. A macOS-t használó Apple számítógépek egy FileVault nevű funkciót biztosítanak, amelyet bekapcsolhat a teljes lemez titkosítására. A pro, vállalati vagy oktatási licencet futtató Windows számítógépek egy BitLocker nevű szolgáltatást kínálnak, amelyet bekapcsolhat a teljes lemez titkosítására. A BitLocker bekapcsolásához kövesse ezeket az utasításokat a Microsofttól, amelyeket először engedélyeznie kell a szervezet rendszergazdájának. Ha a személyzet csak otthoni licenccel rendelkezik a Windows rendszerű számítógépekhez, a BitLocker nem érhető el. Azonban továbbra is bekapcsolhatja a teljes lemezes titkosítást, ha a Windows operációs rendszer beállításai alatt a „Frissítés és biztonság” > „Eszköz titkosítása” menüpontot választja.

A 9.0-s és újabb verziójú Android-eszközökön a fájlalapú titkosítás alapértelmezés szerint be van kapcsolva. Az Android fájlalapú titkosítása eltér a teljes lemezes titkosítástól, de továbbra is erős biztonságot nyújt. Ha viszonylag új Android-telefont használ, és beállított egy jelszót, engedélyeznie kell a fájlalapú titkosítást. Érdemes azonban ellenőrizni a beállításokat, különösen, ha a telefon pár évesnél régebbi. Az ellenőrzéshez lépjen a Beállítások > Biztonság menüpontba az Android-eszközén. A biztonsági beállításokon belül látnia kell egy „titkosítás” vagy „titkosítás és hitelesítő adatok” alszakaszt, amely jelzi, hogy a telefon titkosítva van-e, és ha nem, lehetővé teszi a titkosítás bekapcsolását.

Számítógépeknél (legyen szó Windowsról vagy Macről) különösen fontos, hogy a titkosítási kulcsokat (helyreállítási kulcsoknak) biztonságos helyen tárolják. Ezek a „helyreállítási kulcsok” a legtöbb esetben lényegében hosszú jelszavak vagy jelszófrázisok. Abban az esetben, ha elfelejti normál eszközjelszavát, vagy valami váratlan történik (például az eszköz meghibásodása), a helyreállítási kulcsok az egyetlen módja a titkosított adatok helyreállításának, és szükség esetén új eszközre való áthelyezésének. Tehát a teljes lemezes titkosítás bekapcsolásakor ügyeljen arra, hogy ezeket a kulcsokat vagy jelszavakat biztonságos helyen tárolja, például egy biztonságos felhőalapú fiókban vagy szervezete jelszókezelőjében.

TÁVOLI ESZKÖZ HOZZÁFÉRÉSE – HACKELÉSKÉNT ISMERT

Az eszközök fizikai biztonságának megőrzése mellett fontos, hogy mentesek legyenek a rosszindulatú programoktól. A Tactical Tech Security-in-a-Box hasznos leírást ad arról, hogy mi az a rosszindulatú program, és miért fontos ezeket elkerülni. Ezt a szakasz további részében némileg módosítjuk.

A rosszindulatú programok megértése és elkerülése

A rosszindulatú programok (amelyek rosszindulatú szoftvereket jelentenek) osztályozásának számos módja van. A vírusok, kémprogramok, férgek, trójaiak, rootkitek, zsarolóvírusok és titkosítóprogramok mind rosszindulatú programtípusok. A rosszindulatú programok bizonyos típusai e-mailen, szöveges üzeneteken, rosszindulatú weboldalakon és egyéb módon terjednek az interneten. Néhány olyan eszközökön keresztül terjed, mint az USB-memóriakártyák, amelyeket adatcserére és adatlopásra használnak. És míg néhány rosszindulatú programnak gyanútlan célpontra van szüksége ahhoz, hogy hibát kövessen el, mások csendben megfertőzhetik a sebezhető rendszereket anélkül, hogy bármi rosszat tenne.

Az általános rosszindulatú programokon kívül (amelyeket széles körben bocsátanak ki és a nagyközönséget célozzák meg), a célzott kártevőket jellemzően egy adott személy, szervezet vagy hálózat megzavarására vagy kémkedésére használják. A bűnözők használják ezeket a technikákat, de a katonai és hírszerző szolgálatok, a terroristák, az online zaklatók, a bántalmazó házastársak és az árnyékos politikai szereplők is.

Bárhogy is hívják őket, bárhogyan is terjesztik őket, a rosszindulatú programok tönkretehetik a számítógépeket, ellophatják és megsemmisíthetik az adatokat, csődbe juttathatják a szervezeteket, megsérthetik a magánéletet, és veszélybe sodorhatják a felhasználókat. Röviden: a rosszindulatú programok valóban veszélyesek. Van azonban néhány egyszerű lépés, amelyeket szervezete megtehet, hogy megvédje magát ezzel a gyakori fenyegetéssel szemben.

Vajon megvéd minket egy kártevőirtó eszköz?

A kártevőirtó eszközök sajnos nem jelentenek teljes megoldást. De nagyon jó ötlet néhány alapvető, ingyenes eszközt használni alapként. A rosszindulatú programok olyan gyorsan változnak, és a való világban olyan gyakran jelentkeznek új kockázatok, hogy az ilyen eszközökre való támaszkodás nem lehet az egyetlen védekezés.

Ha Windowst használ, vessen egy pillantást a beépített Windows Defenderre. A Mac és Linux számítógépek nem rendelkeznek beépített kártevőirtó szoftverrel, ahogy az Android és iOS eszközök sem. Telepíthet egy jó hírű, ingyenesen használható eszközt, mint például a Bitdefender vagy a Malwarebytes ezekre az eszközökre (és Windows számítógépekre is). **De ne hagyatkozz erre, mint az egyetlen védelmi vonalra**, mert minden bizonnyal kihagynak néhányat a legcélzottabb, legveszélyesebb új támadások közül.

Ügyeljen arra is, hogy csak megbízható forrásból (például a fent hivatkozott weboldalakról) töltsön le jó hírű kártevő- és vírusirtó eszközöket. Sajnos a kártevő-elhárító eszközöknek sok hamis vagy feltört verziója létezik, amelyek sokkal több kárt okoznak, mint amennyit használnak.

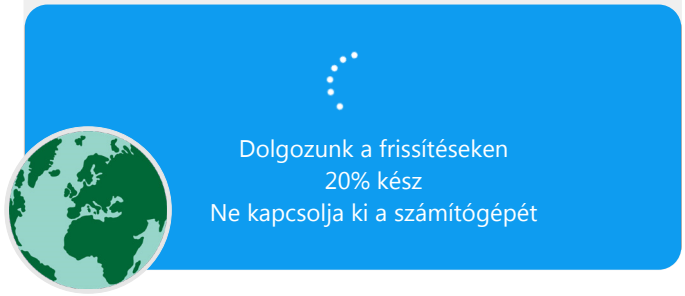
Ha a Bitdefender-t vagy más kártevőirtó eszközt használ a szervezetében, ügyeljen arra, hogy ne futtasson kettőt egyszerre. Sokan közülük gyanúsként azonosítják egy másik kártevőirtó program viselkedését, és leállítják annak futását, így mindkettő hibásan működik. A Bitdefender vagy más jó hírű kártevőirtó programok ingyenesen frissíthetők, a beépített Windows Defender pedig a számítógépével együtt kapja meg a frissítéseket. Gondoskodjon arról, hogy a rosszindulatú szoftverek elleni szoftver rendszeresen frissítse magát (a számítógéppel együtt szállított kereskedelmi szoftverek némelyik próbaverziója a próbaidőszak lejárta után le lesz tiltva, így inkább veszélyes, mint hasznos.) Minden nap új kártevőket írnak és terjesztenek, és számítógépe gyorsan még sebezhetőbbé válik, ha nem tartja a lépést az új rosszindulatú programdefiníciókkal és a rosszindulatú programok elleni technikákkal. Ha lehetséges, konfigurálja a szoftvert úgy, hogy automatikusan telepítse a frissítéseket. Ha a kártevőirtó eszköze opcionális „mindig bekapcsolt" funkcióval rendelkezik, engedélyezze azt, és fontolja meg a számítógépén lévő összes fájl időnkénti átvizsgálását.

Tartsa naprakészen az eszközöket

A frissítések elengedhetetlenek. Használja az eszközön futó operációs rendszer legújabb verzióját (Windows, Mac, Android, iOS stb.), és tartsa naprakészen az operációs rendszert. Tartsa naprakészen a többi szoftvert, böngészőt és minden böngészőbővítményt is. Telepítse a frissítéseket, amint elérhetővé válnak, ideális esetben az **automatikus frissítések bekapcsolásával**. Minél naprakészebb az eszköz operációs rendszere, annál kisebb a sebezhetősége. Gondoljon úgy a frissítésekre, mint egy sebtapasz felhelyezése egy nyitott vágásra. Megszünteti a sebezhetőséget, és nagymértékben csökkenti a fertőzés esélyét. Távolítsa el azokat a szoftvereket is, amelyeket már nem használ. Az elavult szoftverek gyakran biztonsági problémákkal küzdenek, és előfordulhat, hogy olyan eszközt telepített, amelyet már nem frissít a fejlesztő, így kiszolgáltatottabbá válik a hackerekkel szemben.

Rosszindulatú programok a való világban: A frissítések elengedhetetlenek

2017-ben a WannaCry ransomware támadások eszközök millióit fertőzték meg világszerte, kórházakat, kormányzati szerveket, nagy és kis szervezeteket és vállalkozásokat bezárva több tucat országban. Miért volt ilyen hatékony a támadás? Az elavult, „javítatlan" Windows operációs rendszerek miatt, amelyek közül sok kezdetben kalóz volt. A károk – emberi és pénzügyi – nagy része elkerülhető lett volna jobb automatizált frissítési gyakorlattal és legitim operációs rendszerek használatával.



Legyen óvatos az USB-vel

Legyen óvatos, amikor megnyitja azokat a fájlokat, amelyeket mellékletként, letöltési hivatkozásokon keresztül vagy bármilyen más módon küldtek Önnek. Gondolja át **kétszer is, mielőtt cserélhető adathordozókat, például USB-kulcsokat**, flash memóriakártyákat, DVD-ket és CD-ket helyez be a számítógépébe, mivel ezek rosszindulatú programok hordozói lehetnek. Az egy ideje megosztott USB-ken nagy valószínűséggel vírusok találhatók. A fájlok szervezeten belüli biztonságos megosztására vonatkozó alternatív lehetőségekért tekintse meg a kézikönyv fájlmegosztási részét.

Legyen óvatos azzal kapcsolatban is, hogy milyen egyéb eszközökhöz csatlakozik Bluetooth-on keresztül. Rendben van, ha telefonját vagy számítógépét szinkronizálja egy ismert és megbízható Bluetooth-hangszóróval, hogy lejátssza kedvenc zenéit, de legyen óvatos, ha olyan eszközökhöz kapcsolódik vagy fogad kéréseket, amelyeket nem ismer fel. Csak megbízható eszközökhöz engedélyezze a csatlakozást, és ne felejtse el kikapcsolni a Bluetooth-t, ha nem használja.

Legyen okos böngészés közben

Soha ne fogadjon el és ne futtasson olyan weboldalakról származó alkalmazásokat, amelyeket nem ismer és nem bízik benne. Ahelyett, hogy elfogadna például egy felugró böngészőablakban felkínált „frissítést", ellenőrizze a frissítéseket az adott alkalmazás hivatalos weboldalán. Amint azt a Kézikönyv adathalászattal foglalkozó részében tárgyaltuk, elengedhetetlen, hogy éber legyen a weboldalak böngészése során. Mielőtt rákattint, ellenőrizze a hivatkozás rendeltetési helyét (úgy, hogy az egérmutatót fölé viszi), majd a hivatkozás követése után tekintse meg a weboldal címét, és győződjön meg arról, hogy megfelelőnek tűnik, mielőtt érzékeny adatokat, például jelszót ír be. Ne kattintson a hibaüzenetekre vagy figyelmeztetésekre, és figyelje az automatikusan megjelenő böngészőablakokat, és figyelmesen olvassa el őket ahelyett, hogy az Igen vagy az OK gombra kattintana.

Mi a helyzet az okostelefonokkal?

A számítógépekhez hasonlóan tartsa naprakészen telefonja operációs rendszerét és alkalmazásait, és kapcsolja be az automatikus frissítéseket. Csak olyan hivatalos vagy megbízható forrásokból telepítse, mint a Google Play Store és az Apple App Store (vagy az F-droid, egy ingyenes, nyílt forráskódú alkalmazásbolt Androidra). Az alkalmazásokba rosszindulatú programokat lehet beilleszteni, és úgy tűnik, hogy továbbra is normálisan működnek, így nem mindig lehet tudni, hogy rosszindulatúak-e. Győződjön meg arról is, hogy az alkalmazás legális verzióját tölti le. Különösen az Androidokon léteznek népszerű alkalmazások „hamis" verziói. Ezért győződjön meg arról, hogy az alkalmazást a megfelelő cég vagy fejlesztő hozta létre, jó vélemények vannak róla, és a letöltések száma a vártnak felel meg (például előfordulhat, hogy a WhatsApp hamis verziójának csak néhány ezer letöltése van, de a valódi verziónak több mint 5 milliárd). Ügyeljen az alkalmazások által kért engedélyekre. Ha túlzónak tűnnek (például egy számológép, amely hozzáférést igényel a kamerához, vagy az Angry Birds, amely hozzáférést kér a tartózkodási helyéhez), utasítsa el a kérést, vagy távolítsa el az alkalmazást. A már nem használt alkalmazások eltávolítása is segíthet megvédeni okostelefonját vagy táblagépét. A fejlesztők néha eladják alkalmazásaik tulajdonjogát másoknak. Ezek az új tulajdonosok megpróbálhatnak pénzt keresni rosszindulatú kód hozzáadásával.

Rosszindulatú programok a való világban: Rosszindulatú mobilalkalmazások

A hackerek több országban évek óta használnak hamis alkalmazásokat a Google Play Áruházban rosszindulatú programok terjesztésére. 2020 áprilisában napvilágot látott egy vietnami felhasználókat célzó konkrét eset. Ez a kémkampány hamis alkalmazásokat használt, amelyek állítólag segítettek a felhasználóknak megtalálni a közeli kocsmákat, vagy információkat keresni a helyi templomokról. Miután akaratlanul is telepítették az Android-felhasználók, a rosszindulatú alkalmazások hívásnaplókat, helyadatokat, valamint névjegyekre és szöveges üzenetekre vonatkozó információkat gyűjtöttek. Ez csak egy ok a sok közül, hogy ügyeljen arra, hogy milyen alkalmazásokat tölt le eszközére.

Takarítson meg pénzt és növelje az eszközbiztonságot a Tails for your Organisation segítségével

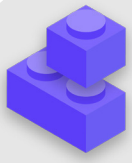
Az egyik nagyon biztonságos lehetőség, amelynek beállítása némi technikai tudást igényel, a Tails operációs rendszer. Ez a hordozható operációs rendszer ingyenesen használható, és közvetlenül USB-ről indítható, elkerülve a licencelt Windows vagy Mac operációs rendszer használatának szükségességét. A Tails a rendkívül magas kockázatnak kitett személyek számára is jó választás, mivel számos adatvédelmi funkciót tartalmaz. Ezek a szolgáltatások magukban foglalják a Tor integrációját (ezt az alábbiakban tárgyaljuk) a webes forgalom biztonsága érdekében, valamint a memória teljes törlését minden alkalommal, amikor leállítja az operációs rendszert. Ezek a szolgáltatások lényegében lehetővé teszik, hogy a számítógép minden újraindításakor tiszta lappal kezdjen. A Tails rendelkezik egy „perzisztencia üzemmóddal" is, amely lehetővé teszi a fontos fájlok és beállítások több munkamenetben történő mentését, ha szükséges.

Egy másik lehetőség az ingyenes, biztonságos operációs rendszerre a Qubes OS. Bár nem a legegyszerűbb lehetőség nem műszaki felhasználók számára, a Qubes célja a rosszindulatú programok fenyegetésének korlátozása, és egy másik lehetőség, amelyet érdemes megfontolni a fejlettebb és magas kockázatú felhasználók számára a szervezetben, különösen, ha a licenckötségek kihívást jelentenek.

Mi van, ha nem engedhetjük meg magunknak a legális szoftvereket?

Drága lehet a népszerű szoftverek, például a Microsoft Office (Word, Powerpoint, Excel) licencelt verzióinak vásárlása az egész szervezet számára, de a korlátozott költségvetés nem jelent ürügyet a szoftverek kalózverzióinak letöltésére vagy azok naprakészen tartására. Ez nem erkölcsi kérdés, hanem biztonság kérdése. A kalózszoftverek gyakran tele vannak rosszindulatú programokkal, és gyakran nem javíthatók a biztonsági réseik. Ha nem engedheti meg magának azt a szoftvert, amelyre a szervezetének szüksége van, nagyszerű ingyenes, nyílt forráskódú szoftverek széles skálája áll rendelkezésre, mint például a LibreOffice (a szabványos Microsoft Office-alkalmazások helyettesítője) vagy a GIMP (helyettesítő Photoshophoz), amely kiszolgálhatja az Ön igényeit. Fontolja meg a Tech Soup szervezeten keresztüli regisztrációt is, amely jelentős kedvezményeket kínál a népszerű szoftverekre nonprofit szervezetek számára. Még ha meg is engedheti magának a legális szoftvereket és alkalmazásokat, eszköze továbbra is veszélyben van, ha az alapul szolgáló operációs rendszer nem legitim.

Ha tehát szervezete nem engedheti meg magának a Windows-licenceket, fontolja meg az olcsóbb alternatívákat, például a Chromebookokat, amelyek nagyszerű, könnyen biztonságossá tehető megoldást jelentenek, ha szervezete többnyire felhőben dolgozik. Ha Google Dokumentumokat vagy Microsoft 365-öt használ, egyáltalán nincs szüksége sok asztali alkalmazásra – az ingyenes böngészőn belüli dokumentum- és táblázatszerkesztők szinte minden felhasználáshoz elegendőek. Egy másik lehetőség, ha rendelkezik megfelelő műszaki ismeretekkel rendelkező személyzettel, az ingyenes Linux-alapú operációs rendszert (a Windows és Mac operációs rendszer nyílt forráskódú alternatíváját) telepítése minden számítógépre. Az egyik népszerű, meglehetősen felhasználóbarát Linux-opció az Ubuntu. Függetlenül attól, hogy melyik operációs rendszert választja, győződjön meg arról, hogy valaki a szervezetben felelős azért, hogy rendszeresen bejelentkezzen a személyzettel, hogy megbizonyosodjon arról, hogy alkalmazták a legújabb frissítéseket.



Eszközök biztonságban tartása

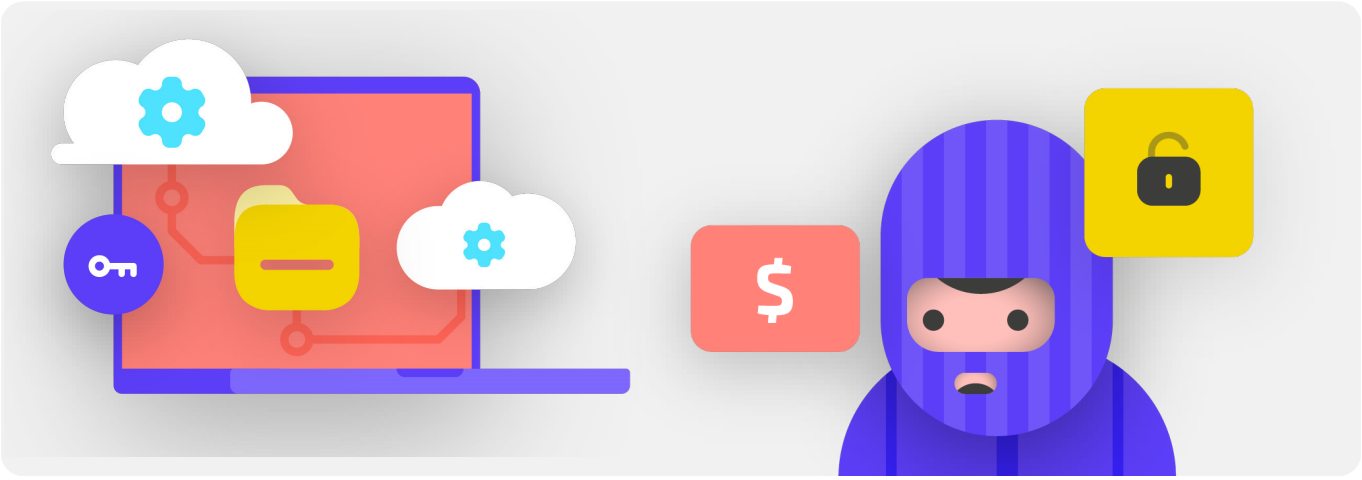
- **A személyzet képzése a rosszindulatú programok kockázatairól és az elkerülésük bevált módszereire.**
  - Irányelvek biztosítása a külső eszközök csatlakoztatásával, a hivatkozásokra való kattintással, a fájlok és alkalmazások letöltésével, valamint a szoftverek és alkalmazások engedélyeinek ellenőrzésével kapcsolatban.
- **Az eszközök, szoftverek és alkalmazások teljes körű frissítésének jóváhagyása.**
  - Ha lehetséges, kapcsolja be az automatikus frissítéseket.
- **Győződjön meg arról, hogy minden eszköz licencelt szoftvert használ.**
  - Ha a költségek túl magasak, váltson egy ingyenes alternatívára.
- **Jelszavas védelem előírása minden szervezeti eszközön, beleértve a személyes mobileszközöket is, amelyeket a munkával kapcsolatos kommunikációhoz használnak.**
- **A teljes lemezes titkosítás engedélyezése az eszközökön.**
- **A személyzet gyakori emlékeztetése arra, hogy tartsák fizikailag biztonságban eszközeiket – és az iroda biztonságáról való gondoskodás megfelelő zárakkal és számítógépvédelmi módszerekkel.**
- **Ne ossza meg a fájlokat USB-n keresztül, és ne csatlakoztasson USB-t a számítógépéhez.**
  - Ehelyett használjon alternatív biztonságos fájlmegosztási lehetőségeket.

Adathalászat: Gyakori fenyegetés az eszközökre és fiókokra

Az adathalászat a legáltalánosabb és leghatékonyabb támadás a szervezetek ellen szerte a világon. A technikát a legkifinomultabb nemzetállami katonaság, valamint apró csalók is használják.

Az adathalászat leegyszerűsítve azt jelenti, hogy az ellenfél megpróbálja rávenni Önt olyan információk megosztására, amelyeket Ön vagy szervezete ellen használhat fel. Az adathalászat történhet e-mailekben, szöveges üzenetekben/SMS-ekben (gyakran SMS-es adathalászatnak vagy „smishingnek" nevezik), üzenetküldő alkalmazásokkal, például a WhatsApp-szal, közösségi média üzenetekkel vagy bejegyzésekkel vagy telefonhívásokkal (ezt gyakran hangos adathalászatnak vagy „vishingnek" nevezik). Az adathalász üzenetek megpróbálhatják rávenni Önt, hogy érzékeny adatokat (például jelszavakat) írjon be egy hamis weboldalra, hogy hozzáférjen egy fiókhoz, és megkérheti, hogy ossza meg személyes adatait

(például hitelkártyaszám) hangon vagy szövegesen, vagy meggyőzhetik Önt arról, hogy töltsön le rosszindulatú programokat (rosszindulatú szoftvereket), amelyek megfertőzhetik eszközét. Egy nem technikai példa: nap mint nap emberek milliói kapnak hamis automatikus telefonhívásokat arról, hogy bankszámlájukat feltörték, vagy személyazonosságukat ellopták – mindezt arra tervezték, hogy a tudatlanokat bizalmas információk megosztására vegyenek rá.



