NDI
NATIONAL DEMOCRATIC INSTITUTE

Îndrumar de securitate cibernetică

pentru

organizațiile societății civile

Un ghid pentru organizațiile societății civile care își doresc să inițieze un plan de securitate cibernetică

NDI
NATIONAL DEMOCRATIC INSTITUTE

Îndrumar de securitate cibernetică

pentru

organizațiile societății civile

Un ghid pentru organizațiile societății civile care își doresc să inițieze un plan de securitate cibernetică

Cuprins

Legendă vizuală

În acest îndreptar veți găsi câteva elemente recurente evidențiate, pe lângă textul principal. Iată o scurtă „legendă” care vă va ajuta să înțelegeți elementele esențiale:

Studiu de caz

Indică studii de caz care evidențiază impactul real al unui anumit subiect asupra organizațiilor societății civile la nivel global sau într-o anumită țară.

Sfaturi suplimentare

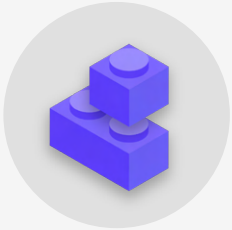
Evidențiază sfaturi și informații suplimentare cărora să le dați atenție în timp ce citiți îndrumarul.

În realitate

Atrage atenția asupra unor exemple comune de instrumente tactice de securitate cibernetică folosite „în realitate”, atât în scopuri rău intenționate, cât și în scopuri bine intenționate.

Nivel avansat

Indică un subiect avansat - informații care sunt importante pentru organizații, dar care ar putea fi prea tehnice sau complicate.



Blocurile componente ale planului de securitate

Indică „blocurile componente ale planului de securitate”, care reprezintă factorii cheie ai fiecărei secțiuni a îndrumarului.

1

Construirea unei culturi a securității

2

O fundație solidă: Securizarea conturilor și dispozitivelor

3

Comunicarea și stocarea securizată a datelor

4

Siguranța pe internet

5

Protejarea securității fizice

6

Ce trebuie să facem când lucrurile merg prost

Primele 10 elemente

Aceste zece elemente sunt de importanță critică pentru planul de securitate al organizației dvs. Dacă nu știți de unde să începeți, începeți cu asta.

1. **Organizați sesiuni regulate de instruire la nivel de organizație**
2. **Fiți atenți la phishing și implementați un sistem de raportare.**
3. **Folosiți o metodă de criptare pentru toate comunicările - de la un capăt la altul, dacă este posibil**
4. **Impuneți obligativitatea de parole puternice și implementați un manager de parole la nivelul organizației**
5. **Impuneți obligativitatea autentificării în doi factori oricând este posibil**
6. **Asigurați-vă că toate dispozitivele și software-urile personalului sunt actualizate**
7. **Folosiți un mediu de stocare în cloud**
8. **Utilizați HTTPS și, dacă este cazul, un VPN, pentru accesarea internetului**
9. **Protejați activele fizice ale organizației dvs.**
10. **Dezvoltați un plan de răspuns la incidente la nivelul organizației**

Autori și mulțumiri

Autor principal: **Evan Summers (NDI)**
Autorii contributori: **Sarah Moulton (NDI); Chris Doten (NDI)**

Pentru dezvoltarea îndrumarului de față, dorim să le mulțumim revizorilor experți externi care ne-au oferit feedback, editări și sugestii valoroase pe durata conceperii acestui conținut, printre care îi amintim pe:

Fiona Krakenburger, Open Technology Fund; Bill Budington și 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; și Whitney Pfeifer, NDI.

Dorim, de asemenea, să aducem mulțumiri tuturor manualelor, ghidurilor, îndreptarelor, modulelor de instruire incredibile și altor materiale dezvoltate și întreținute de comunitatea OrgSec pentru securitate organizațională. Acest îndrumar are rolul de a suplimenta aceste materiale mai aprofundate, combinând lecții cheie într-o singură resursă ușor de lecturat pentru organizațiile societății civile care își doresc să inițieze un plan de securitate cibernetică.

Pe lângă inspirarea indirectă din multe resurse extraordinare redactate de comunitate, în îndrumarul de față am copiat direct texte utile din mai multe resurse existente, în special din Ghidul de autoapărare pentru supraveghere al Electronic Frontier Foundation, Manualul securității holistice al Tactical Tech și o gamă de texte explicative preluate de la Center for Democracy and Technology și Freedom of the Press Foundation. Vei găsi citate specifice din aceste resurse în secțiunile de mai jos, precum și linkuri complete, autori și informații de licențiere în Anexa A.

De asemenea, recomandăm tuturor cititorilor acestui îndrumar să facă uz de biblioteca extinsă de ghiduri și resurse de securitate cibernetică compilată și actualizată de Open Technology Fund.

Cine suntem?

National Democratic Institute for International Affairs (NDI) este o organizație non-profit nepartizană cu sediul în Washington D.C., care activează în parteneriat, în întreaga lume, pentru a întări și proteja instituțiile, procesele, normele și valorile democratice în vederea asigurării unei calități mai bune a vieții tuturor.

NDI consideră că toți oamenii au dreptul să trăiască într-o lume care le respectă demnitatea, securitatea, drepturile politice - și că lumea digitală nu face excepție.

Echipa pentru democrație și tehnologie din cadrul NDI încearcă să promoveze un ecosistem digital global în care valorile democratice sunt protejate, promovate și se pot dezvolta; guvernele sunt mai transparente și mai incluzive; și toți cetățenii sunt împuterniciți să-și tragă guvernul la răspundere. Facem acest lucru prin sprijinirea unei rețele globale de activiști dedicați rezilienței digitale și prin colaborarea cu parteneri care dezvoltă instrumente și resurse precum acest îndrumar. Puteți afla mai multe informații despre activitatea noastră de pe site-ul nostru web, urmărindu-ne pe Twitter sau contactându-ne direct la cyberhandbook@ndi.org. Vă stăm în permanență la dispoziție pentru a vă răspunde la întrebări despre echipa noastră și activitatea noastră în securitate cibernetică, tehnologie și democrație.

La ce servește acest îndrumar?

Îndrumarul de față a fost conceput cu un scop simplu: să ajute partidul dvs. politic să dezvolte un plan de securitate cibernetică ușor de înțeles și de implementat.

În contextul unei lumi care trece tot mai mult online, securitatea cibernetică nu mai este doar un cuvânt tehnic, ci a devenit un concept de o importanță critică pentru succesul unei organizații și siguranța unei echipe. În special în cazul organizațiilor societății civile din spațiul democrației, propagandei, responsabilității și drepturilor omului, securitatea informațiilor (atât online, cât și offline) este o provocare care necesită atenție, investiții și vigilență.

Este foarte probabil ca organizația dvs. – dacă nu a fost până acum – să fie, pe viitor, ținta unui atac cibernetic. Nu ne dorim să provocăm panică; acest lucru se întâmplă chiar și organizațiilor care nu se consideră neapărat ținte.

În cursul unui an, Center for Strategic and International Studies, care publică o **listă curentă** a așa-numitelor „incidente semnificative de securitate cibernetică", cataloghează sute de atacuri cibernetice grave, multe dintre acestea vizând poate chiar sute de organizații în același timp. Pe lângă aceste atacuri raportate, în fiecare an există, probabil, sute de alte atacuri de mică amploare care nu sunt detectate sau raportate, multe vizând organizațiile societății civile care activează în sprijinul democrației, responsabilității și drepturilor omului. Organizațiile care reprezintă femeile sau alte grupuri marginalizate sunt adesea țintele acestor atacuri.

Atacurile cibernetice de acest gen au consecințe semnificative. Fie că au ca scop furtul de bani, înăbușirea exprimării opiniilor, perturbarea operațiunilor organizației, distrugerea reputației dvs. sau chiar furtul de informații care ar putea provoca daune psihologice sau fizice asupra membrilor sau personalului, asemenea amenințări trebuie luate în serios. Partea bună este că nu este nevoie să deveniți programatori sau tehnicieni de înaltă calificare pentru a vă apăra pe dvs. și organizația dvs. de amenințările comune. Cu toate acestea, trebuie să fiți pregătiți să investiți efort, energie și timp pentru dezvoltarea și implementarea unui plan solid de securitate la nivelul organizației. Dacă nu v-ați gândit niciodată la securitatea cibernetică pentru organizația dvs., nu ați avut timp să vă concentrați pe asta, sau dacă aveți niște cunoștințe de bază despre acest subiect, dar considerați că organizația dvs. și-ar putea îmbunătăți securitatea cibernetică, acest îndrumar vi se adresează. Indiferent unde vă aflați, acest îndrumar are rolul de a furniza organizației dvs. informații esențiale de care are nevoie pentru a implementa un plan solid de securitate. Un plan care nu se rezumă la niște instrucțiuni scrise, ci care vă permite să implementați cele mai bune practici.

Ce este un plan de securitate și de ce ar trebui să aibă unul organizația mea?

Un plan de securitate este setul de politici, proceduri și instrucțiuni scrise agreate de organizația dvs. în scopul de a atinge un nivel de securitate pe care dvs. și echipa dvs. îl considerați adecvat pentru siguranța oamenilor, partenerilor și informațiilor dvs.

Un plan de securitate bine făcut și actualizat la nivelul organizației vă poate proteja și vă poate face mai eficienți oferindu-vă liniștea de care aveți nevoie pentru a vă concentra pe munca importantă de zi cu zi a organizației dvs. Fără a reconsidera un plan comprehensiv, este foarte ușor să fiți orbi la anumite tipuri de amenințări, concentrându-vă prea mult pe un risc sau ignorând securitatea cibernetică până la momentul unei crize. Când începeți să concepeți un plan de securitate, există câteva întrebări importante pe care trebuie să vi le puneți și care formează un proces denumit **evaluarea riscurilor.** Răspunsul la aceste întrebări ajută organizația dvs. să înțeleagă amenințările unice cu care vă confruntați și vă permite să vă gândiți bine la ce trebuie să protejați și de cine trebuie să vă protejați. Evaluatori calificați, ajutați de sisteme precum **SAFETAG** de la Internews, vă pot ghida organizația în cursul unui asemenea proces. Dacă puteți obține acces la acest nivel de experiență profesională, merită din plin, însă dacă nu puteți trece printr-o evaluare completă, vă recomandăm să vizitați organizația și să luați în considerare aceste întrebări cheie:

1 Ce active deține organizația dvs. pe care doriți să le protejați?

Puteți începe să răspundeți la aceste întrebări **creând un catalog cu toate activele organizației dvs**. Informațiile precum mesajele, e-mailurile, contactele, documentele, calendarele și locațiile sunt toate posibile active. Telefoanele, computerele și alte dispozitive pot fi active. Iar oamenii, cunoscuții și relațiile pot fi, la rândul lor, active. Faceți o **listă a activelor dvs.** și încercați să le catalogați în funcție de importanța pe care o au pentru organizație, de locul în care le țineți (de pildă, mai multe locații digitale sau fizice) și de ceea ce îi împiedică pe alții să le acceseze, deterioreze sau distrugă. Rețineți, nu toate sunt la fel de importante. Dacă unele date ale organizației dvs. sunt înregistrări publice sau informații pe care deja le-ați publicat, acestea nu mai sunt secrete pe care trebuie să le protejați.

2 Cine sunt adversarii dvs. și care le sunt capabilitățile și motivațiile?

„Adversar" este un termen utilizat frecvent în securitatea la nivel de organizații. În termeni simpli, adversarii sunt actori (fizice sau grupări) care sunt interesați să vă țintească organizația, perturbându-vă activitatea și obținând acces la sau distrugându-vă informațiile; răufăcătorii. Printre potențialii adversari întâlnim escrocii financiari, concurenții, autoritățile locale sau naționale sau guvernele, ori hackeri motivați ideologic sau politic. Este important să faceți o listă a adversarilor dvs. și să vă gândiți critic la cine s-ar putea să vrea să vă afecteze negativ organizația și personalul. Cu toate că e ușor să ne imaginăm actorii externi (precum guverne străine sau un anume grup politic) ca fiind adversari, luați totuși în considerare și faptul că adversari pot fi și persoane pe care le cunoașteți, precum angajați nemulțumiți, foști angajați și rude sau parteneri care nu vă înțeleg. Diferiții adversari reprezintă diferite amenințări și dețin resurse diferite și capacități de a vă perturba activitatea și a obține acces sau a vă distruge informațiile.

De exemplu, guvernele au adesea mulți bani și capacități puternice, inclusiv întreruperea internetului sau utilizarea de tehnologii de supraveghere costisitoare; rețelele mobile și furnizorii de internet au probabil acces la înregistrările apelurilor dvs. și la istoricul browserelor; hackerii pricepuți la rețele Wi Fi au abilitatea de a intercepta comunicările sau tranzacțiile financiare slab securizate. Puteți deveni chiar propriul adversar, de pildă, ștergând accidental fișiere importante sau trimițând mesaje private persoanei greșite.

Motivele adversarilor ar putea diferi în funcție de capacitatea, interesele și strategiile acestora. Sunt interesați să vă discrediteze organizația? Poate intenția lor este să vă înăbușe mesajele? Sau poate vă văd organizația drept concurentă și vor să câștige un avantaj? Este important să înțelegeți motivația adversarului, pentru că procedând astfel veți putea ajuta organizația să evalueze mai bine amenințările la care se expune.

3 Cu ce amenințări se confruntă organizația dvs.? Și care este probabilitatea să devină reale și ce impact ar avea?

Când identificați posibilele amenințări, s-ar putea să obțineți o listă lungă care ar putea fi copleșitoare. Ați putea avea senzația că eforturile dvs. sunt inutile sau să nu știți de unde să începeți. Pentru a ajuta organizația să stabilească următorii pași productivi, este util să analizați fiecare amenințare în funcție de doi factori: probabilitatea ca amenințarea să aibă loc; și impactul dacă se întâmplă acest lucru.

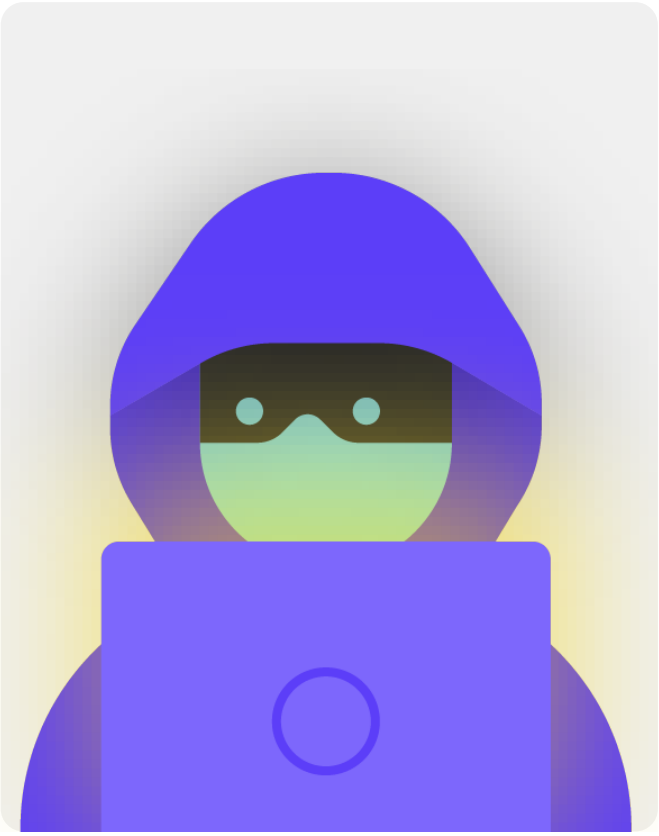
Pentru a măsura probabilitatea amenințării („mică, medie sau mare") în funcție de probabilitatea întâmplării unui eveniment - puțin probabil, probabil sau se întâmplă des - puteți folosi informațiile pe care le cunoașteți despre capacitatea și motivația adversarilor, analize ale incidentelor de securitate anterioare, experiențele altor organizații similare și, desigur, prezența oricăror strategii de diminuare a riscurilor pe care le-a implementat organizația dvs.

Pentru a măsura impactul unei amenințări, gândiți-vă cum ar arăta lumea dvs. dacă amenințarea ar deveni reală. Puneți-vă întrebări precum „Cum a afectat amenințarea organizația în sine și pe oamenii noștri, fizic și mental?", „Cât va dura efectul?", „Va crea alte situații dăunătoare?" și „Cum ne limitează abilitatea de a atinge obiectivele organizației, acum și pe viitor?" Când răspundeți la aceste întrebări, luați în considerare dacă impactul amenințării este mic, mediu sau ridicat.

După ce ați clasificat amenințările în funcție de probabilitate și impact, puteți începe să concepeți un plan de acțiune mai informat. Concentrându-vă pe amenințările care au cel mai înalt grad de probabilitate să devină reale ȘI care ar avea un impact negativ semnificativ, vă veți canaliza resursele limitate în cel mai eficient mod posibil.

Scopul dvs. este să diminuați cât mai mult riscurile, însă nimeni – nici măcar guvernul sau compania care dispune de cele mai multe resurse din lume – nu poate elimina complet riscurile. Și este în regulă: puteți face multe să vă protejați pe dvs., pe colegii dvs. și să vă protejați organizația concentrându-vă pe cele mai mari amenințări.

Pentru a vă ajuta în procesul de evaluare a riscurilor, folosiți o fișă de lucru, precum **aceasta** dezvoltată de Electronic Frontier Foundation. Nu uitați că informațiile pe care le obțineți ca parte a acestui proces (precum o listă a adversarilor și a amenințărilor pe care le prezintă aceștia) pot fi sensibile, prin urmare este important să le mențineți în siguranță.



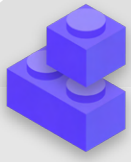
Crearea planului dvs. de securitate cibernetică la nivel de organizație

Cu toate că planul de securitate al fiecărei organizații în parte va arăta puțin diferit în funcție de evaluarea riscurilor și dinamica organizației, anumite concepte de bază sunt aproape universale.

Îndrumarul de față prezintă aceste concepte esențiale în așa fel încât să vă ajute organizația că conceapă un plan concret de securitate în baza soluțiilor practice și aplicațiilor reale.

Acest îndrumar își propune să ofere opțiuni și sugestii cu caracter gratuit să la un preț foarte mic. Rețineți că cel mai semnificativ cost asociat cu implementarea unui plan de securitate efectiv va fi timpul pe care îl veți acorda dvs. și organizația dvs. pentru a discuta, învăța și implementa noul plan. Însă, având în vedere riscurile cu care se poate confrunta organizația dvs., această investiție va merita din plin.

În fiecare secțiune, veți găsi o explicație a unui subiect cheie pe care organizație dvs. și personalul acesteia trebuie să îl cunoască - să știe ce este și de ce este important. Fiecare subiect este însoțit de strategii esențiale, de abordări și instrumente recomandate pentru limitarea riscurilor, precum și de sfaturi și linkuri către resurse suplimentare care vă pot ajuta să implementați recomandările respective la nivelul organizației dvs.



Starter kit pentru planul de securitate

Pentru a vă ajuta organizația să procesați lecțiile din acest îndrumat și a le transforma într-un plan real, folosiți acest starter kit pentru planul de securitate. Puteți fie imprima kitul, fie completa digital pe măsură ce citiți îndrumarul online. Atunci când luați notițe și începeți să actualizați sau să concepeți planul de securitate, consultați „blocurile componente ale planului de securitate" detaliate în fiecare secțiune. Niciun plan de securitate nu este complet fără a aduce în discuție, cel puțin, aceste elemente esențiale.

Folosiți-vă și de alte resurse care să vă ajute să concepeți și să vă implementați planul. În calitate de organizație a societății civile, aplicația SOAP (Securing Organizations with Automated Policymaking) vă poate ajuta să simplificați și să vă automatizați crearea planului de securitate.

Utilizați, de asemenea, resursele de instruire gratuite precum Planificatorul de securitate de pe Consumer Reports,aplicația Umbrella de pe Security First, proiectul Totem al Free Press Unlimited și Greenhost și kitul de instrumente de securitate cibernetică pentru organizații bazate pe misiuni dezvoltat de Global Cyber Alliance, care includ resurse privind cele mai bune practici menționate în acest Îndrumar și linkuri către multe instrumente de instruire care să vă ajute să implementați multe elemente de bază.

Construirea unei culturi a securității

Securitatea se adresează oamenilor, iar pentru a vă proteja organizația, trebuie să vă asigurați că toți cei implicați iau în serios securitatea cibernetică. Schimbarea culturii este dificilă, însă câțiva pași simpli și câteva conversații importante vă pot ajuta mult să creați o atmosferă care va construi rezistența personalului și organizației dvs. în fața amenințărilor de securitate. Unul dintre cei mai simpli, dar cei mai importanți pași de urmat pentru construirea acestei culturi de securitate la nivelul organizației este să discutați despre ea și să îndemnați liderii să fie în permanență un model de bună purtare.

Integrarea securității în structura dvs. operațională regulată

Așa cum se descrie în detaliu în Manualul securității holistice al Tactical Tech, este esențial să creați spații permanente și sigure în care să discutați despre diferite aspecte ale securității.

Astfel, dacă membrii echipei au îngrijorări de securitate, vor fi mai puțin neliniștiți că ar putea să pară paranoici sau că i-ar face pe alții să-și piardă timpul. **Programarea de conversații regulate despre securitate** normalizează, de asemenea, frecvența interacțiunii și reflectarea asupra chestiunilor de securitate, astfel încât problemele să nu fie date uitării și membrii echipei să dea dovadă cel puțin de o conștientizare pasivă a securității în activitatea lor. Nu trebuie să fie o activitate săptămânală, însă faceți-o recurent. Aceste discuții nu trebuie să lase loc doar pentru subiecte de securitate tehnică, ci trebuie să includă și aspecte care afectează confortul și siguranța personalului, precum conflictul comunitar, hărțuirea online (și offline) sau probleme cu utilizarea și implementarea instrumentelor digitale. Conversațiile pot include chiar și subiecte precum obiceiurile de partajare a informațiilor offline și modul în care personalul securizează sau nu informațiile în afara serviciului. La urma urmei, este important să rețineți că securitatea unei organizații este la fel de puternică ca veriga sa cea mai slabă. Un mod de a obține angajamentul consistent este adăugarea securității la agenda unei întâlniri obișnuite.

Puteți, de asemenea, să atribuiți prin rotație responsabilitatea de a organiza și facilita o discuție privind securitatea între membrii organizației dvs., fapt ce va ajuta la dezvoltarea ideii că securitatea este responsabilitatea tuturor și nu doar a unui grup select de persoane sau a echipei IT. Când veți începe să dați o formă discuției despre securitate, personalul s-ar putea să se simtă mai în largul său discutând aceste chestiuni importante între ei, precum și într-un mediu mai puțin formal.

La fel de importantă este și încorporarea elementelor de securitate în funcționarea normală a organizației, de pildă, în timpul procesului de integrare a angajatului – și luarea în considerare a restricționării accesului la sisteme pentru angajații care urmează să părăsească organizația. Securitatea nu trebuie să fie un „lucru în plus" care să ne îngrijoreze, ci mai degrabă o ***parte integrantă a strategiei și operațiunilor noastre.***

Rețineți că toate planurile de securitate trebuie considerate document evolutive și trebuie reevaluate și discutate regulat, în special când noi angajați sau voluntari se alătură organizației dvs. sau contextul de securitate suferă modificări.

Faceți planuri de a vă revizita strategia și de a face actualizări anual sau dacă strategia, instrumentele și amenințările cu care vă confruntați suferă modificări majore.

Obținerea sprijinului la nivel de organizație

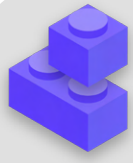
Un plan de securitate de succes include și asigurarea unui sistem de sprijin la nivel de organizație pentru planul dvs. de securitate.

Este de o importanță capitală ca acest plan să includă o asistență solidă și vocală și indicații de la liderii organizației care, în multe cazuri, vor fi cei care iau deciziile finale de alocare a timpului, resurselor și energiei în vederea dezvoltării și implementării unui plan de securitate eficient. Dacă nu luați în serios acest lucru, nu o va face nimeni. Pentru implementarea acestor aprobări în cadrul organizației, gândiți-vă atent la momentul și metoda de introducere a planului, care trebuie să fie limpede, asigurați-vă că liderii întăresc mesajele și explicați-le tuturor toate elementele și toți pașii planului, astfel încât să nu existe probleme sau confuzie în ceea ce privește ceea ce încercați să realizați. Mulți donatori solicită în prezent garanții de menținere a unei securități puternice, prin urmare sublinierea acestui lucru este, de asemenea, o modalitate bună de a crea un sistem de sprijin la nivelul organizației. Atunci când discutați despre securitate, evitați tacticile de amenințare. Uneori, amenințările cu care se confruntă organizația și personalul dvs. pot fi alarmante, prin urma încercați să vă axați pe partajarea detaliilor și crearea unui spațiu calm pentru întrebări și nelămuriri. Dacă dați senzația că pericolele sunt prea amenințătoare, riscați ca oamenii să vă perceapă drept persoană dornică de senzațional sau pur și simplu să renunțe, gândindu-se că eforturile lor nu contează – nimic mai departe de adevăr.

Stabilirea unui plan de instruire

Odată ce ați dezvoltat și v-ați obligat să respectați un plan, gândiți-vă cum veți instrui tot personalul (și voluntarii) cu privire la aceste noi practici.

Obligativitatea unei instruiri regulate - precum și a prezenței la instruire și a unui punct de evaluare pentru performanța personalului - poate fi o tactică utilă. Evitați crearea de consecințe dure și negative pentru personalul care are dificultăți de a înțelege conceptele de securitate. Rețineți că anumiți angajați se pot adapta și pot învăța diferit tehnologia în comparație cu alții, în funcție de nivelele diferite de familiaritate cu instrumentele digitale și internetul. Teama de eșec doar va descuraja personalul să raporteze problemele sau să ceară ajutor. Cu toate acestea, crearea unei răspunderi urmate de recompense pentru instruire și adoptarea cu succes a politicilor poate contribui la motivarea perfecționării la nivelul organizației. Puteți beneficia de un sprijin suplimentar valoros prin intermediul unor rețele locale sau naționale de instruire privind securitatea, precum aplicația Umbrella de pe Security First, proiectul Totem al Free Press Unlimited and Greenhost și Portalul de învățare dezvoltat de Global Cyber Alliance.



Construirea unei culturi a securității

- **Programați conversații și instruire regulate cu privire la securitate și planul dvs. de securitate.**
- **Implicați pe toată lumea - distribuiți responsabilitatea de a implementa planul de securitate la nivelul întregii organizații.**
- **Asigurați-vă că liderii modelează un bun comportament de securitate și un angajament la planul dvs.**
- **Evitați tacticile de amenințare sau pedepsire - recompensați progresul și crea un spațiu confortabil în care personalul să raporteze problemele și să ceară ajutor.**
- **Actualizați-vă planul de securitate anual sau după schimbări majore în organizația dvs.**

O fundație solidă: Securizarea conturilor și dispozitivelor

De ce trebuie să ne axăm pe conturi și dispozitive? Deoarece acestea formează fundația a tot ceea ce face digital organizația dvs.

Aproape sigur accesați informații sensibile, comunicați la nivel intern și extern și salvați informații private pe acestea. Dacă acestea nu sunt securizate, toate cele de mai sus plus altele ar putea fi în primejdie. De exemplu, dacă hackerii vă observă secvențele pe taste sau vă ascultă microfonul, conversațiile private cu colegii vor fi interceptate indiferent de nivelul de securizare al aplicațiilor de mesagerie. Sau, dacă un adversar obține acces la conturile organizației dvs. de pe rețele sociale, aceștia v-ar putea distruge cu ușurință reputația și credibilitatea, sublimând succesul muncii dvs. Prin urmare, este esențial ca o organizație să se asigure că toată lumea urmează niște pași simpli, dar eficienți, de a menține dispozitivele și conturile sigure. Este important de menționat că aceste recomandări includ și conturile și dispozitivele personale, care sunt adesea ținte sigure pentru adversari. Hackerii vor ataca bucuroși cele mai ușoare ținte și vor sparge un cont personal sau un computer personal dacă echipa dvs. le folosește să comunice și acceseze informații importante.

Conturi securizate și societatea civilă

Extrem de mediatizatul atac SolarWinds de la finalul anului 2020, care a compromis peste 250 de organizații, inclusiv majoritatea departamentelor guvernamentale ale SUA, furnizori tehnologici precum Microsoft și Cisco și ONG-uri, a fost parțial rezultatul ghicirii de către hackeri a parolelor slabe utilizate pentru conturi de administrator importante. Per ansamblu, aproximativ 80% dintre toate atacurile hackerilor survin din cauza parolelor slabe sau reutilizate.

Odată cu prevalența tot mai mare a spargerilor de parole precum cea de mai sus și cu accesul mai facil al adversarilor de orice tip la instrumente sofisticate de atacare a parolelor, cele mai bune practici pentru parole și autentificarea cu doi factori sunt esențiale pentru organizațiile societății civile. Un exemplu de atac asupra conturilor unei societăți civile a fost raportat de Facebook în 2020. Conform **reportului** Facebook, câteva grupuri de hackeri din Bangladesh au atacat conturile unor activiști, jurnaliști și minorități religioase ale societății civile locale. Din nefericire, hackerii au reușit să compromită câteva dintre aceste conturi de Facebook, inclusiv pe cel al unui administrator al unei pagini de Facebook a unui grup local. Având acces la contul administratorului, hackerii i-au eliminat pe ceilalți administratori și au preluat și dezactivat pagina, împiedicând grupul să distribuie informații cheie și să comunice cu publicul său. În urma anchetei Facebook, s-a descoperit să aceste conturi au fost probabil compromise prin diverse metode, inclusiv abuzarea de procesul de recuperare a contului. Dacă toate aceste conturi ar fi folosit autentificarea cu doi factori, hackerilor le-ar fi fost mult mai greu să spargă conturile respective.

Conturi securizate: Parole și autentificarea cu doi factori

În ziua de astăzi, probabil că organizația și personalul dvs. au multe, poate chiar sute de conturi care, dacă sunt sparte, ar putea expune informații sensibile sau chiar ar putea afecta siguranța personală.

Gândiți-vă la diferitele conturi pe care un membrii personalului și organizația le dețin: e-mail, aplicații chat, rețele sociale, servicii bancare online, stocare de date în cloud, precum și magazine de haine, restaurante locale, ziare și multe alte site-uri web sau aplicații la care vă conectați. O securitate bună în ziua de azi necesită o abordare sârguincioasă pentru protejarea acestor conturi de atacuri. Acest lucru pornește cu asigurarea unei bune igiene a parolelor și utilizarea autentificării cu doi factori în întreaga organizație.

CE PRESUPUNE O PAROLĂ BUNĂ?

O parolă bună presupune trei elemente cheie: lungime, caracter aleatoriu și unicitate.

LUNGIME	Cu cât parola este mai lungă, cu atât este mai dificil de ghicit de către un adversar. Majoritatea spargerilor de parole se realizează în prezent cu ajutorul unor programe cărora nu le ia mult să spargă o parolă scurtă. Prin urmare, este esențial ca parolele dvs. să conțină cel puțin 16 caractere sau cel puțin cinci cuvinte, preferabil mai multe.
CARACTER ALEATORIU	Chiar dacă o parolă este lungă, nu este foarte bună dacă reprezintă ceva ușor de ghicit de către un adversar. Evitați să includeți informații precum ziua de naștere, orașul, activitățile dvs. preferate sau alte informații pe care cineva le pot găsi despre dvs. printr-o căutare rapidă pe internet.
UNICITATE	Probabil cea mai frecventă „cea mai neinspirată practică” este utilizarea aceleiași parole pe mai multe site-uri. Repetarea parolelor este o mare problemă, deoarece, dacă doar unul dintre site-urile respective este compromis, toate celelalte care folosesc aceeași parolă sunt, la rândul lor, vulnerabile. Dacă folosiți aceeași frază de acces pe mai multe site-uri, impactul unei greșeli sau unei breșe de date poate crește semnificativ. Chiar dacă nu vă pasă de parola pe care o aveți la biblioteca locală, dacă aceasta este spartă și folosiți aceeași parolă pentru un cont mai sensibil, vi se pot fura informații importante.

O modalitate simplă de a atinge obiectivele de lungime, caracter aleatoriu și unicitate este să alegeți trei sau patru cuvinte comune, dar aleatorii. De exemplu, parola dvs. ar putea fi „floare lampă verde urs”, fiind ușor de ținut minte, dar greu de ghicit. Puteți vizita acest site web creat de Better Buys pentru a vedea o estimare a cât de rapid pot fi sparte parolele slabe.

FOLOSIȚI UN MANAGER DE PAROLE

Știți că este important ca toți oamenii din organizația dvs. să folosească o parolă lungă, aleatorie și diferită pentru fiecare dintre conturile lor personale și de organizație, însă știți cum să faceți acest lucru? Memorarea unei parole bune pentru mai multe (dar nu sute) de conturi este imposibilă, așa că suntem nevoiți să trișăm. Metoda greșită ar fi reutilizarea parolelor. Din fericire, putem apela la managerii digitali de parole, care ne pot ușura viața (și ne fac mai sigure practicile pentru parole). Aceste aplicații, dintre care multe pot fi accesate de pe computer sau dispozitivul mobil, pot crea, stoca și gestiona parole pentru dvs. și organizația dvs. Adoptarea unui manager de parole sigur presupune memorarea unei singure parole foarte puternice și lungi, denumită parolă primară (cunoscută anterior sub denumirea de parolă „principală”) care vă asigură beneficiile de securitate de a folosi parole bune și unice pentru toate conturile dvs. Veți folosi această parolă primară (și, ideal, autentificarea în doi factori (2FA), despre care vom discuta în secțiunea următoare) pentru a deschide managerul de parole și debloca accesul la toate celelalte parole. Managerii de parole pot fi partajați și pentru mai multe conturi pentru a facilita partajarea securizată a parolelor în cadrul organizației dvs.

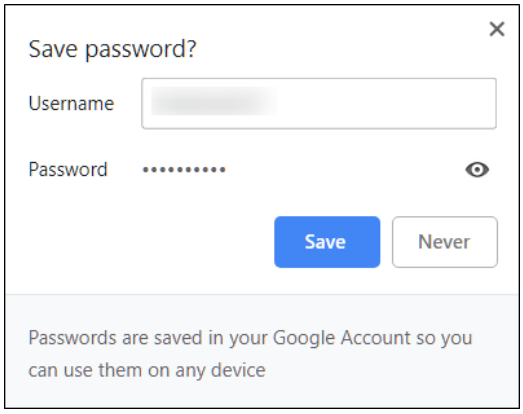
De ce trebuie să folosim ceva nou? Nu le putem, pur și simplu, nota pe hârtie sau într-o foaie de calcul în computer?

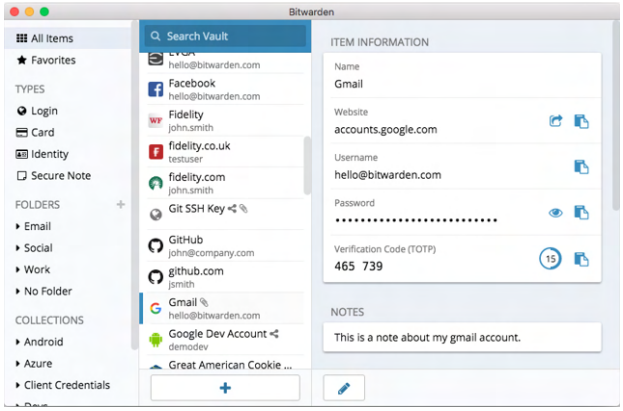
Din păcate, există multe abordări greșite și nesigure de a gestiona parolele. Parolele puternice notate pe hârtie (dacă nu sunt păstrate încuiate într-un seif) riscă să fie furate, văzute de ochi indiscreți sau pierdute și deteriorate ușor. Salvarea parolelor într-un document pe computerul dvs. facilitează accesul hackerilor la ele – sau, dacă cineva vă fură computerul, va avea, pe lângă dispozitivul în sine, acces și la toate conturile dvs. Folosirea unui bun manager de parole este la fel de simplă ca folosirea unui document, însă este mai sigură.

De ce să avem încredere într-un manager de parole?

Managerii de parole de calitate fac eforturi extraordinare (și angajează echipe de securitate excelente) pentru a menține securitatea sistemelor. Bunele aplicații de gestionare a parolelor (câteva dintre ele sunt recomandate mai jos) sunt configurate în așa fel încât să nu vă poată „debloca” conturile. Acest lucru înseamnă că, în majoritatea cazurilor, dacă sunt accesate ilegal sau obligate legal să dezvăluie informații, nu vor putea să vă piardă sau să vă dezvăluie parolele. De asemenea, este important să rețineți că este mult mai probabil ca un adversar să ghicească una dintre parolele dvs. repetate sau să găsească una într-o breșă de date publice decât dacă un bun manager de parole ar fi spart. Este importat să rămâneți sceptici și, desigur, să nu aveți încredere oarbă în toate software-urile și aplicațiile, însă managerii de parole cu reputație bună beneficiază de stimulentele potrivite să acționeze corect.

În loc să folosiți un browser (precum Chrome, în imaginea din stânga) pentru a vă salva parolele, folosiți un manager de parole dedicat (precum Bitwarden, în imaginea din dreapta). Managerii de parole au funcții care contribuie la sporirea securității și comodității în cadrul organizației dvs.





Dar stocarea parolelor în browser?

Salvarea parolelor în browser nu este același lucru cu utilizarea unui manager de parole sigur. Pe scurt, nu este recomandat să folosiți Chrome, Firefox, Safari sau orice alt browser ca manager de parole. Cu toate că, desigur, este o modalitate mai sigură decât notarea lor pe hârtie sau salvarea într-o foaie de calcul, funcțiile de bază pentru salvarea parolelor ale browserului web lasă de dorit în ceea ce privește securitatea. Aceste neajunsuri vă lipsesc, de asemenea, de comoditatea oferită de un bun manager de parole. Pierderea acestei comodități crește probabilitatea ca oamenii din organizația dvs. să continuă să folosească practici mai puțin eficiente de creare și partajare a parolelor.

De pildă, spre deosebire de managerii de parole dedicați, funcțiile integrate „salvează această parolă” sau „memorează această parolă” ale browserelor nu dispun de compatibilitate mobilă simplă, funcționalitate inter-browsere și instrumente de generare de parole puternice și auditare. Aceste funcții reprezintă o parte importantă a ceea ce face dintr-un manager de parole dedicat atât de util și benefic pentru securitatea organizației dvs. Managerii de parole includ, de asemenea, funcții specifice pentru organizații (precum partajarea parolelor) care contribuie atât la securitatea persoanelor, cât și a organizației per ansamblu. Dacă ați salvat parole în browserul dvs. (intenționat sau fără intenție), dedicați un moment pentru a le șterge.

Ce manager de parole ar trebui să folosim?

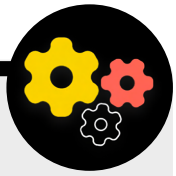
Există multe instrumente de gestionare a parolelor care pot fi configurate în mai puțin de 30 de minute. Dacă sunteți în căutarea unei opțiuni online de încredere pentru organizația dvs., pe care oamenii dvs. să o poată accesa de pe mai multe dispozitive în orice moment, 1Password (de la 2,99 USD per utilizator pe lună) sau Bitwarden, un program open-source gratuit, sunt ambele foarte acceptate și recomandate. O opțiune online precum Bitwarden poate fi perfectă atât din punct de vedere al securității, cât și al caracterului convenabil. Bitwarden, de pildă, vă va ajuta să creați parole unice puternice și să accesați parole de pe mai multe dispozitive, prin

intermediul extensiilor de browser sau al unei aplicații mobile. Versiunea cu plată (10 USD anual) a Bitwarden oferă și rapoarte ale parolelor reutilizate, slabe și posibil sparte, pentru a vă ajuta să mențineți controlul. După ce ați configurat parole primară (cunoscută sub numele de parolă principală), vă recomandăm să activați și autentificarea cu doi factori pentru a menține cât mai puternică securitatea seifului managerului de parole.

Este esențial să **implementați metode eficiente de securitate și atunci când folosiți managerul de parole.** De pildă, dacă folosiți extensia browserului managerului de securitate sau vă autentificați în Bitwarden (sau orice alt manager de parole) de pe un dispozitiv, nu uitați să vă deconectați după ce l-ați utilizat, dacă partajați dispozitivul sau credeți că există un risc ridicat de furt al dispozitivului fizic. Aceasta include deconectarea din managerul de parole dacă lăsați computerul sau dispozitivul mobil nesupravegheat. Dacă partajați parole în cadrul organizației, asigurați-vă, de asemenea, că ați anulat accesul la parole (și schimbați parolele în sine) pentru persoanele care părăsesc organizația. Nu este dorit ca un fost angajat să aibă în continuare acces la parola de Facebook a organizației dvs., de exemplu.

Ce se întâmplă dacă cineva uită parola primară?

Este esențial să vă amintiți parola primară. Sistemele bune de gestionare a parolelor precum cele recomandate mai sus nu vor memora parola primară și nu vor permite resetarea acesteia direct prin e-mail, așa cum o puteți face pe site-urile web. Cu toate că este o funcție eficientă de securitate, vă obligă, de asemenea, să memorați parola primară în momentul configurării inițiale a managerului de parole. Pentru a vă ajuta, vă recomandăm să configurați un memento zilnic de reamintire a parolei primare atunci când creați inițial un cont de manager de parole.



Folosirea unui manager de parole pentru organizația dvs.

Puteți consolida practicile de creare a parolelor la nivelul întregii organizații și vă puteți asigura că întregul personal are acces la (și folosește) un manager de parole implementând unul pentru întreaga organizație. În loc să solicitați fiecărui membru al personalului să își configureze propriul manager de parole, luați în calcul să investiți într-un abonament „de echipă” sau „business”. De exemplu, Bitwarden oferă abonamentul „echipe și organizații” care costă 3 USD per utilizator pe lună. Cu acesta (sau cu alte abonamente de echipă pentru manageri de parole precum 1Password), aveți abilitatea de a gestiona toate parolele partajate în cadrul organizației. Funcțiile unui manager de parole pentru o întreagă organizație nu oferă doar o securitate sporită, ci sunt și convenabile pentru personal. Puteți partaja în siguranță acreditările din managerul de parole unor diferite conturi de utilizatori. Iar Bitwarden, de pildă, oferă și un text criptat de la un capăt la altul și o funcție de partajare de fișiere denumită „Bitwarden Send” în acest abonament. Ambele funcții de mai sus oferă organizației dvs. mai mult control asupra persoanelor care pot vedea și partaja anumite parole și asigură o opțiune mai sigură de partajare a acreditărilor pentru conturile de echipă sau de grup. Atunci când configurați un manager de parole la nivel de organizație, asigurați-vă că atribuiți unei anumite persoane rolul de a șterge conturile angajaților și de schimba parolele partajate atunci când o persoană părăsește echipa.

CE ESTE AUTENTIFICAREA CU DOI FACTORI?

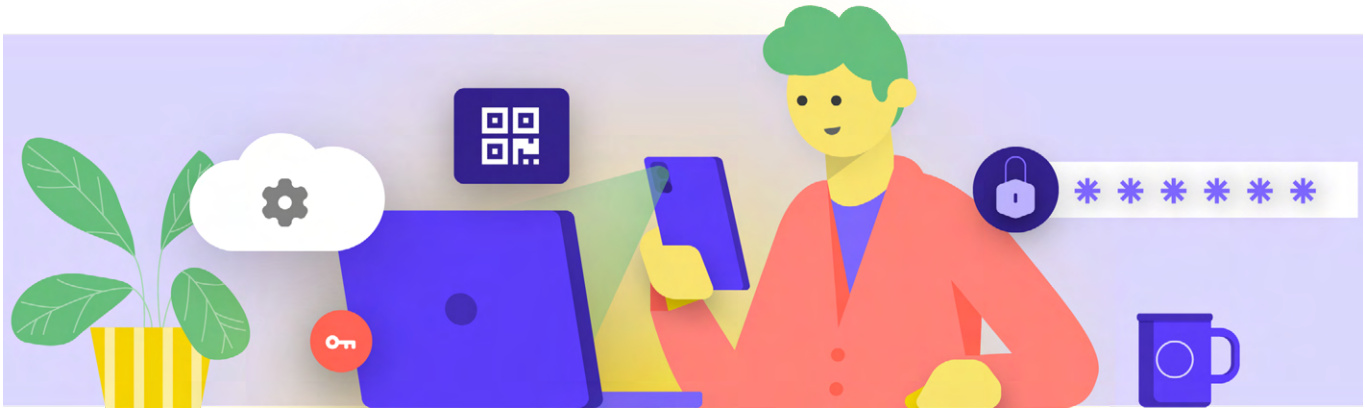
Indiferent de gradul de igienă a parolei dvs., hackerii încă sparg frecvent parolele. Securizarea conturilor împotriva unor amenințări comune din ziua de azi necesită un alt nivel de protecție. Aici intră în scenă autentificarea cu mai mulți factori și cu doi factori – cunoscute sub denumirea de MFA sau 2FA. Există multe ghiduri și resurse foarte bune care explică autentificarea cu doi factori, inclusiv articolul Autentificarea cu doi factori pentru începători scris de Martin Shelton și Ghidul 101 privind securitatea cibernetică în timpul alegerilor al Center for Democracy & Technology. Secțiunea de față se inspiră în mare din aceste resurse, pentru a explica de ce este atât de importantă implementarea 2FA la nivelul organizației dvs. Pe scurt, 2FA sporește securitatea contului solicitând o a doua informație – ceva care reprezintă mai mult decât o parolă – pentru a obține accesul. Cea de-a doua informație este, de obicei, ceva ce deținești, de pildă un cod de la o aplicație de pe telefonul dvs. sau un token sau o cheie digitale. Această cea de-a doua informație acționează drept nivel secundar de apărare. Dacă un hacker vă fură parola sau obține acces la aceasta prin descărcarea parolelor în urma unei breșe de date majore, o 2FA eficientă îi poate împiedica să vă acceseze contul (și, prin urmare, îi ține departe de informații private și sensibile). Este de o importanță critică să vă asigurați că toți oamenii din organizația dvs. implementează 2FA pentru conturile lor.

CUM CONFIGURĂM AUTENTIFICAREA CU DOI FACTORI?

Există trei metode comune pentru 2FA: chei de securitate, aplicații de autentificare și coduri SMS de unică folosință.

Chei de securitate

Cheile de securitate sunt cea mai bună opțiune, în parte, deoarece sunt aproape complet rezistente la atacuri de tip phishing. Aceste „chei" sunt tokenuri hardware (ca niște mini unități USB) care se pot atașa la breloc (sau rămâne în computer), pentru a siguranță și accesare facilă. Atunci când trebuie să folosiți cheia pentru a debloca un anumit cont, trebuie doar să o introduceți în dispozitivul dvs. și să îl atingeți atunci când vi se solicită acest lucru în timpul conectării. Există o gamă largă de modele pe care le puteți achiziționa online (20-50 USD), inclusiv foarte apreciatul YubiKeys. Site-ul Wirecutter al New York Times are un ghid util cu recomandări de chei pe care le puteți achiziționa. Rețineți că puteți folosi aceeași cheie de securitate pentru câte conturi doriți. În vreme ce cheile de securitate sunt destul de costisitoare pentru multe organizații, inițiative precum Programul Protecție avansată al Google sau AccountGuard al Microsoft oferă aceste chei gratuit pentru anumite grupuri. Contactați-i pe cei care v-au furnizat Îndrumarul pentru a vedea dacă vă pot conecta la asemenea programe sau contactați cyberhandbook@ndi.org.



Aplicații de autentificare

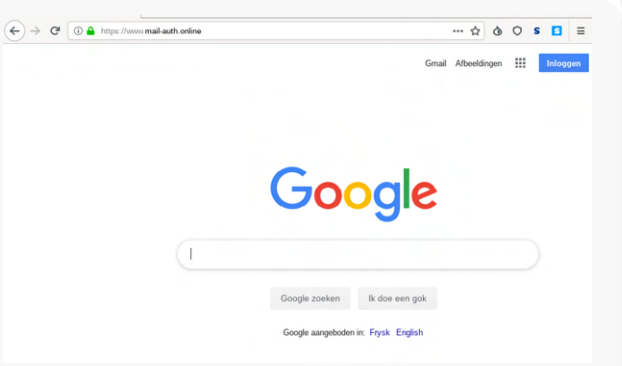
Cea **de-a doua opțiune ca grad de eficiență pentru 2FA o reprezintă aplicațiile de autentificare.** Aceste servicii vă permit să primiți on cod temporar de autentificare cu doi factori, prin intermediul unei aplicații mobile sau printr-o notificare push pe smartphone. Iată câteva opțiuni populare și de încredere: Google Authenticator, Authy și Duo Mobile. Aplicațiile de autentificare sunt eficiente și pentru că funcționează și atunci când nu aveți acces la rețeaua celulară și pot fi folosite gratuit de persoane fizice. Cu toate acestea, aplicațiile de autentificare sunt mai susceptibile de phishing decât cheile de securitate, deoarece utilizatorii pot fi păcăliți să introducă codurile de securitate dintr-o aplicație de autentificare pe un site web fals. Aveți grijă să introduceți coduri de conectare doar pe site-uri legale. Și nu „acceptați" notificări de conectare de tip push decât dacă știți sigur că dvs. ați trimit solicitarea de conectare. De asemenea, atunci când folosiți o aplicație de autentificare, este esențial să fiți pregătiți cu coduri de rezervă (discutate mai jos) în cazul în care telefonul dvs. este pierdut sau furat.

Coduri trimise prin SMS

Cea mai puțin sigură, însă, din nefericite, încă cea mai frecventă formă de 2FA sunt codurile trimise prin SMS. Având în vedere că SMS-urile pot fi interceptate, iar numerele de telefon pot fi falsificate sau atacate de hackeri prin furnizorul de telefonie mobilă, SMS lasă mult de dorit ca metodă de solicitare a codurilor 2FA. Este o metodă mai bună comparativ cu utilizarea simplă a unei parole, însă aplicațiile de autentificare sau o cheie fizică de securitate sunt recomandate atunci când este posibil. Un adversar hotărât poate obține acces la codurile SMS 2FA, de regulă printr-un simplu apel la compania telefonică și schimbarea cartelei dvs. SIM. Atunci când sunteți pregătiți să începeți activarea 2FA pentru toate conturile din organizația dvs., utilizați acest site web (https://2fa.directory/) pentru o căutare rapidă de informații și instrucțiuni pentru anumite servicii (precum Gmail, Office 365, Facebook, Twitter etc.) și pentru a vedea care servicii permit anumite tipuri de 2FA.

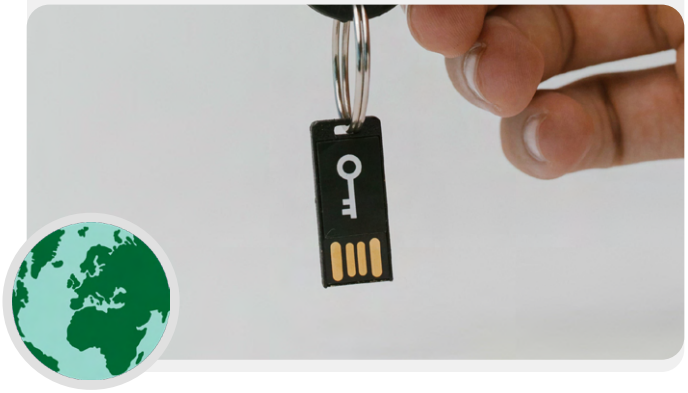
2FA și societatea civilă

Conform unui recent raport Amnesty International, hackeri care aveau ca țintă niște apărători ai drepturilor omului din Uzbekistan au folosit atacuri de tip phishing pentru parole partajate *și* coduri de autentificare cu doi factori pe conturile de e-mail ale acestora prin intermediul unor pagini false de autentificare la Gmail. Asemenea atacuri sunt o modalitate tot mai comună de a „ocoli" autentificarea cu doi factori. Este important - chiar și dacă folosiți 2FA - să fiți atenți unde introduceți codurile. Și mai bine, puteți elimina acest risc adoptând chei de securitate fizice.



Securitatea browserelor în realitate

Prin furnizarea de chei de securitate fizice pentru autentificarea cu doi factori pentru peste 85.000 dintre angajații săi, Google (o organizație cu un risc foarte ridicat și o țintă importantă) a eliminat orice atacuri de tip phishing împotriva organizației sale. Acest caz demonstrează cât de eficiente pot fi cheile de securitate pentru organizațiile care prezintă chiar și riscuri maxime.



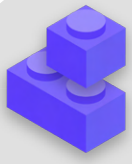
CE SE ÎNTÂMPLĂ DACĂ CINEVA PIERDE UN DISPOZITIV 2FA?

Dacă folosiți o cheie de securitate, tratați-o în același mod în care tratați o cheie a casei sau apartamentului dvs., dacă este cazul. Pe scurt, nu o pierdeți. Însă, ca și în cazul cheii casei dvs., este o idee bună să aveți o cheie de rezervă înregistrată la cont, care să rămână încuiată într-un loc sigur (un seif de acasă sau o cutie de valori), în eventualitatea în care o pierdeți sau vă este furată. Alternativ, vă recomandăm să creați coduri de rezervă pentru conturile care permit acest lucru. Salvați aceste coduri într-un loc foarte sigur, precum managerul de parole sau un seif fizic. Asemenea coduri de rezervă pot fi generate din setările majorității site-urilor 2FA (din același loc din care activați 2FA inițial) și pot fi folosite drept cheie de rezervă în cazul unei urgențe. Cele mai frecvente incidente 2FA survin atunci când vă înlocuiți sau pierdeți telefoanele pe care le utilizați pentru aplicațiile de autentificare. Dacă folosiți Google Authenticator, veți avea ghinion dacă vi se fură telefonul dacă nu ați salvat codurile de rezervă generate la momentul conectării la un cont prin Google Authenticator. Prin urmare, dacă folosiți Google Authenticator drept aplicație 2FA, asigurați-vă că ați salvat într-un loc sigur codurile de rezervă pentru toate conturile la care vă conectați. Dacă folosiți Authy sau Duo, ambele aplicații au funcții integrate, cu setări puternice de securitate, pe care le puteți activa. Dacă alegeți una dintre aceste aplicații, puteți configura opțiunile de rezervă respective în cazul în care dispozitivul se strică, se pierde sau este furat. Consultați instrucțiunile Authy aici și instrucțiunile Duo aici. Asigurați-vă că toți membrii organizației dvs. cunosc acești pași atunci când încep activarea 2FA pentru toate conturile lor.

Impunerea 2FA la nivel de organizație

Dacă organizația dvs. furnizează conturi de e-mail tuturor angajaților prin Google Workspace (cunoscut anterior sub denumirea de GSuite) sau Microsoft 365 folosind propriul dvs. domeniu (de exemplu, @ndi.org), puteți impune 2FA și setări puternice de securitate pentru toate conturile. O asemenea impunere nu ajută doar la protejarea conturilor respective, ci acționează și drept modalitate de a introduce și normaliza 2FA în rândul personalului, pentru a le ușura adoptarea metodei și pentru conturile personale. Dacă sunteți administrator Google Workspace, puteți urma aceste instrucțiuni pentru a impune 2FA pentru domeniul dvs. Puteți proceda similar și pentru Microsoft 365, urmând acești pași dacă sunteți administrator al domeniului.

Vă recomandăm, de asemenea, să înrolați conturile organizației dvs. în Programul Protecție avansată (Google) sau AccountGuard (Microsoft) pentru a impune controale de securitate suplimentare și a solicita chei fizice de securitate pentru autentificarea cu doi factori.