HOGYAN AZONOSÍTHATJUK AZ ADATHALÁSZATOT?

Az adathalászat baljósnak hangzik, és lehetetlen elkapni, de van néhány egyszerű lépés, amelyeket a szervezetben mindenki megtehet, hogy megvédje magát a legtöbb támadástól. A következő adathalász-védelmi tippeket a The Freedom of the Press Foundation által kidolgozott részletes adathalászati útmutató módosította és bővítette, ossza meg őket a szervezetével (és más kapcsolattartókkal), és integrálja a biztonsági tervébe:

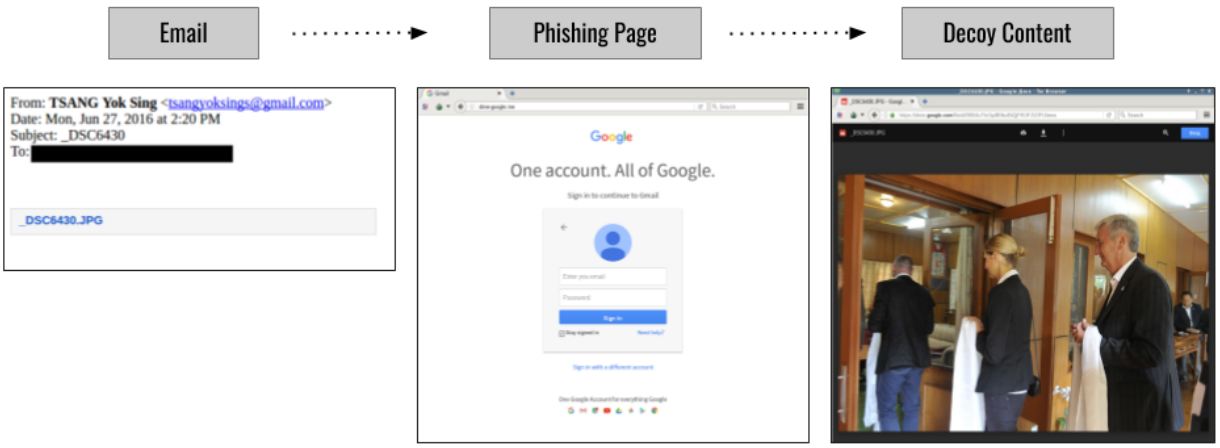
Néha a „feladó” mező hazudik Önnek

Ügyeljen arra, hogy e-mailjei „feladó” mezője hamis lehet vagy arra törekedhet, hogy becsapja Önt. Gyakori, hogy az adathalászok olyan e-mail-címet állítanak be, amely nagyon úgy néz ki, mint egy Ön által ismert, jogos cím, és kissé elgépelve, hogy átverjék Önt. Például kaphat egy e-mailt valakitől, akinek a címe „john@goooogle.com” nem „john@google.com”. Figyelje meg az extra „o” betűt a google-ban. Az is előfordulhat, hogy ismer valakit, akinek e-mail címe „john@gmail.com”, de adathalász e-mailt kap egy csalótól, aki beállította a „johm@gmail.com” címet – az egyetlen különbség az, hogy a végén finoman változnak a betűk. Mielőtt továbblépne, mindig ellenőrizze, hogy ismeri-e az e-mail küldési címét. Hasonló koncepció vonatkozik a szöveges üzeneteken, hívásokon vagy üzenetküldő alkalmazásokon keresztüli adathalászatra is. Ha ismeretlen számról kap üzenetet, gondolja át kétszer, mielőtt válaszolna az üzenetre, vagy kapcsolatba lépne vele.

Adathalászat és a civil társadalom

Nap mint nap kifinomult, személyre szabott adathalász támadások célozzák a civil társadalmi csoportokat szerte a világon.

Az ilyen támadások egyik példáját kiemeli a The Citizen Lab 2018-as jelentése: **Spying on a Budget: Egy adathalász műveleten belüli célpontokkal a tibeti közösségben**. Ez a nagyon olcsó és egyszerű – ugyanakkor hihetetlenül hatékony – adathalász támadás tibeti emberi jogi jogvédők és más aktivisták ellen irányult. A támadás egy adathalász e-maillel indult (a bal oldalon látható) egy szabványos Gmail-címről, amely csak egy képfájl hivatkozást tartalmazott. Rákattintás után a hivatkozás egy hamis Google e-mail bejelentkezési oldalra (középen látható) juttatta a célpontot, amelyet a fiók hitelesítő adatainak ellopására használtak. Ha az áldozatok hitelesítő adatokat adnának meg a hamis oldalhoz, könnyen feltörhetnék a fiókjukat. Miután megadták felhasználónevüket és jelszavukat a hamis weboldalon, az áldozatokat átirányítják egy képre (jobbra látható), amelyen egy tibeti találkozó küldöttei láthatók. A képet csaliként adták hozzá, hogy az adathalász célpontok azt higgyék, valóban bejelentkeztek valódi Google-fiókjukba, és csökkentsék az e-mail valódi rosszindulatú természetével kapcsolatos esetleges gyanút.



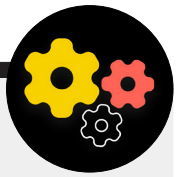
Óvakodjon a mellékletektől

A mellékletek tartalmazhatnak rosszindulatú programokat és vírusokat, és gyakran kísérik az adathalász e-maileket. **A rosszindulatú programok elkerülésének legjobb módja, ha soha nem tölti le azokat**. Általános szabály, hogy ne nyissa meg azonnal a mellékleteket, különösen akkor, ha azok olyan személyektől származnak, akiket nem ismer. Ha lehetséges, kérje meg a dokumentumot küldő személyt, hogy másolja be a szöveget egy e-mailben, vagy ossza meg a dokumentumot olyan szolgáltatáson keresztül, mint a Google Drive vagy a Microsoft OneDrive, amelyek beépített vírusellenőrzéssel rendelkeznek a legtöbb platformjukra feltöltött dokumentumra. Építsen ki olyan szervezeti kultúrát, amelyben a mellékletek kerülendők. Ha feltétlenül meg kell nyitnia a mellékletet, azt csak biztonságos környezetben szabad megnyitni (lásd lent a speciális részt), ahol a potenciális rosszindulatú program nem telepíthető az eszközére.

Ha Gmailt használ, és e-mailben kap egy mellékletet, ahelyett, hogy letöltené és megnyitná a számítógépén, egyszerűen kattintson a csatolt fájlra, és olvassa el a böngészőben „előnézetben". Ez a lépés lehetővé teszi egy fájl szövegének és tartalmának megtekintését anélkül, hogy letöltené azt, vagy lehetővé tenné, hogy lehetséges rosszindulatú programokat töltsön be a számítógépére. Ez jól működik Word dokumentumoknál, pdf-eknél és még diavetítéseknél is. Ha szerkesztenie kell a dokumentumot, fontolja meg a fájl megnyitását egy felhőalapú programban, például a Google Drive-ban, és konvertálja a fájlt Google Dokumentummá vagy Google Diákká.

Ha Outlookot használ, hasonló módon megtekintheti a mellékletek előnézetét anélkül, hogy letöltené őket az Outlook webes ügyfélprogramjából. Ha szerkesztenie kell a mellékletet, nyissa meg OneDrive-ban, ha ez elérhető. Ha Yahoo Mail-t használ, ugyanez a koncepció érvényes. Ne töltsön le mellékleteket, inkább tekintse meg előnézetüket a webböngészőből.

Attól függetlenül, hogy milyen eszközök állnak rendelkezésére, a legjobb megoldás az, ha soha nem tölt le olyan mellékleteket, amelyeket nem ismer vagy nem bízik meg bennük. És függetlenül attól, hogy mennyire fontosnak tűnik egy melléklet, soha ne nyisson meg semmit olyan fájltípussal, amelyet nem ismer fel, vagy nem is szándékozik használni.



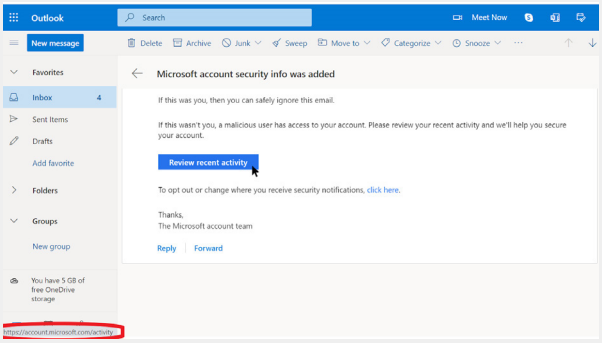
Adathalászat elleni védelem a szervezete számára

Ha szervezete a vállalati Microsoft 365-öt használja az e-mailekhez és egyéb alkalmazásokhoz, a tartomány rendszergazdájának be kell állítania a Biztonságos mellékletekre vonatkozó házirendet a veszélyes mellékletek elleni védelem érdekében. Ha vállalati Google Workspace-t (korábbi nevén GSuite) használ, van egy hasonlóan hatékony lehetőség, amelyet a rendszergazdának be kell állítania, Google Security Sandbox néven. A haladóbb egyéni felhasználók fontolóra vehetik a kifinomult sandbox programokat, például a DangerZone-t, vagy a Windows 10 Pro vagy Enterprise verziójával rendelkezők a Windows Sandbox beállítását. Egy másik speciális lehetőség, amelyet érdemes megfontolni az egész szervezetben, a biztonságos tartománynévrendszer (DNS) szűrőszolgáltatása. A szervezetek ezzel a technológiával megakadályozhatják, hogy az alkalmazottak véletlenül hozzáférjenek a rosszindulatú tartalomhoz vagy interakcióba léphessenek azokkal, így további védelmet nyújtanak az adathalászat ellen. Bár történelmileg egy ilyen technológiához belső informatikai személyzet elkötelezett csapatára volt szükség, az új szolgáltatások, mint a Cloudflare Gateway, technikailag kevésbé kifinomult szervezetek számára is biztosítanak ilyen képességeket anélkül, hogy nagy pénzösszegeket igényelnének (a Gateway például 50 felhasználóig ingyenes). További ingyenes eszközök, köztük a Global Cyber Alliance Toolkit a Quad9-től, segítenek megakadályozni, hogy olyan ismert weboldalakhoz férhessen hozzá, amelyek vírusokat vagy más rosszindulatú programokat tartalmaznak, és amelyek kevesebb mint öt perc alatt bevezethetők.

Óvatosan kattintson

Legyen szkeptikus az e-mailekben vagy más szöveges üzenetekben található hivatkozásokkal kapcsolatban. A hivatkozások álcázhatók rosszindulatú fájlok letöltésére, vagy hamis weboldalakra irányítanak, amelyek jelszavak vagy egyéb bizalmas adatok megadását kérhetik. Számítógépen van egy egyszerű trükk, amellyel megbizonyosodhat arról, hogy egy e-mailben vagy üzenetben lévő hivatkozás oda küldi-e, ahová kell: az egérrel vigye az egérmutatót bármelyik hivatkozás fölé, mielőtt rákattint, és nézze meg a hivatkozást a böngésző ablak alján, hogy megtudja, mi a tényleges URL (lásd az alábbi képet).

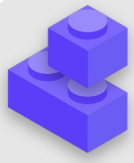
Mobileszközön nehezebb ellenőrizni az e-mailben lévő hivatkozásokat anélkül, hogy véletlenül rájuk kattintana – ezért legyen óvatos. De a legtöbb okostelefonon ellenőrizheti a hivatkozás célhelyét, ha hosszan lenyomja (lenyomva tartja) a hivatkozást, amíg a teljes URL meg nem jelenik. Az SMS-eken és üzenetküldő alkalmazásokon keresztül végzett adathalászat során a rövidített hivatkozások egy nagyon gyakori gyakorlat, amellyel egy URL-címet álcáznak. Ha a teljes URL helyett egy rövid hivatkozást lát (például bit.ly vagy tinyurl.com), ne kattintson rá. Ha a hivatkozás fontos, másolja be egy URL-bővítőbe, például: https://www. expandurl.net/, a rövidített URL tényleges célhelyének megtekintéséhez. Továbbá ne kattintson az Ön számára ismeretlen weboldalakra mutató hivatkozásokra. Ha kétségei vannak, végezzen keresést a weboldalra úgy, hogy a weboldal neve idézőjelek közé kerüljön (például: "www.badwebsite. com"), hogy megtudja, legitim weboldal-e. A potenciálisan gyanús hivatkozásokat a VirusTotal URL-ellenőrzőjén keresztül is futtathatja. Ez nem 100%-ban pontos, de jó elővigyázatossági intézkedés.



Végül, ha rákattint egy üzenet bármely hivatkozására, és felkérik, hogy jelentkezzen be, ne tegye meg, hacsak nem 100%-ig biztos abban, hogy az e-mail legitim, és a megfelelő weboldalra küldi. Számos adathalász támadás tartalmaz hivatkozásokat, amelyek a Gmail, a Facebook vagy más népszerű weboldalak hamis bejelentkezési oldalaira irányítanak. Ne dőljön be nekik. Bármikor megnyithat egy új böngészőt, és közvetlenül felkereshet egy ismert weboldalt, például a Gmail.com-ot, a Facebook.com-ot stb., ha be szeretne jelentkezni vagy be kell jelentkeznie. Ezzel biztonságosan eljuthat a tartalomhoz – ha az eredetileg legitim volt.

Mit tegyünk, ha adathalász üzenetet kapunk?

Ha a szervezeténél bárki kéretlen mellékletet, hivatkozást, képet vagy egyéb gyanús üzenetet vagy hívást kap, fontos, hogy azt azonnal jelentse a szervezet IT-biztonsági pontjának. Ha még nem rendelkezik ilyen személyekkel, a biztonsági terv kidolgozása során azonosítania kell őket. A személyzet közvetlenül a Gmailben vagy az Outlookban is jelentheti az e-mailt spamként vagy adathalászként.
Kulcsfontosságú, hogy legyen egy terv arra vonatkozóan, hogy a személyzet vagy az önkéntesek mit tegyenek, ha/amikor adathalász üzenetet kapnak. Ezenkívül javasoljuk, hogy kövesse ezeket a bevált adathalász gyakorlatokat – ne kattintson a gyanús hivatkozásokra, kerülje a mellékleteket, és ellenőrizze a „feladó" címet –, és ossza meg azokat másokkal, akikkel együttműködik, lehetőleg egy széles körben használt kommunikációs csatornán keresztül. Ez azt mutatja, hogy törődik azokkal az emberekkel, akikkel kommunikál, és olyan kultúrát ösztönöz a hálózataiban, amely éber, és tudatában van az adathalászat veszélyeinek. Az Ön biztonsága azoktól a szervezetektől függ, amelyekben megbízik, és fordítva. A jobb gyakorlatok mindenkit megvédenek. Amellett, hogy megosztja a fenti tippeket az összes alkalmazottal és önkéntessel, gyakorolhatja az adathalászat azonosítását a Google adathalász-kvízzel. Azt is nyomatékosan javasoljuk, hogy tartsanak rendszeres adathalász tréningeket a személyzettel a tudatosság tesztelése és az emberek ébersége érdekében. Az ilyen képzés formálissá tehető rendszeres szervezeti értekezletek részeként, vagy kötetlenebb formában. Az a fontos, hogy a szervezetben mindenki jól érezze magát, mert kérdéseket tehet fel az adathalászattal kapcsolatban, és bejelentheti az adathalászatot (még akkor is, ha úgy érzi, hogy hibát követett el, például egy hivatkozásra kattintva), és mindenki képes legyen megvédeni szervezetét ezen hatás és nagy valószínűséggel fenyegetés ellen.



Adathalászat

- **Rendszeres képzésben részesítse a személyzetet arról, hogy mi az adathalászat, hogyan lehet észrevenni és védekezni ellene, beleértve a szöveges üzenetek, üzenetküldő alkalmazások és telefonhívások adathalászatát, nem csak e-maileket.**
- **Gyakran emlékeztesse a személyzetet a bevált gyakorlatokra, például:**
  - Ne töltsön le ismeretlen vagy potenciálisan gyanús mellékleteket.
  - Kattintás előtt ellenőrizze a hivatkozás URL-jét. Ne kattintson ismeretlen vagy potenciálisan gyanús hivatkozásokra.
  - Ne adjon meg bizalmas vagy privát információkat e-mailben, SMS-ben vagy telefonhívásban ismeretlen vagy meg nem erősített címzetteknek vagy személyeknek.
- **Ösztönözze az adathalászat bejelentését.**
  - Hozzon létre egy jelentési mechanizmust és egy személyt az adathalászathoz a szervezeten belül.
  - Jutalmazza a jelentést, és ne büntesse a kudarcot.

Adatok biztonságos kommunikációja és tárolása

Kommunikáció és adatok megosztása

Ahhoz, hogy szervezete számára a legjobb döntéseket hozhassa a kommunikáció módjával kapcsolatban, alapvető fontosságú, hogy megértse a kommunikációnk különböző típusú védelmi rendszereit, és hogy miért fontos ez a védelem.

A legtöbb kommunikációnál az egyik legfontosabb az üzenetek tartalmának titokban tartása – amiről a modern korban nagyrészt a titkosítás gondoskodik. Megfelelő titkosítás nélkül a privát kommunikációt tetszőleges számú ellenfél láthatja. A nem biztonságos kommunikáció érzékeny információkat és üzeneteket tárhat fel, jelszavakat vagy más személyes adatokat fedhet fel, és veszélybe sodorhatja a személyzetet és a szervezetet az Ön által megosztott kommunikáció és tartalom jellegétől függően.

Biztonságos kommunikáció és civil társadalom

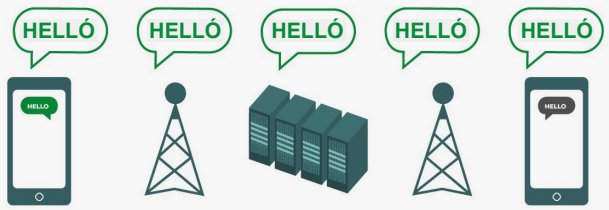
Demokrácia- és emberi jogi aktivisták és szervezetek ezrei támaszkodnak nap mint nap biztonságos kommunikációs csatornákra, hogy megőrizzék a beszélgetések bizalmas kezelését a kihívásokkal teli politikai környezetben. Ilyen biztonsági gyakorlatok nélkül az érzékeny üzeneteket a hatóságok elfoghatják és felhasználhatják aktivisták megcélzására és a tiltakozások feloszlatására. Ennek egyik kiemelkedő és jól dokumentált példája a 2010-es fehéroroszországi választások után történt. Az Amnesty International jelentésében leírtak szerint a telefonfelvételeket és más titkosítatlan kommunikációt a kormány lehallgatta, és a bíróságon felhasználta neves ellenzéki politikusok és aktivisták ellen, akik közül sokan éveket töltöttek börtönben. 2020-ban Fehéroroszországban a választások utáni tiltakozások újabb hulláma során tiltakozók ezrei fogadtak el olyan felhasználóbarát, biztonságos üzenetküldő alkalmazásokat, amelyek tíz évvel azelőtt nem voltak olyan könnyen elérhetőek, hogy megvédjék érzékeny kommunikációjukat.

MI A TITKOSÍTÁS ÉS MIÉRT FONTOS?

A titkosítás egy matematikai folyamat, amellyel egy üzenetet vagy fájlt kódolnak úgy, hogy csak a kulccsal rendelkező személy vagy entitás tudja „dekódolni" és elolvasni. Az Electronic Frontier Foundation Surveillance Self Defense Guide gyakorlati magyarázatot ad (grafikával) a titkosítás jelentésére:

Titkosítatlan üzenetküldés

Titkosítás nélkül mindenki, aki részt vesz az üzenet továbbításában, és bárki, akinek útjába kerül, elolvashatja annak tartalmát. Lehet, hogy ez nem sokat számít, ha csak annyit mond, hogy „helló", de nagy baj lehet, ha valami magánjellegűbb vagy kényesebb információt kommunikál, és nem szeretné, hogy a távközlési szolgáltatója, az internetszolgáltató, egy barátságtalan kormány vagy bármely más ellenfél látná azt. Emiatt elengedhetetlen, hogy kerülje a titkosítatlan eszközök használatát az érzékeny üzenetek (és ideális esetben bármilyen üzenetek) küldésére. Ne feledje, hogy a legnépszerűbb kommunikációs módok némelyike – mint például az SMS és a telefonhívás – gyakorlatilag mindenféle titkosítás nélkül működik (mint ezen a képen).



Amint a fenti képen látható, egy okostelefon zöld, titkosítatlan szöveges üzenetet („helló") küld egy másik okostelefonnak a jobb szélen. Útközben egy mobiltelefon-torony (vagy az interneten keresztül küldött üzenetek esetén az internetszolgáltató) továbbítja az üzenetet a vállalati szervereknek. Innen a hálózaton keresztül egy másik mobiltelefon-toronyhoz ugrik, amely látja a titkosítatlan „helló" üzenetet, és végül a célállomásra irányítja. Fontos megjegyezni, hogy mindenféle titkosítás nélkül mindenki, aki részt vesz az üzenet továbbításában, és bárki, aki találkozik vele, el tudja olvasni az üzenet tartalmát. Lehet, hogy ez nem sokat számít, ha csak annyit mond, hogy „helló", de nagy baj lehet, ha valami magánjellegűbb vagy kényesebb információt kommunikál, és nem szeretné, hogy a távközlési szolgáltatója, az internetszolgáltató, egy barátságtalan kormány vagy bármely más ellenfél látná azt. Emiatt elengedhetetlen, hogy kerülje a titkosítatlan eszközök használatát az érzékeny üzenetek (és ideális esetben bármilyen üzenetek) küldésére. Ne feledje, hogy a legnépszerűbb kommunikációs módok némelyike – például SMS és telefonhívás – gyakorlatilag titkosítás nélkül működik (mint a fenti képen).

Kétféleképpen lehet titkosítani az adatokat mozgás közben: ***szállítási rétegű titkosítás*** és ***végpontok közötti titkosítás***. Fontos tudni, hogy a szolgáltató milyen típusú titkosítást támogat, mivel a szervezet a biztonságosabb kommunikációs gyakorlatok mellett dönt. Az ilyen különbségeket jól leírja a Surveillance Self Defense útmutató, amelyet ismét itt adaptálunk:

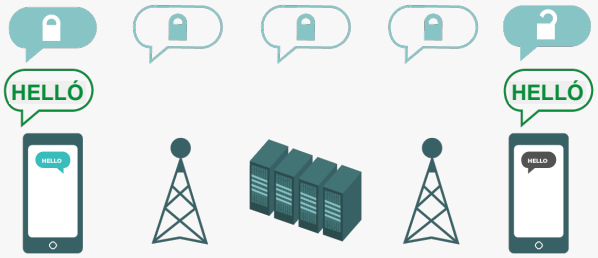
Szállítási rétegű titkosítás

A szállítási rétegű titkosítás, más néven szállítási rétegbiztonság (TLS), megvédi az üzeneteket, amint azok az Ön eszközéről az üzenetküldő alkalmazás/szolgáltatás szervereire, majd onnan a címzett eszközére jutnak. Ez megvédi őket a hálózaton vagy az internet- vagy távközlési szolgáltatóknál ülő hackerek kíváncsi tekintetétől. Középen azonban az üzenetküldő/e-mail szolgáltató, a böngészett weboldal vagy az Ön által használt alkalmazás láthatja az üzeneteinek titkosítatlan másolatait. Mivel üzeneteit láthatják (és gyakran tárolják is) a vállalati szerverek, ki vannak téve a bűnüldözési kéréseknek vagy lopásnak, ha a vállalat szervereit feltörik.