Conturi securizate

- **Impuneți parole puternice pentru toate conturile organizației; încurajați personalul și voluntarii să adopte aceleași măsuri pentru conturile lor personale.**
- **Implementați un manager de parole de încredere pentru organizație (și încurajați personalul să folosească un manager de parole și în scop personal).**
  - Impuneți o parolă primară puternică și 2FA pentru toate conturile din managerul de parole.
  - Reamintiți-le tuturor să se deconecteze din managerul de parole pe dispozitivele partajate sau atunci când dispozitivul prezintă o risc ridicat de furt sau confiscare.
- **Schimbați parolele partajate atunci când angajații părăsesc organizația.**
- **Partajați parolele doar în mod securizat, de pildă prin managerul de parole al organizației dvs. sau folosind aplicații criptate de la un capăt la altul.**
- **Impuneți 2FA pentru toate conturile organizației și încurajați personalul să configureze 2FA și pentru toate conturile personale.**
  - Dacă este posibil, furnizați personalului chei fizice de securitate.
  - Dacă nu vă permiteți chei de securitate, încurajați utilizarea aplicațiilor de autentificare în locul SMS-urilor sau apelurilor telefonice pentru 2FA.
- **Organizați cursuri de instruire regulate, pentru a asigura familiarizarea personalului cu cele mai bune practici privind parolele și 2FA, inclusiv cunoștințe despre ce presupune o parolă puternică și importanța de a nu reutiliza niciodată o parolă, de a accepta doar solicitări 2FA legitime și de a genera coduri 2FA de rezervă.**

Dispozitive securizate

Pe lângă conturi, este esențial să mențineți toate dispozitivele – computere, telefoane, unități USB, unități de hard disk externe – bine protejate.

O asemenea protecție începe prin a fi atenți la ce timp de dispozitive sunt achiziționate și folosite de organizația și personalul dvs. Toți furnizorii sau producătorii pe care îi selectați trebuie să aibă un istoric demonstrat de a respecta standardele globale privind dezvoltarea sigură a dispozitivelor hardware (precum telefoanele sau computerele). Toate dispozitivele pe care le achiziționați sunt produse de companii de încredere care nu sunt încurajate să dezvăluie date și informații unui potențial adversar. Este important de notat că guvernul chinez obligă companiile chineze să furnizeze date guvernului central. Prin urmare, în ciuda omniprezenței smartphone-urilor necostisitoare precum Huawei sau ZTE, acestea trebuie evitate. Cu toate că prețul echipamentelor hardware ieftine poate fi atractiv pentru organizația dvs., potențialele riscuri de securitate pentru organizațiile care susțin democrația, drepturile umane sau responsabilitatea ar trebui să vă îndrepte spre alte opțiuni de dispozitive, având în vedere că accesul la date ajută guvernul chinez și alte guverne să vizeze anumite persoane și comunități. Adversarii dvs. pot compromite securitatea dispozitivelor dvs. - și tot ceea ce faceți folosind aceste dispozitive - fie prin accesarea fizică, fie prin accesarea „de la distanță" a dispozitivelor dvs.

Securitatea dispozitivelor și societatea civilă

Unele dintre cele mai avansate software-uri rău intenționate din lume au fost dezvoltate și implementate în întreaga lume pentru a ataca organizații ale societății civile și apărători ai drepturilor omului. În India, de exemplu, Amnesty International a raportat că cel puțin nouă apărători ai drepturilor omului au fost atacați în 2020 printr-un program spion (un tip de software rău intenționat) pe dispozitivele mobile și computerele lor. Programul spion a fost trimis printr-o serie de e-mailuri de tip phishing care conțineau linkuri către fișiere infectate partajate prin Firefox Send (un program de partajare de fișiere în prezent suspendat). Dispozitivele persoanelor care deschideau fișierele erau infectate cu un software care înregistra materiale audio, intercepta secvențele pe taste și mesajele și, de fapt, au devenit supravegheate total de către atacatori. Asemenea atacuri, care au frecvent drept țintă grupurile societății civile și membrii acestora, le permit frecvent atacatorilor, din păcate, să obțină accesul „de la distanță" asupra dispozitivelor.

ACCESUL FIZIC LA DISPOZITIVE, ÎN URMA PIERDERII SAU FURTULUI

Pentru a preveni compromiterea fizică, este esențial să asigurați siguranța dispozitivelor dvs. Pe scurt, nu ușurați eforturile unui adversar de a vă fura sau chiar însuși temporar dispozitivul. Păstrați dispozitivele încuiate dacă le lăsați acasă sau într-un birou. Sau, dacă credeți că este mai sigur, luați-le cu dvs. Aceasta înseamnă, desigur, că parte a securității dispozitivelor o reprezintă securitatea fizică a spațiilor de lucru (fie la birou, fie acasă). Va trebui să instalați încuietori solide, camere de supraveghere sau alte sisteme de monitorizare - în special dacă organizația dvs. prezintă un risc ridicat. Amintiți personalului să trateze dispozitivele în același mod în care ar trata un teanc gros de bani - nu le lăsați la vedere, nesupravegheate sau neprotejate.

Ce fac dacă mi se fură un dispozitiv?

Pentru a limita impactul în cazul în care cineva reușește să fure un dispozitiv – sau chiar dacă persoana respectivă doar obține acces la acesta pentru o scurtă perioadă de timp – **impuneți utilizarea de parole sau coduri de acces puternice pe computerele și telefoanele tuturor.** Aceleași sfaturi privind parolele din secțiunea Parole a acestui Îndrumar se aplică și unei parole bune pentru un computer sau un laptop. Pentru blocarea telefonului, folosiți coduri care conțin cel puțin între șase și opt cifre și evitați utilizarea de „șablon de desen" pentru a debloca telefonul Pentru sfaturi suplimentare privind blocarea ecranului, consultați ghidul Data Detox Kit oferit de Tactical Tech. Utilizarea de parole bune pentru dispozitive îngreunează mult efortul unui adversar de a accesa rapid informațiile de pe dispozitivul dvs. în caz de furt sau confiscare. Dacă folosiți unui cod de acces puternic, activarea recunoașterii faciale sau deblocarea prin amprentă sunt permise, însă asigurați-vă că le dezactivați (lăsând codul de acces) înainte de orice activități care prezintă risc ridicat, precum proteste sau controale la frontieră dacă dvs. și personalul dvs. aveți îngrijorări că dispozitivul ar putea fi confiscat de către autorități. Dacă dețineți dispozitive primite de la organizație care au funcția „Găsește-mi dispozitivul", precum Găsire iPhone pentru iPhone și Găsește-mi dispozitivul pentru Android, solicitați personalului să o activeze. Încurajați personalul să folosească aceste funcții și pentru dispozitivele personale. Având activate aceste funcții, proprietarul dispozitivului (sau o persoană de contact de încredere) poate localiza dispozitivul sau îi poate șterge conținutul de la distanță în cazul în care acesta este furat, pierdut sau confiscat. Pentru telefoanele iPhone, puteți, de asemenea, configura ștergerea automată a conținutului după mai multe încercări nereușite de autentificare. Aceste funcții de gestionare a dispozitivelor devin de o importanță critică pentru o organizație atunci când un dispozitiv care conține informații sensibile este pierdut sau ajunge pe mâinile cui nu trebuie.

Dar criptarea dispozitivului?

Este important să folosim metode de criptare, să secretizăm datele în așa fel încât acestea să devină imposibil de citit și utilizat, pe toate dispozitivele, în special pe computere și smartphone-uri. Vă recomandăm să configurați, pentru toate dispozitivele din cadrul organizației, așa numita **criptare completă a discului,** dacă este posibil. Prin criptarea completă a discului, întregul conținut al unui dispozitiv este criptat, astfel încât un adversar, dacă l-ar fura fizic, nu ar putea extrage conținutul dispozitivului fără să știe parola sau cheia folosită pentru criptare. Multe smartphone-uri și computere moderne oferă criptarea completă a discului. Dispozitivele Apple precum iPhone și iPad au o opțiune convenabilă de activare a criptării complete a discului atunci când configurați un cod de acces normal pentru dispozitiv. Computerele Apple care folosesc macOS oferă o funcție numită FileVault pe care o puteți activa pentru criptarea completă a discului. Computerele Windows cu licențe pro, enterprise sau education, oferă o funcție numită BitLocker pe care puteți activa pentru criptarea completă a discului. Puteți activa BitLocker urmând aceste instrucțiuni de la Microsoft, care s-ar putea să fie nevoie să fie mai întâi activate de administratorul organizației dvs. Dacă personalul deține doar licențe personale pentru computerele Windows, BitLocker nu este disponibil. Cu toate acestea, puteți totuși activa criptarea completă a discului accesând „Actualizare și securitate" > „Criptare dispozitiv" din setările sistemului de operare Windows.

Dispozitivele Android, începând cu versiunea 9.0, sunt furnizate cu criptarea pe bază de fișiere activată implicit. Criptarea pe bază de fișiere oferită de Android operează diferit de criptarea completă a discului, însă oferă, la rândul său, o securitate puternică. Dacă folosiți un telefon Android relativ nou și ați configurat un cod de acces, criptarea pe bază de fișiere ar trebui să fie activată. Cu toate acestea, este o idee bună să vă verificați setările pentru a vă asigura, în special dacă telefonul dvs. are câțiva ani. Pentru a verifica, accesați Setări > Securitate pe dispozitivul Android. În setările de securitate, ar trebui să vedeți o subsecțiune pentru „criptare" sau „criptare și acreditări", care vă va indica dacă telefonul este criptat și, dacă nu este, vă va permite să activați criptarea.

Pentru computere (fie Windows, fie Mac), este extrem de important să stocați orice cheie de criptare (cunoscute cu denumirea de chei de recuperare) într-un loc sigur. Aceste „chei de recuperare" sunt, în majoritatea cazurilor, niște parole și fraze de acces lungi, în esență. În cazul în care vă uitați parola normală a dispozitivului sau se întâmplă ceva neașteptat (o defectare a dispozitivului, de pildă), cheile de recuperare sunt singura modalitate de a vă recupera datele criptate și, dacă este necesar, de a le transfera pe un nou dispozitiv. Prin urmare, atunci când activați criptarea completă a discului, asigurați-vă că ați salva aceste chei și parole într-un loc sigur, precum un cont de cloud securizat sau managerul de parole al organizației dvs.

ACCESAREA DISPOZITIVULUI DE LA DISTANȚĂ - CUNOSCUT ȘI SUB DENUMIREA DE ACCESARE ILEGALĂ

Pe lângă securizarea fizică a dispozitivelor, este important să le ferim și de software-uri rău intenționate. Security-in-a-Box dezvoltat de Tactical Tech oferă o descriere utilă a ceea ce înseamnă un software rău intenționat și de ce este important să îl evităm, informații ușor adaptate în restul acestei secțiuni.

Înțelegerea și evitarea software-urilor rău intenționate

Există multe moduri de clasificare a software-urilor rău intenționate. Virușii, programele spion, viermii, troienii, rootkit-urile, ransomware-ul și minarea de criptomonedă sunt toate tipuri de software-uri rău intenționate. Anumite tipuri de software-uri rău intenționate se răspândesc pe internet prin e-mailuri, mesaje text, pagini web rău intenționate și alte mijloace. Unele se răspândesc prin dispozitive precum unitățile de memorie USB utilizate pentru schimbul și furtul de date. Și, în vreme ce unele software-uri rău intenționate necesită o greșeală din partea țintei nesuspicioase, altele pot infecta silențios sistemele vulnerabile, fără ca dvs. să faceți ceva greșit.

Pe lângă software-urile rău intenționate generale, care sunt lansate pe scară largă și au ca țintă publicul general, software-urile rău intenționate țintite sunt folosite de regulă pentru a face rău și a spiona anumite persoane, organizații și rețele. Aceste tehnici sunt folosite de infractorii obișnuiți, însă și de armate și servicii de informații, teroriști, hărțuitori online, soți abuzivi și personalități politice necinstite.

Indiferent cum se numesc, indiferent cum sunt distribuite, software-urile rău intenționate pot distruge computerele, fura și distruge date, a duce la faliment organizații, invada intimitatea și expune utilizatorii la riscuri. Pe scurt, software-urile rău intenționate sunt foarte periculoase. Cu toate acestea, există câțiva pași simpli pe care organizația dvs. îi poate urma pentru a se proteja de amenințările comune.

Ne va proteja un program de protecție împotriva software-ului rău intenționat?

Programele de protecție împotriva software-ului rău intenționat nu sunt, din păcate, o soluție completă. Totuși, este o idee bună să folosiți inițial un program de bază gratuit. Software-urile rău intenționate se modifică cu rapiditate, dând naștere la noi riscuri atât de frecvent încât niciun astfel de instrument nu poate oferi protecție completă.

Dacă folosiți Windows, aruncați o privire peste programul integrat Windows Defender. Computerele Mac și Linux nu sunt prevăzute cu programe integrate de protecție împotriva software-ului rău intenționat și nici dispozitivele Android și iOS. Puteți instala un instrument gratuit cu reputație bună precum Bitdefender sau Malwarebytes pentru aceste dispozitive (și pentru computerele Windows). **Dar nu vă bazați pe acesta ca unică linie de apărare,** deoarece nu va face cu siguranță față în fața atacurilor noi, țintite.

În plus, asigurați-vă că descărcați doar programe de protecție împotriva software-ului rău intenționat și antivirus cu o reputație bună, din surse legitime (precum site-urile de mai sus). Din păcate, există multe versiuni false sau compromise ale instrumentelor de protecție împotriva software-ului rău intenționat care fac mai mult rău decât bine.

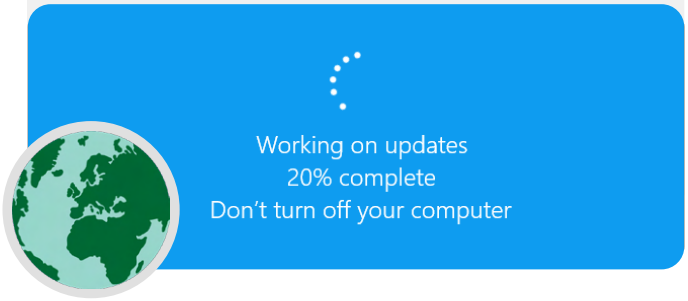
Dacă utilizați Bitdefender sau un alt instrument de protecție împotriva software-ului rău intenționat în organizația dvs., asigurați-vă că nu rulați două programe în același timp. Multe dintre ele vor identifica comportamentul unui program de protecție împotriva software-ului rău intenționat drept suspect și îl va opri, iar ambele vor funcționa defectuos. Bitdefender sau alte programe de protecție împotriva software-ului rău intenționat pot fi actualizate gratuit, iar programul integrat Windows Defender primește actualizări odată cu computerul. Asigurați-vă că programul de protecție împotriva software-ului rău intenționat se actualizează automat regulat (anumite versiuni de încercare ale software-urilor comerciale furnizate împreună cu computerul vor fi dezactivate după expirarea perioadei de încercare, devenind mai mult periculoase decât utile). Noi software-uri rău intenționate sunt scrise și distribuite zi de zi, iar computerul dvs. va deveni și mai vulnerabil dacă nu țineți pasul cu noile definiții și tehnici rău intenționate. Dacă este posibil, vă recomandăm să vă configurați software-ul să instaleze automat actualizările. Dacă programul dvs. de protecție împotriva software-ului rău intenționat are funcția opțională „activat permanent”, activați-o și scanați ocazional toate fișierele de pe computer.

Mențineți dispozitivele la zi

Actualizările sunt esențiale. Utilizați cea mai recentă versiune a sistemelor de operare ale dispozitivelor (Windows, Mac, Android, iOS etc) și mențineți sistemul de operare la zi. Mențineți la zi și celelalte software-uri, browsere și toate pluginurile de browser. Instalați actualizările imediat ce acestea devin disponibile, ideal prin activarea actualizărilor automate. Cu cât este mai la zi sistemul de operare al dispozitivului, cu atât mai puțin vulnerabil este acesta. Comparați actualizările cu un plasture aplicat pe o rană deschisă: protejează împotriva vulnerabilității și reduce semnificativ șansa de infectare. De asemenea, dezinstalați software-urile pe care nu le mai folosiți. Software-urile neactualizate prezintă adesea probleme de securitate și s-ar putea să fie instalat un instrument care nu mai este actualizat de dezvoltator, lăsându-l mai vulnerabil în fața hackerilor.

Software-urile rău intenționate în realitate Actualizările sunt esențiale

În 2017, atacurile ransomware WannaCry au infectat milioane de dispozitive din întreaga lume, sistând activitatea mai multor spitale, entități guvernamentale, organizații și companii mari și mici din mai multe țări. De ce a fost atât de eficient atât atacul? Din cauza sistemelor de operare Windows neactualizate, „fără corecție", dintre care multe au fost inițial piratate. O mare parte din daune – umane și financiare – ar fi putut fi evitate cu practici mai bune de actualizare automată și prin utilizarea unor sisteme de operare legitime.



Fiți precauți cu unitățile USB

Aveți grijă când deschideți fișiere care vă sunt trimise drept atașări, prin linkuri de descărcare sau prin orice alte metode. De asemenea, **gândiți-vă de două ori înainte de a introduce suporturi amovibile precum unități USB**, carduri de memorie flash, DVD-uri și CD-uri în computer, deoarece ar putea fi vectori de software-uri rău intenționate. Există o mare probabilitate ca unitățile USB care au fost partajate pentru o perioadă de timp să conțină viruși. Pentru opțiuni alternative de a partaja fișiere în siguranță în cadrul organizației, consultați secțiunea Partajare fișiere a Îndrumarului.

Fiți foarte precauți și cu orice alte dispozitive pe care le conectați prin Bluetooth. Este în regulă să vă sincronizați telefonul sau computerul cu un difuzor Bluetooth de încredere pentru a reda muzica preferată, însă fiți atenți atunci când asociați sau acceptați solicitări de la orice dispozitive pe care nu le recunoașteți. Acceptați doar conexiunile la dispozitive de încredere și nu uitați să dezactivați Bluetooth atunci când nu îl folosiți.

Navigați inteligent pe internet

Nu acceptați niciodată și nu rulați aplicații care provin de pe site-uri pe care nu le cunoașteți și în care nu aveți încredere. În loc să acceptați o „actualizare" oferită de o fereastră pop-up a browserului, de exemplu, verificați dacă există actualizări pe site-ul oficial al aplicației respective. Așa cum am discutat în secțiunea Phishinga acestui Îndrumar, este esențial să fiți precauți atunci când navigați pe site-uri web. Verificați destinația unui link (prin trecerea cu mouse-ul peste acesta) înainte de a face clic și verificați rapid adresa site-ului după ce urmați un link și asigurați-vă că pare corectă înainte de a introduce informații sensibile precum parolele. Nu faceți clic pe mesajele de eroare sau pe atenționări și fiți atenți la ferestrele de browser care apar automat și citiți-le cu atenție, în loc să apăsați pur și simplu pe Da sau OK.

Dar smartphone-urile?

La fel ca în cazul computerelor, actualizați sistemul de operare și aplicațiile din telefon și activați actualizările automate. Instalați doar din surse oficiale sau de încredere precum Google Play și App Store (sau F-droid, un magazin de aplicații open-source gratuit pentru Android). Aplicațiile pot conține software-uri rău intenționate și pot părea că funcționează normal, prin urmare nu veți ști întotdeauna dacă sunt rău intenționate. De asemenea, asigurați-vă că descărcați versiunea legitimă a aplicației. În special în cazul dispozitivelor Android, există versiuni „false" ale aplicațiilor populare. Asigurați-vă că o aplicație este creată de o companie reală sau de un dezvoltator real, are recenzii bune și un număr de descărcări corespunzător o versiune falsă a WhatsApp poate avea doar câteva mii se descărcări, în vreme ce versiunea reală are peste cinci miliarde. Fiți atenți la permisiunile pe care le solicită aplicația. Dacă par excesive (de pildă, un calculator vă solicită acces la camera foto, sau Angry Birds vă solicită acces la locație), refuzați solicitarea sau dezinstalați aplicația. Dezinstalarea aplicațiilor pe care nu le mai folosiți poate ajuta, de asemenea, la protejarea smartphone-ului sau tabletei dvs. Uneori, dezvoltatorii vând dreptul de proprietate aplicațiilor altor persoane. Acești noi proprietari ar putea încerca să câștige bani adăugând coduri rău intenționate.

Software-urile rău intenționate în realitate Aplicații mobile rău intenționate

Hackerii din mai multe țări folosesc, de ani de zile, aplicații false din Google Play pentru a distribui software-uri rău intenționate. Un **exemplu în acest sens** care a vizat utilizatorii din Vietnam a ieșit la iveală în aprilie 2020. Această campanie de spionaj folosea aplicații false, care chipurile ajutau utilizatorii să găsească puburi în apropiere sau să caute informații despre bisericile locale. Odată instalate de utilizatorii Android inocenți, aplicațiile rău intenționate colectau jurnale de apeluri, date privind locația și informații despre contacte și mesaje text. Acesta este doar unul dintre numeroasele motive pentru care trebuie să fiți atenți ce aplicații descărcați pe dispozitivele dvs.

Economisiți bani și sporiți securitatea dispozitivelor folosind Tails

O opțiune foarte sigură care necesită niște abilități tehnice pentru configurare este sistemul de operare **Tails**. Acest sistem de operare portabil poate fi folosit gratuit și poate fi instalat direct de pe o unitate USB, nemaifiind necesar să vă bazați pe sisteme de operare Windows sau Mac licențiate. Tails este o opțiune bună și pentru cei care prezintă un risc extrem de mare, deoarece încorporează o gamă largă de funcții de îmbunătățire a confidențialității. Aceste funcții includ integrarea Tor (discutat mai sus) pentru a securiza traficul web și ștergerea completă a memoriei de fiecare dată când închideți sistemul de operare. Aceste funcții vă permit în esență să începeți de la zero de fiecare dată când reporniți computerul. Tails are și un mod de persistență, care vă permite să salvați fișiere importante și setări în mai multe sesiuni dacă doriți.

O altă opțiune de sistem de operare sigur gratuit este **Qubes OS**. Cu toate că nu este cea mai simplă opțiune pentru utilizatorii fără abilități tehnice, Qubes este destinat limitării amenințărilor software-urilor rău intenționate și reprezintă o altă opțiune de luat în considerare pentru utilizatorii mai avansați și expuși la riscuri ridicate din cadrul organizației dvs., în special dacă costurile asociate cu licențele sunt o provocare.

Ce se întâmplă în cazul în care nu ne permitem un software legal?

Achiziționarea unor versiuni licențiate ale unor software-uri populare precum t Office (Word, Powerpoint, Excel) pentru întreaga organizație ar putea fi costisitoare, însă un buget limitat nu este o scuză să descărcați versiuni piratate sau să nu le actualizați. Nu este o chestiune de moralitate – este o chestiune de securitate. Software-urile piratate sunt conțin frecvent software-uri rău intenționate și adeseori nu pot fi corectate pentru vulnerabilitate. Dacă nu vă puteți permite software-ul de care are nevoie organizația dvs., există o varietate largă de opțiuni open-source gratuite precum LibreOffice (care înlocuiește aplicațiile Microsoft Office standard) sau GIMP (care înlocuiește Photoshop) care pot veni în întâmpinarea nevoilor dvs. Luați, de asemenea, în considerare înregistrarea pe Tech Soup, o organizație care oferă organizațiilor non-profit reduceri semnificative la software-uri populare. Chiar dacă vă permiteți software-uri și aplicații legitime, dispozitivul dvs. va fi expus în continuare riscului dacă sistemul de operare subiacent nu este legitim. Așadar, dacă organizația dvs. nu își permite licențe Windows, luați în considerare alternative mai ieftine precum Chromebooks, care sunt o opțiune excelentă și ușor de securizat dacă organizația dvs. lucrează mai mult în cloud. Dacă folosiți Google Docs sau Microsoft 365, nu aveți nevoie de multe aplicații desktop - editoarele în browser gratuite pentru documente și foi de calcul sunt mai mult decât eficiente pentru aproape orice utilizare. O altă opțiune, dacă aveți personal cu abilități tehnice, este de a instala un sistem de operare Linux gratuit (o alternativă open-source la sistemele de operare Windows și Mac) pe fiecare computer. O opțiune populară Linux destul de ușor de utilizat este Ubuntu. Indiferent de sistemul de operare ales, asigurați-vă că o persoană din cadrul organizației dvs. este responsabilă pentru verificarea regulată cu personalul, pentru a vedea dacă s-au aplicat ultimele actualizări.

Atunci când optați pentru un nou instrument sau sistem, gândiți-vă cum îl poate sprijini tehnic și financiar organizația dvs. pe termen lung. Puneți-vă întrebări precum: Vă puteți permite să angajați și să păstrați personalul necesar pentru întreținerea acestuia? Puteți plăti abonamentele recurente? Aveți acces la reduceri de grup precum Tech Soup, menționat anterior? Răspunsul la aceste întrebări vă pot ajuta să vă asigurați că strategiile dvs. software și tehnologice vor fi mai eficiente în timp.

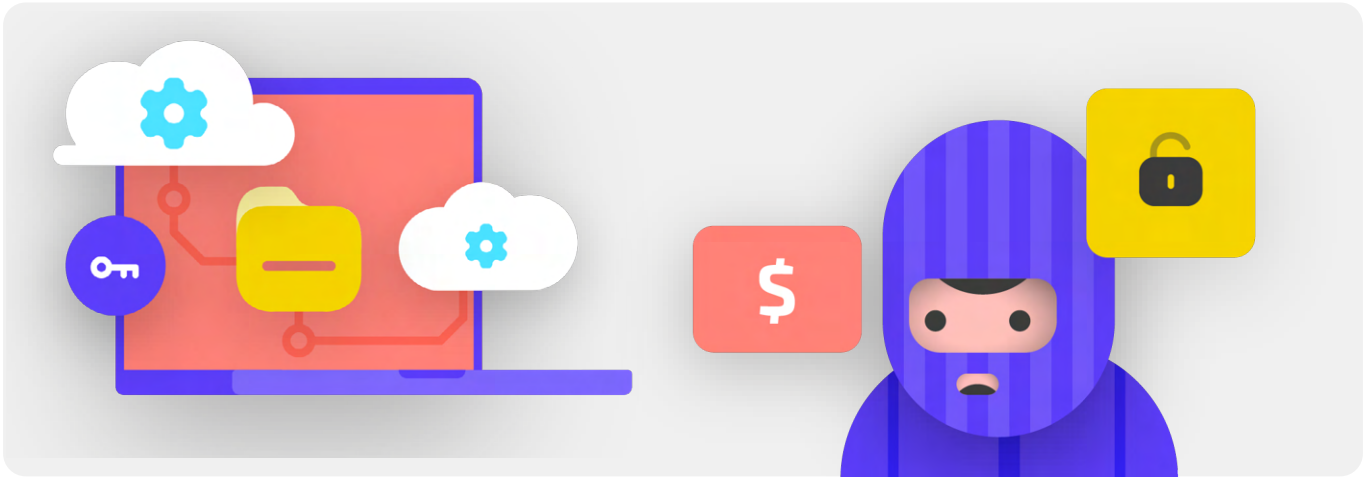
Securizarea dispozitivelor

- **Instruiți personalul privind riscurile de software-uri rău intenționate și cele mai bune practici pentru a le evita.**
  - Furnizați politici privind conectarea dispozitivelor externe, accesarea linkurilor, descărcarea de fișiere și aplicații și verificarea permisiunilor pentru software-uri și aplicații.
- **Impuneți actualizarea permanentă a dispozitivelor, software-urilor și aplicațiilor.**
  - Activați actualizările automate, dacă este posibil.
- **Asigurați-vă că toate dispozitivele folosesc software-uri licențiate.**
  - În cazul în care costurile sunt prohibitive, optați pentru o alternativă gratuită.
- **Impuneți protecția cu parolă a tuturor dispozitivelor din cadrul organizației, inclusiv a dispozitivelor mobile personale care sunt folosite pentru comunicări de serviciu.**
- **Activați criptarea completă a discului pe dispozitive.**
- **Reamintiți frecvent personalului să își securizeze fizic dispozitivele - și puneți la dispoziție spații încuiate și alte modalități de securizare a computerelor.**
- **Nu partajați fișiere cu ajutorul unităților USB sau nu conectați unități USB la computerele dvs.**
  - Folosiți, în schimb, opțiuni alternative sigure de partajare a fișierelor.

Phishing: O amenințare frecventă pentru dispozitive și conturi

Atacurile de tip phishing sunt cele mai frecvente și eficiente atacuri asupra organizațiilor din întreaga lume. Tehnica este folosită de cele mai sofisticare armate naționale, precum și hoții mărunți.

Pe scurt, atacurile de tip phishing sunt încercări ale unui adversar de a vă păcăli să partajați informații care ar putea fi folosite împotriva dvs. și organizației dvs. Atacurile de tip phishing pot fi realizate prin intermediul e-mailurilor, mesajelor text/SMS (cunoscute adesea sub denumirea de SMS phishing sau „smishing"), aplicațiilor de mesagerie precum WhatsApp, mesajelor sau postărilor de pe rețele sociale sau apelurilor telefonice (cunoscute adesea sub denumirea de phishing vocal sau „vishing"). Mesajele de tip phishing ar putea încerca să vă determine să tastați informații sensibile (precum parolele) pe un site web fals pentru a obține acces la un cont, să partajați informații confidențiale (precum numărul unui card de credit) prin mesaj vocal sau text, sau v-ar putea convinge să descărcați un software rău intenționat care să vă infecteze dispozitivul. De exemplu, milioane de persoane primesc zilnic apeluri telefonice automate false prin care sunt informate că le sunt compromise conturile bancare sau că li s-a furat identitatea - acestea au scopul de a păcăli persoanele naive să partajeze informații sensibile.



CUM IDENTIFICĂM PHISHINGUL?

Phishingul poate părea cumplit și imposibil de detectat, însă există câțiva pași simpli pe care orice membru al organizației dvs. îi poate urma pentru a se proteja împotriva majorității atacurilor. Următoarele sfaturi pentru protejarea împotriva phishingului au fost modificate și extinse pornind de la ghidul aprofundat privind phishingul dezvoltat de Freedom of the Press Foundation și trebuie distribuite la nivelul organizației dvs. (și altor persoane de contact) și integrate în planul dvs. de securitate:

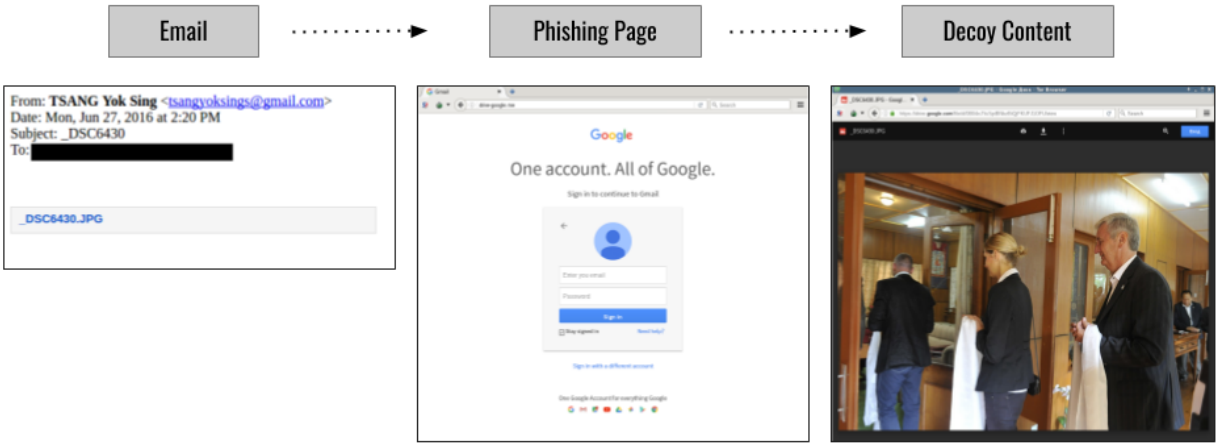
Uneori, câmpul „De la” este mincinos

Câmpul „De la” din e-mailurile dvs. poate fi fals sau falsificat pentru a vă păcăli. Atacatorii creează frecvent adrese de e-mail care sunt asemănătoare cu cele legitime care vă sunt familiare, dar conțin mici erori de ortografie, pe care e posibil să nu le sesizați. De exemplu, ați putea primi un e-mail de la cineva cu adresa „john@goooogle.com”, în loc de „john@google.com”. Observați că cuvântul „google” conține mai multe o-uri. De asemenea, e posibil să știți pe cineva care are adresa de e-mail „john@gmail.com”, dar să primiți un e-mail de tip phishing de la un personificator care a creat adresa „johm@gmail.com” - singura diferență este un subtil schimb de litere la final. Verificați întotdeauna adresa expeditorului unui e-mail înainte de a continua. Un concept similar se aplică și phishingului prin mesaje text, apeluri vocale sau aplicații de mesagerie. Dacă primiți un mesaj de la un număr necunoscut, gândiți-vă de două ori înainte să răspundeți sau să interacționați cu mesajul.

Phishingul și societatea civilă

Atacurile sofisticate personalizate de tip phishing au ca țintă, zi de zi, grupuri ale societății civile din întreaga lume.

Un exemplu de asemenea atac este evidențiat în raportul The Citizen Lab din 2018, Spionarea necostisitoare: Detalii de interior ale unei operațiuni de phishing care a vizat comunitatea tibetană. Acest atac de tip phishing foarte ieftin și simplu - însă incredibil de eficient - a avut ca țintă apărători tibetani ai drepturilor omului și alți activiști. Atacul a început cu un e-mail de tip phishing (prezentat în partea stângă) trimis de pe o adresă Gmail standard, care conținea doar un link către un fișier imagine. Dacă era accesat, linkul direcționa ținta la o pagină falsă de autentificare de e-mail Google (prezentată în mijloc) care era folosită pentru a fura acreditările contului. Dacă victimele furnizau acreditările pe pagina falsă, conturile lor puteau fi compromise cu ușurință. După furnizarea numelui de utilizator și a parolei pe site-ul fals, victimele erau redirecționate la o imagine (prezentată în dreapta) care ilustra câțiva delegați într-o întâlnire tibetană. Imaginea era o capcană care făcea țintele să creadă că s-au autentificat în conturile Google reale și care avea rolul de a reduce orice posibile suspiciuni privind adevărata natură rău intenționată a e-mailului.



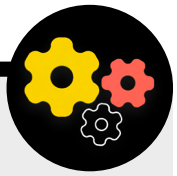
Atenție la atașări

Atașările pot conține software-uri rău intenționate sau viruși și însoțesc, de regulă, e-mailurile de tip phishing. **Cea mai bună metodă de a evita software-urile rău intenționate din atașări este să nu le descărcați niciodată.** Ca regulă generală, nu deschideți imediat atașările, în special dacă provin de la persoane pe care nu le cunoașteți. Dacă este posibil, rugați persoana respectivă să vă trimită documentul prin copiere și lipire într-un e-mail sau să partajeze documentul printr-un serviciu precum Google Drive sau Microsoft OneDrive, care au funcții integrate de scanare pentru majoritatea documentelor încărcate pe platformele lor. Construiți, în cadrul organizației, o cultură în care atașările sunt descurajate.
Dacă trebuie neapărat să deschideți o atașare, deschideți-o doar într-un mediu sigur (consultați secțiunea Nivel avansat de mai jos) în care potențialele software-uri rău intenționate nu pot fi implementate pe dispozitivul dvs.

Dacă folosiți Gmail și primiți o atașare la un e-mail, în loc să o descărcați și să o deschideți în computer, faceți clic pe fișierul atașat și citiți-l în modul de previzualizare direct în browser. Acest pas vă permite să vizualizați textul și conținutul unui fișier fără a-l descărca sau a-i permite să încarce un potențial software rău intenționat pe computerul dvs. Această metodă este eficientă în cazul documentelor Word, PDF și chiar al prezentărilor PowerPoint. Dacă trebuie să editați documentul, puteți deschide fișierul într-un program cloud precum Google Drive și puteți converti fișierul într-un Google Doc sau Google Slides.

Dacă folosiți Outlook, puteți previzualiza atașările în mod similar, fără a le descărca, folosind clientul web Outlook. Dacă trebuie să editați o atașare, o puteți deschide în OneDrive, dacă îl aveți la dispoziție. Dacă folosiți Yahoo Mail, se aplică același concept. Nu descărcați atașări, vă recomandăm să le previzualizați direct în browserul web.

Indiferent de instrumentele pe care le aveți la dispoziție, cea mai bună abordare este pur și simplu să nu descărcați niciodată atașări pe care nu le cunoașteți sau în care nu aveți încredere și, indiferent de cât de importantă ar putea părea o atașare, să nu deschideți niciodată o atașare care conține un tip de fișier pe care nu îl recunoașteți sau nu aveți intenția să îl folosiți vreodată.



Protejarea împotriva phishingului la nivelul organizației dvs.

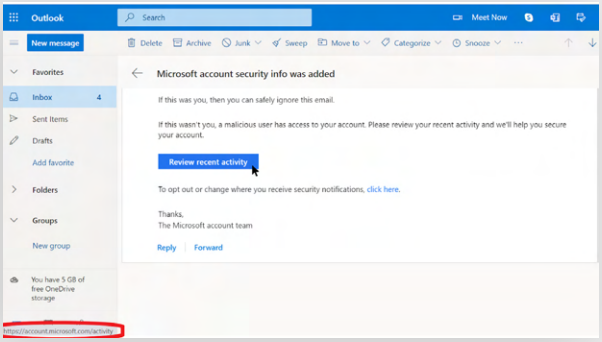
Dacă organizația dvs. folosește Microsoft 365 pentru întreprinderi pentru e-mail și alte aplicații, administratorul domeniului dvs. trebuie să configureze Politica privind atașările sigure pentru protejarea împotriva atașărilor periculoase. Dacă folosiți Google Workspace pentru întreprinderi (cunoscut anterior sub denumirea de GSuite), există o opțiune similar eficientă pe care administratorul trebuie să o configureze, numită Google Security Sandbox. Utilizatorii mai avansați ar putea configura programe sandbox sofisticate, precum Dangerzone sau, pentru cei care folosesc versiunea Pro sau Enterprise a Windows 10, Windows Sandbox. O altă opțiune avansată pe care o puteți implementa la nivelul organizației este un serviciu de filtrare Sistem nume de domeniu (DNS). Organizațiile pot folosi această tehnologie pentru a împiedica personalul să acceseze sau să interacționeze accidental cu conținut rău intenționat, oferind un nivel suplimentar de protecție împotriva phishingului. Noi servicii precum Gateway de la Cloudflare oferă asemenea capabilități organizațiilor, fără a necesita sume mari de bani (Gateway, de exemplu, este gratuit pentru până la 50 de utilizatori). Alte câteva instrumente gratuite, inclusiv Quad9 din kitul de instrumente al Global Cyber Alliance, vă vor împiedica să accesați site-uri cunoscute care conțin viruși sau alte software-uri rău intenționate și pot fi implementate în mai puțin de cinci minute.

Atenție pe ce faceți clic

Fiți sceptici în ceea ce privește linkurile din e-mailuri sau alte mesaje text. Linkurile pot fi capcane pentru descărcarea de fișiere rău intenționate sau vă pot direcționa la site-uri false care v-ar putea solicita să furnizați parole sau alte informații sensibile. Pe computer, există un truc simplu de a vă asigura că un link dintr-un e-mail sau mesaj vă va trimite unde trebuie: Folosiți mouse-ul să treceți peste link înainte de a face clic pe acesta și uitați-vă în partea de jos a ferestrei browserului pentru a vedea care este URL-ul real (ca în imaginea de mai jos).

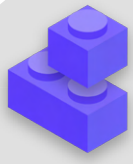
Este mai dificil să verificați linkurile dintr-un e-mail de pe un dispozitiv mobil fără a face clic pe el accidental - așadar, mare atenție. Puteți verifica destinația unui link pe majoritatea smartphone-urilor apăsând lung (și menținând apăsat) pe un link până când apare URL-ul complet.
În cazul atacurilor de tip phishing prin SMS și aplicații de mesagerie, linkurile prescurtate sunt o practică foarte comună utilizată pentru a deghiza destinația unui URL. Dacă observați un link scurt (de ex., bit.ly sau tinyurl.com) în locul URL-ului complet nu faceți clic pe el. Dacă linkul este important, copiați-l într-un extensor de URL, precum https://www.expandurl.net/, pentru a vedea destinația reală a URL-ului prescurtat. Mai mult, nu faceți clic pe linkuri către site-uri web care nu vă sunt familiare. Dacă aveți îndoieli, căutați site-ul punându-i numele între ghilimele (de ex., „www.badwebsite.com”) pentru a vedea dacă este un site legitim. De asemenea, puteți verifica linkurilor suspecte cu ajutorul scanerului URL VirusTotal. Această metodă nu este 100% exactă, însă este o bună metodă de precauție.

În final, dacă faceți clic pe un link dintr-un mesaj și vi se cere să vă autentificați undeva, nu faceți acest lucru decât dacă sunteți 100% siguri că e-mailul este legitim și vă trimite la site-ul adecvat. Multe atacuri de tip phishing vor furniza linkuri care vă vor trimite la pagini false se autentificare pentru Gmail, Facebook sau alte site-uri populare. Nu cădeți în capcană. Puteți deschide un nou browser și accesa direct un site cunoscut precum Gmail.com, Facebook.com etc. dacă doriți sau trebuie să vă autentificați. Astfel, veți putea și accesa conținutul, în siguranță – dacă a fost legitim de la început.



Ce trebuie să facem când primim un mesaj phishing?

Dacă cineva din cadrul organizației dvs. primește o atașare, un link, o imagine nesolicitate sau orice alt mesaj sau apel suspect, este important să raportați imediat responsabilului cu securitatea IT din organizația dvs. Dacă nu aveți un responsabil, trebuie să numiți unul ca parte a dezvoltării planului de securitate. De asemenea, personalul poate raporta e-mailul ca spam sau phishing direct în Gmail sau Outlook.
Implementarea unui plan de acțiune pentru personal și voluntari în cazul în care aceștia primesc un mesaj potențial de tip phishing este de o importanță crucială. În plus, vă recomandăm să urmați aceste bune practici privind phishingul - nu faceți clic pe linkuri suspecte, evitați atașările și verificați adresa „De la” - și să le partajați celorlalte persoane cu care lucrați, preferabil prin intermediul unui canal de comunicare utilizat pe scară largă. Prin aceasta, demonstrați că vă pasă de oamenii cu care comunicați și că încurajați, în rețeaua dvs., o cultură care este alertă și conștientă de pericolele phishingului. Siguranța dvs. depinde de organizațiile în care aveți încredere și vice versa. Practicile mai bune protejează pe toată lumea.
Pe lângă partajarea sfaturilor de mai sus personalului și voluntarilor dvs., puteți identifica phishingul și cu ajutorul acestui chestionar Google privind phishingul. Vă recomandăm, de asemenea, să organizați instruiri regulate privind phishingul pentru personal, pentru a testa conștientizarea și a menține oamenii vigilenți. Aceste instruiri pot fi sub forma unor întâlniri regulate sau pot fi mai puțin formale. Important este ca toți membrii organizației dvs. să se simtă în largul lor să adreseze întrebări despre phishing, raportarea phishingului (chiar și dacă cred că e posibil să fi făcut o greșeală, de pildă, făcând clic pe un link) și ca toată lumea să aibă dreptul de a contribui la apărarea organizației împotriva acestui impact important și riscului ridicat de amenințări.



Phishing

- **Instruiți regulat personalul privind definiția phishingului și cum să îl identifice și să se apere de el, inclusiv phishingul prin mesaje text, aplicații de mesagerie și apeluri telefonice, nu doar prin e-mail.**
- **Reamintiți frecvent personalului de cele mai bune practici, precum:**
  - Nu descărcați atașări necunoscute sau potențial suspecte.
  - Verificați URL-ul unui link înainte de a face clic pe acesta. Nu faceți clic pe linkuri necunoscute sau potențial suspecte.
  - Nu furnizați informații sensibile sau confidențiale prin e-mail, mesaje text sau apeluri telefonice unor persoane sau adrese necunoscute sau neconfirmate.
- **Încurajați raportarea phishingului.**
  - Dezvoltați un mecanism de raportare și o persoană responsabilă pentru phishing în cadrul organizației dvs.
  - Recompensați raportarea și nu pedepsiți greșelile.

Comunicarea și stocarea securizată a datelor

Comunicările și partajarea de date

Pentru a lua cele mai bune decizii pentru organizația dvs. în ceea ce privește metoda de comunicare, este esențial să înțelegeți diferitele tipuri de protecție de care pot dispune comunicările noastre și de ce este importantă această protecție.

Unul dintre cele mai importante elemente ale securității comunicărilor presupune menținerea confidențialității comunicărilor private - lucru are, în vremurile moderne, este realizat prin criptare. Fără o criptare adecvată, comunicările interne ar putea fi interceptate de adversari. Comunicările nesigure pot da în vileag informații și mesaje sensibile sau stânjenitoare, divulga parole sau alte date confidențiale și ar putea expune personalul și organizația la riscuri, în funcție de natura comunicărilor dvs. și conținutului partajat.

Comunicări securizate și societatea civilă

Mii de activiști și organizații pentru democrație și drepturile omului se bazează pe canale sigure de comunicare, zi de zi, pentru a menține confidențialitatea conversațiilor în medii politice dificile. Fără aceste practici de securitate, mesajele sensibile pot fi interceptate și utilizate de autorități pentru a viza activiști și a înăbuși proteste. Un exemplu evident și bine documentat al acestei chestiuni a survenit în perioada ulterioară alegerilor in Belarus din 2010. După cum se detaliază în acest raport Amnesty International, înregistrări telefonice și alte comunicări necriptate au fost interceptate de către guvern și folosite în instanță împotriva unor politicieni proeminenți și unor activiști. Mulți dintre aceștia au fost pedepse cu închisoarea. În 2020, în timpul unui alt val de proteste post-electorale din Belarus, mii de protestatari au folosit aplicații de mesagerie sigure ușor de utilizat, care nu erau disponibile zece ani mai devreme, pentru a-și proteja comunicările sensibile.

CE ESTE CRIPTAREA ȘI DE CE ESTE IMPORTANTĂ?

Criptarea este un proces matematic folosit pentru a secretiza un mesaj sau un fișier, astfel încât doar o persoană sau o entitate care deține cheia să îl poată „decripta" și citi. Ghid de autoapărare contra supravegherii dezvoltat de Electronic Frontier Foundation oferă o explicație practică (însoțită de grafice) a ceea ce presupune criptarea:

Mesaje necriptate

Fără niciun tip de criptare, toate părțile implicate în retransmisia mesajului și orice persoană care și-ar dori să-l intercepteze pe parcurs îi poate citi conținutul. Un mesaj ca „Bună!" nu ar pune o mare problemă, însă ar putea fi o mare problemă în cazul în care comunicați informații confidențiale sau sensibile care nu ați vrea să fie interceptate de furnizorul de telecomunicații, de internet și de guverne neprietenoase. Din acest motiv, este esențial să evitați utilizarea de instrumente necriptate pentru a trimite mesaje sensibile (și, ideal, orice tip de mesaj). Rețineți că unele dintre cele mai populare metode de comunicare - precum SMS-urile sau apelurile telefonice - operează practic fără criptare (ca în imaginea de mai sus).

În imaginea de mai sus puteți observa cum un smartphone trimite un mesaj text verde necriptat („Bună!") altui smartphone, ilustrat în partea dreaptă. Pe parcurs, un turn de telefonie mobilă (sau, în cazul unui mesaj trimis prin internet, furnizorul de servicii de internet) transmite mesajul serverelor companiei. De aici, acestea trece prin rețeaua unui alt turn de telefonie mobilă, care poate vedea mesajul necriptat „Bună!", iar în final, acesta este direcționat către destinație. Este important de menționat că, fără niciun tip de criptare, toate părțile implicate în retransmisia mesajului și orice persoană care și-ar dori să-l intercepteze pe parcurs îi poate citi conținutul. Un mesaj ca „Bună!" nu ar pune o mare problemă, însă ar putea fi o mare problemă în cazul în care comunicați informații confidențiale sau sensibile care nu ați vrea să fie interceptate de furnizorul de telecomunicații, de internet și de guverne neprietenoase. Din acest motiv, este esențial să evitați utilizarea de instrumente necriptate pentru a trimite mesaje sensibile (și, ideal, orice tip de mesaj). Rețineți că unele dintre cele mai populare metode de comunicare - precum SMS-urile sau apelurile telefonice - operează practic fără criptare (ca în imaginea de mai sus).

Există două metode de criptare a datelor în timpul transmiterii: ***criptarea în stratul de transport*** **și** ***criptarea*** de la un capăt la altul. Este important să cunoașteți tipul de criptare acceptat de un furnizor de servicii atunci când organizația dvs. optează să adopte practici și sistemele mai sigure de comunicare. Aceste diferențe sunt bine explicate în Ghid de autoapărare contra supravegherii pe care îl adaptăm și aici:

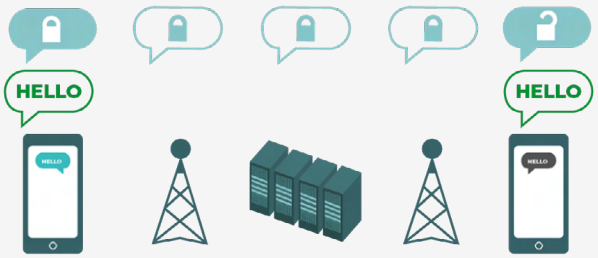
Criptarea în stratul de transport

Criptarea în stratul de transport, cunoscută și sub denumirea de Transport Layer Security (TLS), protejează mesajele în timp ce sunt transportate de la dispozitivul dvs. la serverele aplicațiilor/serviciilor de mesagerie și, de acolo, la dispozitivul destinatarului. Aceasta le protejează de privirile indiscrete ale hackerilor care au acces la rețeaua dvs. sau ale furnizorilor dvs. de servicii de internet și telecomunicații. Cu toate acestea, la mijloc, furnizorul dvs. de servicii de mesagerie/e-mail, site-ul web pe care navigați sau aplicația pe care o folosiți pot vedea copii necriptate ale mesajelor dvs. Având în vedere că mesajele dvs. pot fi văzute (și sunt adesea stocate) de serverele companiei, acestea ar putea fi vulnerabile în fața solicitărilor agențiilor de aplicare a legii sau în fața furtului dacă serverele companiei sunt compromise.

Imaginea de mai sus indică un exemplu de criptare în stratul de transport. În stânga, un smartphone trimite un mesaje verde necriptat: „Bună!" Acest mesaj este criptat și ulterior transmis către un turn de telefonie mobilă. La mijloc, serverele companiei pot decripta mesajul, citi conținutul, decide unde să îl trimită, îl pot recripta și trimite la următorul turn de telefonie mobilă, înspre destinație. La final, celălalt smartphone primește mesajul criptat și îl decriptează pentru a citi „Bună!".

Criptarea de la un capăt la altul

Criptarea de la un capăt la altul protejează mesajele aflate în tranzit tot drumul de la expeditor la destinatar. Se asigură că informațiile sunt transformate într-un mesaj secret de către expeditorul original (primul „capăt") și decodate doar de destinatarul final (cel de-al doilea „capăt"). Nimeni, nici măcar aplicația sau serviciul sau aplicația pe care le utilizați, nu poate „asculta" sau trage cu urechea la activitatea dvs.



Imaginea de mai sus indică un exemplu de criptare de la un capăt la altul. În stânga, un smartphone trimite un mesaje verde necriptat: „Bună!" Acest mesaj este criptat și ulterior transmis către un turn de telefonie mobilă, iar mai apoi la serverele aplicației/serviciului, care nu pot citi conținutul, însă va trimite mesajul secret mai departe la destinatar. La final, celălalt smartphone primește mesajul criptat și îl decriptează pentru a citi „Bună!". Spre deosebire de criptarea în stratul de transport, furnizorul dvs. de internet sau serviciul de mesagerie nu poate decripta mesajul. Doar capetele (dispozitivele originale care trimit și primesc mesaje criptate) au chei de decriptare și citire a mesajului.

DE CE TIP DE CRIPTARE AVEȚI NEVOIE?

Atunci când decideți dacă organizația dvs. are nevoie de criptarea de la un capăt la altul sau de criptare în stratul de transport pentru comunicări (sau o combinație a acestora, pentru diferite sisteme și activități), întrebările majore pe care ar trebui să vi le adresați implică încrederea. De pildă, aveți încredere în aplicația sau serviciul pe care le folosiți? Aveți încredere în infrastructura tehnică a acestora? Aveți îngrijorări referitor la posibilitatea ca un guvern neprietenos să forțeze compania să vă predea mesajele – și, în acest caz, aveți încredere că politicile companiei vă protejează împotriva solicitărilor agențiilor de aplicare a legii?
Dacă răspunsul la oricare dintre aceste întrebări este „nu", aveți nevoie de criptarea de la un capăt la altul. Dacă răspunsul la aceste întrebări este „da", atunci un serviciu care acceptă doar criptarea în stratul de transport poate fi suficient - însă, în general, este mai bine să optați pentru servicii care acceptă criptarea de la un capăt la altul, dacă este posibil.

Atunci când trimiteți mesaje de grup, rețineți că securitatea mesajelor dvs. depinde și de securitatea tuturor destinatarului mesajelor. Pe lângă alegerea cu atenție a unor aplicații și sisteme sigure, este important ca toți membrii grupului să respecte alte cele mai bune practici privind securitatea contului și a dispozitivului. Nu este nevoie decât de un actor rău sau de un dispozitiv infectat pentru a scurge conținutul întregii conversații sau apelului de grup.

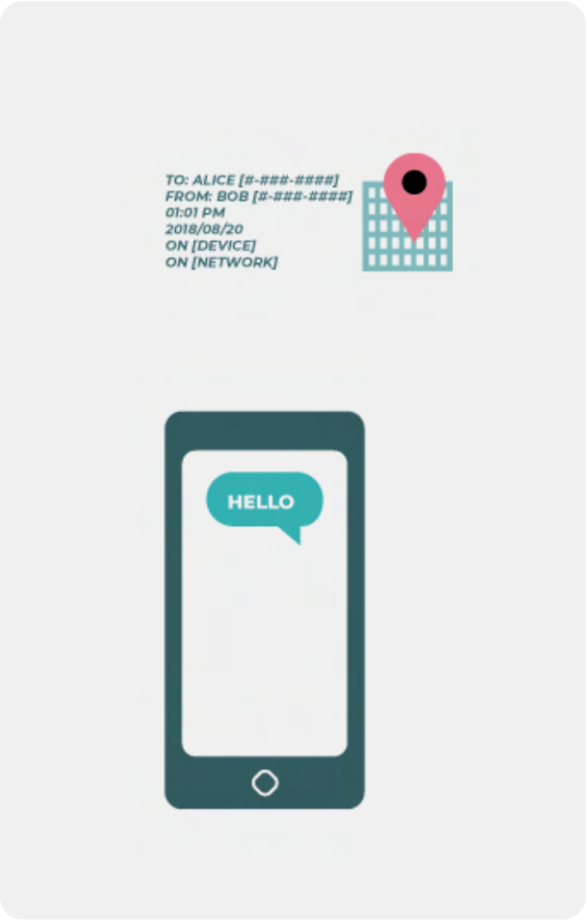
CE INSTRUMENTE DE CRIPTARE DE LA UN CAPĂT LA ALTUL TREBUIE SĂ FOLOSIM (ÎNCEPÂND CU 2022)?

Dacă trebuie să folosiți criptarea de la un capăt la altul, sau doar doriți să adoptați cele mai bune practici, indiferent de contextul amenințărilor asupra organizației dvs., iată câteva exemple de încredere de servicii care, **începând cu 2022,** oferă mesaje și apeluri criptate de la un capăt la altul. Această secțiune a Îndrumarului va fi actualizată regulat online, însă rețineți că lucrurile se schimbă rapid în lumea mesajelor securizate, prin urmare aceste recomandări ar putea să nu mai fie la zi în momentul în care citiți secțiunea. Nu uitați: comunicările dvs. sunt sigure în măsura în care dispozitivul în sine este sigur. Prin urmare, pe lângă adoptarea de practici de trimitere sigură a mesajelor, este esențial să implementați cele mai bune practici descrise în secțiunea Dispozitive securizate a acestui Îndrumar.

Instrumente recomandate de comunicare criptate de la un capăt la altul

MESAJE TEXT (INDIVIDUALE SAU DE GRUP)	• **Signal** • **WhatsApp (doar folosind configurările de setări detaliate mai jos)**
APELURI AUDIO ȘI VIDEO	• **Signal (până la 40 de persoane)** • **WhatsApp (până la 32 de persoane pentru audio și opt pentru video)**
PARTAJAREA FIȘIERELOR	• **Signal** • **Keybase/Keybase Teams** • **OnionShare + o aplicație de mesagerie criptată de la un capăt la altul, precum Signal**

CE SUNT METADATELE ȘI AR TREBUI SĂ REPREZINTE UN MOTIV DE ÎNGRIJORARE?