A fenti kép egy példát mutat a szállítási rétegű titkosításra. A bal oldalon egy okostelefon zöld, titkosítatlan üzenetet küld: "Helló." Ezt az üzenetet titkosítják, majd továbbítják egy mobiltelefon-toronyhoz. Középen a vállalati szerverek képesek visszafejteni az üzenetet, elolvasni a tartalmát, eldönteni, hogy hova küldjék, újratitkosítsák, majd elküldik a következő mobiltelefon-toronyba a cél felé. A végén a másik okostelefon megkapja a titkosított üzenetet, és visszafejti, hogy elolvassa a „Helló” szöveget.

Végpontok közötti titkosítás

A végpontok közötti titkosítás védi az üzeneteket a küldőtől a címzettig. Biztosítja, hogy az információt az eredeti feladó titkos üzenetté alakítsa (az első „vége”), és csak a végső címzettje dekódolja (a második „vége”). Senki, beleértve az Ön által használt alkalmazást vagy szolgáltatást, nem „hallgathatja meg” és nem hallgathatja le tevékenységét.



A fenti kép egy példát mutat a végpontok közötti titkosításra. A bal oldalon egy okostelefon zöld, titkosítatlan üzenetet küld: "Helló." Ezt az üzenetet titkosítják, majd továbbítják egy mobiltelefon-toronyhoz, majd az alkalmazás/szolgáltatás szervereihez, amelyek nem tudják elolvasni a tartalmat, de továbbítják a titkos üzenetet a célállomásnak. A végén a másik okostelefon megkapja a titkosított üzenetet, és visszafejti, hogy elolvassa a „Helló” szöveget. A szállítási rétegű titkosítással ellentétben az internetszolgáltató vagy az üzenetküldő gazdagép nem tudja visszafejteni az üzenetet. Csak a végpontok (a titkosított üzeneteket küldő és fogadó eredeti eszközök) rendelkeznek az üzenet visszafejtéséhez és olvasásához szükséges kulcsokkal.

MILYEN TÍPUSÚ TITKOSÍTÁSRA VAN SZÜKSÉGÜNK?

Amikor eldönti, hogy szervezetének szállítási rétegű titkosításra vagy végpontok közötti titkosításra van szüksége a kommunikációhoz, a nagy kérdések, amelyeket fel kell tennie, a bizalomra is vonatkoznak. Például megbízik az Ön által használt alkalmazásban vagy szolgáltatásban? Bízik a műszaki infrastruktúrájában? Aggasztja az a lehetőség, hogy egy barátságtalan kormány arra kényszerítheti a vállalatot, hogy átadja az Ön üzeneteit – és ha igen, bízik-e a cég irányelvében, amely megvédi a bűnüldözési kérelmektől? Ha e kérdések bármelyikére nemmel válaszol, akkor végpontok közötti titkosításra van szüksége. Ha igennel válaszol rájuk, akkor elegendő lehet egy olyan szolgáltatás, amely csak a szállítási rétegű titkosítást támogatja – de általában jobb, ha lehetőség szerint olyan szolgáltatásokat választunk, amelyek támogatják a végpontok közötti titkosítást.

Amikor csoportokkal üzen, ne feledje, hogy üzenetei biztonsága csak annyira jó, mint mindenkié, aki megkapja az üzeneteket. Ezért a biztonságos alkalmazások gondos kiválasztásán túl fontos, hogy a csoport minden tagja kövesse a fiók- és eszközbiztonsággal kapcsolatos egyéb bevált módszereket. Csak egy rossz színész vagy egy fertőzött eszköz kell ahhoz, hogy egy teljes csoportos csevegés vagy hívás tartalma kiszivárogjon.

MILYEN VÉGPONTOK KÖZÖTT TITKOSÍTOTT ÜZENETKÜLDŐ ESZKÖZÖKET KELL HASZNÁLJUK (2021-TŐL)?

Ha végpontok közötti titkosítást kell használnia, vagy csak a bevált gyakorlatot szeretné átvenni, függetlenül a szervezet fenyegetettségétől, íme néhány megbízható példa azokra a szolgáltatásokra, amelyek 2021-től végpontok közötti titkosítást kínálnak üzenetküldéshez és hívásokhoz. A Kézikönyv ezen részét rendszeresen frissítjük online, de kérjük, vegye figyelembe, hogy a dolgok gyorsan változnak a biztonságos üzenetküldés világában, ezért előfordulhat, hogy ezek az ajánlások már nem naprakészek, amikor ezt a részt olvassa. Ne feledje azt sem, hogy a kommunikációja csak annyira biztonságos, mint maga az eszköz. Tehát a biztonságos üzenetkezelési gyakorlatok mellett elengedhetetlen a jelen kézikönyv eszközbiztonsági részében leírt legjobb gyakorlatok alkalmazása.

Ajánlott végpontok közötti titkosított kommunikációs eszközök

SZÖVEGES ÜZENET (EGYÉNI VAGY CSOPORTOS)	• **Signal** • **WhatsApp (csak az alább részletezett speciális beállításokkal)**
AUDIO- ÉS VIDEOHÍVÁSOK	• **Signal (max. 8 fő)** • **WhatsApp (max. 8 fő)** • **Duo (max. 32 fő)**
FÁJLMEGOSZTÁS	• **Signal** • **Keybase / Keybase Teams** • **OnionShare + egy végpontok közötti titkosított üzenetküldő alkalmazás, például a Signal**

MIK AZOK A METAADATOK, ÉS AGGÓDNUNK KELL-E MIATTUK?

Az, hogy Ön és munkatársai kivel, mikor és hol beszélnek, gyakran ugyanolyan érzékeny lehet, mint az, amiről beszélnek. Fontos megjegyezni, hogy a végpontok közötti titkosítás csak a kommunikáció tartalmát (a „mit") védi. Itt jönnek képbe a metaadatok. Az EFF Surveillance Self Defense Guide áttekintést nyújt a metaadatokról és arról, hogy miért fontosak a szervezetek számára (beleértve a metaadatok kinézetének szemléltetését is):

A metaadatokat gyakran úgy írják le, mint minden, kivéve a kommunikáció tartalmát. A metaadatokat a boríték digitális megfelelőjének tekintheti. Csakúgy, mint egy boríték információkat tartalmaz az üzenet feladójáról, címzettjéről és célállomásáról, úgy a metaadatok is. A metaadatok az Ön által küldött és fogadott digitális kommunikációra vonatkozó információk.

Néhány példa a metaadatokra:

- akivel kommunikál
- az e-mailek tárgysora
- beszélgetéseinek hossza
- az időpont, amikor a beszélgetés zajlott
- tartózkodási helye kommunikáció közben

Még a metaadatok egy parányi mintája is bőséges adatokkal szolgálhat szervezete tevékenységeiről. Vessünk egy pillantást arra, hogy a metaadatok mennyire feltáróak a hackerek, kormányzati szervek és vállalatok számára, amelyek gyűjtik azokat:

Tudják, hogy felhívott egy újságírót, és egy órán keresztül beszélt velük, mielőtt az újságíró közzétett egy történetet egy névtelen idézettel. De nem tudják, miről beszéltek.

Tudják, hogy a szervezetén belül több alkalmazott is üzent egy kiemelkedő helyi digitális biztonsági oktatónak. De az üzenetek témája továbbra is titok marad.

Tudják, hogy e-mailt kapott egy COVID-tesztelő szolgálattól, majd felhívta orvosát, majd ugyanabban az órában felkereste az Egészségügyi Világszervezet weboldalát. De nem tudják, mi volt az e-mailben, vagy miről beszélt telefonon.

Tudják, hogy e-mailt kapott egy helyi emberi jogi jogvédő csoporttól, amelynek tárgya „Mondd el a kormánynak: Hagyják abba a hatalmukkal való visszaélést". De az e-mail tartalma láthatatlan számukra.

A metaadatokat nem védi a legtöbb üzenetszolgáltatás által biztosított titkosítás. Tehát, ha például a WhatsApp-on küld üzenetet, ne feledje, hogy bár az üzenet tartalma végpontokig titkosított, mások továbbra is tudják, hogy kivel, milyen gyakran és (a telefonhívások) mennyi ideig beszél. Emiatt szem előtt kell tartania, hogy milyen kockázatok állnak fenn (ha vannak ilyenek), ha bizonyos ellenfelek megtudhatják, kivel beszél a szervezete, mikor beszélt velük, és (e-mailek esetén) megtudhatják az Ön szervezete általános tárgysorait a szervezet kommunikációjából.

Az egyik oka annak, hogy a **Signal** olyan erősen ajánlott, hogy a végpontok közötti titkosításon túlmenően olyan funkciókat is bevezetett, **és kötelezettségeket vállalt az általa rögzített és tárolt metaadatok mennyiségének csökkentésére**. Például a Signal lezárt feladó funkciója titkosítja a metaadatokat arról, hogy ki kivel beszél, így a Signal csak az üzenet címzettjét ismeri, a feladót nem. Alapértelmezés szerint ez a funkció csak akkor működik, ha olyan meglévő névjegyekkel vagy profilokkal (személyekkel) kommunikál, akikkel már kommunikált, vagy akiket a névjegyzékében tárolt. Engedélyezheti azonban ezt a „Lezárt feladó" beállítást „Engedélyezés bárkitől" értékre, ha fontos az ilyen metaadatok eltávolítása az összes Signal beszélgetésből, még az Ön számára ismeretlen emberekkel folytatott beszélgetésekből is.

SZÜKSÉGEM VAN VÉGPONTOK KÖZÖTTI TITKOSÍTOTT E-MAILRE?

A legtöbb e-mail szolgáltató, például a Gmail, a Microsoft Outlook és a Yahoo Mail, szállítási rétegű titkosítást alkalmaz. Ha különösen érzékeny információkat kell közölnie, az e-mail nem a legjobb megoldás. Ehelyett válassza a biztonságos üzenetkezelési lehetőségeket, mint például a Signal. Még a végpontok között titkosított e-mail opciók is hagynak kívánnivalót maguk után biztonsági szempontból, például nem titkosítják az e-mailek tárgysorait és nem védik a metaadatokat. Ennek ellenére, ha kényes tartalmat kell közölnie e-mailben, és attól tart, hogy az e-mail szolgáltatója jogilag kötelezhető arra, hogy tájékoztatást adjon a kommunikációjáról egy kormánynak vagy más ellenfélnek, érdemes megfontolni egy végpontok között titkosított e-mail, például a ProtonMail vagy a Tutanota használatát.

VALÓBAN BÍZHATUNK a WHATSAPP-BAN?

A WhatsApp népszerű választás a biztonságos üzenetküldéshez, és a széleskörű elterjedtsége miatt jó választás lehet. Vannak, akik aggódnak amiatt, hogy a Facebook tulajdona és az irányítása alatt áll, amely azon dolgozik, hogy integrálja más rendszereivel. Az embereket az is aggasztja, hogy a WhatsApp mennyi metaadatot (azaz információt arról, hogy kivel és mikor kommunikál) gyűjt. Ha úgy dönt, hogy a WhatsApp-ot biztonságos üzenetküldési lehetőségként használja, feltétlenül olvassa el a fenti metaadatokról szóló részt. Van néhány beállítás is, amelyek megfelelő konfigurálásról gondoskodnia kell. A legkritikusabb, hogy kapcsolja ki a felhőalapú biztonsági mentéseket, jelenítse meg a biztonsági értesítéseket, és ellenőrizze a biztonsági kódokat. Itt talál egyszerű útmutatót ezen beállítások konfigurálásához Android telefonokhoz, iPhone készülékekhez pedig itt. **Ha az alkalmazottak *és azok, akikkel mindannyian kommunikálnak*, nem konfigurálják megfelelően ezeket a beállításokat, akkor ne tekintse a WhatsApp-ot jó lehetőségnek a végpontok közötti titkosítást igénylő érzékeny kommunikációhoz**. A Signal továbbra is a legjobb megoldás az ilyen végpontok közötti titkosított üzenetküldési igényekhez, tekintettel a biztonságos alapértelmezett beállításokra és a metaadatok védelmére.

MI A HELYZET A SZÖVEGES ÜZENETEKKEL?

Az alapvető szöveges üzenetek nagyon nem biztonságosak (a szabványos SMS-ek gyakorlatilag titkosítatlanok), ezért kerülni kell azokat minden olyan helyzetben, amely nem nyilvános. Míg az Apple iPhone-ról iPhone-ra küldött üzenetei (más néven iMessages) végpontok közötti titkosítással vannak ellátva, ha nem iPhone-os személy vesz részt a beszélgetésben, az üzenetek nincsenek biztonságban. A legjobb, ha biztonságban vagyunk, és kerüljük a **bármilyen érzékeny, privát vagy bizalmas jellegű szöveges üzenetek távoli küldését.**

MIÉRT NEM AJÁNLOTT BIZTONSÁGOS CSEVETÉSHEZ A TELEGRAM, A FACEBOOK MESSENGER VAGY A VIBER?

Egyes szolgáltatások, mint például a Facebook Messenger és a Telegram, csak akkor kínálnak végpontok közötti titkosítást, ha szándékosan bekapcsolja (és csak a személyes csevegésekhez), így ezek nem megfelelőek az érzékeny vagy privát üzenetek küldésére, különösen egy szervezet számára. Ne hagyatkozzon ezekre az eszközökre, ha végpontok közötti titkosítást kell használnia, mert nagyon könnyen elfelejtheti az alapértelmezett, kevésbé biztonságos beállításoktól való eltérést. A Viber azt állítja, hogy végpontok közötti titkosítást kínál, de nem tette elérhetővé a kódját külső biztonsági kutatók számára. A Telegram kódja szintén nem került nyilvános ellenőrzésre. Ennek eredményeként sok szakértő attól tart, hogy a Viber titkosítása (vagy a Telegram „titkos csevegései") nem felel meg a szabványnak, és ezért nem alkalmas olyan kommunikációra, amely valódi végpontok közötti titkosítást igényel.

KAPCSOLATAINK ÉS KOLLÉGÁINK MÁS ÜZENETKÜLDŐ ALKALMAZÁSOKAT HASZNÁLNAK – HOGYAN GYŐZHÜK MEG ŐKET, HOGY TÖLTSÉK LE AZ ÚJ ALKALMAZÁST A VELÜNK VALÓ KOMMUNIKÁCIÓHOZ?

Néha kompromisszumot kell kötni a biztonság és a kényelem között, de megér egy kis erőfeszítést az érzékeny kommunikáció esetén. Mutasson jó példát kapcsolatai számára. Ha más, kevésbé biztonságos rendszert kell használnia, legyen biztos abban, amit mond. Kerülje a kényes témák megbeszélését. Egyes szervezeteknél az egyik rendszert az általános csevegéshez, a másikat pedig vezetőikkel, a legbizalmasabb megbeszélésekhez használhatják. Természetesen a legegyszerűbb, ha minden mindig automatikusan titkosítva van – semmi emlékeznivaló vagy gondolkodnivaló.

Szerencsére a végpontok között titkosított alkalmazások, mint például a Signal, egyre népszerűbbek és felhasználóbarátabbak – nem is beszélve arról, hogy több tucat nyelvre lokalizálták őket globális használatra. Ha partnereinek vagy más kapcsolattartóinak segítségre van szüksége a kommunikációnak egy végpontok közötti titkosított opcióra, például a Signalra való átállásához, szánjon egy kis időt arra, hogy megbeszélje velük, miért olyan fontos a kommunikáció megfelelő védelme. Ha mindenki megérti ennek fontosságát, nem tűnik nagy ügynek az a néhány perc, ami egy új alkalmazás letöltéséhez szükséges, és az a néhány nap, amelybe beletelhet, hogy megszokja a használatát.

VANNAK EGYÉB BEÁLLÍTÁSOK A VÉGPONTOK KÖZÖTT TITKOSÍTOTT ALKALMAZÁSOKHOZ, AMELYEKKEL TISZTÁBAN KELL LENNI?

A Signal alkalmazásban a biztonsági kódok (amelyekre biztonsági számokként hivatkoznak) ellenőrzése is fontos. A biztonsági szám megtekintéséhez és a Signal alkalmazásban történő ellenőrzéséhez nyissa meg a csevegést egy partnerrel, koppintson a nevére a képernyő tetején, majd görgessen le a „Biztonsági szám megtekintése" elemre. Ha a biztonsági szám megegyezik a névjegyével, ugyanazon a képernyőn megjelölheti őt „ellenőrzöttként". Különösen fontos odafigyelni ezekre a biztonsági számokra, és ellenőrizni az elérhetőségeit, ha chaten értesítést kap arról, hogy megváltozott a biztonsági szám egy adott kapcsolatnál. Ha Önnek vagy más alkalmazottaknak segítségre van szüksége a beállítások konfigurálásához, maga a Signal ad hasznos utasításokat. Ha Signalt használ, amelyet széles körben a legjobb felhasználóbarát lehetőségnek tartanak a biztonságos üzenetküldéshez és a két fél közötti hívásokhoz, feltétlenül **állítson be egy erős PIN-kódot** is. Használjon legalább hat számjegyet, és ne olyan könnyen kitalálható dolgot, mint a születési dátuma. Ha további tippeket szeretne kapni a Signal és a WhatsApp megfelelő konfigurálásával kapcsolatban, tekintse meg az EFF által a Surveillance Self-Defense Guide című kiadványban található eszköz útmutatókat mindkettőhöz.

A csevegőalkalmazások használata a való világban

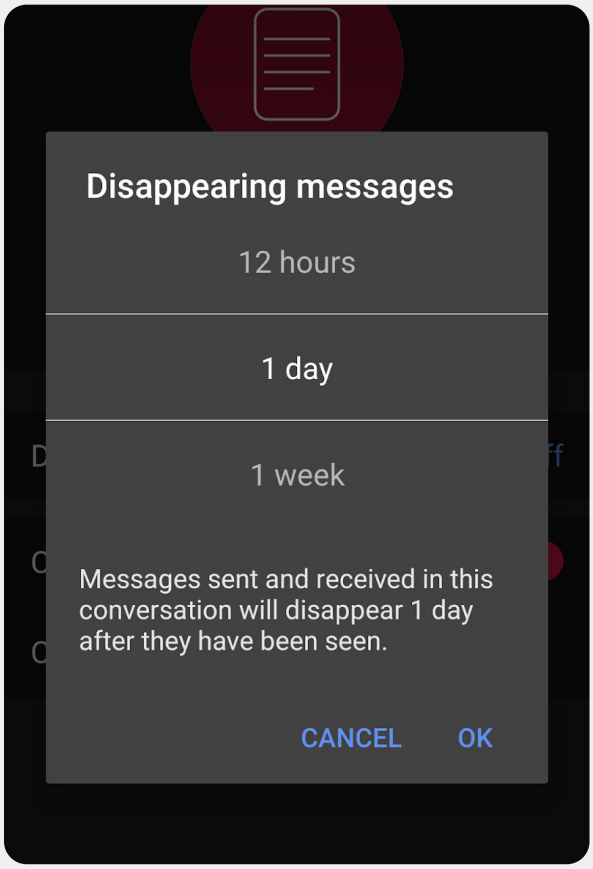
A telefon elvesztése, ellopása vagy elkobzása esetén keletkező károk korlátozása érdekében a legjobb gyakorlat a telefonra mentett üzenetek előzményeinek minimalizálása. Ennek egyik egyszerű módja az, hogy bekapcsolja az **„eltűnő üzenetek”** funkciót szervezete csoportos csevegéseiben, és a személyzetet a személyes csevegéseik során is erre ösztönzi.

A Signalban és más népszerű üzenetküldő alkalmazásokban beállíthat egy időzítőt, amellyel az üzenetek bizonyos számú perccel vagy órával az olvasás után eltűnnek. Ez a beállítás testreszabható az egyéni csevegés vagy csoport alapján. Legtöbbünk számára, ha egy hétre állítjuk be az eltűnő ablakot, bőven van időnk utánanézni a dolgoknak, miközben nem őrzünk meg olyan üzeneteket, amelyekre soha nem lesz szükségünk – de amelyeket a jövőben esetleg felhasználhatnak ellenünk. Ne feledje, ami nincs, azt nem lophatják el.

Az eltűnt üzenetek bekapcsolásához a Signal alkalmazásban nyisson meg egy csevegést, koppintson annak a személynek/csoportnak a nevére, akivel cseveg, koppintson az eltűnt üzenetekre, válasszon időzítőt, és koppintson az OK gombra. Hasonló beállítás létezik a WhatsApp-ban is.

Súlyosabb helyzetekben, amikor szükség van egy üzenet azonnali törlésére, esetleg azért, mert valakinek ellopták a telefonját, vagy rossz személynek küldött üzenetet, vegye figyelembe, hogy a Signal lehetővé teszi egy csoportnak vagy egyénnek küldött üzenetek törlését mindenki fiókjából az elküldésétől számított három órán belül csupán a csevegésből való törlésével. A Telegram továbbra is népszerű sok országban, annak ellenére, hogy titkosítási korlátai vannak egy hasonló funkciónak, amely lehetővé teszi a felhasználók számára, hogy korlátozások nélkül töröljék az üzeneteket az eszközökről.

Ezzel együtt, ha szervezete aggódik a személyzet biztonsága miatt a telefonjukon esetleg látható kommunikáció miatt, akkor valószínűleg a legegyszerűbb és legfenntarthatóbb megoldás az eltűnő üzenetek rövid időzítőkkel történő használata.



MI VAN A NAGYOBB CSOPORTOS VIDEÓHÍVÁSOKKAL? VANNAK VÉGPONTOK KÖZÖTTI TITKOSÍTÁSI OPCIÓK?

A távmunka számának növekedésével fontos, hogy legyen biztonságos lehetőség a szervezet nagy, csoportos videohívásaihoz. Sajnos jelenleg nincs olyan nagyszerű lehetőség, amely az összes négyzetet bejelölné: felhasználóbarát, nagyszámú résztvevőt és együttműködési funkciókat támogat, és alapértelmezés szerint lehetővé teszi a végpontok közötti titkosítást.

Ha az értekezletek nem igényelnek együttműködési funkciókat, például képernyőmegosztást vagy szekciószobákat, akkor van néhány lehetőség. Legfeljebb nyolc fős csoportok számára a Signal erősen ajánlott. A Signal csoportos videohívásaihoz okostelefonról vagy számítógépen a Signal asztali alkalmazásból is csatlakozhat. Ne feledje azonban, hogy csak a Signalt használó kapcsolatai vehetők fel a Signal csoportba.