Cu cine vorbiți dvs. și personalul dvs. și când și unde vorbiți cu persoanele respective pot fi adesea informații la fel de sensibile ca despre ce vorbiți. Este important să rețineți că criptarea de la un capăt la altul protejează doar conținutul („ce") comunicărilor dvs. Aici intră în scenă metadatele. **Ghidul de autoapărare contra supravegherii** al EFF oferă o prezentare generală a metadatelor și explică de ce acestea sunt importante pentru organizații (inclusiv o imagine a acestora):

Metadatele sunt adesea descrise drept toate elementele, cu excepția conținutului comunicărilor dvs. Metadatele sunt un fel de echivalent digital al unui plic. La fel cum un plic conține informații despre expeditor, destinatar și destinația mesajului, aceleași lucruri le implică și metadatele. Metadatele sunt informații despre comunicările digitale pe care trimiteți și primiți.

Iată câteva exemple de metadate:

- persoanele cu care comunicați
- linia de subiect a e-mailurilor dvs.
- durata conversațiilor dvs.
- ora la care a avut loc o conversație
- locația dvs. în momentul comunicării

Chiar și un exemplu nesemnificativ de metadate poate divulga informații confidențiale despre activitatea organizației dvs. Haideți să vedem cât de revelatoare pot fi metadatele pentru hackeri, agenții guvernamentale și companiile care le colectează:

Se știe dacă ați sunat un jurnalist și ați discutat cu el timp de o oră înainte ca jurnalistul respectiv să fi publicat un articol cu un citat anonim. Însă nu se știe despre ce ați discutat.

Se știe că mai mulți membri ai personalului organizației dvs. au trimis mesaje unui instructor local important de securitate digitală. Însă subiectul mesajelor rămâne un secret.

Se știe că ați primit un e-mail de la un centru de testare COVID, că apoi v-ați sunat medicul și ați vizitat site-ul Organizației Mondiale a Sănătății în aceeași oră. Însă nu se cunoaște conținutul e-mailului sau ce ați discutat la telefon.

Se știe că ați primit un e-mail de la un grup local care susține drepturile omului, cu linia de subiect „Spuneți guvernului: nu mai abuzați de puterea voastră". Însă nu se poate accesa conținutul e-mailul.

Metadatele nu sunt protejate de criptarea oferită de majoritatea serviciilor de mesagerie. Dacă trimiteți un mesaj pe WhatsApp, de exemplu, rețineți că, cu toate că conținutul mesajului este criptat de la un capăt la altul, este totuși posibil ca alte persoane să afle cui îi trimiteți mesaje, cât de frecvent faceți acest lucru și, în cazul apelurilor telefonice, care este durata acestora. Prin urmare, luați în considerare la ce riscuri v-ați supune (dacă este cazul) dacă anumiți adversari ar afla cu cine vorbește organizația dvs., când fac acest lucru și (în cazul e-mailurilor) liniile de subiect generale ale comunicărilor organizației dvs.

Unul dintre motivele pentru care **Signal** este atât de recomandat este că, pe lângă furnizarea de criptare de la un capăt la altul, a **introdus funcții și s-a angajat să reducă cantitatea de metadate pe care le stochează și înregistrează**. De pildă, funcția Expeditor sigilat oferită de Signal criptează metadatele despre cine cu cine vorbește, astfel încât Signal cunoaște doar destinatarul mesajului, nu și expeditorul acestuia. Implicit, această funcție funcționează doar atunci când comunicați cu contacte sau profiluri (persoane) existente cu care ați mai comunicat anterior sau pe care i-ați salvat în lista de contacte. Însă puteți activa setarea pentru „Expeditor sigilat" la „Permite pentru toată lumea" dacă este important pentru dvs. să eliminați toate metadatele respective pentru toate conversațiile Signal, chiar și pentru cele purtate cu persoane pe care nu le cunoașteți.

DAR E-MAILUL?

Majoritatea furnizorilor de e-mail, de exemplu, Gmail, Microsoft Outlook și Yahoo Mail, folosesc criptarea în stratul de transport. Așadar, dacă trebuie să comunicați conținut sensibil prin e-mail și aveți îngrijorări că furnizorul de e-mail ar putea fi obligat legal să furnizeze informații despre comunicările dvs. unui guvern sau altui adversar, vă recomandăm să luați în calcul utilizarea unei opțiuni de e-mail cu criptare de la un capăt la altul. Rețineți, totuși, că până și opțiunile de e-mail cu criptare de la un capăt la altul lasă cumva de dorit în ceea ce privește securitatea, de exemplu, necriptarea liniilor de subiect ale e-mailurilor și neprotejarea metadatelor. Dacă trebuie să comunicați informații extrem de sensibile, e-mailul s-ar putea să nu fie cea mai bună opțiune. În schimb, optați pentru opțiuni sigure de mesagerie precum Signal.

Dacă organizația dvs. continuă totuși să folosească e-mailul, este de importanță critică să adoptați un sistem la nivelul întregii organizații. Acest lucru vă ajută să limitați riscurile la care vă expuneți atunci când personalul folosește adrese de e-mail pentru muncă, precum practici ineficiente de securitate a conturilor. De exemplu, prin furnizarea de conturi de e-mail de serviciu personalului dvs., puteți impune cele mai bune practici precum parole puternice și 2FA pentru toate conturile administrate de organizația dvs. În cazul în care, conform analizei de mai sus, este necesară criptarea de la un capăt la altul pentru e-mailul dvs., atât Protonmail, cât și Tutanota, oferă abonamente pentru organizații. Dacă criptarea în stratul de transport este adecvată pentru e-mailul organizații dvs., puteți utiliza opțiuni precum Google Workspace (Gmail) sau Microsoft 365 (Outlook).

CHIAR PUTEM AVEA ÎNCREDERE ÎN WHATSAPP?

WhatsApp este o alegere populară de mesagerie securizată și poate fi o opțiune bună având în vedere omniprezența sa. Unele persoane sunt îngrijorate că este deținut și controlat de Facebook, care lucrează la integrarea acestuia în alte sistemele ale sale. Lumea este îngrijorată și de cantitatea de metadate (adică de informații despre cu cine și când comunicați) pe care WhatsApp le colectează. Dacă alegeți să folosiți WhatsApp ca opțiune securizată de mesagerie, asigurați-vă că ați citit secțiunea de mai sus referitoare la metadate. Există, de asemenea, câteva setări pe care trebuie să le configurați corect. Cel mai important este să vă asigurați că ați dezactivat copiile de rezervă în cloud sau că ați activat măcar noua funcție de copii de rezervă criptate de la un capăt la altul a WhatsApp folosind o cheie de criptare de 64 de cifre sau un cod de acces lung, aleatoriu și unic, salvat într-un loc sigur (precum un manager de parole). De asemenea, asigurați-vă că se afișează notificările de securitate și verificați codurile de securitate. Puteți găsi ghiduri cu instrucțiuni simple de configurare a acestor setări pentru telefoanele Android aici și pentru telefoanele iPhone aici. **Dacă personalul* dvs. și cei cu care comunicați* cu toții nu configurează corect aceste opțiuni, nu vă recomandăm să luați în considerare folosirea aplicației WhatsApp drept opțiune sigură pentru comunicările sensibile care necesită criptarea de la un capăt la altul.** Signal rămâne în continuare cea mai bună opțiune de mesagerie cu criptare de la un capăt la altul, datorită setărilor sale de securitate implicite și protecției metadatelor.

DAR MESAJELE TEXT?

Mesajele text obișnuite sunt extrem de nesigure (SMS-ul standard este practic necriptat) și ar trebui evitate pentru transmiterea oricăror informații care nu sunt destinate publicului. În vreme ce mesajele trimise de pe un iPhone pe alt iPhone (cunoscute drept mesaje iMessage) sunt criptate de la un capăt la altul, dacă în conversație se folosește un alt tip de telefon, mesajele nu sunt securizate. Vă recomandăm să fiți precauți și să **evitați mesajele text pentru transmiterea de informații sensibile, private sau confidențiale**.

DE CE TELEGRAM, FACEBOOK MESSENGER SAU VIBER NU SUNT RECOMANDATE PENTRU CONVERSAȚII SIGURE?

Anumite servicii precum Facebook Messenger și Telegram oferă doar criptarea de la un capăt la altul dacă o activați intenționat (și doar pentru conversațiile unu-la-unu), așadar nu sunt opțiuni bune pentru transmiterea de mesaje sensibile sau confidențiale, în special pentru o organizație. Nu vă bazați pe aceste instrumente dacă trebuie să utilizați criptarea de la un capăt la altul, deoarece este destul de ușor să uitați să modificați setările implicite care sunt mai puțin sigure. Viber susține că oferă criptare de la un capăt la altul, însă nu a pus la dispoziție codul pentru a fi verificat de cercetători externi din domeniul securității. Nici codul folosit de Telegram nu a fost pus la dispoziția unui audit public. Prin urmare, mulți experți se tem că criptarea oferită de Viber (sau „conversațiile secrete" ale Telegram) ar putea fi sub standarde și, în consecință, neadecvate pentru comunicări care necesită o reală criptare de la un capăt la altul.

CONTACTELE ȘI COLEGII NOȘTRI FOLOSESC ALTE APLICAȚII DE MESAGERIE - CUM ÎI PUTEM CONVINGE SĂ DESCARCE O NOUĂ APLICAȚIE PENTRU A COMUNICA CU NOI?

Uneori, trebuie să facem un compromis între securitate și caracter convenabil, însă comunicările sensibile merită puțin efort suplimentar. Fiți un exemplu bun pentru contactele dvs. Dacă trebuie să folosiți alte sisteme mai puțin sigure, aveți mare grijă la ceea ce spuneți. Evitați să discutați subiecte sensibile. Unele organizații ar putea utiliza un sistem pentru conversații generale și altul folosit de conducere pentru discuții confidențiale. Desigur, este mai simplu dacă totul ar fi criptat automat în permanență - nu va trebui să țineți minte sau să vă îngrijoreze nimic.

Din fericire, aplicațiile cu criptare de la un capăt la altul precum Signal devin din ce în ce în ce mai populare și ușor de utilizat - în plus, au fost localizate în numeroase limbi pentru a fi utilizate la nivel global. Dacă partenerii dvs. sau alte contacte au nevoie de ajutor pentru a comuta comunicațiile la o opțiune cu criptare de la un capăt la altul precum Signal, explicați-le de ce este atât de important să vă protejați corespunzător comunicările. Dacă toată lumea înțelege importanța, cele câteva minute necesare pentru descărcarea unei noi aplicații și cele câteva zile pentru învățarea folosirii acesteia nu vor mai părea mare lucru.

EXISTĂ ȘI ALTE SETĂRI PENTRU APLICAȚIILE CU CRIPTARE DE LA UN CAPĂT LA ALTUL PE CARE AR TREBUI SĂ LE CUNOSC?

În aplicația Signal, verificarea codurilor de securitate (pe care ei le numesc Numere de siguranță) este, de asemenea, importantă. Pentru a vedea un număr de siguranță și a-l verifica în Signal, puteți deschide conversația cu un contact, atingeți numele acestuia în partea de sus a ecranului și defilați în jos pentru a atinge „Vezi numărul de siguranță". Dacă numărul de siguranță corespunde cu contactul dvs., îl puteți marca drept „verificat" din același ecran. Este extrem de important să fiți atenți la aceste numere de siguranță și să vă verificați contactele dacă primiți o notificare într-o conversație prin care sunteți informați că numărul de siguranță al unui anumit contact s-a modificat. Dacă dvs. sau alți membri ai personalului aveți nevoie de ajutor pentru configurarea acestor setări, Signal **pune la dispoziție instrucțiuni utile.** Dacă folosiți Signal, o opțiune de mesagerie securizată și apeluri unu-la-unu considerată de mulți ca fiind cel mai ușor de utilizat, asigurați-vă că **setați un cod PIN puternic.** Folosiți cel puțin șase cifre și nu ceva ușor de ghicit, precum data dvs. de naștere. Pentru mai multe sfaturi privind configurarea corectă a **Signal** și **WhatsApp**, puteți consulta **ghidurile instrumentelor** pentru ambele aplicații, dezvoltate de EFF în Ghid de autoapărare contra supravegherii.

Folosirea aplicațiilor de chat în realitate

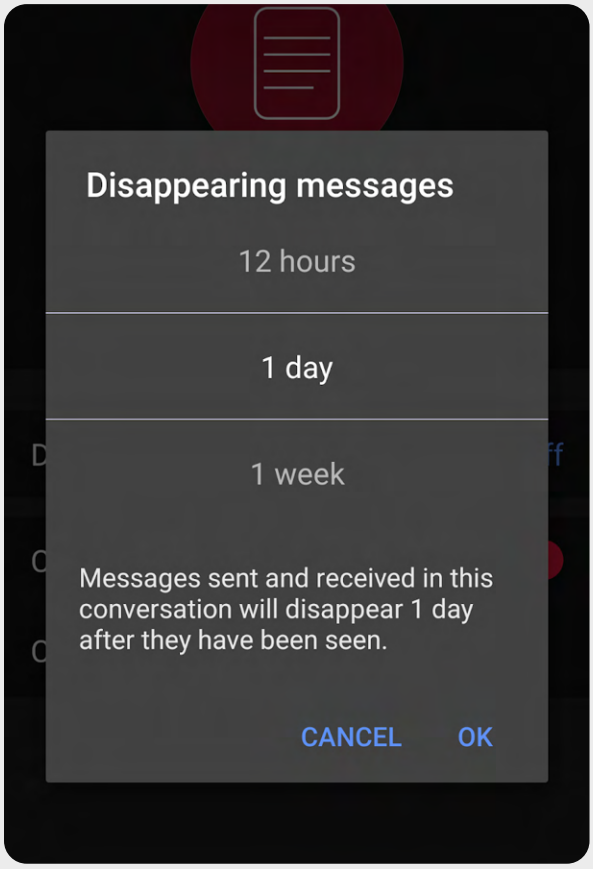
Pentru a limita neplăcerile provocate de situațiile în care un telefon se pierde, este furat sau confiscat, cea mai bună metodă este să reduceți la minimum istoricul mesajelor salvate în telefon. O modalitate simplă de a face lucru este să activați **„dispariția mesajelor”** pentru conversațiile de grup ale organizației dvs. și să încurajați personalul să facă același lucru și pentru conversațiile personale.

În Signal și în alte aplicații populare de mesagerie, puteți configura un temporizator pentru dispariția mesajelor într-un anumit număr de minute sau ore după ce au fost citite. Această setare poate fi personalizată în funcție de conversație individuală sau de grup. Pentru majoritatea dintre noi, configurarea unui interval de dispariție la o săptămână vă oferă suficient timp să realizați căutări fără a păstra mesaje de care nu veți avea niciodată nevoie – dar care ar putea fi folosite împotriva dvs. pe viitor. Nu uitați, nu vi se poate fura ceva ce nu aveți.

Pentru a activa dispariția mesajelor în Signal, deschideți o fereastră de chat, atingeți numele persoanei/grupului cu care conversați, atingeți Dispariție mesaje, alegeți un temporizator și atingeți pe OK. O setare similară există și în WhatsApp.

În situații mai grave în care trebuie să ștergeți imediat un mesaj, poate din cauză că telefonul cuiva a fost furat sau ați trimis un mesaj unei persoane greșite, rețineți că Signal vă permite să ștergeți un mesaj trimis unui grup sau unei persoane din telefoanele tuturor, în interval de trei ore de la trimiterea acestuia prin simpla ștergere a acestuia din conversație. Telegram rămâne popular în multe țări, în ciuda limitărilor sale de criptare, pentru o funcție similară care le permite utilizatorilor să șteargă mesaje de pe toate dispozitivele, fără restricții.

Acestea fiind spuse, dacă organizația dvs. este îngrijorată de siguranța personalului ca rezultat al comunicărilor care ar fi putut fi văzute pe telefoanele acestora, dispariția mesajelor cu temporizatoare scurte este probabil cea mai simplă și potrivită opțiune.



DAR VIDEOCONFERINȚELE ÎN GRUPURI MAI MARI? EXISTĂ OPȚIUNI DE CRIPTARE DE LA UN CAPĂT LA ALTUL PENTRU ACESTEA?

În contextul în care telemunca este tot mai frecventă, este important să avem o opțiune sigură pentru videoconferințele în grupuri mari ale organizației dvs. Din păcate, momentan nu există opțiuni prea bune care să îndeplinească toate cerințele: să fie ușor de utilizat, să accepte un număr mare de participanți și funcții de colaborare și să activeze, implicit, criptarea de la un capăt la altul.

Pentru grupuri de până la 40 de persoane, Signal este o opțiune cu criptare de la un capăt la altul extrem de recomandată. Videoconferințele de grup de pe Signal pot fi accesate fie de pe smartphone, fie prin aplicația Signal pentru desktop de pe un computer, care permite partajarea ecranului. Rețineți, totuși, că doar contactele dvs. care folosesc deja Signal pot fi adăugate la un grup Signal.

Dacă sunteți în căutare de alte opțiuni, o platformă care a adăugat recent setarea de criptare de la un capăt la altul este **Jitsi Meet**. Jitsi Meet este o soluție web pentru audio- și videoconferințe care poate accepta audiențe mari (până la 100 de persoane) și nu necesită descărcarea unei aplicații sau al unui software special. Rețineți că dacă folosiși această funcție pentru grupuri mari (peste 15-20 de persoane), calitatea apelului ar putea scădea. Pentru a configura o întâlnire în Jitsi Meet, puteți accesa **meet.jit.si**, introduce un cod de întâlnire și partaja apoi linkul (printr-un canal securizat precum Signal) participanților doriți. Pentru a folosi criptarea de la un capăt la altul, consultați aceste **instrucțiuni** oferite de Jitsi. Rețineți că fiecare utilizator trebuie să activeze separat criptarea de la un capăt la altul pentru a funcționa. Atunci când folosiți Jitsi, asigurați-vă că creați nume de camere aleatorii și că folosiți coduri de acces pentru a proteja apelurile.

Dacă această opțiune nu este valabilă pentru organizația dvs., puteți folosi o opțiune comercială populară precum Webex sau Zoom, activând criptarea de la un capăt la altul. Webex permite de multă vreme criptarea de la un capăt la altul, însă această opțiune nu este activa implicit și necesită descărcarea programului Webex de către participanți pentru a putea accesa întâlnirea. Pentru a activa opțiunea de criptare de la un capăt la altul pentru contul dvs. Webex, trebuie să deschideți un tichet de asistență Webex și să urmați **aceste instrucțiuni** pentru a vă asigura că criptarea de la un capăt la altul este configurată. Doar gazda întâlnirii trebuie să activeze criptarea de la un capăt la altul. Dacă aceasta face asta, întreaga întâlnire va fi criptată de la un capăt la altul. Dacă folosiți Webex pentru a vă securiza întâlnirile de grup și atelierele, asigurați-vă că activați și coduri de acces puternice pentru apeluri.

După câteva luni de publicitare negativă, Zoom a dezvoltat **opțiunea de criptarea de la un capăt la altul** pentru apelurile sale. Cu toate acestea, opțiunea respectivă nu se activează implicit, ci este nevoie ca gazda apelului să își asocieze contul la un număr de telefon și funcționează doar dacă toți participanții se alătură prin versiunea Zoom pentru desktop sau prin aplicația mobilă, nu prin apelare. Având în vedere că este ușor să configurați greșit aceste setări, nu este ideal să vă bazați pe Zoom drept opțiune de criptare de la un capăt la altul. Însă dacă criptarea de la un capăt la altul de obligatorie, iar Zoom este singura dvs. opțiune, puteți urma **instrucțiunile** furnizate de Zoom pentru a configura. Însă nu uitați să verificați fiecare apel înainte de inițiere, pentru a vă asigura că este într-adevăr criptat de la un capăt la altul, făcând clic pe lacătul verde din colțul din stânga sus al ecranului Zoom și verificând dacă în dreptul setării de criptare apare „de la un capăt la altul". Vă recomandăm, de asemenea, să creați un cod de acces puternic pentru fiecare întâlnire Zoom.

Pe lângă instrumentele menționate mai sus, **acest grafic** dezvoltat de Frontline Defenders prezintă câteva opțiuni de videoconferințe și conferințe care, în funcție de contextul riscului dvs., ar putea fi potrivite pentru organizația dvs.

Cu toate acestea, merită remarcat faptul că anumite funcții populare ale instrumentelor de mai sus funcționează doar cu criptare în stratul de transport. De exemplu, activarea criptării de la un capăt la altul în Zoom dezactivează sălile pentru subgrupuri, capacitățile de sondaj și înregistrarea în cloud. În Jitsi Meet, sălile pentru subgrupuri pot dezactiva funcția de criptare de la un capăt la altul, rezultând într-o scădere involuntară a securității.

DAR DACĂ NU AVEM, DE FAPT, NEVOIE DE CRIPTARE DE LA UN CAPĂT LA ALTUL PENTRU TOATE COMUNICĂRILE NOASTRE?

Dacă criptarea de la un capăt la altul nu este necesară pentru toate comunicările organizației dvs. în funcție de evaluarea riscurilor, ați putea opta pentru utilizarea de aplicații protejate de criptare în stratul de transport. Rețineți că pentru acest tip ce criptare trebuie să aveți încredere în furnizorul de servicii, precum Google pentru Gmail, Microsoft pentru Outlook/ Exchange sau Facebook pentru Messenger, deoarece aceștia (și cei care i-ar putea obliga să partajeze informații) pot vedea/auzi comunicările dvs. Încă o dată, cele mai bune opțiuni vor depinde de modelul de amenințări (de exemplu, dacă nu aveți încredere în Google sau dacă guvernul SUA este adversarul dvs., atunci Gmail nu este o opțiune bună), însă iată câteva opțiuni populare și în general de încredere:

E-MAIL	• **Gmail (via Google Workspace)** • **Outlook (via Office 365)** • Nu găzduiți propriul server Microsoft Exchange pentru e-mailul organizației dvs. **Dacă faceți acest lucru în prezent, vă recomandăm să migrați la Office 365.**
MESAJE TEXT (INDIVIDUALE SAU DE GRUP)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CONFERINȚE DE GRUP, APELURI AUDIO ȘI VIDEOCONFERINȚE	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
PARTAJAREA FIȘIERELOR	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

NOTĂ PRIVIND PARTAJAREA FIȘIERELOR

Pe lângă partajarea în siguranță a mesajelor, partajarea în siguranță a fișierelor poate fi parte importantă a planului de securitate al organizației dvs. Majoritatea opțiunilor de partajare a fișierelor sunt integrate în aplicațiile sau serviciile de mesagerie pe care s-ar putea să le folosiți deja. De pildă, partajarea de fișiere via Signal este o opțiune excelentă dacă este necesară criptarea de la un capăt la altul. Dacă criptarea în stratul de transport nu este suficientă, utilizarea Google Drive sau Microsoft SharePoint poate fi opțiune bună pentru organizația dvs. Trebuie doar să vă asigurați că ați configurat corect setările de partajare, în așa fel încât doar persoanele adecvate să aibă acces la un anumit document sau folder, și să vă asigurați că aceste servicii sunt conectate la conturile de e-mail de serviciu (nu personale) ale personalului dvs. Dacă este posibil, interziceți partajarea fișierelor sensibile prin atașări la e-mail sau fizic, prin unități USB. Utilizarea de dispozitive cum sunt unitățile USB în cadrul organizației dvs. crește semnificativ probabilitatea de software-uri rău intenționate și furt, iar dacă vă bazați pe atașări pe e-mail sau alte forme de atașări slăbește apărarea organizației dvs. împotriva atacurilor de tip phishing.

Alternative de partajare a fișierelor pentru organizații

În cazul în care căutați o opțiune sigură de partajare a fișierelor pentru organizația dvs. care să fie încorporată direct într-o platformă de mesagerie (sau poate întâmpinați limite de dimensiune a fișierelor atunci când doriți să partajați documente mari), luați în considerarea utilizarea OnionShare. OnionShare este un instrument open-source care vă permite să partajați anonim și în siguranță fișiere de orice dimensiune. Expeditorul descarcă aplicația OnionShare (disponibilă pe computerele Mac, Windows și Linux), încarcă fișierul(erele) pe care doresc să le partajeze și generează un link unic. Acest link, care poate fi procesat doar în Tor Browser, poate fi apoi partajat prin orice canal de mesagerie sigur (de pildă, Signal) destinatarului dorit. Destinatarul poate deschide linkul în Tor Browser și descărca fișierul(erele) pe computerul său. Rețineți că siguranța fișierelor depinde de metoda prin care distribuiți linkul. Tor va fi explicat mai detaliat într-o secțiune ulterioară pentru „Nivel avansat” din acest Îndrumar, însă, pentru partajarea fișierelor la nivelul organizației dvs., rețineți că OnionShare este o alternativă mai sigură de partajare a fișierelor decât prin unități USB dacă nu dispuneți de o opțiune de furnizor cloud de încredere.

Dacă organizația dvs. investește deja într-un manager de parole, conform descrierii din secțiunea referitoare la parole din acest Îndrumar, și alege un cont Bitwarden premium sau de echipă, funcția Bitwarden Send este altă opțiune de partajare în siguranță a fișierelor. Această funcție permite utilizatorilor să creeze linkuri sigure prin care să partajeze fișiere criptate prin orice canal sigur de mesagerie (precum Signal). Dimensiunea fișierului este limitată la 100 MB, însă Bitwarden Send vă permite să configurați o dată de expirare pentru linkuri, să protejați prin parolă accesul la fișierele partajate și să limitați numărul de deschideri ale fișierului.

Comunicarea și partajarea a datelor în siguranță

- **Impuneți utilizarea de servicii de mesagerie de încredere cu criptare de la un capăt la altul pentru comunicările sensibile ale organizației dvs. (și, ideal, pentru toate comunicările).**
  - Explicați personalului și partenerilor externi de ce sunt atât de importante comunicările sigure; acest lucru va contribui la succesul planului dvs.
- **Implementați o politică privind durata de păstrare a mesajelor și când/dacă organizația dvs. va folosi comunicările „care dispar".**
- **Asigurați-vă că setările aplicațiilor de comunicare sunt sigure, inclusiv:**
  - Asigurați-vă că întregul personal acordă atenție notificărilor de securitate și, dacă folosiți WhatsApp, nu faceți copii de siguranță ale conversațiilor.
  - Dacă folosiți o aplicație care nu activează implicit criptarea de la un capăt la altul (de ex., Zoom sau Webex), asigurați-vă că utilizatorii au activat setările adecvate atunci când configurează un apel sau o conferință.
- **Folosiți servicii de e-mail în cloud precum Office 365 sau Gmail pentru organizația dvs.**
  - Nu încercați să găzduiți propriul server de e-mail.
  - Nu permiteți personalului să folosească conturi de e-mail personale pentru serviciu.
- **Reamintiți-le frecvent membrilor organizației cele mai bune practici de securitate privind mesajele în grup și metadatele.**
  - Fiți atenți pe cine includeți în mesaje de grup, conversații și fire de e-mail.

Stocarea securizată a datelor

Pentru majoritatea organizațiile societății civile, una dintre cele mai importante decizii este locul în care își stochează datele.

Unde este „mai sigură" stocarea datelor? Pe computere personalului, pe un server local, pe dispozitive de stocare externe sau în cloud? În 99% dintre situații, cea mai simplă și cea mai sigură opțiune este păstrarea datelor în servicii de cloud de încredere. Probabil cele mai comune exemple includ Microsoft 365 și Google Drive. Fără un plan de stocare comprehensiv în cloud, cel mai probabil datele organizației dvs. vor fi stocate într-o varietate de locuri - inclusiv computerele personalului, hard-diskuri externe și chiar câteva servere locale.

Cu toate că securizarea datelor pe toate aceste dispozitive este posibilă, este foarte greu de implementat cu succes fără a cheltui mulți bani și a angaja personal IT semnificativ.

Atunci când alegeți un instrument sau serviciu de stocare a datelor dvs., asigurați-vă că aveți încredere în compania sau grupul din spatele acesteia. O căutare rapidă de Google și consultarea unor experți în securitatea digitală v-ar putea ajuta mult să verificați corectitudinea unui potențial furnizor tehnologic. Iată câteva întrebări pe care trebuie să vi le puneți: Vând sau partajează date confidențiale? Au resurse adecvate de securitate pentru personal? Oferă funcții de securitate (precum 2FA) pentru a vă ajuta să vă protejați contul?

Stocarea datelor și societatea civilă

Apariția opțiunilor accesibile (uneori gratuite) de stocare a datelor în cloud a ușurat viața și a sporit nivelul de securitate pentru multe organizații ale societății civile. Din păcate, multe încearcă încă să găzduiască propriile servere cu un buget, personal și asistență IT relativ limitate. În martie 2021, amenințarea unei asemenea infrastructuri organizaționale a devenit reală pentru zeci de mii de organizații din întreaga lume atunci când un grup de spionaj cibernetic afiliat guvernului chinez, numit Hafnium, a declanșat o catastrofă cibernetică globală printr-un atac sofisticat asupra serverelor găzduite de Microsoft Exchange. Atacul a compromis servere locale, permițându-le hackerilor să obțină acces la conturi de e-mail organizaționale, să instaleze software-uri rău intenționate pe serverele victimelor și sistemele conectate și, în final, **să extragă date sensibile**. Cu toată că Microsoft a publicat repede o actualizare și instrucțiunile de identificare și îndepărtare a potențialilor intruși după ce atacurile au fost făcute publice, multe organizații nu dispuneau de capacitatea IT care să le permită să aplice rapid aceste actualizări, rămânând expuse pe perioade prelungite de timp. Scopul și impactul acestui atac global demonstrează pericolul la care se expun organizațiile civice care aleg să găzduiască propriile servere de e-mail și alte tipuri de date sensibile. în special fără o investiție semnificativă în personal dedicat securității cibernetice.

BENEFICIILE STOCĂRII DE DATE

Chiar dacă urmați pașii adecvați pentru a vă proteja computerele împotriva software-urilor rău intenționate și furtului fizic, tot este posibil ca un adversar hotărât să vă acceseze ilegal computerul sau serverul local. Acestora le este mai greu să treacă de scuturile de securitate ale Google sau Microsoft, de exemplu. Companiile care dețin spații de stocare sigure în cloud au resurse de securitate de neegalat și stimulente puternice pentru furnizarea unei securități maxime utilizatorilor lor. Pe scurt: o strategie de stocare în cloud de încredere va fi mai ușor de implementat și va rămâne sigură în timp. Așadar, în loc să vă complicați să încercați să vă securizați propriul server, vă puteți canaliza energia pe câteva sarcini mai simple. Păstrarea informațiilor dvs. în cloud vă ajută în cazul unei game de riscuri comune. Cineva și-a lăsat computerul într-un restaurant sau telefonul în autobuz? Copilul dvs. a vărsat un pahar de suc pe tastatura dvs., dispozitivul devenind neoperabil? Un membru al personalului a instalat un software rău intenționat și trebuie să șteargă toate datele de pe computer? Dacă majoritatea documentelor și datelor sunt salvate în cloud, este ușor să resincronizați și să o luați de la capăt pe un computer curat sau nou-nouț. De asemenea, dacă un computer este infectat cu un software rău intenționat sau un hoț scanează o unități de hard disk, nu mai are ce fura dacă majoritatea documentelor sunt accesate prin browserul web.

CE FURNIZOR DE STOCARE ÎN CLOUD AR TREBUI SĂ FOLOSIM?

Cele mai populare opțiuni de stocare în cloud sunt Google Workspace (cunoscut anterior sub denumirea de GSuite) și Microsoft 365. Dacă dvs. și personalul dvs. folosiți deja Gmail, abonarea organizației dvs. la Google Workspace și stocarea datelor în Google Drive cu aplicațiile integrate Google Docs, Sheets și Slides pentru procesarea documentelor, foilor de calcul și prezentărilor poate fi o soluție. În mod similar, dacă organizația dvs. se bazează pe Excel și Word, alegerea facilă ar fi un abonament Microsoft 365, care oferă acces la Outlook și versiuni licențiate de Microsoft Word, Excel, Powerpoint și Teams. Indiferent de furnizorul pe care îl alegeți, depozitarea datelor în siguranță în cloud necesită implementarea unor setări adecvate de partajare și instruirea personalului pentru a înțelege cum și unde să partajeze (și să nu partajeze) foldere și documente. În general, trebuie să configurați folderele din unitatea de stocare în cloud să ofere acces exclusiv personalului care are nevoie de fișierele respective. Realizați audituri de rutină ale sistemului dvs., pentru a vă asigura că nu „partajați excesiv" niciun fișier (de pildă, prin activarea partajării fișierelor printr-un link universal care, în schimb, ar trebui să fie limitat la doar câteva persoane).

CE SE ÎNTÂMPLĂ DACĂ NU AVEM ÎNCREDE ÎN GOOGLE SAU MICROSOFT SAU ALȚI FURNIZORI DE STOCARE ÎN CLOUD?

Dacă unul dintre adversarii dvs. (de pildă, un guvern străin sau local) poate forța, pe căi legale, Google sau Microsoft (sau alt furnizor de stocare în cloud) să predea date, atunci s-ar putea să nu fie în regulă să alegeți aceste opțiuni de stocare de date. Riscul ar putea fi mai mare dacă adversarul este guvernul Statelor Unite, de exemplu, însă mult mai mic dacă adversarul este o regim autoritar. Rețineți că Google și Microsoft au ambele politici privind predarea datelor doar atunci când sunt obligate prin lege și recunosc faptul că organizația dvs. ar putea fi vulnerabilă în fața aceluiași tip de solicitări legale din partea propriului guvern, dacă datele sunt găzduite la nivel local. În situațiile în care mediile de stocare Google sau Microsoft nu par o idee bună pentru organizația dvs., ați putea lua în considerare **Keybase** ca opțiune alternativă. Funcția destinată echipelor din Keybase permite organizației dvs. să partajeze fișiere și mesaje utilizând criptarea de la un capăt la altul într-un mediu cloud sigur, fără a fi nevoie să vă bazați pe un furnizor terț. Prin urmare, poate fi o opțiune bună pentru stocarea în siguranță a documentelor și fișierelor la nivelul organizației dvs. Cu toate acestea, Keybase este mai puțin familiar utilizatorilor, așa că rețineți că adoptarea acestui instrument ar putea necesita mai mult efort și mai multă instruire decât în cazul celorlalte soluții menționate anterior. Acestea fiind spuse, dacă optați totuși să acționați individual și să nu folosiți deloc stocarea în cloud, este de o importanță crucială să investiți timp și resurse în îmbunătățirea metodelor de protecție digitală ale dispozitivelor organizației dvs. și să vă asigurați că serverele locale sunt configurate și criptate corespunzător și păstrate în siguranță din punct de vedere fizic. Cu toate că ați face economii neplătind abonamente lunare, organizația dvs. va plăti pentru timpul personalului și pentru resurse și va fi mai vulnerabilă la atacuri.

COPIERE DE REZERVĂ A DATELOR

Indiferent dacă organizația dvs. stochează datele pe dispozitive fizice sau în cloud, este important să faceți copii de rezervă. Rețineți că dacă vă bazați pe stocarea pe dispozitive fizice, este destul de ușor să pierdeți accesul la date. Ați putea vărsa cafea pe computer și distruge unitatea de hard disk. Computerele personalului ar putea fi atacate de hackeri și toate fișierele

locale blocate de ransomware. Cineva ar putea pierde un dispozitiv în tren sau i s-ar putea fura împreună cu servieta. Așa cum am menționat anterior, există și alt motiv pentru care utilizarea stocării în cloud poate fi benefică, acela că nu este legată de un anumit dispozitiv care ar putea fi infectat, pierdut sau furat. Computere Mac au software de copiere de rezervă integrat denumit Time Machine, care este folosit împreună cu un dispozitiv de stocare extern; pentru dispozitivele Windows, Istoric fișiere oferă funcționalități similare. Telefoanele iPhone și Android pot crea automat copii de rezervă pentru conținutul important în cloud, dacă funcția este activată din setările telefonului. Dacă organizația dvs. folosește stocarea în cloud (precum Google Drive), riscul ca Google să fie oprit sau ca datele dvs. să fie distruse într-un dezastru este destul de mic, însă încă există posibilitatea unei erori umane (precum ștergerea accidentală a fișierelor importante). Explorarea unei soluții de copiere de rezervă în cloud precum Backupify sau SpinOne Backup ar putea merita osteneala. Dacă datele sunt stocate pe un server local și/sau dispozitive locale, o copie de rezervă sigură devine de o importanță și mai critică. Puteți crea copii de rezervă ale datelor organizației dvs. pe o unitate de hard disk externă, însă asigurați-vă că criptați unitatea cu o parolă puternică. Time Machine vă poate cripta unitățile de hard disk, sau puteți utiliza instrumente de criptare de încredere pentru întreaga unitate de hard disk, precum VeraCrypt sau BitLocker. Asigurați-vă că păstrați dispozitivele cu copii de rezervă într-un loc separat de alte dispozitive și fișiere. Nu uitați, un fișier care distruge atât computerele, cât și copiile de rezervă vă va prima de orice copii de rezervă. Vă recomandăm să păstrați o copie într-un loc foarte sigur, cum ar fi o cutie de valori securizată.

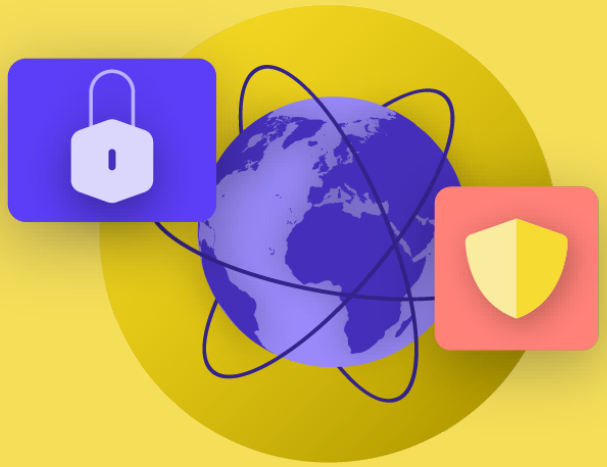
Notă: dacă folosiți un furnizor cloud dintr-o țară cu legi specifice privind localizarea datelor, consultați-vă cu juriști pentru a înțelege mai bine cum o soluție de stocare în cloud ar putea respecta reglementările locale. Mulți furnizori de stocare în cloud, inclusiv Google și Microsoft, oferă acum opțiuni care le permit anumitor clienți să aleagă locația geografică a datelor lor din cloud, de exemplu.

Îmbunătățirea securității conturilor din cloud ale organizațiilor

Dacă organizația dvs. optează să configureze un domeniu în Google Workspace sau Microsoft 365, țineți cont de faptul că ambele companii permit niveluri ridicate de securitate (în multe cazuri, gratuit) pentru organizațiile societății civile. Programul Protecție avansată al Google și AccountGuard al Microsoft oferă niveluri suplimentare de securitate robustă tuturor conturilor din cloud ale organizației dvs. și vă ajută să reduceți cu mult probabilitatea de phishing și compromiterea contului. Dacă credeți că organizația dvs. se califică și sunteți interesați să vă înscrieți organizația în oricare dintre aceste servicii, vizitați site-urile web din linkurile de mai sus sau contactați cyberhandbook@ndi.org pentru asistență suplimentară.

Stocarea securizată a datelor

- **Stocați datele sensibile exclusiv într-un serviciu de stocare în cloud de încredere.**
  - Asigurați-vă că toate conturile conectate utilizate pentru accesarea serviciului respectiv au parole puternice și 2FA.
- **Creați și implementați o politică de limitare a setărilor de partajare în cloud.**
  - Instruiți întregul personal să partajeze adecvat (și să nu partajeze excesiv) documente.
- **Dacă organizația dvs. optează pentru stocarea datelor la nivel local, investiți în personal IT calificat.**
- **Păstrați în siguranță copiile de rezervă - criptați unitățile de hard disk cu copii de rezervă sau alte dispozitive care conțin copii de rezervă.**



Siguranța pe internet

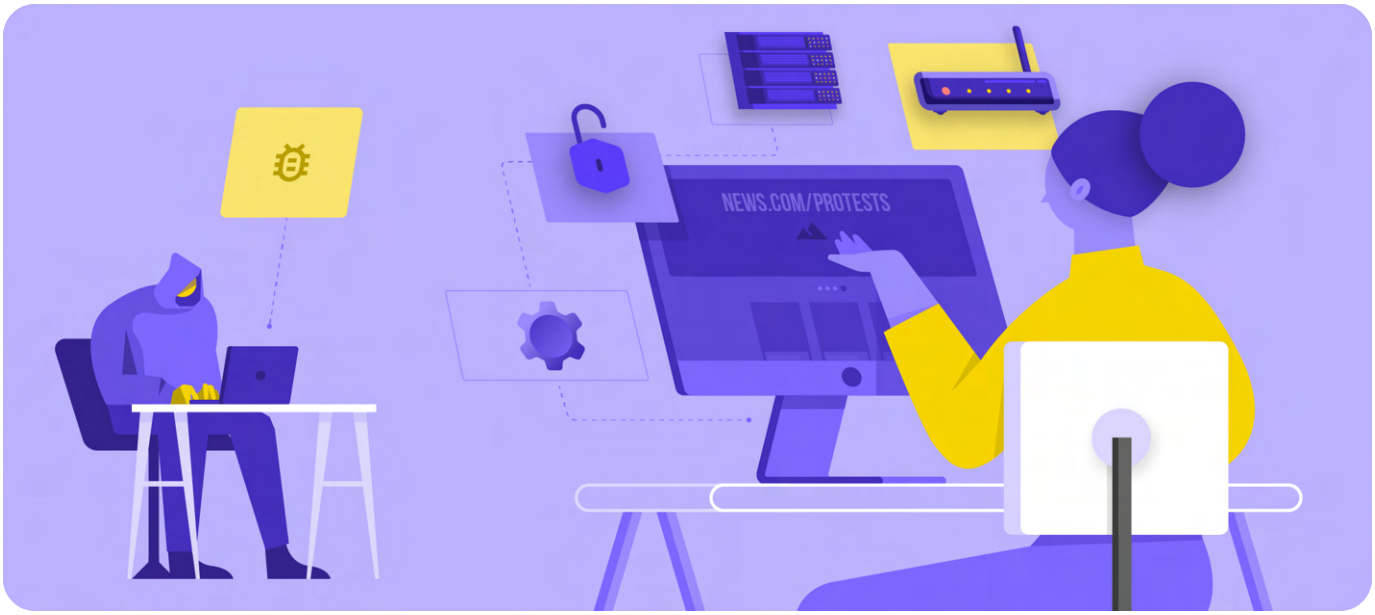
Atunci când folosiți internetul de pe telefon sau computer, activitatea dvs. poate spune multe despre dvs. și despre organizația dvs.

Este important să țineți informațiile sensibile – precum numele de utilizator și parolele pe care le introduceți pe un site web, postările de pe rețele sociale sau, în anumite situații, chiar numele site-urilor pe care le vizitați – departe de ochii indiscreți. O altă îngrijorare frecventă este blocarea sau restricționarea accesului la anumite site-uri și aplicații. Aceste două probleme – monitorizarea internetului și cenzura pe internet – merg mână în mână, iar strategiile de a le reduce impactul sunt similare.

Navigarea în siguranță

UTILIZAREA HTTPS

Cel mai important pas în limitarea capacității unui adversar de a vă supraveghea organizația online este de a reduce la minimum cantitatea de informații disponibile despre activitatea pe internet a dvs. și a colegilor dvs. Asigurați-vă întotdeauna că vă conectați securizat la site-uri web: asigurați-vă că URL-ul (locația) începe cu „https” și arată o mică pictogramă lacăt în bara de adrese a browserului dvs. Atunci când navigați pe internet **fără criptare**, informațiile pe care le introduceți pe site (precum parole, numere de cont sau mesaje) și detaliile site-ului și paginile pe care le vizitați sunt toate expuse. Aceasta înseamnă că (1) orice hackeri din rețeaua dvs., (2) administratorul dvs. de rețea, (3) furnizorul dvs. de internet și orice entitate căreia acesta i-ar putea partaja date (precum autoritățile guvernamentale), (4) furnizorul de internet al site-ului pe care îl vizitați și orice entitate căreia i-ar putea acesta i-ar putea partaja date și, desigur, (5) site-ul propriu-zis pe care îl vizitați, toate au acces la destul de multe informații potențial sensibile.

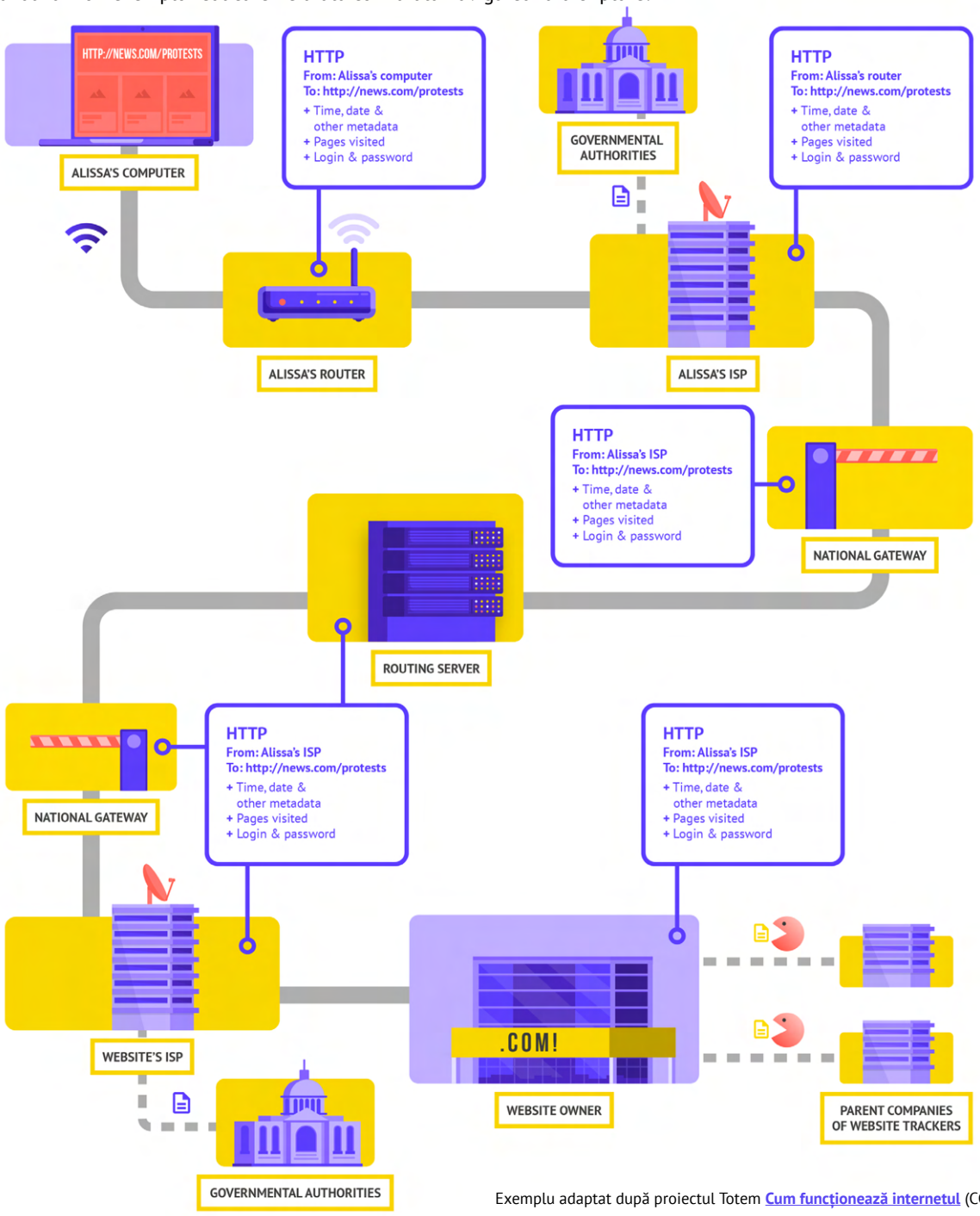


Supravegherea, cenzura și societatea civilă

Guvernele fac tot mai mult trafic de influență și autoritate asupra furnizorilor de servicii de internet și altor infrastructuri locale de internet pentru a împiedica persoanele și grupurile societății civile să acceseze informații pe internet. În unele cazuri, aceste întreruperi ale internetului au ca scop închiderea platformelor importante de comunicare și partajare de informații, inclusiv rețele sociale și site-uri de știri. De exemplu, ca răspuns la protestele iscate de o lovitură de stat, armata din Myanmar le-a impus operatorilor de telefonie mobilă să întrerupă temporar întreaga rețea de date mobile din țară. Aceasta a survenit la scurt timp după blocarea mai țintită a Facebook, Twitter și Instagram. Pe lângă blocarea accesului la internet și site-uri web, guvernele și alți actori de amenințare din întreaga lume folosesc tehnologie de supraveghere tot mai accesibilă pentru a monitoriza activitatea online a cetățenilor. De pildă, conform raportului Libertatea pe internet în 2020 al Freedom House, guvernul Ugandei a colaborat cu compania tehnologică chineză Huawei pentru a **supraveghea opozanți și activiști civici** în perioada premergătoare și ulterioară alegerilor prezidențiale controversate din țară.

Frecvența tot mai mare a acestor atacuri asupra accesului la informații și libertății de informare online subliniază cât este de important pentru grupurile societății civile să înțeleagă riscurile operării pe internet și să dezvolte planuri despre metode de conectare atunci când conectivitatea are de suferit.

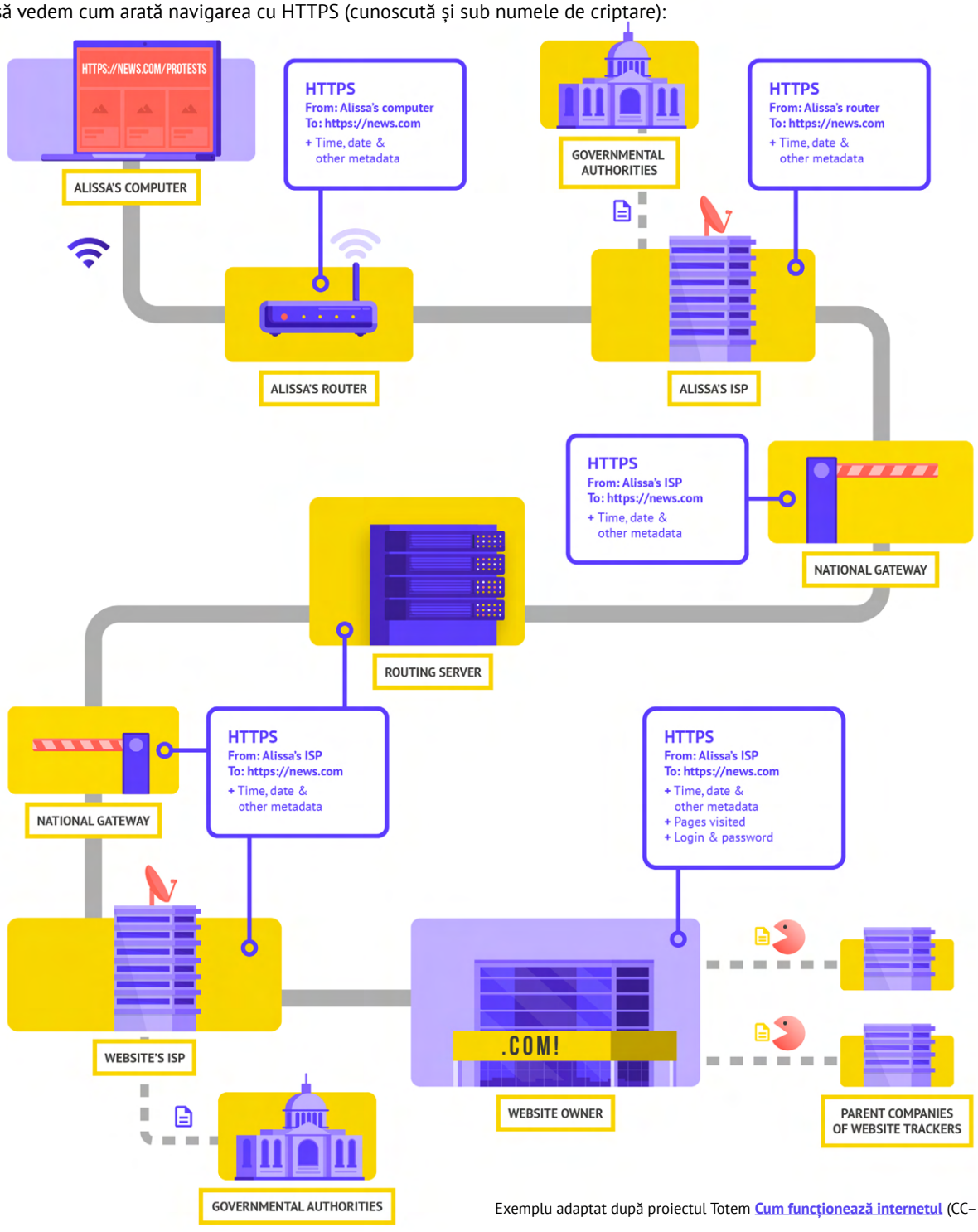
Haideți să analizăm un exemplu real care ne arată cum arată navigarea fără criptare:



Exemplu adaptat după proiectul Totem Cum funcționează internetul (CC–BY–NC–SA)

Atunci când navigați fără criptare, toate datele dvs. sunt expuse. Așa cum se arată în exemplul de mai sus, un adversar poate vedea cine sunteți, că accesați news.com și vă uitați exact la pagina dedicată protestelor din țara dvs. și vă vede parola pe care o partajați atunci când vă autentificați la site-ul propriu-zis. Asemenea informații care ajung pe mâinile cui nu trebuie nu doar vă expun contul, ci și le oferă potențialilor adversari o idee asupra ceea ce ați putea face sau gândi.

Utilizarea HTTPS (unde „s” înseamnă sigur) înseamnă că criptarea este activă. Acest lucru vă oferă mult mai multă protecție. Haideți să vedem cum arată navigarea cu HTTPS (cunoscută și sub numele de criptare):



Exemplu adaptat după proiectul Totem Cum funcționează internetul (CC–BY–NC–SA)

Dacă utilizați HTTPS, o potențial adversar nu vă mai poate vedea parola sau alte informații sensibile pe care le-ați putea partaja pe un site web. Cu toate acestea, adversarii tot pot vedea ce domenii (de exemplu, news.com) vizitați. Și, cu toate că HTTPS criptează și informațiile despre paginile individuale de pe un site (de exemplu, website.com/protests) pe care îl vizitați, adversarii sofisticați încă pot vedea aceste informații prin inspectarea traficului dvs. pe internet. Dacă utilizați HTTPS, un adversar ar putea ști că accesați news.com, însă nu vor putea să vă vadă parola și i-ar fi mai greu (dacă nu chiar imposibil) să vadă că ați căutat informații despre proteste (pentru a folosi exemplul de față). Aceasta este o diferență importantă. Verificați întotdeauna dacă utilizați HTTPS înainte de a naviga pe un site web și de a introduce informații sensibile. Puteți, de asemenea, folosi **extensia de browser HTTPS Everywhere** pentru a vă asigura că utilizați tot timpul HTTPS, sau, în cazul în care folosiți Firefox, activa **modul Doar HTTPS** în browser.
Dacă în browser vă apare o atenționare că un site web ar putea fi nesigur, nu o ignorați. Ceva nu este în regulă. Ar putea să nu fie nimic grav – de pildă, site-ul are un certificat de securitate expirat – sau site-ul ar putea fi falsificat. Indiferent de situație, este important să țineți seama de avertizare și să nu intrați pe site. HTTPS este esențial, iar DNS-ul criptat oferă o protecție suplimentară împotriva privirilor indiscrete și blocării site-ului, însă, dacă organizația dvs. este îngrijorată în ceea ce privește supravegherea extrem de țintită a activității online și se confruntă cu cenzură sofisticată online (precum blocarea site-urilor web și a aplicațiilor), este recomandat să utilizați o rețea virtuală privată (VPN).

Utilizarea unui DNS criptat

Dacă doriți să îngreunați (fără a avea pretenția că acest lucru va fi imposibil) eforturile unui furnizor de internet de a afla detalii despre site-urile web pe care le vizitați, puteți utiliza un DNS criptat.