A Google Duo végpontok közötti titkosított videohívásokat biztosít akár 32 résztvevő számára, így jó választás lehet kicsit nagyobb megbeszélésekhez, amelyekhez nincs szükség képernyőmegosztásra vagy szekciószobákra. A Duót okostelefonos alkalmazáson keresztül vagy a számítógép webböngészőjéből használhatja. A résztvevőknek nem kell letölteniük a Duo alkalmazást, hogy számítógépükön csatlakozhassanak egy csoportos híváshoz, azonban be kell jelentkezniük egy Google-fiókba. Ez nem csak a használat gátja, hanem azt is jelenti, hogy a Duo sok metaadatot gyűjt arról, hogy ki kivel beszél. Tehát ha ez aggodalomra ad okot, akkor lehet, hogy a Duo nem a legjobb megoldás. Ha használja a Duót, ügyeljen arra, hogy biztonságosan ossza meg a csoport hivatkozásokat, és mindenki törölje a csoportot minden hívás után. Ha végpontok közötti titkosításra van szüksége nagyobb csoportos hívásokhoz vagy workshopokhoz, amelyekhez olyan funkciókra van szükség, mint a képernyőmegosztás és a szekciószobák, akkor van néhány lehetőség. De ne feledje, hogy ezek a beállítások egy kicsit nagyobb körültekintést igényelnek a teljes körű titkosítás engedélyezése és a biztonság fenntartása érdekében.

Az egyik platform, amely a közelmúltban egy végpontok közötti titkosítási lehetőséget adott hozzá, a **Jitsi Meet.** A Jitsi Meet egy webalapú audio- és videokonferencia-megoldás, amely nagy közönség számára (legfeljebb 75 fő) működik, és nem igényel alkalmazást vagy speciális szoftvert. A Jitsi 2020-ban kiadott egy kísérleti, végpontok közötti titkosítási lehetőséget, és e kézikönyv megjelenése óta a Jitsi aktívan dolgozik a javításán. Ha megbeszélést szeretne beállítani a Jitsi Meetben, menjen a meet.jit.si weboldalra, írja be a megbeszélés kódját, és megoszthatja a hivatkozást (biztonságos csatornán, például a Signal segítségével) a kívánt résztvevőkkel. A végpontok közötti titkosítás használatához tekintse meg ezeket a Jitsi által felvázolt utasításokat. Vegye figyelembe, hogy minden egyes felhasználónak magának kell engedélyeznie a végpontok közötti titkosítást, hogy az működjön. A Jitsi használatakor ügyeljen arra is, hogy véletlenszerű tárgyalótermi neveket hozzon létre, és erős jelkódokat használjon a hívások védelme érdekében.

Ha ez a lehetőség nem működik az Ön szervezetében, fontolóra veheti egy népszerű kereskedelmi lehetőség, például a WebEx vagy a Zoom használatát, engedélyezve a végpontok közötti titkosítást. A WebEx már régóta lehetővé teszi a végpontok közötti titkosítást, azonban ez a lehetőség alapértelmezés szerint nincs bekapcsolva, és a résztvevőknek le kell tölteniük a WebEx-et, hogy csatlakozhassanak az értekezlethez. A végpontok közötti titkosítás beállításához WebEx-fiókjához meg kell nyitnia egy WebEx támogatási csomagot, és követnie kell ezeket az utasításokat a végpontok közötti titkosítás konfigurálása érdekében. Csak a megbeszélés házigazdájának kell engedélyeznie a végpontok közötti titkosítást. Ha így tesznek, a teljes megbeszélés végpontok között titkosítva lesz. Ha a WebEx-et biztonságos csoportos értekezletekhez és workshopokhoz használja, ügyeljen arra, hogy az erős jelkódokat is engedélyezze hívásaiban.

Több hónapos negatív sajtó után a Zoom kifejlesztett egy végpontok közötti titkosítási lehetőséget a hívásaihoz. Ez az opció azonban alapértelmezés szerint nincs bekapcsolva, megköveteli, hogy a hívásgazda társítsa fiókját egy telefonszámhoz, és csak akkor működik, ha minden résztvevő a Zoom asztali vagy mobilalkalmazáson keresztül csatlakozik betárcsázás helyett. Mivel ezek a beállítások könnyen véletlenül rosszul konfigurálhatók, nem javasoljuk, hogy a Zoom-ot végpontok közötti titkosítási lehetőségként használja. Ha azonban végpontok közötti titkosítás szükséges, és a Zoom az egyetlen lehetőség, a Zoom utasításait követve konfigurálhatja. Csak győződjön meg róla, hogy minden hívás megkezdése előtt ellenőrizze, hogy valóban végpontok között titkosított-e. Ehhez kattintson a zöld zárra a Zoom képernyő bal felső sarkában, és figyelje meg a „végpontok" feliratot a Titkosítás beállítása mellett. Ezenkívül minden Zoom-találkozóhoz erős jelszót kell beállítania.

A fent említett eszközökön kívül ez a Frontline Defenders által kidolgozott folyamatábra rávilágít néhány videohívási és konferencia-lehetőségre, amelyek a kockázati kontextustól függően hasznosak lehetnek szervezete számára.

MI VAN, HA TÉNYLEG NINCS SZÜKSÉGÜNK MINDEN KOMMUNIKÁCIÓNK VÉGPONTOK KÖZÖTTI TITKOSÍTÁSÁRA?

Ha a kockázatértékelés alapján nincs szükség végpontok közötti titkosításra a szervezet összes kommunikációjához, fontolóra veheti a szállítási rétegű titkosítással védett alkalmazások használatát. Ne feledje, hogy az ilyen típusú titkosításhoz meg kell bíznia a szolgáltatóban, például a Google for Gmailben, a Microsoft for Exchange-ben vagy a Facebook for Messengerben, mert ők (és bárki, akivel esetleg kénytelenek megosztani információkat) láthatják/hallhatják az Ön kommunikációját. A legjobb lehetőségek a fenyegetési modelltől függenek (például ha nem bízik a Google-ban, vagy ha az Egyesült Államok kormánya az ellenfél, akkor a Gmail nem jó választás), de néhány népszerű és általánosan megbízható lehetőség a következő:

EMAIL	• **Gmail** • **Outlook (Office 365-ön keresztül)** • Ne kezeljen gazdaként saját Microsoft Exchange-kiszolgálót szervezete e-mailjeinél. Ha jelenleg ezt teszi, akkor **át kell térnie** az Office 365-re.
SZÖVEGES ÜZENET (EGYÉNI VAGY CSOPORTOS)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CSOPORTOS KONFERENCIA, AUDIO- ÉS VIDEOHÍVÁSOK	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **WebEx** • **GotoMeeting** • **Zoom**
FÁJLMEGOSZTÁS	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

MEGJEGYZÉS A FÁJLMEGOSZTÁSHOZ

Az üzenetek biztonságos megosztása mellett a fájlok biztonságos megosztása valószínűleg fontos része szervezete biztonsági tervének. A legtöbb fájlmegosztási lehetőség be van építve olyan üzenetküldő alkalmazásokba vagy szolgáltatásokba, amelyeket esetleg már használ. Például a fájlok Signal segítségével történő megosztása nagyszerű lehetőség, ha végpontok közötti titkosításra van szükség. És ha elegendő a szállítási rétegű titkosítás, a Google Drive vagy a Microsoft Sharepoint használata jó választás lehet szervezete számára. Csak ügyeljen arra, hogy megfelelően konfigurálja a megosztási beállításokat, hogy csak a megfelelő személyek férhessenek hozzá az adott dokumentumhoz vagy mappához, és győződjön meg arról, hogy ezek a szolgáltatások csatlakoznak a személyzet szervezeti (nem személyes) e-mail fiókjához. Ha teheti, tiltsa le az érzékeny fájlok megosztását e-mail mellékleteken keresztül vagy fizikailag USB-n keresztül. Az olyan eszközök, mint például az USB-k használata a szervezeten belül nagymértékben megnöveli a rosszindulatú programok vagy a lopások valószínűségét, az e-mailekre vagy a csatolmányok egyéb formáira támaszkodva pedig gyengíti a szervezet védekezőképességét az adathalász támadásokkal szemben.

Szervezeti alternatívák a fájlmegosztáshoz

Ha olyan biztonságos fájlmegosztási lehetőséget keres szervezete számára, amely nincs közvetlenül beágyazva egy üzenetküldő platformba (vagy esetleg fájlméret-korlátokba ütközik nagy dokumentumok megosztása során), fontolja meg az OnionShare szolgáltatást. Az OnionShare egy nyílt forráskódú eszköz, amely lehetővé teszi bármilyen méretű fájlok biztonságos és névtelen megosztását. Ez úgy működik, hogy a feladó letölti az OnionShare alkalmazást (elérhető Mac, Windows és Linux számítógépeken), feltölti a megosztani kívánt fájl(oka)t, és létrehoz egy egyedi hivatkozást. Ezt a hivatkozást, amely csak a Tor Browserben lehet feldolgozni, bármely biztonságos üzenetküldő csatornán (például a Signalon) keresztül megoszthatja a kívánt címzettnek. A címzett ezután megnyithatja a hivatkozást a Tor Browserben, és letöltheti a fájl(oka)t a számítógépére. Ne feledje, hogy a fájlok csak annyira biztonságosak, mint a hivatkozás megosztásának módja. A Torról részletesebben a kézikönyv egy későbbi „haladó” részében lesz szó, de a szervezeten belüli fájlmegosztás céljából tartsa szem előtt az OnionShare-t, mint egy biztonságosabb alternatívát a nagy fájlok USB-n történő megosztására az irodában, ha nem megbízható felhőszolgáltató opcióval rendelkezik.

Ha szervezete már beruház egy jelszókezelőbe, amint azt jelen Kézikönyv jelszavakkal foglalkozó részében leírtuk, és a Bitwarden prémium vagy csapatfiókját választja, a Bitwarden Send funkció egy másik lehetőség a biztonságos fájlmegosztásra. Ez a funkció lehetővé teszi a felhasználók számára, hogy biztonságos hivatkozásokat hozzanak létre a titkosított fájlok megosztásához bármely biztonságos üzenetküldő csatornán (például Signal) keresztül. A fájl mérete 100 MB-ra van korlátozva, de a Bitwarden Send lehetővé teszi a hivatkozások lejárati dátumának beállítását, a megosztott fájlok hozzáférésének jelszóvédelmét, és korlátozza a hivatkozás megnyitásának számát.

Biztonságos kommunikáció és adatmegosztás

- **Követelje a megbízható, végpontok közötti titkosított üzenetküldő szolgáltatások használatát szervezete érzékeny kommunikációjához (és ideális esetben minden kommunikációhoz).**
  - Szánjon időt arra, hogy elmagyarázza a személyzetnek és a külső partnereknek, miért olyan fontos a biztonságos kommunikáció; ez növeli a terve sikerét.
- **Állítson be egy szabályzatot arra vonatkozóan, hogy mennyi ideig fogja megőrizni az üzeneteket, amikor/ha használ a szervezet „eltűnő" kommunikációt.**
- **Győződjön meg arról, hogy megfelelő beállítások vannak megadva a biztonságos kommunikációs alkalmazásokhoz, beleértve:**
  - Győződjön meg arról, hogy a személyzet minden tagja odafigyel a biztonsági értesítésekre, és ha WhatsApp-ot használ, ne készítsen biztonsági másolatot a csevegésekről.
  - Ha olyan alkalmazást használ, ahol a végpontok közötti titkosítás alapértelmezés szerint nincs engedélyezve (pl. Zoom vagy Webex), győződjön meg arról, hogy a szükséges felhasználók bekapcsolták a megfelelő beállításokat minden hívás vagy megbeszélés elején.
- **Használjon felhőalapú e-mail szolgáltatásokat szervezete számára, például Office 365-öt vagy Gmailt.**
  - Ne próbáljon meg saját e-mail kiszolgálót üzemeltetni.
  - Ne engedje meg a személyzetnek, hogy személyes e-mail fiókokat használjanak munkához.
- **Gyakran emlékeztesse a szervezetet a csoportos üzenetekkel és metaadatokkal kapcsolatos biztonsági bevált gyakorlatokra.**
  - Ügyeljen arra, hogy kik szerepelnek a csoportos üzenetekben, csevegésekben és e-mail-szálakban.

Az adatok biztonságos tárolása

A legtöbb civil szervezet számára az egyik legfontosabb döntés, hogy hol tárolják adatait.

„Biztonságosabb" az adatok tárolása a személyzet számítógépein, egy helyi szerveren, külső tárolóeszközökön vagy a felhőben? Az esetek 99%-ában a legegyszerűbb és legbiztonságosabb megoldás az adatok megbízható felhőalapú tárolási szolgáltatásokban való tárolása. Néhány gyakori példa a Microsoft 365, a Google Drive vagy a Dropbox. Átfogó felhőalapú tárolási terv nélkül valószínű, hogy a szervezet adatait számos helyen tárolják – beleértve a személyzet számítógépeit, a külső merevlemezeket és esetleg egy helyi szervert is. Bár ezeken az eszközökön lehetséges az adatok biztonságossá tétele, nagyon nehéz ezt sikeresen megtenni sok pénz elköltése és jelentős informatikai személyzet alkalmazása nélkül.

Adattárolás és civil társadalom

A megfizethető (néha ingyenes) felhőalapú adattárolás megjelenése megkönnyítette (és biztonságosabbá) sok erőforrás-korlátozott civil társadalmi szervezet életét. Sajnos sokan még mindig megpróbálják saját szervereiket hosztolni, korlátozott informatikai ismeretekkel vagy támogatással. 2021 márciusában az ilyen szervezeti infrastruktúra fenyegetése valóságossá vált világszerte több tízezer szervezet számára, amikor a kínai kormányhoz kötődő fenyegetési szereplő, a Hafnium globális kiberbiztonsági katasztrófát robbantott ki a saját üzemeltetésű Microsoft Exchange szerverek elleni kifinomult támadással. A támadás a helyi szervereket veszélyeztette, lehetővé téve a hackerek számára, hogy hozzáférjenek a szervezeti e-mail fiókokhoz, és további rosszindulatú programokat telepítsenek az áldozat szervereire és a kapcsolódó rendszerekre. Míg a Microsoft gyorsan közzétett egy frissítést és utasításokat a potenciális behatolók azonosítására és eltávolítására, sok kisebb szervezet nem rendelkezett az ilyen frissítések gyors alkalmazásához szükséges informatikai kapacitással, így azok hosszabb ideig láthatóak voltak. Ennek a globális feltörésnek a terjedelme és hatása rávilágít arra a veszélyre, hogy a civil szervezetek – különösen a kisebb, korlátozott informatikai személyzettel rendelkező szervezetek – az e-mail szerverek és más típusú érzékeny adatok saját üzemeltetését választják.

A FELHŐTÁROLÁS ELŐNYEI

Még ha meg is tesz minden megfelelő lépést számítógépe rosszindulatú programokkal és fizikai lopással szembeni védelmére, akkor is előfordulhat, hogy egy határozott ellenfél feltöri számítógépét vagy helyi szerverét. Sokkal nehezebben tudják legyőzni például a Google vagy a Microsoft biztonsági védelmét. A jó felhőalapú tárolóvállalatok páratlan biztonsági erőforrásokkal rendelkeznek, és erős üzleti ösztönzést jelentenek, hogy maximális biztonságot nyújtsanak felhasználóik számára. Röviden: egy megbízható felhőalapú tárolási stratégia sokkal könnyebben és olcsóbban megvalósítható, és idővel biztonságosabb lesz. Így ahelyett, hogy saját szerverének biztonságáért aggódna, energiáját néhány egyszerűbb feladatra összpontosíthatja. Az adatok nagy részének a felhőben tartása számos egyéb gyakori kockázat ellen is segít. Valakinek a számítógépét az étteremben hagyták, vagy a telefonját a buszon? Kiöntött gyermeke egy pohár gyümölcslevet a billentyűzetére, így a készülék működésképtelenné vált? Van egy alkalmazottnak valamilyen rosszindulatú programja, és mindent törölnie kell a számítógépről, és újra kell kezdenie? Ha a legtöbb dokumentum és adat a felhőben található, könnyen újraszinkronizálható, és újrakezdhető egy megtisztított vagy teljesen új számítógépen. Ha rosszindulatú program kerül a számítógépbe, vagy ha egy tolvaj átvizsgál egy merevlemezt, akkor nincs mit ellopni, ha a legtöbb dokumentumhoz a webböngészőn keresztül férnek hozzá.

MILYEN FELHŐALAPÚ TÁROLÓ-SZOLGÁLTATÓT KELL VÁLASZTANUK?

A két legnépszerűbb felhőalapú tárolási lehetőség a Google Workspace (korábbi nevén GSuite) és a Microsoft 365. Ha Ön és munkatársai már használják a Gmailt, akkor a szervezete Google Workspace szolgáltatásba való regisztrációja és a beépített Google Dokumentumok, Táblázatok és Diák alkalmazásokkal a Google Drive-ban való tárolása nagyon logikus. Hasonlóképpen, ha Ön egy Excel- és Word-alapú szervezet, akkor egyszerű választás a Microsoft 365-re való regisztráció, amely hozzáférést biztosít szervezete számára az Outlookhoz e-mailekhez, valamint a Microsoft Word, Excel, Powerpoint és Teams licencelt verzióihoz. Függetlenül attól, hogy melyik szolgáltatót választja, az adatok biztonságos felhőben való tárolása megfelelő megosztási beállításokat és a személyzet képzését igényli, hogy megértsék, hogyan és mikor kell megosztani (és nem megosztani) mappákat és dokumentumokat. Általánosságban elmondható, hogy olyan mappákat kell beállítania a felhőalapú tárolómeghajtón belül, amelyek csak az adott fájlokhoz szükséges személyzetre korlátozzák a hozzáférést. Rendszeresen ellenőrizze a rendszert, hogy megbizonyosodjon arról, hogy nem „oszt meg túl nagyon" egyetlen fájlt sem (például kapcsolja be az univerzális hivatkozások megosztását olyan fájlok esetében, amelyek ehelyett csak néhány személyre korlátozódnak).

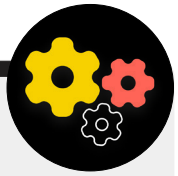
MI VAN, HA NEM BÍZUNK A GOOGLE-BAN, VAGY MICROSOFTBAN VAGY MÁS FELHŐALAPÚ TÁROLÓ-SZOLGÁLTATÓKBAN?

Ha az Ön egyik ellenfele (például egy külföldi vagy helyi önkormányzat) törvényesen kényszerítheti a Google-t vagy a Microsoftot (vagy egy másik felhőalapú tárolási szolgáltatót) adatok átadására, akkor előfordulhat, hogy nincs értelme adattárolási lehetőségként őket választani. Ez a kockázat magasabb lehet, ha az Ön ellenfele például az Egyesült Államok kormánya, de sokkal alacsonyabb, ha ellenfele tekintélyelvű rezsim. Ne feledje, hogy a Google és a Microsoft is rendelkezik arra vonatkozó szabályzattal, hogy csak akkor adják át az adatokat, ha erre törvény kötelezi, és ismerje el, hogy az Ön szervezete maga is kiszolgáltatott lehet a saját kormánya hasonló jogi követeléseinek, ha helyben tárolja az adatokat. Azokban a helyzetekben, amikor a Google vagy a Microsoft felhőalapú tárolása nem megfelelő az Ön szervezete számára, egy másik lehetőség a Keybase. A **Keybase** „csapatok" funkciója lehetővé teszi, hogy szervezete végpontok közötti titkosítással ossza meg fájljait és üzeneteit egy biztonságos felhőalapú környezetben anélkül, hogy külső szolgáltatóra kellene hagyatkoznia. Ennek eredményeként jó lehetőség lehet dokumentumok és fájlok biztonságos tárolására a szervezetben. A Keybase azonban kevésbé ismert a legtöbb felhasználó számára, ezért ügyeljen arra, hogy ennek az eszköznek az elfogadása valószínűleg több képzést és erőfeszítést igényel, mint a többi fent említett megoldás. Ezzel együtt, ha úgy dönt, hogy egyedül megy, és nem használ teljes egészében felhőalapú tárhelyet, döntő fontosságú, hogy időt és erőforrásokat fektessen be szervezete eszközeinek digitális védelmének megerősítésébe, valamint annak biztosítására, hogy a helyi szerverek megfelelően legyenek konfigurálva, titkosítva és fizikailag biztonságban tartják. Megspórolhatja a havi előfizetési díjakat, de ez szervezetének személyzeti idejébe és erőforrásaiba kerül, és sokkal sebezhetőbb lesz a támadásokkal szemben.

ADATOK BIZTONSÁGI MENTÉSE

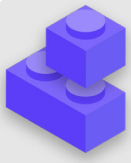
Akár a szervezete fizikai eszközökön, akár a felhőben tárol adatokat, fontos, hogy legyen biztonsági másolat. Különösen akkor, ha az eszköz fizikai tárolására támaszkodik, nagyon könnyű elveszíteni az adatokhoz való hozzáférést. Kávét önthet a számítógépére, és tönkreteheti a merevlemezt. A személyzet számítógépeit feltörhetik, és minden helyi fájlt zárolhatnak zsarolóvírussal. Valaki elveszítheti

egy eszközt a vonaton, vagy ellophatják a táskájával együtt. Ahogy fentebb említettük, ez egy másik ok, amiért a felhőalapú tárhely használata előnyt jelenthet, mivel nincs egy adott eszközhöz kötve, amely megfertőződhet, elveszhet vagy ellopható. A Mac-ek beépített biztonsági mentési szoftverrel rendelkeznek, ez az úgynevezett Time Machine, amelyet külső tárolóeszközzel együtt használnak; Windows-eszközökön a Fájlelőzmények hasonló funkciókat kínál. Az iPhone és Android készülékek automatikusan biztonsági másolatot készíthetnek a legfontosabb tartalmaikról a felhőbe, ha engedélyezve van a telefon beállításaiban. Ha a szervezete felhőalapú tárhelyet használ (például a Google Drive-ot), annak a kockázata, hogy a Google-t leállítják, vagy adatai megsemmisülnek egy katasztrófa során, meglehetősen alacsony, de az emberi hiba (például a fontos fájlok véletlen törlése) továbbra is fennáll. Érdemes tehát felfedezni egy felhőalapú biztonsági mentési megoldást, mint például a Backupify. Ha az adatokat helyi szerveren és/vagy helyi eszközökön tárolják, a biztonságos biztonsági mentés még kritikusabbá válik. A szervezet adatairól biztonsági másolatot készíthet egy külső merevlemezre, de mindenképpen erős jelszóval titkosítsa a merevlemezt. A Time Machine titkosíthatja a merevlemezeket, vagy használhat megbízható titkosítási eszközöket a teljes merevlemezhez, például a VeraCrypt vagy a BitLocker. Ügyeljen arra, hogy a biztonsági másolatot készítő eszközöket a többi eszköztől és fájltól külön helyen tárolja. Ne feledje, hogy egy tűz, amely elpusztítja mind a számítógépeit, mind a biztonsági másolatait, azt jelenti, hogy nincs biztonsági másolata. Fontolja meg, hogy egy másolatot nagyon biztonságos helyen tároljon, például széfben.



A szervezeti felhőalapú fiókok biztonságának fokozása

Ha szervezete úgy dönt, hogy tartományt állít be a Google Workspace vagy a Microsoft 365 szolgáltatásban, vegye figyelembe, hogy mindkét vállalat magasabb szintű biztonságot kínál (sok esetben ingyenes) a civil szervezetek számára. A Google Speciális védelmi programja és a Microsoft AccountGuard programja még erőteljesebb biztonságot nyújt szervezete összes felhőalapú fiókjában, és jelentősen csökkenti a hatékony adathalászat és fiókkompromittálódás valószínűségét. Ha úgy gondolja, hogy szervezete megfelel a követelményeknek, és szeretné felvenni szervezetét valamelyik tervbe, keresse fel a fent hivatkozott weboldalakat, vagy forduljon a cyberhandbook@ndi.org címhez további segítségért.



Biztonságos kommunikáció és adatmegosztás

- **Az érzékeny adatokat kizárólag megbízható felhőalapú tárolási szolgáltatásban tárolja.**
  - Győződjön meg arról, hogy az ilyen szolgáltatások eléréséhez használt összes kapcsolódó fiók erős jelszavakkal és 2FA-val rendelkezik.
- **Állítson be és kényszerítsen ki egy házirendet a felhőn belüli megosztási beállítások korlátozására.**
  - Tanítsd meg az összes alkalmazottat a dokumentumok megfelelő megosztására (és nem túlzott megosztására).
- **Ha szervezete úgy dönt, hogy helyben tárolja az adatokat, fektessen be képzett informatikai személyzetbe.**
- **Tartsa biztonságban az adatok biztonsági másolatait – titkosítsa a biztonsági mentési merevlemezeket vagy más biztonsági mentési eszközöket.**

Hogyan maradjon biztonságban az interneten

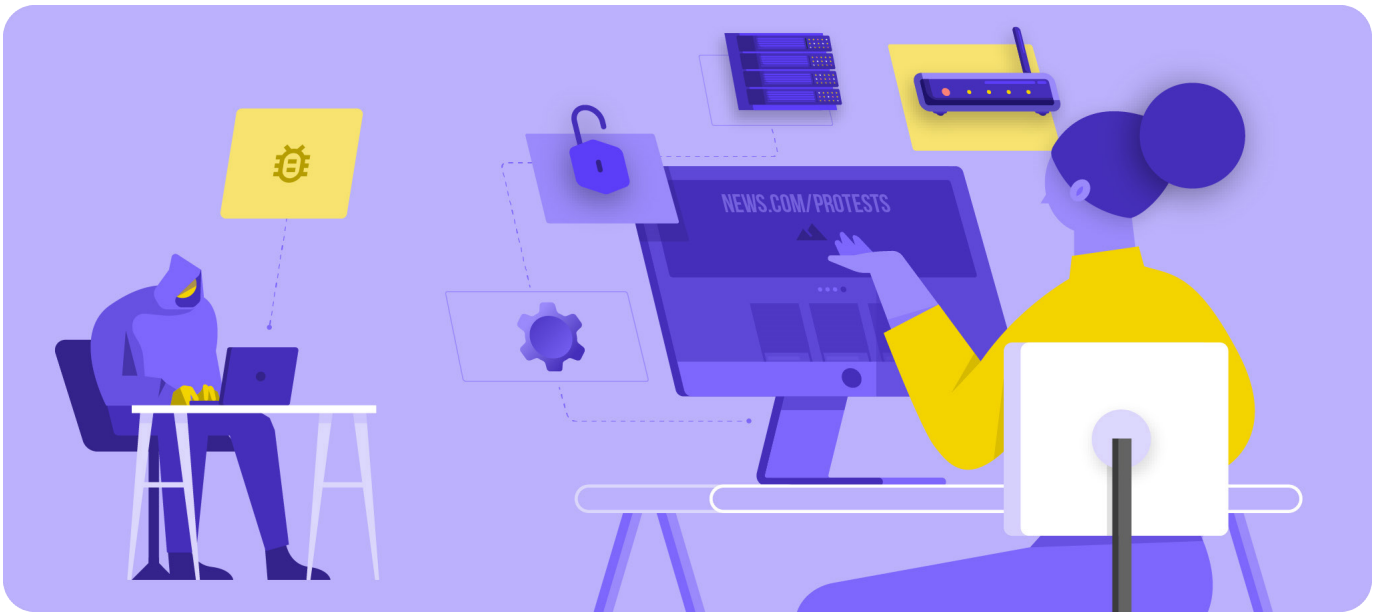
Amikor az internetet telefonon vagy számítógépen használja, tevékenysége sokat elárulhat Önről és szervezetéről.

Fontos, hogy az érzékeny információkat – például a weboldalakon beírt felhasználóneveket és jelszavakat, a közösségi média bejegyzéseit vagy bizonyos összefüggésekben még a felkeresett weboldalak nevét is – távol tartsa a kíváncsi szemek elől. Szintén gyakori probléma, hogy bizonyos weboldalakhoz vagy alkalmazásokhoz való hozzáférését blokkolják vagy korlátozzák. Ez a két probléma – az internetes megfigyelés és az internetes cenzúra – kéz a kézben jár, és a hatások csökkentésére irányuló stratégiák hasonlóak.

Biztonságos böngészés

HTTPS HASZNÁLATA

A legfontosabb lépés annak korlátozására, hogy az ellenfél azon képességét korlátozza, hogy felügyelje szervezetét az interneten, az Önről és kollégáinak internetes tevékenységéről elérhető információk mennyiségének minimalizálása. Mindig győződjön meg arról, hogy biztonságosan csatlakozik a weboldalakhoz: győződjön meg arról, hogy az URL (hely) „https" előtaggal kezdődik, és egy kis lakat ikont mutat a böngésző címsorában. Amikor **titkosítás nélkül** böngészik az interneten, a weboldalra beírt információk (például jelszavak, számlaszámok vagy üzenetek), valamint a meglátogatott weboldalak és helyek adatai mind megjelennek. Ez azt jelenti, hogy (1) a hálózaton lévő hackerek, (2) az Ön hálózati rendszergazdája, (3) az internetszolgáltató és minden olyan entitás, akivel adatokat oszthatnak meg (például kormányzati hatóságok), (4) a meglátogatott weboldal internetszolgáltatója és minden entitás, amellyel adatokat osztanak meg, és természetesen (5) maga a meglátogatott weboldal is hozzáfér sok potenciálisan érzékeny információhoz.

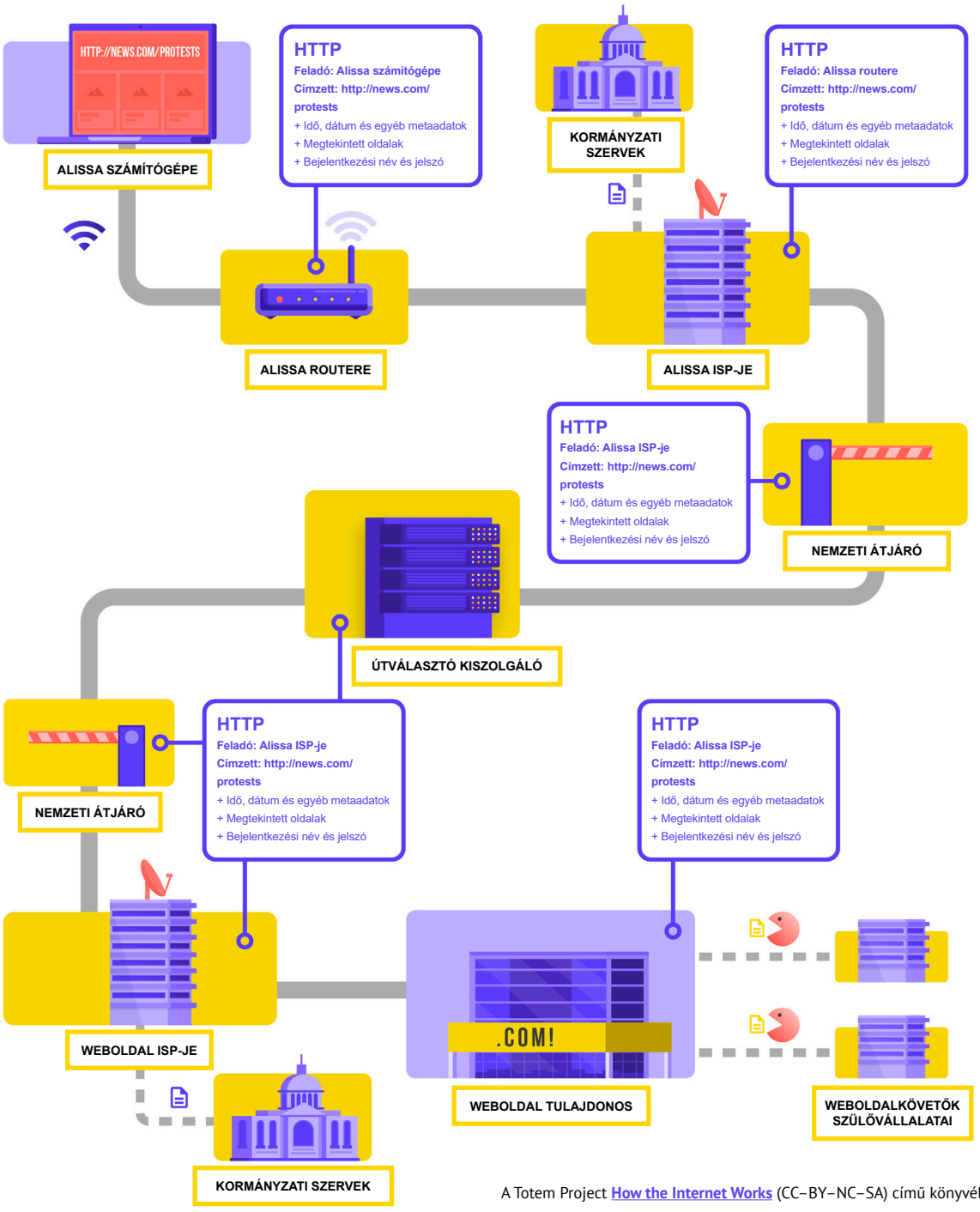


Felügyelet, cenzúra és civil társadalom

A kormányok egyre inkább használják befolyásukat és hatalmukat az internetszolgáltatókra és más helyi internetes infrastruktúrákra, hogy megakadályozzák az egyéneket és a civil társadalmi csoportokat abban, hogy hozzáférjenek az interneten található információkhoz. Egyes esetekben az ilyen internetes fennakadások célja a kulcsfontosságú kommunikációs és információmegosztó platformok, köztük a közösségi médiák és a híroldalak megszüntetése. Például a katonai puccsból eredő tiltakozásokra válaszul a mianmari hadsereg arra utasította a mobilszolgáltatókat, hogy ideiglenesen állítsák le a teljes mobil adathálózatot az országban. Ez röviddel a Facebook, Twitter és Instagram célzottabb blokkolása után történt. Amellett, hogy blokkolják az internet-hozzáférést és a weboldalakat, a kormányok és más fenyegetett szereplők szerte a világon egyre hozzáférhetőbb megfigyelési technológiát használnak a polgárok online tevékenységének nyomon követésére. Például a Freedom House Freedom on the Net 2020-as jelentése szerint az ugandai kormány együttműködött a kínai Huawei technológiai vállalattal, hogy **felügyelje az ellenzéki szereplőket és civil aktivistákat** a vitás elnökválasztás előtt és után az országban.

Az online információszabadság elleni ilyen támadások növekvő gyakorisága rávilágít arra, hogy mennyire elengedhetetlen a civil társadalmi csoportok számára, hogy megértsék az internetes működés kockázatait, és terveket dolgozzanak ki a kapcsolódásra, ha a kapcsolat korlátozott.

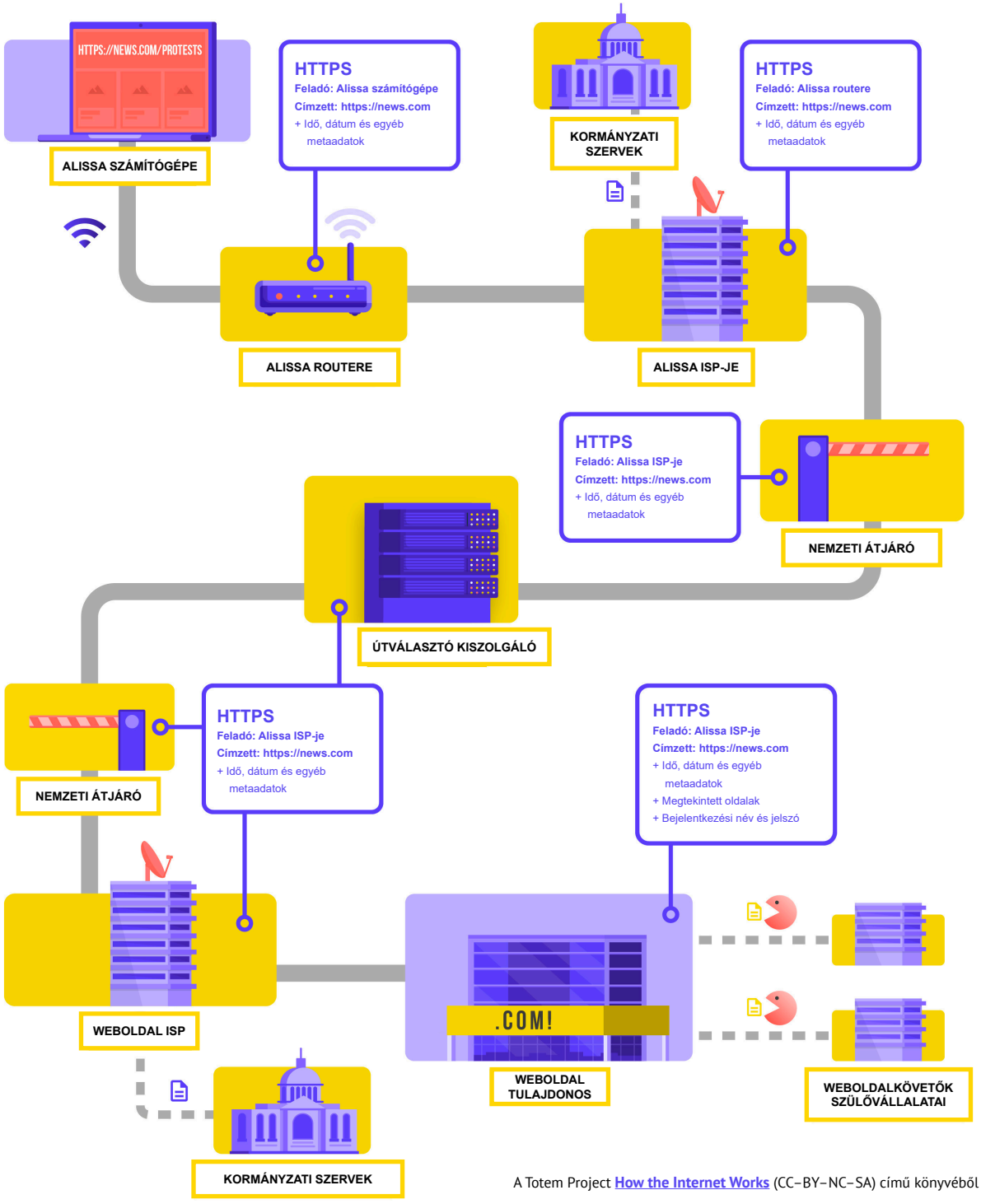
Vegyünk egy valós példát arra, hogyan néz ki a titkosítás nélküli böngészés:



A Totem Project How the Internet Works (CC–BY–NC–SA) című könyvéből adaptálva

Ahogy fentebb is látható, az ellenfél láthatja, hol van Ön, hogy Ön a news.com-ra megy, és megnézi az országában zajló tiltakozásokról szóló oldalt, és láthatja jelszavát, amelyet megosztva bejelentkezik magára az oldalra. Az ilyen rossz kezekben lévő információk nemcsak az Ön fiókját fedik fel, hanem az ellenfelei számára is jó képet adnak arról, hogy Ön mit csinál vagy min gondolkodik.

A HTTPS használata (az „s” jelentése “secure”, vagyis biztonságos) azt jelenti, hogy titkosítás van érvényben. Ez sokkal nagyobb védelmet kínál. Nézzük meg, hogyan néz ki a HTTPS-sel (más néven titkosítással) történő böngészés:



A Totem Project How the Internet Works (CC–BY–NC–SA) című könyvéből adaptálva

Ha a HTTPS be van kapcsolva, a potenciális ellenfél többé nem láthatja jelszavát vagy egyéb érzékeny információkat, amelyeket esetleg megoszt egy weboldalon. Ennek ellenére továbbra is láthatják, hogy milyen domaineket (például news.com) keres fel. És bár a HTTPS titkosítja az Ön által meglátogatott weboldal egyes oldalaira vonatkozó információkat is (például weboldal.com/tiltakozas), a kifinomult ellenfelek továbbra is láthatják ezeket az információkat, ha megvizsgálják az Ön internetes forgalmát. Tehát HTTPS alkalmazása esetén az ellenfél tudhatja, hogy Ön a news.com webhelyre megy, de nem látná a jelszavát, és nehezebb (de nem lehetetlen) lenne látnia, hogy Ön tiltakozásokról (hogy a példánkat használjuk) szóló információkat keres fel. Ez egy fontos különbség. Mindig ellenőrizze, hogy alkalmaz-e HTTPS-t, mielőtt egy weboldalon navigál vagy bizalmas információkat ír be. A **HTTPS Everywhere böngészőbővítményt** is használhatja annak biztosítására, hogy mindig HTTPS-t használjon, vagy ha Ön Firefox felhasználó, kapcsolja be a **Csak HTTPS módot** a böngészőben. Ha a böngésző figyelmeztetést kap arra vonatkozóan, hogy egy weboldal nem biztonságos, ne hagyja figyelmen kívül. Valami nem stimmel. Lehet, hogy a weboldal biztonsági tanúsítványa lejárt –, vagy rosszindulatúan hamisított. Akárhogy is, fontos, hogy figyeljen a figyelmeztetésre, és ne lépjen tovább a wegoldalra. A HTTPS alapvető fontosságú, és a titkosított DNS extra védelmet nyújt a leskelődés és a weboldal blokkolása ellen, de ha szervezete aggódik az online tevékenységeinek célzott felügyelete miatt, és kifinomult online cenzúrával néz szembe (például blokkolják a weboldalakat és alkalmazásokat), érdemes lehet egy megbízható virtuális magánhálózatot (VPN) használni.

Titkosított DNS használata

Ha a fenyegetési környezet miatt meg akarja nehezíteni (de nem ellehetetleníteni) az internetszolgáltató számára, hogy megismerje a felkeresett weboldalak részleteit, használhat titkosított DNS-t.

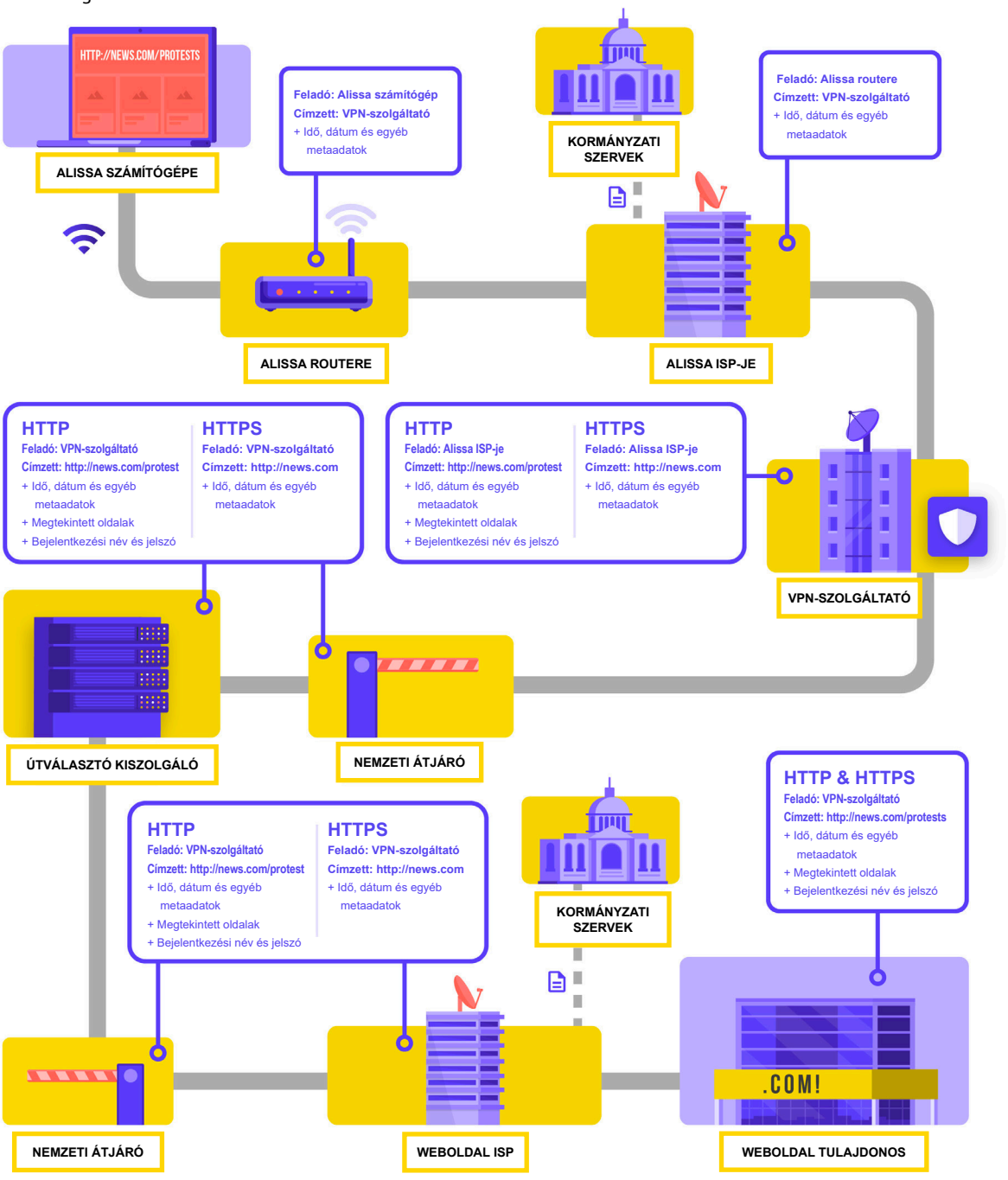
Ha kíváncsi, a DNS a Domain Name System (Tartománynév rendszer) rövidítése. Lényegében az internet telefonkönyve, amely az emberbarát tartományneveket (például az ndi.org) webbarát IP-címekre fordítja. Ez lehetővé teszi az emberek számára, hogy webböngészők segítségével könnyedén keressenek és töltsenek be internetes forrásokat, és felkeressenek weboldalakat. Alapértelmezés szerint azonban a DNS nincs titkosítva.

A titkosított DNS használatához és az internetes forgalom egy kis védelméhez egy egyszerű lehetőség a **Cloudflare 1.1.1.1 alkalmazásának** letöltése és bekapcsolása számítógépén és mobileszközén. Más titkosított DNS-beállítások, köztük a Google 8.8.8.8-as verziója is elérhetők, de a konfiguráláshoz **további technikai lépések** szükségesek. Ha Firefox böngészőt használ, a titkosított DNS most alapértelmezés szerint be van kapcsolva. A Chrome vagy Edge böngészők felhasználói **bekapcsolhatják a titkosított DNS-t** a böngésző speciális biztonsági beállításain keresztül, ha bekapcsolják a „Biztonságos DNS használata" lehetőséget, és kiválasztják az „A következővel: Cloudflare (1.1.1.1)" opciót vagy az általuk választott szolgáltatót.