Daca vă **întrebați**, DNS înseamnă sistem de nume de domeniu. În esență, acesta este agenda telefonică a internetului, traducând numele de domenii obișnuite (precum ndi.org) în adrese IP (protocol de internet). Acest lucru le permite oamenilor să utilizeze browserele web pentru a căuta cu ușurință și a încărca resurse de internet și site-uri web. Însă, implicit, DNS nu este criptat.

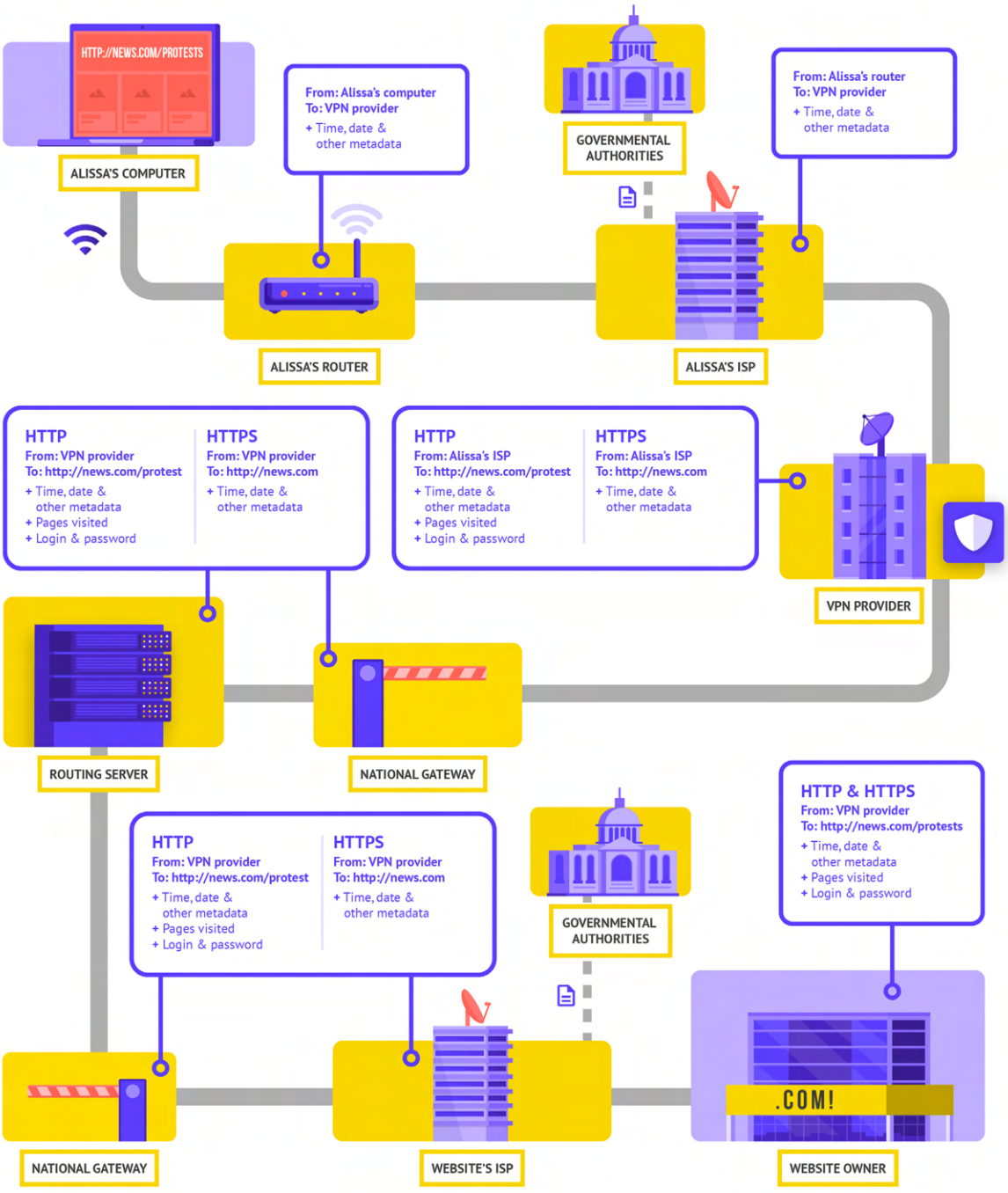
Pentru a utiliza un DNS criptat și a spori deopotrivă protecția traficului dvs. pe internet, o opțiune facilă ar fi să descărcați și să activați **aplicația 1.1.1.1 dezvoltată de Cloudflare** pe computerul sau dispozitivul dvs. mobil. Sunt disponibile și alte opțiuni de DNS criptate, inclusiv 8.8.8.8 dezvoltat de Google, însă acestea necesită **pași mai tehnici** pentru configurare. Dacă folosiți browserul Firefox , DNS-ul criptat este acum activat implicit.

Utilizatorii de browsere precum Chrome sau Edge pot **activa DNS-ul criptat** din setările avansate de securitate ale browserului, activând „Utilizare DNS sigur” și selectând „Cu: Cloudflare (1.1.1.1)” sau furnizorul ales de dvs.

1.1.1.1 de la Cloudflare cu WARP vă criptează DNS-ul și vă criptează datele de navigare - oferind un serviciu similar unui VPN tradițional. În vreme ce WARP nu vă protejează complet locația de toate site-urile web pe care le vizitați, este o funcție ușor de utilizat care poate ajuta personalul organizației dvs. să profite de beneficiile DNS-ului criptat și de protecția suplimentară oferită de furnizorul dvs. de internet în situații în care un VPN complet fie nu este funcțional, fie nu este necesar în respectivul context al amenințărilor. Setările avansate pentru DNS ale 1.1.1.1 cu WARP le permit angajaților să activeze și 1.1.1.1 pentru Familii, care oferă protecție suplimentară împotriva software-urilor rău intenționate în timpul accesării internetului.

CE ESTE UN VPN?

Un VPN este, în esență, un tunel care protejează împotriva supravegherii și blocării traficului dvs. pe internet de către hackerii din rețeaua dvs., administratorul rețelei dvs., furnizorul dvs. de internet și cei cu care acesta partajează datele. Utilizarea HTTPS este la fel de esențială pentru a vă asigura că puteți avea încredere în VPN-ul folosit de organizația dvs. Exemplul de mai jos indică cum arată navigarea folosind un VPN:



Exemplu adaptat după proiectul Totem Cum funcționează internetul (CC–BY–NC–SA)

În vederea unei descrieri aprofundate a VPN-urilor, această secțiune are drept referință ghidul Surveillance Self-Defense dezvoltat de EFF:

VPN-urile tradiționale au rolul de a vă deghiza adresa IP propriu-zisă și crea un tunel criptat pentru traficul de internet dintre computerul dvs. (sau telefonul ori orice dispozitiv inteligent conectat la rețea) și serverul VPN. Deoarece traficul în tunel este criptat și trimis la VPN-ul dvs., terților precum furnizorii de internet și hackerii de pe rețelele Wi Fi publice le este mult mai greu să vă monitorizeze, modifice sau blocheze traficul. După ce a trecut prin tunelul de la dvs. la VPN, traficul părăsește VPN-ul și pornește spre destinația finală, mascându-vă adresa IP originală. Aceasta ajută la deghizarea locației dvs. fizice în fața oricui vede traficul după ce părăsește VPN-ul. Aceasta vă oferă mai multă confidențialitate și securitate, însă utilizarea unui VPN nu vă asigură anonimitatea completă online: traficul dvs. este încă vizibil pentru operatorul VPN-ului. Și furnizorul dvs. de internet ar putea ști că folosiți un VPN, ceea ce ar putea să vă crească profilul de risc.

Asta înseamnă că **alegerea unui furnizor VPN de încredere este esențială**. În anumite locuri, precum Iran, guvernele ostile și-au configurat propriile VPN-uri să poată monitoriza ce fac cetățenii. Pentru a afla ce VPN este potrivit pentru organizația dvs. și personalul acesteia, puteți evalua VPN-urile în funcție de modelul și reputația companiei, de ce date creează sau colectează și, desigur, de securitatea instrumentului în sine.

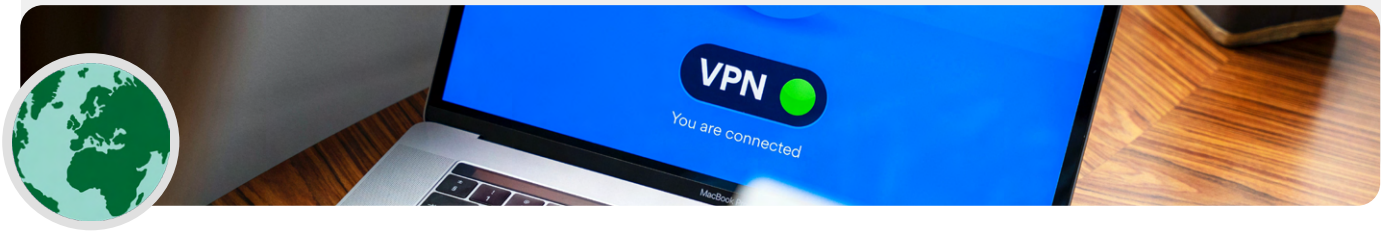
De ce să nu folosim pur și simplu un VPN gratuit? Pe scurt, pentru că majoritatea VPN-urilor gratuite, inclusiv cele preinstalate pe unele smartphone-uri, au o problemă. La fel ca toate afacerile și furnizorii de servicii, VPN-urile trebuie să se susțină singure. Dacă VPN-ul nu își vinde serviciile, cum rămâne afacerea pe linia de plutire? Solicită donații? Cere un preț pentru servicii premium? Este sprijinit de organizații caritabile sau finanțatori? Din nefericire, multe VPN-uri gratuite fac bani din colectarea și vânzarea datelor dvs.

Un furnizor VPN care nu colectează din start date este cea mai bună alegere. Dacă datele nu sunt colectate, nu pot fi vândute sau predate unui guvern care le-ar putea solicita. Consultați politica de confidențialitate a unui furnizor VPN pentru a vedea dacă VPN-ul colectează sau nu datele utilizatorilor. Dacă nu se specifică explicit că datele utilizatorului nu sunt înregistrate, există șanse să fie colectate. Chiar dacă o companie pretinde că nu înregistrează datele de conectare, aceasta nu este întotdeauna o garanție de comportament corespunzător.

Merită să cercetați compania din spatele VPN-ului. Este sprijinită de profesioniști independenți din domeniul securității? S-au scris articole în presă despre VPN-ul respectiv? S-a descoperit vreodată că și-a înșelat sau mințit clienții? Dacă VPN-ul a fost dezvoltat de persoane cu renume în comunitatea securității informațiilor, probabilitatea de a fi de încredere este mai mare. Fiți precauți în ceea ce privește un VPN care oferă un serviciu pentru care nimeni nu vrea să-și pună în joc reputația sau unul oferit de o companie absolut necunoscută.

VPN-urile false în realitate

La finalul lui 2017, în urma unui val de proteste în țară, iranienii au început să descopere o versiune „gratuită" (dar falsă) a unui VPN popular care era distribuită prin mesaje text. VPN-ul gratuit, care, de fapt, nu funcționa, promitea să acorde acces la Telegram, care, la vremea respectivă, era blocat la nivel local. Din nefericire, aplicația falsă nu era decât un software rău intenționat care permitea autorităților să urmărească mișcarea și să monitorizeze comunicările celor care o descărcau.



În concluzie, ce VPN ar trebui să folosim?

Dacă utilizarea unui VPN este potrivită pentru organizația dvs., două dintre opțiunile de încredere sunt TunnelBear și ProtonVPN. O altă opțiune este de a vă configura propriul server utilizând Outline de la Jigsaw, în cazul în care contul dvs. nu este administrat de o companie, ci trebuie să vă configurați propriul server. Dacă organizația este puțin mai mare, vă recomandăm să utilizați un VPN business care oferă funcții de gestionare a contului, cum ar fi abonamentul Teams al TunnelBear. Pentru anumite organizații din spațiul societății civile și drepturilor omului care se califică, TunnelBear oferă credite pentru utilizarea gratuită a VPN-ului său (care, de obicei, costă aproximativ 3 USD pe lună). Dacă credeți că organizația dvs. se califică și sunteți interesați, contactați cyberhandbook@ndi.org pentru mai multe informații.

Cu toate că majoritatea VPN-urilor moderne prezintă îmbunătățiri în ceea ce privește performanța și viteza, rețineți că folosirea unui VPN vă poate încetini viteza browserului dacă sunteți pe o rețea cu lățime de bandă foarte îngustă, aveți latență înaltă sau întârzieri de rețea sau vă confruntați cu întreruperi intermitente ale internetului. Dacă rețeaua dvs. este mai rapidă, vă recomandăm să folosiți tot timpul un VPN.

Dacă recomandați personalului să folosească un VPN, este important și să vă asigurați că angajații mențin VPN-ul activat. Poate părea evident, însă un VPN care este instalat, însă nu rulează, nu oferă protecție.

Anonimat prin Tor

Pe lângă VPN-uri, poate că ați auzit de Tor, un alt instrument care asigură o utilizare mai sigură a internetului. Este important să înțelegeți ce sunt amândouă, de ce ați putea folosi fie un instrument, fie pe celălalt și ce impact ar putea ambele asupra organizației.

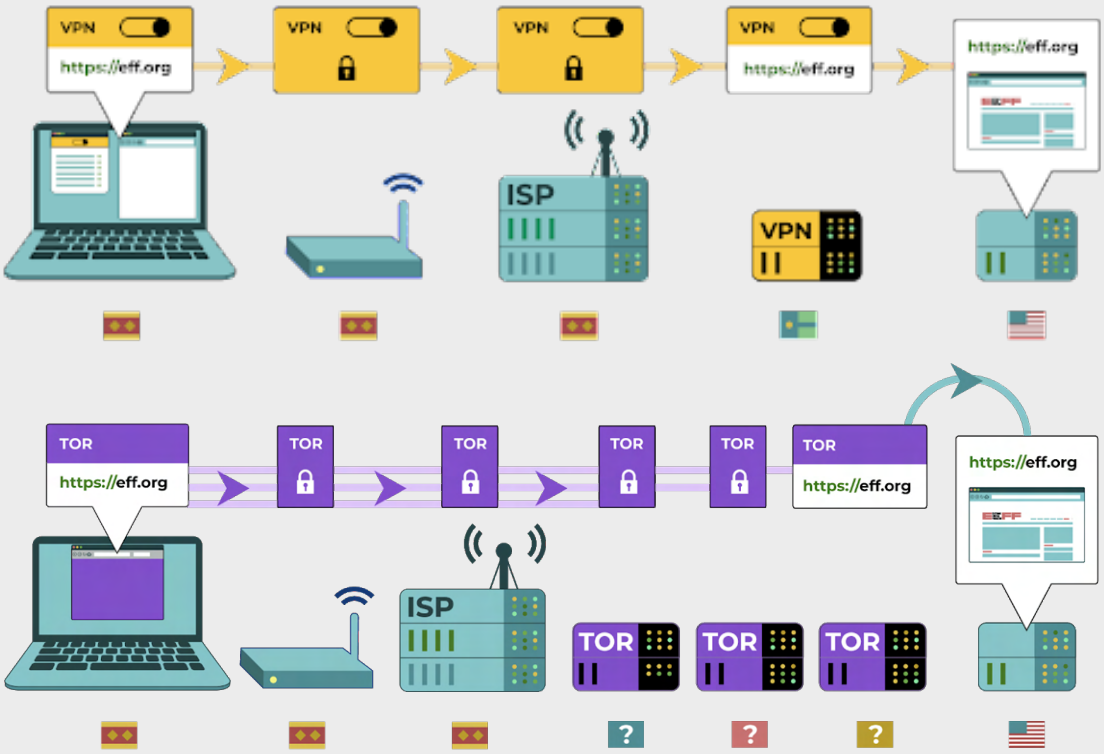
Tor este un protocol pentru transmiterea anonimă a datelor pe internet prin rutarea mesajelor și datelor printr-o rețea decentralizată. Puteți afla cum funcționează Tor aici, dar, pe scurt, acesta vă rutează traficul prin mai multe puncte în drumul acestuia spre destinație, în așa fel încât niciun punct să nu aibă suficiente informații prin care să expună cine sunteți și ce faceți online simultan.

Tor se diferențiază de un VPN în mai multe moduri. În esență, diferă pentru că nu se bazează pe încrederea unui anumit punct (spre deosebire de un furnizor VPN).

Acest grafic, dezvoltat de EFF, indică diferența dintre un VPN tradițional și Tor.

Cel mai simplu mod de a folosi Tor este prin browserul Tor. Operează ca orice browser normal, însă vă rutează traficul prin rețeaua Tor. Puteți descărca browserul Tor pe dispozitive Windows, Mac, Linux sau Android. Atunci când folosiți Tor Browser, rețineți că vă protejați doar informațiile pe care le accesați **cât folosiți browserul.** Nu oferă nicio protecție altor aplicații sau fișierelor descărcate pe care le-ați putea deschide separat pe dispozitivul dvs. Rețineți, de asemenea, că Tor nu vă criptează traficul, prin urmare - la fel ca în cazul utilizării unui VPN - este la fel de esențial să folosiți cele mai bune practici HTTPS atunci când navigați pe internet.

Dacă doriți să extindeți protecțiile de anonimat ale Tor pe întregul computer, utilizatorii mai experimentați pot instala Tor drept conexiune la internet în tot sistemul sau puteți folosi sistemul de operare Tails, care rutează implicit tot traficul prin Tor. Utilizatorii Android pot utiliza, de asemenea, aplicația Orbot pentru a rula Tor pentru tot traficul pe internet și toate aplicațiile de pe dispozitivele lor. Indiferent de modul în care folosiți Tor, este important de știut că atunci când îl folosiți,



furnizorul dvs. de internet nu poate vedea ce site-uri vizitați, însă *pot* vedea că folosiți Tor. La fel ca în cazul utilizării unui VPN, acest lucru ar putea crește considerabil profilul de risc al organizației dvs., deoarece Tor nu este un instrument prea comun și, prin urmare, poate fi ușor observat de adversarii care ar putea să vă monitorizeze traficul pe internet.

Așadar, ar trebui organizația dvs. să folosească Tor? Răspunsul este: depinde. Pentru majoritatea organizațiilor care prezintă riscuri, un VPN de încredere care este utilizat corect de tot personalul în permanență este cea mai ușoară și convenabilă metodă, iar, în era utilizării tot mai frecvente a VPN-ului la nivel global, mai puțin probabil să declanșeze semnale de alertă. Cu toate acestea, dacă fie nu vă permiteți un VPN de încredere, fie operați într-un mediu în care VPN-urile sunt de regulă blocate, Tor poate fi o opțiune bună, dacă este legală, pentru limitarea impactului urmăririi și evitarea cenzurii online.

Există vreun motiv pentru care nu ar trebui să folosim un VPN sau Tor?

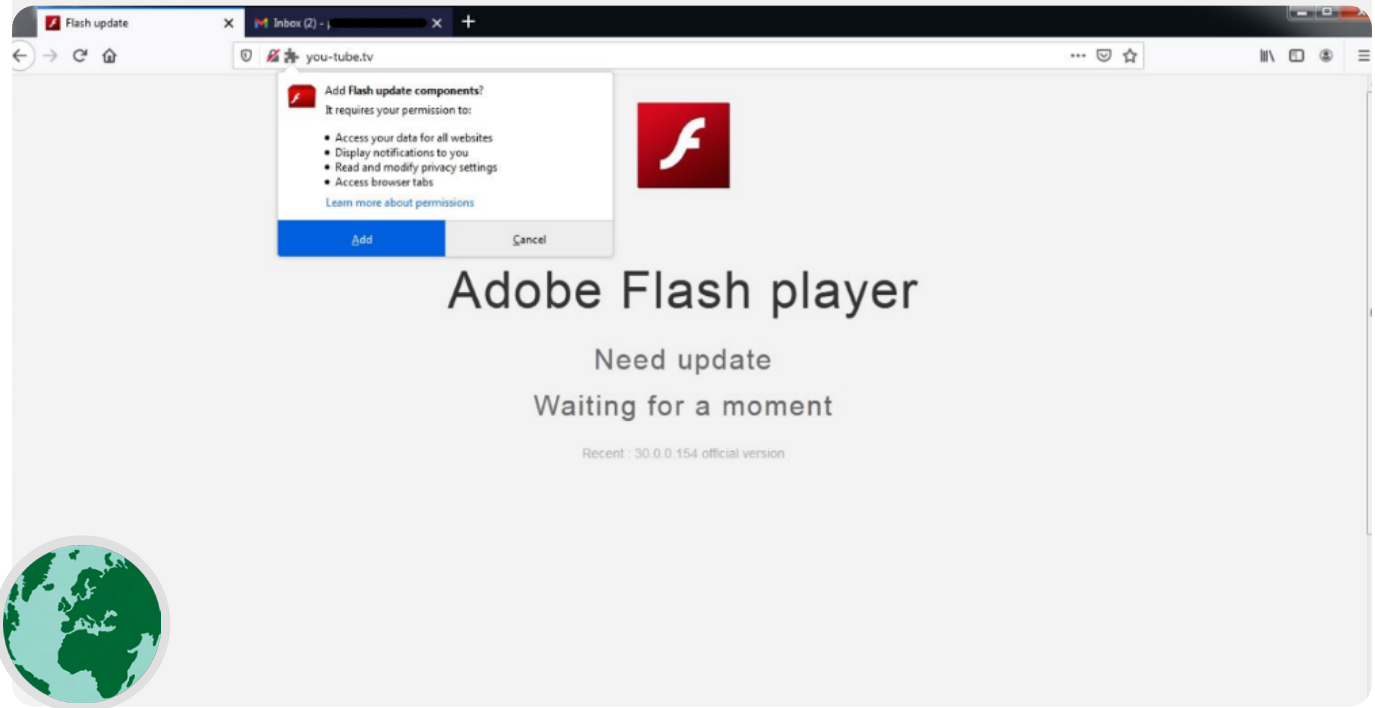
În afară de îngrijorările privind serviciile VPN nerespectabile, cel mai important este să luați în considerare dacă utilizarea unui VPN sau Tor ar putea atrage atenție nedorită sau, în anumite jurisdicții, încălca legea. Cu toate că furnizorul dvs. de internet nu va ști ce site-uri vizitați în timp ce utilizați aceste servicii, va putea vedea că sunteți conectat la Tor sau la un VPN. Dacă în zona în care operează organizația dvs. este ilegal, sau ar putea atrage mai multă atenție și riscuri decât simpla navigare pe web cu HTTPS standard și DNS criptat, probabil un VPN sau, în special Tor (care este mult mai puțin folosit și, prin urmare, un „semnal de alertă" mai mare) nu este alegerea potrivită pentru organizația dvs. Cu toate acestea, în contextul în care utilizarea VPN-urilor este din ce în ce mai frecventă, acesta este mai puțin un factor distinctiv. Utilizarea implicită a unui VPN în permanență este cea mai bună alegere dacă acest lucru este legal și posibil.

CE BROWSER AR TREBUI SĂ FOLOSIM?

Folosiți un browser care se bucură de o reputație bună, precum Chrome, Firefox, Brave, Safari, Edge sau Tor Browser. Atât Chrome, cât și Firefox sunt folosite la scară largă și sunt extrem de sigure. Unele persoane preferă Firefox datorită accentului pus pe confidențialitate. Orice ați alege, este important să reporniți atât browserele, cât și computerul relativ frecvent, pentru a menține browserul la zi. Dacă doriți să comparați funcțiile browserelor, consultați această resource pusă la dispoziție de Freedom of the Press Foundation. Indiferent de browser, e o idee bună să folosiți o extensie sau un program de completare precum Privacy Badger, uBlock Origin sau Privacy Essentials de la DuckDuckGo, care împiedică comercianții și alți urmăritori de terță parte să urmărească unde mergeți și ce site-uri vizitați. Iar când navigați pe internet, luați în considerare comutarea căutărilor implicite pe web pe de Google pe DuckDuckGo, Startpage sau alt motor de căutare cu protecție a confidențialității. Această comutare ar ajuta și la limitarea comercianților și urmăritorilor de terță parte.

Securitatea browserelor în realitate

La începutul anului 2021, mai mulți activiști ai societății civile tibetani au fost ținta unui inteligent program de completare pentru browser rău intenționat, care le fura datele din e-mail și browser. Programul de completare, intitulat „Componente actualizare Flash" era prezentat utilizatorilor care vizitau site-uri web asociate cu e-mailuri de tip phishing. Aceste atacuri prin extensii sau programe de completare pot fi la fel de dăunătoare ca software-urile rău intenționate partajate direct prin descărcări de tip phishing sau alte software-uri.



Siguranța pe rețelele sociale

Organizația dvs. poate divulga multe informații – uneori, mai mult decât intenționează – prin postările și comentariile de pe rețelele sociale.

Fie că folosiți Facebook, Twitter, Instagram, YouTube, fie că folosiți rețele sociale regionale precum VKontakte și Odnoklassniki, ar trebui să fiți mereu precauți la ceea ce postați și să configurați corespunzător setările de confidențialitate disponibile. Acest lucru nu se aplică doar paginilor oficiale ale organizației, ci, în unele cazuri, și conturilor personale ale personalului și ale rudelor și familiilor acestora.

Securitatea rețelelor sociale și societatea civilă

Chiar și organizațiile cu un risc scăzut pot fi luate în vizor și hărțuite pe rețelele sociale, dacă nu sunt implementate politici de securitate adecvate. În acest exemplu din 2018, un adăpost de animale non-profit a pierdut mii de dolari și mulți susținători după ce un administrator de cont neautorizat a inițiat o strângere de fonduri falsă, iar mai multe conturi false care uzurpau identitatea unor angajați au apărut pe platformă. Dacă hackerii sunt dispuși la asemenea eforturi pentru a face câte mii de dolari pe seama unui adăpost de animale, gândiți-vă de ce daune ar fi capabili niște adversari sofisticați dacă ar obține acces la conturile organizației dvs. sau v-ar uzurpa identitatea online.

Pe lângă atacarea conturilor, grupurile societății civile și utilizatorii individuali din multe țări se confruntă, de asemenea, cu repercusiuni ale conținutului postat pe rețele sociale. Un exemplu ar fi cel din Zambia din 2020, când poliția a arestat un elev de 15 ani în urma acuzației de defăimare a președintelui într-o postare pe Facebook. Copilul, care a postat folosind un pseudonim, a fost identificat în baza numărului de telefon utilizat pentru înregistrarea contului și a adresei IP.

DEZVOLTAȚI O POLITICĂ PRIVIND REȚELELE SOCIALE PENTRU ORGANIZAȚIE

Presupuneți că tot ceea ce postați pe rețele sociale ar putea deveni public și concepeți o politică corespunzătoare privind rețele sociale pentru organizație. Această politică ar trebui să răspundă la întrebări precum: Cine are acces la conturile de pe rețelele sociale? Cui îi este permis să posteze și cine trebuie să aprobe postările? Ce informații nu trebuie partajate pe rețelele sociale? Dacă postați fotografii, informații despre locație sau alte informații de identificare despre personalul, partenerii dvs. sau participanții la evenimente, ați cerut permisiunea acestora, iar aceștia au luat în considerare riscurile? Pe lângă dezvoltarea politicii și explicarea acesteia personalului, asigurați-vă că ați configurat adecvat setările de confidențialitate și securitate (adesea numită „siguranță"). Iată câteva întrebări importante pe care trebuie să vi le adresați atunci când decideți ce setări de confidențialitate și siguranță sunt cele mai potrivite pentru conturile personalului și organizației dvs.:

- Doriți să partajați postările dvs. publicului sau doar unui anumit grup de persoane interne sau externe?
- Ar trebui să acceptați comentarii, răspunsuri sau interacțiuni la mesaje sau postări?
- Ar trebui să puteți fi găsiți, dvs. sau organizația, în baza adresei de e-mail sau numărului de telefon (personal sau de serviciu)?
- Vreți ca locația dvs. să fie partajată automat atunci când postați?
- Doriți să blocați sau să dezactivați interacțiune cu conturile ostile?
- Doriți să blocați anumite cuvinte sau hashtaguri?