A Cloudflare 1.1.1.1-es verziója WARP-pal titkosítja a DNS-t és titkosítja a böngészési adatokat – a hagyományos VPN-hez hasonló szolgáltatást nyújtva. Bár a WARP nem védi teljes mértékben az Ön tartózkodási helyét az összes meglátogatott weboldaltól, ez egy könnyen használható funkció, amely segíthet a szervezet munkatársainak kihasználni a titkosított DNS előnyeit és az internetszolgáltatótól származó további védelmet olyan helyzetekben, amikor a teljes VPN vagy nem működőképes, vagy szükséges a fenyegetettség környezetében. A WARP speciális DNS-beállításokkal rendelkező 1.1.1.1-es verziójában a személyzet bekapcsolhatja az 1.1.1.1 for Families verziót is, hogy további védelmet nyújtson a rosszindulatú programok ellen az internet elérése közben.

MI A VPN?

A VPN alapvetően egy alagút, amely megvédi az internetes forgalom megfigyelését és blokkolását a hálózaton lévő hackerek, a hálózati rendszergazda, az internetszolgáltató és bárki ellen, akivel esetleg adatot osztanak meg. Íme egy példa arra, hogyan néz ki a VPN-nel történő böngészés:



A Totem Project How the Internet Works (CC–BY–NC–SA) című könyvéből adaptálva

A VPN-ek részletesebb leírása érdekében ez a szakasz az EFF Surveillance Self Defense Guide című dokumentumára hivatkozik:

A hagyományos VPN-ek célja az Ön tényleges hálózati IP-címének álcázása, és titkosított alagút létrehozása az internetes forgalom számára a számítógépe (vagy telefonja vagy bármely hálózati „okos" eszköze) és a VPN szervere között. Mivel az alagútban lévő forgalom titkosítva van, és a VPN-hez küldi, a harmadik felek, például az internetszolgáltatók vagy a nyilvános Wi-Fi-hálózaton lévő hackerek sokkal nehezebben figyelhetik, módosíthatják vagy blokkolhatják a forgalmat. Miután áthaladt az alagúton Öntől a VPN-hez, a forgalom a VPN-t a végső célállomásra küldi, elfedve az eredeti IP-címét. Ez segít elrejteni a fizikai tartózkodási helyét bárki számára, aki a VPN elhagyása után nézi a forgalmat. Ez nagyobb adatvédelmet és biztonságot kínál, de a VPN használata nem teszi teljesen névtelenné az interneten: forgalmát továbbra is láthatja a VPN üzemeltetője. Az internetszolgáltató is tudni fogja, hogy VPN-t használ, ami növelheti a kockázati profilját.

Ez azt jelenti, hogy **a megbízható VPN-szolgáltató kiválasztása elengedhetetlen**. Egyes helyeken, például Iránban, az ellenséges kormányok valóban létrehozták saját VPN-jüket, hogy nyomon tudják követni, mit csinálnak az állampolgárok. Ahhoz, hogy megtalálja a szervezete és munkatársai számára megfelelő VPN-t, értékelheti a VPN-eket üzleti modelljük és hírnevük, az általuk gyűjtött vagy nem gyűjtött adatok, valamint természetesen magának az eszköznek a biztonsága alapján.

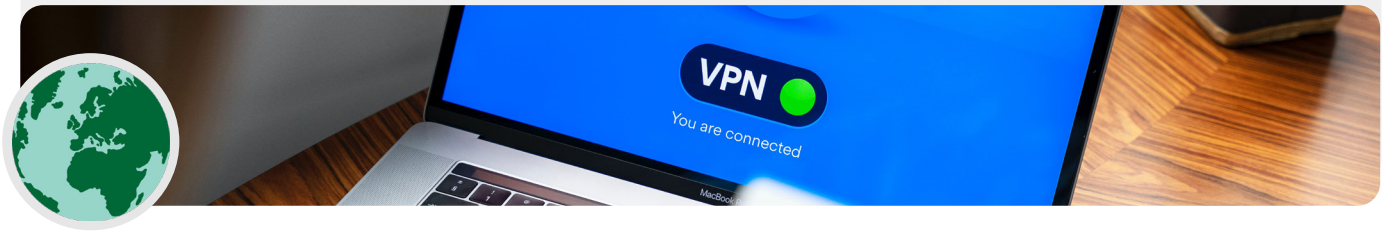
Miért ne használjon ingyenes VPN-t? A rövid válasz az, hogy a legtöbb ingyenes VPN, beleértve azokat is, amelyek egyes okostelefonokra előre telepítve vannak, nagy trükköt rejtenek magukban. Mint minden vállalkozásnak és szolgáltatónak, a VPN-eknek is fenn kell tartaniuk magukat valahogy. Ha a VPN nem adja el a szolgáltatását, hogyan tartja fenn az üzletét? Adományokat kér? Díjat számít fel a prémium szolgáltatásokért? Jótékonysági szervezetek vagy finanszírozók támogatják? Sajnos sok ingyenes VPN úgy keres pénzt, hogy összegyűjti, majd eladja az Ön adatait.

Az a VPN-szolgáltató, amely eleve nem gyűjt adatokat, a legjobb választás. Ha az adatokat nem gyűjtik össze, azokat nem lehet eladni vagy kérésre átadni a kormánynak. Amikor átnézi a VPN-szolgáltató adatvédelmi szabályzatát, ellenőrizze, hogy a VPN valóban gyűjt-e felhasználói adatokat. Ha nem jelzi kifejezetten, hogy a felhasználói kapcsolati adatok nem kerülnek naplózásra, akkor valószínűleg igen. Még ha egy vállalat azt is állítja, hogy nem naplózza a kapcsolati adatokat, ez nem biztos, hogy mindig garancia a helyes magatartásra.

Érdemes rákeresni a VPN mögött álló cégre. Támogatják a független biztonsági szakemberek? A VPN-nek vannak róla hírcikkek? Előfordult már, hogy rajtakapták, hogy félrevezette vagy hazudott az ügyfeleknek? Ha a VPN-t az információbiztonsági közösségben ismert emberek hozták létre, akkor valószínűbb, hogy megbízható. Legyen szkeptikus azokkal a VPN-ekkel kapcsolatban, amelyek olyan szolgáltatást kínálnak, amelyre senki sem akarja rákockáztatni a személyes hírnevét, vagy olyanokat, amelyeket egy olyan cég üzemeltet, amelyről senki sem tud.

Hamis VPN-ek a való világban

2017 végén, az országban megugrott tiltakozást követően, az irániak elkezdték felfedezni a népszerű VPN „ingyenes" (de hamis) változatát, amelyet szöveges üzenetekkel osztanak meg. Az ingyenes VPN (ami valójában nem működött) megígérte, hogy hozzáférést biztosít a Telegramhoz, amelyet akkoriban helyben blokkoltak. Sajnos a hamis alkalmazás nem volt más, mint rosszindulatú program, amely lehetővé tette a hatóságok számára, hogy nyomon kövessék a mozgást, és figyelemmel kísérjék a letöltők kommunikációját.

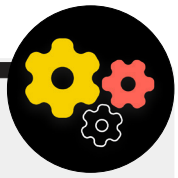


Tehát milyen VPN-t használjunk?

Ha a VPN használata ésszerű a szervezete számára, néhány megbízható lehetőség közé tartozik a TunnelBear és a ProtonVPN. Egy másik lehetőség a saját szerver konfigurálása a Jigsaw Outline segítségével, ahol nem egy cég kezeli a fiókját, de cserébe be kell állítania saját szerverét. Ha a szervezete egy kicsit nagyobb, érdemes fontolóra vennie egy olyan üzleti VPN-t, amely fiókkezelési funkciókat biztosít, például a TunnelBear Teams terméke. A civil társadalom és az emberi jogi területek bizonyos minősített szervezetei számára a TunnelBear jóváírást biztosít VPN-jük ingyenes használatához (amely általában havi 3 dollárba kerül). Ha úgy gondolja, hogy szervezete megfelel a követelményeknek, és felkeltette érdeklődését, további információért forduljon a cyberhandbook@ndi.org címhez.

Bár a legtöbb modern VPN javult a teljesítmény és a sebesség tekintetében, érdemes szem előtt tartani, hogy a VPN használata lelassíthatja a böngészési sebességet, ha nagyon alacsony sávszélességű hálózatot használ, magas késleltetést vagy hálózati késéseket szenved, vagy ha időszakos internetkimaradásokat tapasztal. Ha gyorsabb hálózatot használ, alapértelmezés szerint mindig VPN-t kell használnia.

Ha azt javasolja, hogy a személyzet VPN-t használjon, akkor azt is fontos biztosítani, hogy a VPN bekapcsolva maradjon. Nyilvánvalóan hangzik, de a telepített, de nem futó VPN nem nyújt védelmet.



Anonimitás a Toron keresztül

A VPN-ek mellett valószínűleg hallott már a Torról, mint egy másik eszközről, amellyel biztonságosabbá válik az internet. Fontos megérteni, hogy mi mindkettő, miért használhatja az egyiket vagy a másikat, és mindkettő milyen hatással lehet a szervezetére.

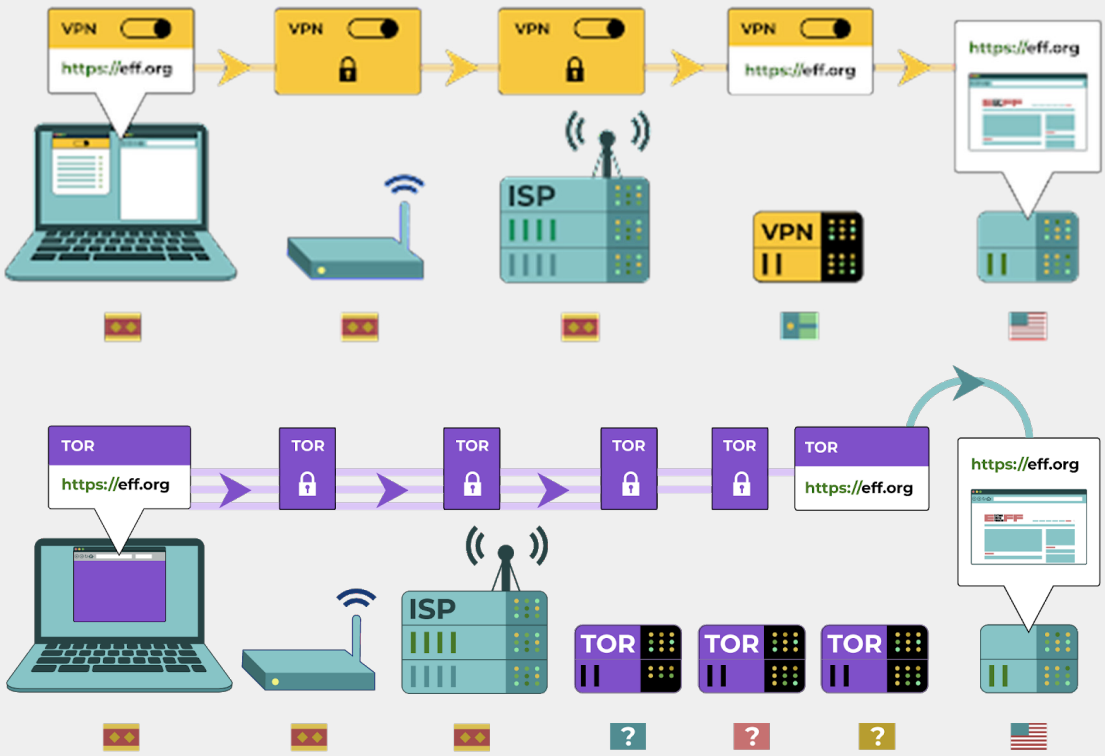
A Tor egy protokoll adatok névtelen továbbítására az interneten keresztül, üzenetek vagy adatok decentralizált hálózaton keresztül történő továbbításával. A Tor működéséről többet tudhat meg itt, de röviden összefoglalva, több ponton keresztül irányítja a forgalmat a célhely felé, így egyetlen pont sem rendelkezik elegendő információval ahhoz, hogy egyszerre felfedje, ki Ön és mit csinál online.

A Tor néhány szempontból különbözik a VPN-től. Alapvetően azért különbözik, mert nem támaszkodik egyetlen konkrét pont (például egy VPN-szolgáltató) bizalmára sem.

Ez az EFF által kifejlesztett grafika bemutatja a különbséget a hagyományos VPN és a Tor között.

A Tor használatának legegyszerűbb módja a Tor webböngésző. Úgy működik, mint bármely normál böngésző, kivéve, hogy a forgalmat a Tor hálózaton keresztül irányítja. Letöltheti a Tor böngészőt Windows, Mac, Linux vagy Android eszközökre. Ne feledje, hogy a Tor Browser használatakor csak azokat az információkat védi, amelyekhez **a böngészőben** hozzáfér. Nem nyújt védelmet más alkalmazásoknak vagy letöltött fájloknak, amelyeket esetleg külön nyithat meg eszközén. Ne feledje továbbá, hogy a Tor nem titkosítja a forgalmat, ezért – hasonlóan a VPN használatához – továbbra is elengedhetetlen a bevált gyakorlatok, például a HTTPS alkalmazása a böngészés során.

Ha ki szeretné terjeszteni a Tor anonimitásvédelmét az egész számítógépére, a technikában jártasabb felhasználók telepíthetik a Tor-t rendszerszintű internetkapcsolatként, vagy fontolóra vehetik a Tails operációs rendszer használatát, amely az összes forgalmat a Toron keresztül irányítja alapértelmezettként. Az Android-felhasználók az Orbot alkalmazást is használhatják a Tor futtatására az eszközükön lévő összes internetes forgalom és alkalmazás számára. Függetlenül attól, hogy hogyan használja a Tor-t, fontos tudnia, hogy használatakor az internetszolgáltató nem láthatja, hogy milyen weboldalakra látogat el, de *látja*, hogy magát a Tor-t használja.



Hasonlóan a VPN használatához, ez jelentősen megnövelheti szervezete kockázati profilját, mivel a Tor nem túl gyakori eszköz, és ezért kitűnik az internetes forgalmat esetleg figyelő ellenfeleknél.

Tehát a szervezete használjon Tor-t? A válasz: attól függ. A legtöbb veszélyeztetett szervezet számára a legegyszerűbb és a legkényelmesebb egy megbízható VPN, amelyet minden munkatárs megfelelően használ, és a globális VPN-használat korában kevésbé valószínű, hogy piros zászlókat mutat. Ha azonban nem engedhet meg magának egy megbízható VPN-t, vagy olyan környezetben működik, ahol a VPN-ek rutinszerűen blokkolva vannak, a Tor jó lehetőség lehet a felügyelet hatásának korlátozására és az online cenzúra elkerülésére.

Van valami oka annak, hogy ne használjunk VPN-t vagy Tor-t?

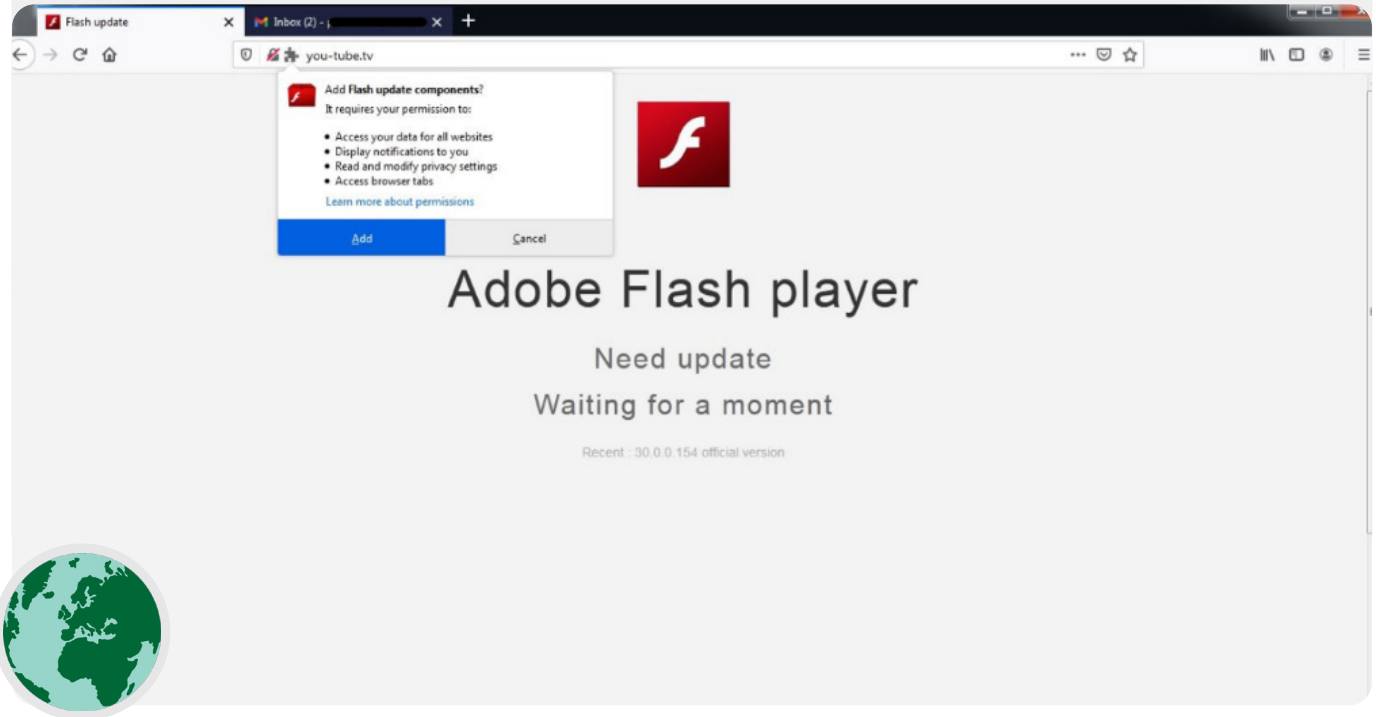
A nem jó hírű VPN-szolgáltatásokkal kapcsolatos aggodalmak mellett a legnagyobb megfontolandó dolog az, hogy a VPN vagy a Tor használata felkeltheti-e a nem kívánt figyelmet, vagy egyes joghatóságokban törvénybe ütközik-e. Bár az internetszolgáltató nem fogja tudni, hogy milyen weboldalakat keres fel, miközben ezeket a szolgáltatásokat használja, láthatják, hogy Tor-hoz vagy VPN-hez csatlakozik. Tehát ha ez illegális ott, ahol az Ön szervezete működik, vagy nagyobb figyelmet vagy kockázatot jelenthet, mint a szabványos HTTPS-sel és titkosított DNS-sel, esetleg VPN-nel vagy különösen Tor-ral (ami sokkal ritkábban használt, és ezért nagyobb a „piros zászló”) egyszerűen navigálni az interneten, akkor ez nem a megfelelő választás az Ön szervezete számára. Azonban, ahogy a VPN-használat egyre gyakoribbá válik, ez kevésbé megkülönböztető tényező. Alapértelmezés szerint a VPN állandó bekapcsolása a legjobb választás, ha legális és lehetséges.

MILYEN BÖNGÉSZŐT KELL HASZNÁLJUK?

Használjon jó hírű böngészőt, például Chrome, Firefox, Brave, Safari, Edge vagy Tor Browser. A Chrome-ot és a Firefoxot is nagyon széles körben használják, és nagyszerű munkát végeznek a biztonság terén. Vannak, akik a Firefoxot részesítik előnyben, tekintettel az adatvédelemre. Akárhogy is, fontos, hogy viszonylag gyakran indítsa újra őket és a számítógépet, hogy a böngésző naprakész legyen. Ha érdekli a böngésző funkcióinak összehasonlítása, nézze meg ezt a forrást a Sajtószabadság Alapítványtól. Böngészőtől függetlenül érdemes olyan bővítményeket vagy kiegészítőket is használni, mint a Privacy Badger, a uBlock Origin vagy a DuckDuckGo Privacy Essentials, amelyek megállítják a hirdetőket, és más, harmadik féltől származó nyomkövetők általi nyomon követést, hogy merre jár és milyen weboldalakat keres fel. Az internet böngészésekor pedig fontolja meg, hogy alapértelmezett internetes kereséseit a Google helyett a DuckDuckGo, Startpage vagy más adatvédelmi keresőmotorra váltsa. Egy ilyen váltás segít korlátozni a hirdetőket és a külső nyomkövetőket is.

Böngészőbiztonság a való világban

A tibeti civil társadalmi aktivistákat 2021 elején célozták meg egy okosan megtervezett, rosszindulatú böngészőbővítménnyel, amely ellopta az e-maileiket és a böngészési adataikat. A „Flash frissítési összetevők” elnevezésű kiegészítőt azoknak a felhasználóknak mutatták be, akik adathalász e-mailekre hivatkozó weboldalakra látogattak el. Az ilyen böngészőbővítmény- vagy kiegészítő támadások ugyanolyan károsak lehetnek, mint az adathalász letöltéseken vagy más szoftvereken keresztül közvetlenül megosztott rosszindulatú programok.



A közösségi média biztonsága

Szervezete sok mindent felfedhet – és néha többet is, mint amennyit szándékozik –, ha közzétesz és kommentál a közösségi médiában.

Legyen szó Facebookról, Twitterről, Instagramról, YouTube-ról vagy régióspecifikus közösségi oldalakról, mint például a VKontakte és az Odnoklassniki, mindig alaposan gondolja át, mit tesz közzé, és megfelelően konfigurálja az esetlegesen elérhető adatvédelmi beállításokat. Ez nem csak a szervezet hivatalos oldalaira igaz, hanem bizonyos esetekben az alkalmazottak személyes fiókjaira, valamint családtagjaik és barátaik fiókjaira is.

A közösségi média biztonsága és a civil társadalom

Még az alacsony kockázatú szervezeteket is megcélozhatják és zaklathatják a közösségi médiában megfelelő biztonsági irányelvek nélkül. Ebben a 2018-as példában egy non-profit állatmenhely több ezer dollárt veszített, és elidegenítette támogatóit, miután egy jogosulatlan fiókadminisztrátor hamis adománygyűjtést indított, és hamis számlák jelentek meg a platformon, amelyekkel alkalmazottaknak adták ki magukat. Ha a hackerek mindent megtesznek azért, hogy néhány ezer dollárt keressenek egy állatmenhelyen, elképzelhető, hogy milyen károkat okozhatnak a kifinomult ellenfelek, ha hozzáférnek a szervezet fiókjaihoz, vagy sikeresen kijátsszák Önt az interneten. A fiókok feltörése mellett számos országban a civil társadalmi csoportok és az egyéni felhasználók is szembesülnek a közösségi médiában közzétett tartalmak következményeivel. Egy 2020-as zambiai példában a rendőrség letartóztatott egy 15 éves diákot, mert állítólag egy Facebook-bejegyzésben rágalmazta az elnököt. Az álnéven posztoló gyermeket a fiók regisztrálásához használt telefonszám és az IP-címe alapján azonosították.

SZERVEZETI SZOCIÁLIS MÉDIAIRÁNYELV KIALAKÍTÁSA

Tételezzük fel, hogy bármi, amit a közösségi médiában közzétesz, köztudomásúvá válhat, és ennek megfelelően alakítsunk ki szervezeti közösségi médiairányelvet. Ennek az irányelvnek meg kell válaszolnia a következő kérdéseket: Ki fér hozzá a közösségi média fiókjaihoz? Ki posztolhat és kinek kell jóváhagynia a bejegyzéseket? Milyen információkat szabad/nem szabad megosztani a közösségi médiában? Ha fotókat, helyadatokat vagy egyéb azonosításra alkalmas információkat tesz közzé munkatársairól, partnereiről vagy egy rendezvény résztvevőiről, kérte-e az engedélyüket, és mérlegelték-e a kockázatokat? Azon túl, hogy kidolgozza a szabályzatot és világossá teszi a személyzet számára, ügyeljen arra, hogy megfelelően konfigurálja az adatvédelmi és biztonsági (gyakran „biztonsággal kapcsolatos") beállításokat. Néhány kulcsfontosságú kérdés, amelyet fel kell tennie magának, amikor eldönti, hogy személyes és szervezeti fiókjaiban mely adatvédelmi és biztonsági beállítások a legmegfelelőbbek:

- Szeretné megosztani bejegyzéseit a nyilvánossággal, vagy csak az emberek egy meghatározott csoportján belül vagy kívül?
- Bárki kommentelhet, válaszolhat vagy interakcióba léphet az üzeneteivel vagy bejegyzéseivel?
- Megtalálhatják az embereknek Önt vagy szervezetét az Ön e-mail címe vagy (privát vagy munkahelyi) telefonszáma alapján?
- Szeretné automatikusan megosztani tartózkodási helyét, amikor közzétesz valamit?
- Szeretné blokkolni vagy elnémítani az ellenséges fiókokat?
- Szeretne bizonyos szavakat vagy hashtageket blokkolni?

Minden közösségi oldalnak más-más adatvédelmi és biztonsági beállításai vannak, de ezek az általános koncepciók általánosan érvényesek. Amikor ezeket a kérdéseket mérlegeli, használja ki a főbb platformok hasznos adatvédelmi útmutatóit: **Facebook**, **Twitter**, **Instagram** és **YouTube**. Különösen a Facebook esetében legyen óvatos a Csoportokkal kapcsolatos adatvédelmi döntései során. A Facebook-csoportok népszerű helyszínek az elköteleződésre, az érdekképviseletre és az információmegosztásra, de a korlátlan csoportokhoz bárki csatlakozhat. Nem ritka, hogy a „hamis" fiókok valódi embereknek adják ki magukat, hogy beszivárogjanak magán közösségi médiacsoportokba vagy oldalakra. Tehát gondosan járjon el a „barát" és „követés" kéréseknél. Ne feledje, hogy szervezete közösségimédia-fiókjai csak annyira biztonságosak, mint a hozzájuk „kapcsolt" fiókok. Ezt különösen fontos megjegyezni a Facebook esetében, ahol a szervezet oldalát esetleg valaki összekapcsolt személyes fiókja kezelheti.

ONLINE ZAKALTÁS

Sajnos sok szervezet szembesül jelentős zaklatással az interneten, különösen a közösségi médiában. Az ilyen zaklatás **gyakran még nagyobb intenzitással a nőkre és a marginalizált lakosságra irányul.** A nők elleni online erőszak különösen ellenséges környezetet teremthet, amely öncenzúrához vagy a politikai vagy polgári diskurzustól való elzárkózáshoz vezethet. Amint azt az NDI Gender, Women and Democracy csapata **Tweets that Chill** jelentésében megállapították, amikor a politikailag aktív nők elleni támadásokat online közvetítik, a közösségi média kiterjedt hatóköre felerősítheti a zaklatás és a pszichológiai bántalmazás hatását, aláásva a nők személyes biztonságérzetét a férfiak által nem tapasztalt módon.

Ahogy szervezete kialakítja közösségi média irányelvét, fontos, hogy tisztában legyen ezzel a dinamikával. Építsen be a biztonsági tervébe strukturált támogatást azoknak a munkatársaknak, akik negatív üzenetekkel, sértésekkel és fenyegetésekkel néznek szembe a közösségi médiában (mind munkájuk részeként, mind magánéletükben). Fejlesszen ki egy zaklatás elleni infrastruktúrát a szervezetén belül, beleértve a személyzetnél végzett felmérést, hogy megértse, milyen hatással van rájuk az online zaklatás, és hozzon létre egy gyors reagálású csapatot, amely segít a személyzetnek a kihívásokkal teli helyzetekben. A PEN America **Online Harassment Field Manual** részletes ajánlásokat is tartalmaz arra vonatkozóan, hogy miként tud segíteni az ilyen zaklatással szembesülő személyzetnek. Ha a munkatársai jól érzik magukat, megfontolhatja, hogy közvetlenül a platformoknak is **jelentse a** zaklatással és/vagy problémás fiókokkal **kapcsolatos incidenseket**.

Fontos, hogy érzékenyek legyünk olyan munkatársakkal, akik online (és a fizikai világban is) zaklatás áldozataivá váltak. Amint azt az Association for Progressive Communications' Women's Rights Program **Take Back the Tech** programja felvázolja, meg kell értenie, hogy az illető esetleg traumával küzd, és ismerje el, hogy az erőszak (online vagy offline) soha nem az áldozat hibája. Gondoskodjon arról, hogy az ilyen kérdéseket bizalmas és biztonságos környezetben, névtelenség lehetőségével fel lehessen vetni és megvitatni (ha az alkalmazottak számára kényelmes). És szerepeljen szervezete biztonsági tervében azoknak a helyi szakembereknek, szervezeteknek és bűnüldöző szerveknek a listája, akikhez jogi, orvosi, mentális egészségügyi és technikai segítségnyújtás céljából kapcsolatba léphet. További ötletekért tekintse meg a Feminist Frequency **online biztonsági útmutatóját**.

Tartsa weboldalait online

Amellett, hogy megvédi az internethez való biztonságos hozzáférést, az is fontos, hogy mindent megtegyen annak érdekében, hogy mások hozzáférhessenek szervezete weboldalaihoz vagy internetes tulajdonságaihoz.

A közösségi oldalak esetében ez azt jelenti, hogy ezeket a fiókokat erős, egyedi jelszavakkal és kéttényezős hitelesítéssel kell védeni. A weboldal számára ez azt jelenti, hogy meg kell védeni a feltörésekkel és a szolgáltatás-megtagadási támadásokkal szemben. Az elosztott szolgáltatás-megtagadási (DDoS) támadások során a számítógépek nagy csoportja egyszerre árasztja el a szervert rosszindulatú forgalommal. Ha Ön civil társadalmi szervezet vagy más non-profit szervezet, akkor valószínűleg jogosult az ingyenes DDoS védelemre – ami sokkal nehezebbé teszi az ellenfél számára, hogy tönkretegye weboldalát – a Cloudflare Project Galileo révén, A Google Project Shield vagy az eQualitie Deflect szolgáltatása által.

Szervezete weboldalának biztonságos üzemeltetése

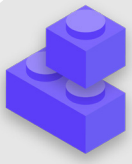
A weboldalakat számítógépek tárolják – és ezek ugyanúgy ki vannak téve a feltörésnek, mint a saját eszközei. Ha lehetséges, a szervezetnek ki kell használnia a meglévő hosting szolgáltatásokat, például a Wordpress.com, a Wix vagy más olyan szolgáltatásokat, amelyek a weboldal teljes biztonságát kezelik Ön helyett. Ha ezt a kézikönyvet olvassa, szervezete valószínűleg jogosult egy Wordpress-weboldal ingyenes biztonságos tárhelyére is az eQualitie által az eQPress Hosting szolgáltatáson keresztül. Ez egy nagyszerű lehetőség a civil szervezetek számára, amelyek már meglévő Wordpress-weboldalakkal rendelkeznek, vagy ha szervezete új weboldalt szeretne felépíteni. Ha saját magának kell tárolnia a weboldalát, akkor ügyeljen arra, hogy az operációs rendszer és a webtárhely-szoftver naprakészen tartsa, akárcsak saját számítógépe esetében. Fontolja meg olyan jól bevált felhőtárhely-szolgáltatók használatát, mint például az Amazon Web Services (AWS), a Microsoft Azure vagy a Greenhost's Eclips.is, amelyek fokozott biztonsági lehetőségeket kínálnak a hosztolt weboldalakhoz. És természetesen függetlenül attól, hogy milyen eszközöket használ weboldala tárolására, győződjön meg arról, hogy a tartalomszerkesztéshez és a konfigurációs beállításokhoz való hozzáféréshez használt fiókok erős jelszavakkal és kétfaktoros hitelesítéssel védettek.

Ha szervezete rendelkezik a saját weboldalának üzemeltetéséhez szükséges műszaki hozzáértéssel, akkor fontolja meg az úgynevezett „statikus weboldal" vagy fix weboldal választását is. A dinamikus weboldalakkal ellentétben az ilyen típusú weboldalak csökkentik a hackerek támadási felületét, és támadásokkal szemben ellenállóbbá teszik a weboldalát.

Védje WiFi hálózatát

Mindezek a lépések a webes forgalom felügyelettől és cenzúrától való védelmére fontosak, de nem helyettesítik az alapvető hálózati biztonságot az irodában (és otthon).

Ne felejtse el az olyan alapokat, mint például az erős jelszó (nem az alapértelmezett jelszó) használata a WiFi útválasztón, annak biztosítása, hogy csak a jogosult felhasználók férhessenek hozzá a hálózathoz a jelszó gyakori megváltoztatásával, valamint a vezeték nélküli útválasztó beépített tűzfalának engedélyezése. Fontolja meg egy vendéghálózat létrehozását az irodájában is, ha az épületben internetet használó látogatók járkálnak ki-be.



Hogyan maradjon biztonságban az interneten

- **Rendszeres képzésben részesítse a személyzetet az alapvető webes biztonsági intézkedések betartásának fontosságáról.**
- **Emlékeztesse a személyzetet, hogy mindig HTTPS-sel és titkosított DNS-sel böngésszenek.**
- **Kérje meg a személyzetet, hogy rendszeresen indítsa újra böngészőjét a frissítések telepítéséhez.**
- **Ösztönözze az adatvédelmi böngészők és bővítmények használatát.**
- **Ha a VPN megfelelő a szervezete körülményei között, válasszon egy jó hírű VPN-t, képezze ki a személyzetet a használatáról, és gondoskodjon a konzisztens használatáról.**
- **Dolgozzon ki és terjesszen egy, a közösségi média használatára vonatkozó egyértelmű szervezeti szabályzatot. o Engedélyezze az adatvédelmi és biztonsági beállításokat az összes közösségimédia-fiókban.**
- **Értse meg az online zaklatás hatásait, és készüljön fel az érintett személyzet támogatására.**
- **Készítsen listát azokról a helyi szakemberekről, szervezetekről és bűnüldöző szervekről, akikkel kapcsolatba léphetnek a munkatársai jogi, mentális egészségügyi és technikai segítségnyújtás céljából az online zaklatás esetén.**
- **Regisztráljon weboldalai DDOS-védelmére.**
- **Használjon jó hírnevű és megbízható webtárhely-szolgáltatót.**
- **Használjon erős jelszót és vendéghálózatot az irodai WiFi-hez.**

A fizikai biztonság védelme

Elengedhetetlen ahhoz, hogy eszközei fizikailag biztonságosak legyenek. A fizikai biztonság azonban túlmutat az eszközökön, és magában kell foglalnia minden másnak a védelmére szolgáló stratégiákat is: például a nyomtatott dokumentumokat, a szervezet irodai vagy munkahelyi tereit, és természetesen Önt, munkatársait és önkénteseit.

Felügyelet, cenzúra és civil társadalom

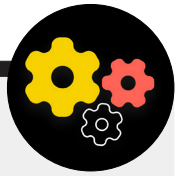
A civil társadalmi szervezetek elleni fizikai támadások sajnos gyakori jelenségek, és gyakran jelentős hatással vannak mind a fizikai, mind az információbiztonságra. Az egyik gyakori taktika, amelyet az ellenfelek a civil szervezetek tevékenységének visszaszorítására alkalmaznak, többek között az irodák portyázására és bezárására irányul – mind a személyzet megfélemlítése, mind pedig bizonyos esetekben az információk és technológiai berendezések ellopása vagy elkobzása. Az ilyen fenyegetések gyakran a demokrácia és a kormányzás terén működő kisebbségi és emberi jogi csoportokat és civil szervezeteket célozzák. Például az LGBT+ Rights Ghana nevű civil szervezet irodáit, amely 2021 elején nyitotta meg az ország első közösségi központját a helyi LMBTQI+ közösség számára, felgyújtással fenyegették, és a rendőrség végül megrohanta és bezárta őket. Az ilyen razziák nemcsak a szervezet fizikai működését érintik, hanem az alkalmazottak biztonságérzetét is károsíthatják.

Fizikai javak védelme

Az információbiztonság lényeges eleme az eszközeinek fizikai biztonsága.

Amellett, hogy a lezárási képernyők és jelszavak használatával, a teljes lemeztitkosítás megvalósításával és a távoli törlési funkciók bekapcsolásával mérsékelheti az ellopott eszközök hatását, azt is meg kell fontolnia, hogyan lehet megakadályozni, hogy ezeket az eszközöket ellopják. A lopás megnehezítése érdekében ügyeljen arra, hogy erős zárakat szereljen fel (és forgassa őket, amikor a személyzet változik) az irodában és/vagy otthon. Fontolja meg laptopszéf vagy zárható szekrény vásárlását is, hogy az eszközöket éjszaka jobban védje.
A biztonsági kamerák sokkal olcsóbbak lettek, az otthoni használatra tervezett egyszerű változatok szélesebb körben elérhetők. Az ilyen kamera- vagy mozgásérzékelő rendszerek az épület körül képesek észlelni és remélhetőleg megakadályozni a fizikai betöréseket és lopásokat. Keressen az Ön országában elérhető, a magánélet tiszteletben tartására irányuló lehetőségeket, és mindenképpen olyan megbízható vállalatok által biztosított kamerákat válasszon, amelyek nem motiválnak adatokat és információkat átadni egy potenciális ellenfélnek.

Ha nagy a betörés vagy az irodai razzia kockázata, tartsa távol a szervezet legérzékenyebb adatait az irodától – akár úgy, hogy biztonságosan tárolja őket a felhőben (ahogyan korábban tárgyaltuk), akár úgy, hogy fizikailag kevésbé célzott helyre helyezi át őket. Ha a régi eszközökön még vannak tárolva adatok, de már nem használja őket, fontolja meg azok törlését – ez az útmutató a WireCuttertől nagyszerű forrást nyújt a legtöbb modern eszközhöz. Ha az eszközök törlése nem lehetséges, akkor azokat fizikailag is megsemmisítheti. Ennek legegyszerűbb, ha nem a leginkább környezetkímélő módja, ha kalapáccsal széttöri az eszközöket és merevlemezeket. Néha még mindig a legrégebbi megoldások működnek a legjobban!
Még e technikai lépések előtt szánjon egy pillanatot a szervezet összes berendeze leltárának az elkészítésére. Ha nincs listája az összes eszközéről, nehezebb nyomon követni, hogy mi hiányozhat, ha valamit ellopnak.



Saját irodai biztonsági rendszer beállítása

Ha egy teljes irodai biztonsági rendszer nem kerül ki a szervezet költségvetéséből, és Ön különösen aggódik az adatvédelem miatt, próbálkozzon egy kreatív lehetőséggel, mint például a Guardian Project Haven App, amely értesítheti Önt az esetleges irodai behatolásról.
A Haven egy okostelefonos alkalmazás, amely bármely Android telefont mozgás-, hang-, rezgés- és fényérzékelővé alakíthat. Az alkalmazást olcsón beállíthatja Android-eszközök az iroda különböző pontjain, hogy értesítsék és rögzítsék a váratlan vendégeket és a nem kívánt behatolókat. A Haven App hasznos lehet egy szállodai szobában vagy apartmanban is, ha fokozott kockázatnak van kitéve. A teljes biztonsági rendszer a legjobb, de ha ez nem elérhető, és szeretne többet megtudni a Haven alkalmazás használatáról, látogasson el a projekt weboldalára.

MIT TEGYÜNK EZZEL A SOK PAPÍRRAL?

Valószínűleg szervezete sok olyan információval rendelkezik, amelyet papírra nyomtatnak, jegyzetfüzetekbe írnak, vagy post-it jegyzetekre firkáltak. Ezek egy része nagyon kényes lehet: a költségvetések kinyomtatása, a résztvevők listája, az adományozók kényes levelei és a magántalálkozókról készült feljegyzések. Elengedhetetlen ezen információk biztonságára is gondolni. Ha feltétlenül meg kell őriznie az érzékeny információk nyomtatott példányát, gondoskodjon arról, hogy azokat biztonságosan, zárt szekrényben vagy más biztonságos helyen tárolja. Ne tartson magánjellegű vagy bizalmas információkat (beleértve a jelszavakat is) az asztalon heverve vagy fehér táblára felírva. Ha úgy gondolja, hogy szervezeténél nagy a betörés vagy razzia kockázata, tartsa a rendkívül érzékeny információkat kevésbé kitett helyen. Amennyire lehetséges, törekedjen a szükségtelen nyomtatott információk ártalmatlanítására. Ne feledje: ha nincs meg, nem lehet ellopni. Állítson be szervezeti szabályzatot a nyomtatott jegyzetek tulajdonjogára vonatkozóan, és ügyeljen arra, hogy minden papíralapú jegyzetet gyűjtsön be az alkalmazottaktól, ha úgy döntenek, hogy elhagyják a szervezetet, vagy elengedik őket a szervezettől (akárcsak egy szervezet által kiadott számítógépet vagy telefont). Az érzékeny papír eltávolításához vásároljon minőségi iratmegsemmisítőt. A hét végi szórakoztató tevékenység lehet egy 15 perces szünet a személyzettel, hogy feldarabolják az előző héten megmaradt, érzékeny dokumentumokat vagy feljegyzéseket.

AZ IRODA IRÁNYELVE

Bár sokak számára az „iroda" valósága jelentősen megváltozott a COVID-19 világjárvány kezdete óta, továbbra is fontos, hogy szervezete világos szabályzatot határozzon meg az irodai hozzáféréssel kapcsolatban. Ennek az irányelvnek a kulcsfontosságú kérdésekkel kell foglalkoznia, beleértve azt, hogy ki léphet be az irodába (és mikor), ki milyen irodai erőforrásokhoz férhet hozzá (például a WiFi hálózathoz), és mit kell tennie a vendégekkel.

Egy egyszerű, de fontos megválaszolandó kérdés, hogy ki kapja meg az irodai kulcsot. Csak megbízható személyzet rendelkezhet kulcsokkal, és a zárakat a személyzet távozásakor és/vagy rendszeres időközönként kell cserélni. A nap folyamán minden záratlanul hagyott ajtónak folyamatosan szem előtt kell lennie valakinek, akiben megbíznak a szervezetben. Gondolja át azt is, hogy a szervezetnek van-e megbízható kapcsolata a bérbeadóval vagy a takarító személyzettel. Gondolja át, milyen információkhoz vagy eszközökhöz férhetnek hozzá ezek az emberek, és gondoskodjon ezek védelméről, különösen akkor, ha Ön nem rendelkezik ezzel a megbízható kapcsolattal. Bárki is fér hozzá, mindig ki kell jelölni egy megbízható személyt, aki bezárja az irodát, és gondoskodik az eszközök megfelelő biztonságáról, mielőtt a nap végén távozna.

Beengedik a vendégeket az irodába? Ha igen, győződjön meg arról, hogy nincs hozzáférésük (vagy legalább felügyelet nélküli hozzáférésük) eszközökhöz vagy érzékeny nyomtatott adatokhoz. Ha követelmény vagy elvárás, hogy a vendégeknek internet-hozzáféréssel kell rendelkezniük, amikor meglátogatják, akkor hozzon létre egy „vendég" hálózatot, hogy az ilyen vendégek ne figyelhessék a rendszeres forgalmát. Általában csak megbízható személyzet férhet hozzá a hálózathoz és a hálózati eszközökhöz, például nyomtatókhoz. Általában célszerű előírni a vendég regisztrációját is, hogy legyen naplója arról, hogy kik jártak Önöknél.

Az irodai szabályzat kidolgozásakor a cél az kell legyen, hogy csak megbízható személyek férhessenek hozzá az érzékeny eszközökhöz, dokumentumokhoz, terekhez és rendszerekhez.

TÁMOGATÓ SZEMÉLYZET ÉS ÖNKÉNTESEK

A szervezetét fenyegető fizikai biztonsági fenyegetések az alkalmazottakra is hatással lehetnek. A közösségi médiában történő zaklatáshoz hasonlóan ezek a fizikai biztonsági fenyegetések gyakran aránytalanul nagy hatással vannak a nőkre és a marginalizált közösségekre. Nem csak a betört ablakokról és az ellopott laptopokról van szó. A megfélemlítés, a fenyegetés vagy a fizikai vagy szexuális erőszak, a családon belüli bántalmazás és a támadástól való félelem súlyos negatív hatással lehet a személyzet életére. Azon szervezetek számára, amelyek különösen politikailag aktív nőkkel dolgoznak vagy támogatnak, az NDI **#Think10** Biztonsági Tervezési Eszköze hasznos forrás azoknak, akik tevékenységük következtében fokozott személyes kockázatnak vannak kitéve.

A munkatársak jóléte nyilvánvalóan fontos érték számukra, mint egyéneknek, de egyben az egészséges és jól működő szervezet alapvető eleme is. Ennek érdekében fontolja meg, hogy milyen további erőforrásokat biztosíthat a személyzetnek a védelem megőrzése érdekében, és fizikai vagy digitális támadások esetén segítse a helyreállítást. Amint azt a Kézikönyvben korábban említettük, ez minimálisan azt jelenti, hogy össze kell állítani egy olyan erőforráslistát, amellyel jogi, orvosi, mentális egészségügyi és technikai segítségnyújtás céljából kapcsolatba léphet a személyzet, ha szükséges. A PEN America **Online Field Harassment Manual** újból ötleteket tartalmaz arra vonatkozóan, hogy a szervezetek hogyan támogathatják a személyzetet válságok alatt és után, a Tactical Tech **Holistic Security Manual** pedig releváns tartalmat nyújt arról, gyakran hogyan reagálnak a szervezetek az intenzív fenyegetés idején.

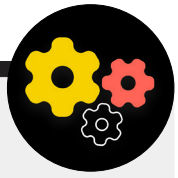
BIZTONSÁG AZ UTAZÁS ALATT

Az utazás – akár egy másik országba, akár a következő városba – gyakran fokozza a fizikai információbiztonsági kockázatokat. Általában nyugodtan feltételezhető, hogy Önnek és eszközeinek nincs adatvédelmi joga a határok átlépésekor. Ezért célszerű olyan szervezeti utazási szabályzatot beépíteni a biztonsági tervébe, amely emlékeztetőket tartalmaz a legfontosabb biztonsági bevált gyakorlatokról. Szervezete utazási szabályzatának tartalmaznia kell sok, a Kézikönyv más részeiben tárgyalt információt, ideértve az internet biztonságos használatát, valamint az eszközök és egyéb információforrások fizikai biztonságban tartását, és magánál tartását utazás közben. Ha lehetséges, hagyja hátra bizalmas adatait, és csak egy frissen törölt számítógépet használjon, a feltétlenül szükséges fájlokat a felhőből érje el, majd törölje azokat, amikor újra hazaér.

Az utazásra való felkészülés és az utazás során megosztott adatok minimalizálása mellett van néhány alapvető üzemeltetési tipp, amelyeket érdemes átgondolni, és belefoglalni a szervezeti utazási szabályzatba.

Fontolja meg olyan utazási célú laptopok vagy telefonok használatát, amelyeken kevés, vagy egyáltalán nincs érzékeny adat. Ha a szervezet munkájának nagy részét a felhőben végzik, akkor egy viszonylag olcsó Chromebook jó választás lehet egy ilyen eszközhöz. Állítsa vissza a gyári beállításokat, vagy „törölje ki" ezeket az eszközöket visszatérésükkor, mielőtt csatlakozna az otthoni vagy irodai általános WiFi hálózatokhoz. Készítse fel a személyzetet arra, hogy mit kell tennie, ha a hatóságok kihallgatják, vagy megállítják őket egy határátkelőn. Fontolja meg, hogyan korlátozhatja az utazó információk mennyiségét, ha ez aggodalomra ad okot, és hozzon létre bejelentkezési protokollokat az érzékeny területekre utazó személyzet számára. Adja meg a személyzetnek elérhetőségi adatait és cselekvési tervet arra vonatkozóan, hogy mit kell tenniük, ha valami baj történik az utazás során. Ez magában foglalja a helyi kórházakkal, klinikákkal vagy gyógyszertárakkal kapcsolatos információkat, amennyiben utazásuk során orvosi segítségre van szükségük.

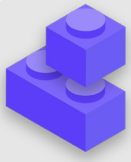
A személyzetnek utazás közben is minden eszközt magánál kell tartania. Például, amikor buszon, vonaton vagy repülőn utazik, tartsa a laptopját a lábánál (ne a felső rekeszben vagy a feladott poggyászban). Ne gondolja, hogy a szállodai szoba – vagy akár a szállodai széf – „biztonságos hely" az érzékeny eszközök és tárgyak tárolására. És ne bízzon a nyilvános USB-töltőportokban. A repülőtereken, állomásokon és járműveken található USB-töltőportok egyre gyakoribb látványt nyújtanak, és nagyon kényelmes módja az eszközök bekapcsolásának. De könnyen használható vektorok lehetnek a rosszindulatú programok felszedésére. Ezért mindenképpen hagyományos módon töltse fel az eszközöket fali csatlakozón keresztül, vagy vásároljon USB-adatblokkolókat, hogy az utazó személyzet USB-n keresztül biztonságosan tölthesse eszközeit.



Foglaljon biztonságos utazást szervezete számára

Az utazási irányelv összeállításakor azt is tartsa szem előtt, hogy milyen információk jelenhetnek meg az utazás megszervezése vagy lefoglalása során. Ez különösen fontos lehet, ha nagy eseményeket, képzéseket vagy konferenciákat szervez, amelyekhez különféle alkalmazottaktól, partnerektől vagy résztvevőktől származó érzékeny információkat kezel.

Gondosan gondolja át, hogyan osztja meg és tárolja (ha szükséges) biztonságosan a személyes adatokat, például útlevéladatokat, utazási útvonalakat és egészségügyi feljegyzéseket. A Tactical Tech Organizer Activity Book című könyvében található egy nagyszerű munkalap, amely segít a szervezetnek átgondolni az utazási biztonsággal kapcsolatos kulcsfontosságú kérdéseket - itt található hivatkozás.



Fizikai biztonságának védelme

- **Emlékeztesse a személyzetet, hogy az eszközöket mindig fizikailag védjék.**
- **Ellenőrizze és biztosítsa az összes módot, ahogyan az emberek bejuthatnak a terébe – ajtókat és ablakokat.**
- **Dolgozzon ki egy irodai vendég- és hozzáférési szabályzatot.**
- **Használjon erős zárakat, és szükség esetén forgassa/cserélje ki őket.**
- **Fontolja meg kamera vagy más irodai biztonsági rendszer beállítását.**
- **Vegyen iratsemmisítőt és használja azt.**
  - Határozzon meg időt a személyzetnek az érzékeny információkat tartalmazó nyomtatott dokumentumok megsemmisítésére.
- **Készítsen listát azokról a helyi szakemberekről, szervezetekről és bűnüldöző szervekről, akiknél kapcsolatba léphet a személyzettel jogi, orvosi és mentális egészségügyi segítségnyújtás céljából fizikai támadásokra vagy fenyegetésekre adott válaszként.**
- **Dolgozzon ki szervezeti utazási szabályzatot.**
- **Győződjön meg arról, hogy a személyzet tudja, mit kell tennie vészhelyzet esetén az utazás során, beleértve a személyzet felkészítését arra, hogy mit kell tennie, ha megállítják a határon vagy az ellenőrző ponton.**
- **Minden helyi, országos vagy nemzetközi utazás előtt emlékeztesse a személyzetet, hogy korlátozza az eszközökön tárolt információkat.**
- **Utazások vagy események szervezésekor ügyeljen a létrehozott és megosztott további adatokra.**

Mi a teendő, ha a dolgok rosszul mennek

Tehát tudja, mit kell tennie. Bevezette az irányelveket, és a szervezetben mindenkit kioktatott a legjobb gyakorlatokra. Még ennyi kemény munka mellett is nagyon valószínű, hogy valami végül elromlik.

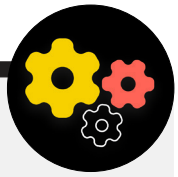
Történnek dolgok. Ha ez megtörténik, elengedhetetlen, hogy rendelkezzen egy incidens-elhárítási tervvel. Az incidensre adott válasz kulcsfontosságú, és gyakran alulértékelt része a szervezet biztonsági tervének, mert ez lehet a különbség aközött, hogy egy támadás tönkreteszi a szervezet hírnevét, vagy egy kellemetlen zökkenő az úton. Ne feledje, hogy csak akkor tud reagálni egy eseményre, ha tud róla. Nagyon fontos az erős szervezeti biztonsági kultúra megléte és a személyzet ösztönzése a problémák bejelentésére. Ez az oka annak, hogy jobb a jó biztonsági magatartást jutalmazni, mint a biztonsági hibák vagy hibák büntetését. Szintén fontos az empátia kifejezése és a személyzet jóllétének ellenőrzése, amikor incidenst jelentenek. Azt szeretné, ha az alkalmazottak azonnal jelentenék az adathalász üzenetben szereplő kattintott hivatkozást, egy ellopott telefont vagy egy feltört közösségimédia-fiókot – ne féljen a megtorlástól vagy a támogatás hiányától. Végtére is, az incidensekre való reagálás, csakúgy, mint a Kézikönyv más részeiben említett mérséklési stratégiák, az egész szervezetre kiterjedő erőfeszítés.

- Szóval mire kell terveznie? Röviden, bármire, ami némileg valószínűsíthető. Ez minden szervezetnél másként fog kinézni, de a gyakori kérdések, amelyeket az incidensre adott választerv segít megválaszolni, a következők:
- Mit tegyünk, ha fiókjainkat vagy weboldalainkat feltörik?
- Mit tegyünk, ha valaki egy adathalász e-mailre kattint, vagy ha egy eszköz gyanúsan működik?
- Mit tegyünk, ha e-mailjeinket vagy legérzékenyebb dokumentumainkat ellopják és kiszivárogtatják?
- Mit tegyünk, ha egyik alkalmazottunkat fizikai veszélybe sodorják vagy letartóztatják? Vagy ha stresszesek és szorongással küzdenek az ilyen fenyegetések miatt?
- Mit tegyünk, ha tűz, árvíz vagy természeti katasztrófa következtében megsérül az irodánk?
- Mit tegyünk, ha egy alkalmazott számítógépe vagy telefonja elveszett vagy ellopták?

Az ezekre és a többi kérdésre adott válaszok szervezetenként eltérőek, de fontos, hogy ezeket együtt gondoljuk végig, és világosan megfogalmazzuk és megosszuk a tervet, hogy szervezetében mindenki készen álljon azonnali lépésekre a károk korlátozása érdekében.

A Tactical Tech Holistic Security Guide című dokumentumából kölcsönözve jó kiindulópont az incidensreagálási terv elkészítéséhez, ha meghatároz egy eseményt vagy vészhelyzetet a szervezet kontextusában. Döntse el, hogy mi a „vészhelyzet” – vagyis az a pont, ahol el kell kezdenünk a tervezett cselekvések és vészhelyzeti intézkedések végrehajtását. Ez azért fontos, mert néha nem egyértelmű – ha elképzel egy olyan forgatókönyvet, mint a kapcsolat elvesztése egy helyszíni küldetésben lévő kollégájával; meddig várna a vészhelyzet kihirdetésével? Nem akarunk túl korán ugrani, de a túl hosszú várakozás bizonyos körülmények között katasztrofális lehet. Szintén fontos végiggondolni a **műveletek** lépéseit. Rendeljen hozzá minden személyhez egy világos szerepet, amellyel tisztában van, és amelyben előzetesen megállapodott – ez csökkenti a szervezetlenséget és a pánikot egy incidens esetén. Minden egyes fenyegetés esetén vegye figyelembe a különböző szerepeket, amelyeket esetleg fel kell töltenie, és a vészhelyzetre való reagálás gyakorlati szempontjait. Ezen a vészhelyzetekre vonatkozó fontos stratégián belül egy támogató hálózat aktiválása szerepel – a szövetségesek széles hálózata, amely magában foglalhat barátokat és családot, közösséget, helyi szövetségeseket, kormányzati forrásokat és nemzeti vagy nemzetközi szövetségeseket, például civil szervezeteket és újságírókat. Hogyan támogathatják a szövetségesei? Előzetesen fel kell vennie velük a kapcsolatot, hogy megbizonyosodjon arról, hogy készek lesznek-e segíteni vészhelyzetben, és tudassa velük, mit vár el tőlük.

Egy eseményre való reagálás során a hatékony **kommunikáció** egyre fontosabbá válik. Döntse el, hogy az egyes szereplőkkel való kommunikációnak melyik a legbiztonságosabb és leghatékonyabb módja a különböző forgatókönyvekben, és határozzon meg egy tartalék eszközt is. Legyen tudatában annak, hogy vészhelyzet esetén hasznos lehet egyértelmű iránymutatás arra vonatkozóan, hogy mit (és mit ne) kommunikáljunk, mikor kommunikáljunk, milyen csatornákat használjunk a kommunikációhoz, és kivel kommunikáljunk. Vegye figyelembe azt is, hogy egy incidens milyen hatással van a szervezetére gyakorolt hírnévre, és készüljön fel a megfelelő reagálásra. Győződjön meg arról, hogy a szervezet kommunikációs vezetője (egyes szervezetekben csak az lehet, aki a Facebook-oldalt vagy a Twitter-fiókot kezeli) tisztában van az incidenssel, és figyelheti a közösségi médiát vagy más médiát a lehetséges hatások miatt. Fel kell készülnie arra is, hogy adott esetben nyilvános vagy médiaérdeklődést intézhetnek egy incidenssel kapcsolatban. Ez különösen fontos az esetleges negatív történetek vagy a hírnévkárosodás megelőzéséhez. Bár minden incidens és kontextus más és más, az őszinte és átlátható kommunikáció gyakran segít a bizalom kiépítésében az incidensek következményeivel kapcsolatban.



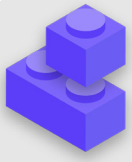
Korai riasztási és reagálási rendszer létrehozása

Fontolja meg egy korai riasztási és reagálási rendszer létrehozását. Egy ilyen rendszer furcsán hangzik, de lényegében csak egy központi (elektronikus vagy egyéb) dokumentum, amelyet vészhelyzet esetén megnyitnak. A dokumentumban rögzítenie kell minden részletet a biztonsági mutatókról és a bekövetkezett incidensekről egy idővonalon, világosan le kell írnia a tervezett válaszlépéseket és azok sorrendjét, és jeleznie kell, mit kell elérni annak jelzéséhez, hogy a fennálló kockázat ismét csökkent. Tartalmaznia kell az incidens után végrehajtandó intézkedéseket is, hogy megvédje az érintetteket a további sérülésektől, és segítse őket a fizikai és érzelmi felépülésükben. A korai riasztási és reagálási rendszer hasznos dokumentációt nyújthat a bűnüldöző szervekkel való megosztáshoz (ha van), a történtek későbbi elemzéséhez, valamint útmutatást nyújthat a megelőzési taktikák és a fenyegetésekre adott válaszok javításához a jövőben.

Ezeken a fontos incidensreakciókon kívül szervezetének minden konkrét technikai válaszra is fel kell készülnie. Egyes esetekben a technikai választ belső informatikai személyzet vagy rendszergazdák kezelhetik. Ha például úgy tűnik, hogy egy e-mail fiókot feltörtek, a fiókrendszergazdának fel kell készülnie, és képesnek kell lennie az érintett fiók leállítására vagy letiltására. Egyes technikai események azonban olyan szakértelmet igényelhetnek, amellyel a szervezeten belül nem rendelkeznek. Az ehhez hasonló helyzetekben fontos, hogy azonosítsa a külső műszaki szakértők megbízható listáját, akik segíthetnek az incidensek megoldásában. Egyes esetekben érdemes előzetesen megtárgyalni a feltételeket a szolgáltatókkal (például a webhelygazda vagy egy informatikai tanácsadó) annak biztosítása érdekében, hogy elérhetőek legyenek (és ne számítsanak fel külön díjat) az ilyen technikai incidensek kezelésére.

Végül, de nem utolsósorban érdemes megfontolni a jogi lépéseket. Fontos megérteni az esetleges jogi védelemeket, valamint azokat a jogi kötelezettségeket vagy következményeket, amelyekkel a szervezetnek szembe kell néznie egy adatvédelmi incidens vagy más biztonsági incidens következtében. Az első lépés az lehet, hogy olyan megbízható jogi tanácsadót keresünk, aki ismeri az Ön országa vagy települése sajátos törvényeit és előírásait. Szánjon egy kis időt a lehetséges incidensek áttekintésére ezzel a személlyel, és készítsen egy tervet arra vonatkozóan, hogy mit tenne válaszul. Célszerű megállapodni ezzel a megbízható tanácsadóval, aki szükség esetén egy incidens után is képviseli Önt és érdekeit. A jogi előkészítés részeként győződjön meg arról, hogy megértette a szállítók vagy partnerek jogi kötelezettségeit. Saját adatvédelmi incidens esetén kötelesek értesíteni Önt? Milyen támogatásra van szükségük (ha van ilyen) incidens esetén? A külső szállítókkal kötött szerződések és megállapodások kidolgozása során tartsa szem előtt az adatszivárgás vagy egyéb incidens lehetőségét.

Noha az incidensek megoldására nincs mindenkire érvényes megközelítés, elengedhetetlen a világos működési, kommunikációs, műszaki és jogi tervek megalkotása. Az incidensreagálási terv összeállítása során határozottan javasoljuk, hogy használjon néhány kiváló meglévő erőforrást, amelyek célja, hogy segítsék a civil társadalmi szervezeteket és más magas kockázatú csoportokat az incidensek válaszadásában. Ezek a források közé tartozik a RaReNet és a CiviCERT által kifejlesztett Digital First Aid Kit, a PEN America Online Harassment Field Manual, a Belfer Center Cybersecurity Campaign Playbook és a Cyber Incident Communications Plan Template, és elérheti a Now digitális biztonsági segélyvonalát is.



Incidensre adott válasz

- **Dolgozzon ki egy szervezeti incidenselhárítási tervet, és gyakorolja azt.**
  - Gondolja át a lehetséges eseményeket, és készüljön fel a válaszra, mielőtt az megtörténik.
- **Győződjön meg arról, hogy a szervezetben mindenki tisztában van azzal, hogyan fog kommunikálni, és milyen technikai lépéseket kell tenni egy incidens esetén.**
- **Szánjon időt arra, hogy megértse a jogi védelmét és kötelezettségeit.**
- **Legyen készen arra, hogy a szervezeti személyzet számára megfelelő érzelmi és szociális támogatást nyújtson egy esemény után.**

„A” függelék: Ajánlott források

- Tactical Tech Holistic Security Manual ; Creative Commons Attribution-ShareAlike 4.0 nemzetközi licenc
  - 2.4 fejezet – Információink megértése és katalogizálása
  - 1.5 fejezet – Kommunikáció a fenyegetésekről csapatokban és szervezetekben
  - 3.4 fejezet – Biztonság csoportokban és szervezetekben
- Az Electronic Frontier Foundation Security Education Companion ; Creative Commons Attribution 3.0 amerikai licenc
  - Fenyegetés-modellezési tevékenység tájékoztatója
- A Sajtószabadság Alapítvány adathalászat-megelőzési és e-mail-higiéniai útmutatója; Creative Commons Attribution 4.0 nemzetközi licenc
- A Sajtószabadság Alapítvány Lezárási jelzési útmutatója ; Creative Commons Attribution 4.0 nemzetközi licenc
- Az Electronic Frontier Foundation Surveillance Self Defense (SSD) útmutatója ; Creative Commons Attribution 3.0 amerikai licenc
  - Mit kell tudnom a titkosításról
  - Másokkal való kommunikáció
  - Az Ön számára megfelelő VPN kiválasztása
- A Frontline Defenders útmutatója a biztonságos csoportos csevegési és konferenciaeszközökhöz
- A Tactical Tech Data Detox készlete
  - Engedje be a megfelelőt: Erősítse meg jelszavait
  - Erősítse meg a képernyőzárakat
- A Center for Democracy and Technology választási biztonsági útmutatója a jelszavakról; Creative Commons Attribution 4.0 nemzetközi licenc
- A Center for Democracy and Technology választási biztonsági útmutatója a kéttényezős hitelesítésről; Creative Commons Attribution 4.0 nemzetközi licenc
- Martin Shelton kétfaktoros hitelesítése kezdőknek; Creative Commons Attribution 4.0 nemzetközi licenc
- Tactical Tech és Frontline Defender Security in a Box ; Creative Commons Attribution-ShareAlike 3.0 nem portolt licenc
  - Védje eszközét a rosszindulatú programoktól és az adathalász támadásoktól
  - Védje meg adatait a fizikai fenyegetésektől
- SANS Ouch! Hírlevél: Állítsa le a rosszindulatú programokat
- Az Apple eszköz- és adathozzáférése, ha a személyes biztonság veszélyben van
- Global Cyber Alliance Kiberhigiénia küldetésalapú szervezetek számára

B függelék: Biztonsági terv kezdőkészlet

A következő kezdőcsomag segítségével jegyzeteket készíthet, miközben Ön és szervezete elolvassa a Kézikönyvet és megemészti az anyagot, és fontolja meg a kapcsolódó kérdéseket kollégáival, hogy segítse a termékeny vitát.

Ügyeljen arra, hogy a Kézikönyv egyes részeiben hivatkozzon a kulcsfontosságú „építőelemekre", hogy biztosítsa, hogy a biztonsági terv elkészítése során lefedje a fontos témákat. A Kézikönyv végére az építőelemek, az ezekre a vitakérdésekre adott válaszok és az Ön jegyzetei képezhetik egy sikeres biztonsági terv alapját!

Biztonsági kultúra építése

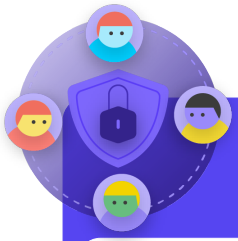
Erős alapok: Fiókok és eszközök védelme

Adatok biztonságos kommunikációja és tárolása

Hogyan maradjon biztonságban az interneten

A fizikai biztonság védelme

Mi a teendő, ha a dolgok rosszul mennek



Biztonsági kultúra építése

MEGFONTOLHATÓ KÉRDÉSEK:

- Mikor ütemezhet be egy beszélgetést a biztonsági terv áttekintésére az egész szervezettel?
- Mely napokon vagy időpontokban jó a szervezet számára a rendszeres biztonsággal kapcsolatos beszélgetések és képzések ütemezése?
- Milyen lépéseket tehet a vezetés a jó biztonsági magatartás és a biztonsági terv iránti elkötelezettség modellezésére? Hogyan játszhatnak szerepet mások a szervezetben a biztonságban?

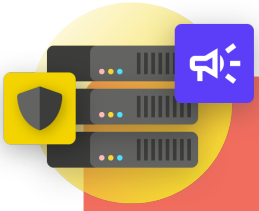
MEGJEGYZÉSEI ÉS ÖTLETEI:

Erős alapok: Fiókok és eszközök védelme

MEGFONTOLHATÓ KÉRDÉSEK:

- Hogyan valósítja meg a fiókbiztonsági intézkedéseket – például a jelszókezelőt és a 2FA-t – az egész szervezetben? Milyen akadályokba ütközhet a megvalósítás során?
- Hogyan biztosítja a szervezete az eszközök biztonságát és frissítését? Ennek részeként a szervezetnek szüksége lesz egy tervre a licenc nélküli szoftverek vagy számítógépek kezelésére?
- Mikor van itt az ideje, hogy képzést szervezzen minden alkalmazott számára az adathalászat, a rosszindulatú programok és az eszközbiztonság bevált gyakorlatairól?

MEGJEGYZÉSEI ÉS ÖTLETEI:



Adatok biztonságos kommunikációja és tárolása

MEGFONTOLHATÓ KÉRDÉSEK:

- Hogyan valósítja meg szervezete a végpontok közötti titkosított üzenetküldést a biztonságos kommunikáció érdekében? Milyen akadályokba ütközhet a megvalósítás során?
- Hogyan fogja a szervezete érvényesíteni a biztonságos fájlmegosztási megoldást a szervezeten belül és kívül egyaránt? Milyen akadályokba ütközhet a megvalósítás során?
- Hogyan valósítja meg szervezete a biztonságos adattárolási és biztonsági mentési megoldást? Milyen akadályokba ütközhet a megvalósítás során?

MEGJEGYZÉSEI ÉS ÖTLETEI:

Hogyan maradjon biztonságban az interneten

MEGFONTOLHATÓ KÉRDÉSEK:

- Hogyan valósítja meg szervezete a biztonságos böngészés követelményeit, például a HTTPS-t, a megbízható böngészőt és adott esetben a VPN-t a személyzet számára?
- Melyek lesznek szervezete közösségimédia-irányelvének kulcselemei? Hogyan lesz érvényesítve?
- Hogyan fogja szervezete megvédeni weboldalait és internetes tulajdonát?

MEGJEGYZÉSEI ÉS ÖTLETEI:

A fizikai biztonság védelme

MEGFONTOLHATÓ KÉRDÉSEK:

- Hogyan fogja a szervezet terjeszteni és érvényesíteni az irodai vendég- és hozzáférési szabályzatát?
- Ki a felelős a személyzet felkészítéséért azokra a fizikai és digitális biztonsági kihívásokra, amelyekkel munkahelyi utazásuk során szembesülhetnek?
- Milyen lépéseket tehetnek a munkatársak, hogy az irodában és utazás közben is biztonságban tartsák eszközeiket?

MEGJEGYZÉSEI ÉS ÖTLETEI:

Mi a teendő, ha a dolgok rosszul mennek

MEGFONTOLHATÓ KÉRDÉSEK:

- Hogyan fogja a szervezet terjeszteni és gyakorolni az incidensreagálási irányelvé?
- Rendelkezésre állnak-e erőforrások azon alkalmazottak számára, akiknek szükségük lehet érzelmi és szociális támogatásra egy incidens után? Ha nem, hogyan tudná a szervezet biztosítani ezeket az erőforrásokat incidens esetén?

MEGJEGYZÉSEI ÉS ÖTLETEI:

NDI
NATIONAL
DEMOCRATIC
INSTITUTE