Fiecare rețea socială are diferite setări de confidențialitate și siguranță, însă aceste concepte generale se aplică universal. Când luați în considerare aceste întrebări, ajutați-vă de ghidurile utile de confidențialitate disponibile pe majoritatea platformelor: **Facebook**, **Twitter**, **Instagram**, și **YouTube**. În special pentru Facebook, fiți precauți în ceea ce privește opțiunile de confidențialitate ale Grupurilor. Grupurile de Facebook sunt un loc popular pentru implicare, propagandă și partajarea de informații, însă grupurile nerestricționate pot fi accesate de toată lumea. Destul de des, conturile „false" se dau drept persoane reale, pentru a se infiltra în grupuri sau pagini private de pe rețele sociale. Prin urmare, fiți precauți când acceptați cererile de „prietenie" sau „urmărire". Rețineți că siguranța conturilor organizației dvs. de pe rețelele sociale depinde de securitatea conturilor „asociate" cu acestea. Acest lucru este în special important în cazul Facebook, unde pagina organizației dvs. ar putea fi administrată de contul personal asociat al cuiva.

HĂRȚUIREA ONLINE

Din păcate, multe organizații se confruntă cu hărțuire semnificativă online, în special pe rețele sociale. Această **hărțuire este adesea îndreptată cu și mai mare intensitate asupra femeilor și populațiilor marginalizate**. Violența online împotriva femeilor, în special, poate crea un mediu ostil care duce la auto-cenzură sau retragerea din discursul politic sau civic. Conform raportului echipei pentru egalitate de gen, egalitatea femeilor și democrație din cadrul NDI, **Tweeturi care ne taie aripile**, atunci când atacurile împotriva femeilor active în politică au loc online, acoperirea vastă a rețelelor sociale pot amplifica efectul hărțuirii și abuzului psihologic, subminând sentimentul de securitate personală al femeilor în moduri neexperimentate de bărbați.

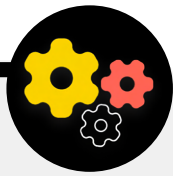
Atunci când organizația dvs. dezvoltă o politică privind rețelele sociale, este important să cunoașteți aceste dinamici. Includeți în planul de securitate un sprijin structurat pentru personalul care primește mesaje negative, insulte sau amenințări pe rețelele sociale, atât ca parte a jobului, cât și în viața personală. Dezvoltați o infrastructură anti-hărțuire la nivelul organizației dvs., care să includă chestionare pentru personal, care să ajute la înțelegerea modului în care hărțuirea online îi afectează și creați o echipă de răspuns rapid pentru a ajuta personalul să facă față situațiilor dificile. **Manual de apărare contra hârțuirii online** creat de PEN America oferă, de asemenea, recomandări detaliate despre modul în care vă puteți sprijini personalul care se confruntă cu asemenea hărțuire. Dacă personalul nu are probleme să o facă, puteți, de asemenea, implementa **raportarea incidentelor** de hărțuire și/sau conturile problematice direct pe platformă.

Atunci când interacționați cu angajați care au fost victima hărțuirii online (precum și în lumea fizică), este important să dați dovadă de sensibilitate. Așa cum subliniază Association for Progressive Communications Women's Rights Programme (WRP) în **Take Back the Tech**, trebuie să înțelegeți că un supraviețuitor ar putea fi traumatizat și să recunoașteți că violența (online și offline) nu este niciodată vina supraviețuitorului. Asigurați-vă că asemenea probleme pot raportate și discutate (dacă personalul nu are probleme să facă acest lucru) într-un mediu confidențial și sigur, cu opțiunea anonimatului. Și includeți în planul de securitate al organizației dvs. o listă a profesioniștilor locali, organizațiilor și agențiilor locale de aplicare a legii la care personalul poate apela pentru asistență juridică, medicală, de sănătate mintală și tehnică, dacă este nevoie. Pentru idei suplimentare, consultați **Ghidul privind siguranța online** al Feminist Frequency.

Păstrarea site-urilor active

Pe lângă protejarea abilității dvs. de a accesa internetul în siguranță, este la fel de important să faceți ceea ce puteți pentru a vă asigura că ceilalți pot accesa site-urile sau proprietățile web ale organizației dvs.

Pentru paginile de pe rețelele sociale, aceasta presupune protejarea conturilor cu parole puternice unice și autentificarea cu doi factori. Pentru site-ul dvs., aceasta presupune protejarea împotriva atacurilor hackerilor și atacurilor de tip refuz-serviciu. Atacurile distribuite de refuzare a serviciilor (DDoS) survin atunci când un grup mare de computere vă inundă simultan serverul cu trafic rău intenționat. Dacă sunteți organizație a societății civile sau altă organizație non-profit, este foarte probabil să vă calificați pentru protecție DDoS gratuită - îngreunând mult eforturile unui adversar de a vă închide site-ul web. Iată câteva opțiuni disponibile: **proiectul Galileo** dezvoltat de Cloudflare, **proiectul Shield**dezvoltat de Google sau serviciul **Deflect** al eQualitie.



Găzduirea sigură a site-ului web al organizației dvs.

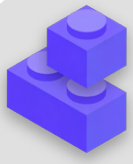
Site-urile sunt găzduite pe computere - iar acestea sunt vulenabile la atacurile hackerilor, la fel ca dispozitivele dvs. Dacă este posibil, organizația dvs. ar trebui să utilizeze servicii de găzduire existente precum Wordpress.com, Wix sau altele care gestionează toată securitatea site-ului în locul dvs. Dacă citiți acest îndrumat, este posibil ca organizația dvs. să se califice pentru găzduirea sigură gratuită a unui site Wordpress oferită de **eQualitie** prin **serviciul de găzduire eQPress**. Aceasta este o opțiune excelentă pentru organizațiile civice cu site-uri Wordpress existente sau dacă organizația dvs. vrea să construiască un nou site. Dacă nevoile site-ului dvs. sunt mai complexe, sau dacă trebuie să găzduiți singuri site-ul, asigurați-vă că vă axați pe menținerea la zi a sistemului de operare și software-ului de găzduire web, exact cum faceți cu computerul dvs. personal. Luați în considerare folosirea unor furnizori de găzduire în cloud cu vechime, precum Amazon Web Services (AWS), Microsoft Azure sau **eclips.is** de la Greenhost, care oferă opțiuni de securitate îmbunătățite pentru site-urile găzduite. Indiferent de ce instrumente folosiți pentru a vă găzdui site-ul, asigurați-vă că toate conturile utilizate pentru accesarea setărilor de editare și configurare a conținutului sunt protejate cu parole puternice și autentificarea cu doi factori.

Dacă organizația dvs. dispune de resursele tehnice pentru a găzdui propriul site, vă recomandăm să optați pentru un așa-numit „site static” sau un site web simplu. Opusul site-urilor dinamice, aceste tipuri de site-uri reduc suprafața de atac pentru hackeri și vor îmbunătăți rezistența site-ului la atacuri.

Protejarea rețelei Wi Fi

Toți acești pași pentru protejarea traficului pe web împotriva supravegherii și cenzurii sunt importanți, însă nu înlocuiesc securitatea de bază a rețelei de la birou sau de acasă.

Nu uitați aspecte de bază precum utilizarea unei parole puternice (nu a parolei implicite) pentru routerul(ele) Wi Fi, asigurarea că doar utilizatorii autorizați au acces la rețeaua dvs. prin schimbarea frecventă a parolei și activarea paravanului de protecție implicit al routerelor wireless. Vă recomandăm că creați și o rețea pentru oaspeți la birou, pentru vizitatorii care folosesc internetul.



Siguranța pe internet

- **Organizați cursuri regulate de instruire privind importanța respectării măsurilor de securitate pe web de bază pentru personal.**
- **Reamintiți personalului să navigheze întotdeauna utilizând HTTPS și un DNS criptat.**
- **Impuneți personalului să își repornească regulat browserele pentru a instala actualizările.**
- **Încurajați utilizarea de browsere și extensii cu protecție a confidențialității.**
- **Dacă un VPN este adecvat organizației dvs., alegeți unul cu renume, instruiți personalul cum să-l folosească și asigurați-vă că este folosit în mod constant.**
- **Dezvoltați șu distribuiți o politică clară privind utilizarea rețelelor sociale la nivelul organizației.**
- **Activați setările de confidențialitate și securitate pe conturile de pe rețelele sociale.**
- **Înțelegeți impactul hărțuirii online și fiți pregătiți să sprijiniți personalul afectat.**
- **Creați o listă a profesioniștilor, organizațiilor și agențiilor locale de aplicare a legii la care personalul poate apela pentru asistență juridică, de sănătate mintală și tehnică, ca răspuns la hărțuirea online.**
- **Solicitați protecție DDOS pentru site-urile dvs.**
- **Folosiți un furnizor de găzduire web fiabil și de încredere.**
- **Folosiți o parolă puternică și o rețea pentru oaspeți pentru rețeaua Wi Fi de la birou.**

Protejarea securității fizice

Este esențial să asigurați securitatea fizică a dispozitivelor dvs. Rețineți că securitatea fizică nu se rezumă doar la dispozitive, ci trebuie să includă strategii care să protejeze și restul posesiunilor. Acestea includ documente pe hârtie, biroul sau spațiile de lucru ale organizației; și, desigur, dvs., personalul și voluntarii.

Supravegherea, cenzura și societatea civilă

Din păcate, atacurile fizice asupra organizațiilor societății civile nu sunt o noutate și au adesea implicații semnificative atât asupra securității fizice, cât și a securității informațiilor. O tactică obișnuită utilizată de adversari pentru a suprima activitatea OSC-urilor include razia și încheierea birourilor - atât pentru a intimida personalul, cât și, în unele cazuri, pentru a fura sau confisca informații și echipamente tehnice. Asemenea amenințări au adesea ca țintă grupuri minoritare și pentru drepturile omului și OSC-uri care operează în spațiul democrației și administrației. De exemplu, birourile LGBT+ Rights Ghana, o organizație civică care la începutul anului 2021 a deschis primul centru comunitar pentru comunitatea LGBTQI+ din țară, au fost amenințate că vor fi arse din temelie și, în final, au fost percheziționate și închise de poliție. Asemenea razii nu au impact doar asupra operațiunilor fizice ale organizației, ci afectează și sentimentul de securitate al personalului.

Protejarea activelor fizice

O componentă esențială a securității informațiilor este securitatea fizică a dispozitivelor dvs.

Pe lângă diminuarea impactului unui dispozitiv furat prin blocarea ecranului și parole, implementarea criptării complete a discului și activarea funcțiilor de ștergere de la distanță, trebuie să acordați atenție și felului în care ați putea împiedica în primul rând furtul dispozitivelor. Pentru a îngreuna furtul, asigurați-vă că instalați încuietori robuste (și schimbați-le dacă există schimbări de personal) la birou și/sau acasă. În plus, vă recomandăm să cumpărați un seif de laptop sau un dulap care poate fi încuiat, pentru protejarea dispozitivelor peste noapte. Camerele de supraveghere sunt tot mai ieftine și aveți la dispoziție tot mai multe versiuni simple destinate utilizării la domiciliu. Camerele sau sistemele cu senzor de mișcare instalate în incinte pot detecta și, sperăm noi, împiedica spargerile și furtul. Căutați o opțiune care respectă confidențialitatea, disponibilă în țara dvs., și asigurați-vă că optați pentru camere furnizate de companii de încredere care nu sunt stimulate să predea date și informații unui potențial adversar.

Dacă biroul prezintă un risc ridicat de intrare cu forța sau de razie, nu păstrați datele sensibile ale organizației în birou - fie salvați-le într-un cloud (așa cum am discutat mai sus), fie mutându-le fizic într-o locație mai puțin vizată. Dacă dispozitivele vechi încă au informații stocate pe ele, însă nu mai sunt în uz, vă recomandăm să le ștergeți - acest ghid oferit de Wirecutter este o resursă excelentă cu instrucțiuni pentru majoritatea dispozitivelor moderne. Dacă ștergerea dispozitivelor nu este posibilă, le puteți distruge fizic. Cea mai ușoară, poate chiar și cea mai ecologică, metodă este să spargeți dispozitivele și unitățile de hard disk cu un ciocan. Uneori, cele mai vechi soluții sunt încă cele mai eficiente! Chiar înainte de acești pași tehnici, creați un inventar al tuturor echipamentelor organizației. Dacă nu aveți o listă a tuturor dispozitivelor, este mai greu să țineți evidența a ceea ce ar putea lipsi în cazul în care se fură.

Instalarea propriului sistem de securitate în birou

Dacă bugetul organizației dvs. nu vă permite un sistem de supraveghere complet pentru birou și vă preocupă confidențialitatea, puteți încerca o opțiune creativă precum aplicația Haven dezvoltată de Guardian Project, care să vă notifice în cazul în care un intrus pătrunde în birou. Haven este o aplicație pentru smartphone care poate transforma orice telefon Android într-un detector de mișcare, sunet, vibrație și lumină. Puteți configura aplicația pe câteva dispozitive Android ieftine, în diferite puncte ale biroului, pentru a vă notifica dacă detectează oaspeți nepoftiți și intruși nedoriți. Aplicația Haven poate fi utilă și într-o cameră de hotel sau într-un apartament, dacă prezentați un risc ridicat. Cea mai bună alegere este un sistem de supraveghere complet, însă, dacă nu vă permiteți și doriți să aflați mai multe despre utilizarea aplicației Haven, vizitați site-ul proiectului.

CE SĂ FACEM CU ATÂTEA HÂRTII?

Este posibil ca organizația dvs. să aibă multe informații imprimate pe hârtie, notate în agende sau mâzgălite pe notițe adezive. Unele dintre acestea pot fi foarte sensibile: imprimări de bugete, liste de participanți, scrisori sensibile de la donatori și notițe de la întâlniri private. Este esențial să vă gândiți și la securitatea acestor informații. Dacă trebuie neapărat să păstrați copii pe hârtie a unor informații sensibile, asigurați-le că acestea sunt păstrate în siguranță într-un dulap încuiat sau în alt loc sigur. Nu păstrați informații confidențiale sau sensibile (inclusiv parole) pe birou sau notate pe o tablă. Dacă credeți că organizația dvs. prezintă un risc ridicat de intrare cu forța sau de razie, păstrați informațiile extrem de sensibile într-o locație mai puțin vizată.
În măsura în care acest lucru este posibil, străduiți-vă să eliminați informațiile pe hârtie de care nu aveți nevoie. Nu uitați, nu vi se poate fura ceva ce nu aveți. Creați, la nivel de organizație, o politică privind proprietatea notițelor pe hârtie și colectați toate notițele de la personalul care decide să părăsească organizația sau care este concediat, la fel cum ați colecta un computer sau un telefon de) serviciu. Pentru a elimina documentele sensibile, achiziționați un distrugător de documente de calitate. O activitate distractivă la sfârșit de săptămână este să luați o pauză de 15 minute împreună cu personalul și să distrugeți hârtiile sensibile sau notițele luate pe hârtie în săptămâna respectivă.

POLITICA BIROULUI

Cu toate că multe aspecte ale „biroului" s-au schimbat semnificat de la începutul pandemiei COVID-19, este încă important ca organizația dvs. să implementeze o politică clară privind accesul în birouri. O asemenea politică trebuie să aducă în discuție întrebări cheie, inclusiv cui îi este permis să intre în birou (și când), cine poate accesa resursele biroului (precum rețeaua Wi Fi) și ce să facem cu oaspeții.

O întrebare simplă, doar importantă, la care trebuie să răspundem este cine primește o cheie a biroului. Doar personalul de încredere ar trebuie să aibă chei, iar încuietorile trebuie schimbate dacă cineva părăsește organizația și/sau în mod semi-regulat. Pe timpul zilei, ușile care sunt lăsate descuiate trebuie supravegheate constant de o persoană de încredere din cadrul organizației. Gândiți-vă, de asemenea, dacă organizația dvs. are o relație bazată pe încredere cu proprietarul clădirii sau cu personalul de curățenie. Gândiți-vă la ce informații sau dispozitive ar putea avea acces aceștia și asigurați-vă că sunt protejate, în special dacă nu aveți o relație bazată pe încredere. Indiferent de cine are acces, trebuie să desemnați pe cineva de încredere să încuie biroul și să se asigure că dispozitivele sunt bine securizate înainte de a părăsi biroul la finalul zilei de lucru.

Primiți vizitatori în birou? Dacă da, asigurați-vă că aceștia nu au acces (sau, cel puțin, acces nesupravegheat) la dispozitive sau date sensibile scrise pe hârtie. Dacă vi se solicită sau se așteaptă de la dvs. să le oferiți vizitatorilor acces la internet, vă recomandăm să configurați o rețea pentru „oaspeți", pentru ca aceștia să nu vă poată monitoriza traficul obișnuit. În general, doar personalul de încredere ar trebui să poată accesa rețeaua și dispozitivele din rețea precum imprimantele. O altă idee bună este să solicitați înregistrarea vizitatorilor, pentru a ține o evidență a acestora.

Atunci când creați o politică a biroului, obiectul ar fi să permiteți doar persoanelor de încredere acces la dispozitive, documente, spații și sisteme sensibile.

SPRIJINIREA PERSONALULUI ȘI VOLUNTARILOR

Amenințările asupra securității fizice a organizației dvs. pot afecta și personalul. Ca și în cazul hărțuirii pe rețelele sociale, aceste amenințări asupra securității fizice afectează adesea disproporționat femeile și comunitățile marginalizate. Nu vorbim doar de ferestre sparte și laptopuri furate. Intimidarea, amenințările sau episoadele de violență fizică sau sexuală, abuzul domestic și frica de atac pot avea un impact negativ semnificativ asupra vieților personalului. Pentru organizațiile care lucrează cu și sprijină în special femeile active în politică, instrumentul de planificare a siguranței **#Gândește10** oferit de NDI este o resursă utilă pentru persoanele care prezintă un risc crescut din cauza activității lor.

Bunăstarea personalului este, evident, un activ important pentru ei, ca persoană, însă reprezintă și un element crucial pentru o organizație sănătoasă și funcțională. În acest scop, gândiți-vă de ce resurse suplimentare aveți nevoie pentru a vă proteja personalul și, în cazul unui atac fizic sau digital, să îi ajutați să își revină. Așa cum s-a menționat anterior în Îndrumar, acest lucru înseamnă cel puțin dezvoltarea unei liste de resurse prin care să conectați personalul la asistență juridică, medicală, de sănătate mintală și tehnică. Încă o dată, **Manual de apărare contra hărțuirii online** creat de PEN America conține idei care să ajute organizațiile să își sprijine personalul în timpul și în urma crizelor, iar **Manualul securității holistice** al Tactical Tech include conținut relevant despre cum reacționează adesea organizațiile în timpul atacurilor intense.

SECURITATEA ÎN TIMPUL CĂLĂTORIILOR

Călătoriile - fie ele spre altă țară, fie spre un oraș apropiat - intensifică adesea riscurile de securitate a informațiilor. În general, este sigur să presupuneți că dvs. și dispozitivele dvs. nu aveți drepturi de confidențialitate atunci când traversați granița. Prin urmare, este o idee bună să includeți o politică privind călătoriile în planul de securitate al organizației dvs., care să conțină mementouri privind cele mai bune practici de securitate. Politica de călătorie a organizației dvs. trebuie să includă multe dintre informațiile dezbătute în alte secțiuni ale Îndrumarului, inclusiv utilizarea în siguranță a internetului și securizarea fizică a dispozitivelor și a altor surse de informații, pe care să le aveți la dvs. în permanență în timp ce călătoriți. Dacă este posibil, nu luați cu dvs. informații sensibile, folosiți un computer care nu conține date, accesați fișierele de care chiar aveți nevoie din cloud, iar apoi ștergeți-le când ajungeți acasă.

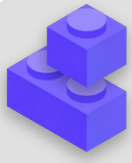
Pe lângă pregătirea pentru călătorie și reducerea la minimum a datelor partajate în timpul călătoriei, există câteva sfaturi operaționale esențiale pe care să le luați în considerare și să le includeți în politica de călătorie a organizației dvs.

Vă recomandăm să folosiți laptopuri și telefoane destinate special călătoriilor, care să conțină o cantitate minimă de date sensibile. Dacă majoritatea activității organizației dvs. se desfășoară în cloud, un dispozitiv Chromebook, care este relativ necostisitor, poate fi o opțiune bună. Realizați o resetare la setările din fabrică sau „ștergeți complet" aceste dispozitive la întoarcere, înainte de a vă conecta la rețelele Wi Fi comune de acasă sau de la birou.
Instruiți personalul ce să facă dacă sunt interogați de autorități sau opriți la un punct de trecere a frontierei. Căutați modalități de a limita cantitatea de informații cu care călătorește cineva, dacă acest lucru creează îngrijorări, și creați protocoale de check-in pentru personalul care călătorește în regiuni sensibile. Furnizați personalului informații de contact și un plan de acțiune pentru situațiile în care ceva nu merge bine în călătorie. Acestea includ informații despre spitale, clinici sau farmacii locale, în cazul în care au nevoie de asistență medicală în timp ce călătoresc.

De asemenea, personalul trebuie să țină toate dispozitivele asupra lor în timpul călătoriilor. De exemplu, țineți-vă laptopul la picioare (nu în compartimentul de deasupra capului sau în bagajul de cală) atunci când călătoriți cu autobuzul, trenul sau avionul. Nu presupuneți că o cameră de hotel – sau chiar seiful din hotel – este un „loc sigur" pentru păstrarea dispozitivelor și articolelor sensibile. Nu vă încredeți în porturile de încărcare publice prin USB. Porturile de încărcare prin USB din aeroporturi, stații și vehicule sunt din ce în ce mai răspândite și o modalitate convenabilă de a vă alimenta dispozitivele. Cu toate acestea, ar putea fi un vector simplu de infectare cu software-uri rău intenționate. Încărcați-vă dispozitivele fie prin metoda tradițională, folosind o priză, fie achiziționați **dispozitive care blochează transferul de date prin USB**, pentru a permite personalului care călătorește să-și încarce dispozitivele prin USB.

Rezervarea în siguranță a călătoriilor pentru organizația dvs.

Atunci când creați o politică de călătorie, rețineți că informațiile ar putea fi expuse atunci când organizați sau rezervați călătorii. Acest lucru poate fi deosebit de important dacă organizați evenimente importante, instruiri sau conferințe pentru care manevrați informații sensibile ale unei varietăți de personal, parteneri sau participanți. Gândiți-vă atent la cum veți partaja și stoca (dacă este cazul) în siguranță date cu caracter personal precum detaliile din pașaport, itinerarele de călătorie și fișele medicale. Manualul activității unui organizator, dezvoltat de Tactical Tech, cuprinde o foaie de lucru excelentă care să vă ajute organizația să reconsidere întrebări cheie privind securitatea călătoriilor, pe care o puteți **accesa aici**.



Protejarea securității fizice

- **Reamintiți personalului că își protejeze fizic în permanență dispozitivele.**
- **Verificați și securizați toate căile prin care persoanele pătrund în spațiul dvs. - uși și ferestre.**
- **Creați o politică privind vizitatorii și accesul în birouri.**
- **Folosiți încuietori robuste și schimbați-le prin rotație/înlocuiți-le când este nevoie.**
- **Luați în considerare să instalați camere de supraveghere sau alte sisteme de supraveghere în birouri.**
- **Achiziționați un distrugător de documente.**
  - Programați un interval în care personalul să elimine documentele pe hârtie care conțin informații sensibile.
- **Creați o listă a profesioniștilor, organizațiilor și agențiilor locale de aplicare a legii la care personalul poate apela pentru asistență juridică, medicală, de sănătate mintală și tehnică, ca răspuns la atacuri fizice sau amenințări.**
- **Dezvoltați o politică privind călătoriile pentru organizație.**
- **Asigurați-vă că personalul știe ce să facă în cazul unei urgențe în timpul călătoriilor, inclusiv instruiți personalul ce să facă dacă sunt opriți la un punct de trecere a frontierei.**
- **Înainte de orice călătorie locală, națională sau internațională, reamintiți personalului să limiteze informațiile stocate pe dispozitive.**
- **Fiți atenți la datele suplimentare care sunt create și partajate atunci când organizați călătorii sau evenimente.**

Ce trebuie să facem când lucrurile merg prost

Acum știți cum trebuie să procedați corect. Ați implementat politicile și ați instruit pe toată lumea din organizație cu privire la cele mai bune practici. Chiar și după tot acest efort, probabilitatea ca ceva să meargă prost este încă destul de ridicată.

Se mai întâmplă. Iar atunci, este esențial să aveți implementat un plan de răspuns la incidente. Răspunsul la incidente este o parte de o importanță crucială, adesea subestimată, a planului de securitate al organizației dvs., deoarece poate face diferența între un atac care vă poate distruge reputația organizației și o piedică neplăcută. Rețineți că nu veți putea răspunde la un incident decât dacă sunteți conștienți de acesta. Este foarte important să aveți o cultură puternică de securitate la nivelul organizației și să încurajați personalul să raporteze problemele. De aceea, este mai bine să recompensați un bun comportament de securitate decât să pedepsiți breșele sau greșelile de securitate. La fel de important este și să fiți empatici și să vă preocupe bunăstarea personalului atunci când se raportează un incident. Este de dorit ca personalul să raporteze imediat că a accesat un link dintr-un mesaj de tip phishing, că i s-a furat telefonul sau că un cont de pe rețele sociale a fost atacat de hackeri - nu să ezite de frica represaliilor sau lipsa de sprijin. La urma urmei, răspunsul la incidente, la fel ca strategiile de diminuare menționate în alte secțiuni ale Îndrumarului, este un efort care trebuie făcut la nivelul întregii organizației.

- Pentru ce trebuie să vă pregătiți? Pe scurt, pentru orice s-ar putea întâmpla. Aceasta diferă de la o organizație la alta, însă iată câteva întrebări comune la care vă poate ajuta să răspundeți un plan de răspuns la incidente:
- Ce facem dacă site-urile sau conturile noastre sunt atacate de hackeri?
- Ce facem dacă cineva face clic pe un e-mail de tip phishing sau dacă un dispozitiv se comportă ciudat?
- Ce facem dacă e-mailurile noastre sau documentele sensibile sunt furate sau scurse?
- Ce facem dacă unul dintre angajații noștri este pus în pericol fizic sau arestat? Sau dacă se confruntă cu stres și anxietate din cauza unor asemenea amenințări?
- Ce facem dacă biroul nostru suferă daune în urma unui incendiu, unei inundații sau unui dezastru natural?
- Ce facem dacă telefonul sau computerul unui angajat este pierdut sau furat?

Răspunsul la aceste întrebări poate diferi în funcție de organizație, însă este important să le analizați împreună și să creați și distribuiți un plan clar, pentru ca toți membrii organizației dvs. să fie pregătiți să acționeze imediat și să limiteze daunele.
Conform Manualului securității holistice al Tactical Tech, un bun punct de pornire pentru un plan de răspuns la incidente este definirea unui incident sau a unei urgența în contextul organizației dvs. Stabiliți ce este o „urgență" – adică, punctul în care trebuie să începeți să implementați acțiunile și măsurile de urgență plănuite. Acest lucru este important, pentru că uneori va fi neclar – imaginați-vă un scenariu în care pierdeți contactul cu un coleg aflat pe teren; cât de mult ați aștepta înainte să declarați o urgență? Nu ne-am dori să ne pripim prea devreme, însă o așteptare prea lungă poate fi dezastruoasă în anumite situații.
De asemenea, este important să vă gândiți și la pașii **operațiunii**. Atribuiți fiecărei persoane un rol clar pe care să îl conștientizeze și pe care l-a acceptat în avans – acest lucru va reduce dezorganizarea și panica în eventualitatea unui incident. În cazul fiecărei amenințări, luați în considerare diferite roluri pe care s-ar putea să fie nevoie să vi le asumați și la aspectele practice pe care le implică răspunsul în fața unei urgențe. Parte a acestei strategii importante pentru situații de urgență este activarea unei rețele de sprijin – o rețea largă de aliați, care poate include prieteni și rude, comunitatea, aliați locali, resurse guvernamentale și aliați naționali sau internaționali cum sunt ONG-urile sau jurnaliștii. Cum vă pot sprijini aliații? Ar trebui să îi contactați în avans pentru a vă asigura că sunt dispuși să vă ajute în cazul unei urgențe și pentru a le spune ce așteptări aveți de la ei?

Atunci când răspundeți la un incident, **comunicările** eficiente devin tot mai importante. Stabiliți care sunt cele mai sigure și eficiente mijloace de comunicare cu fiecare actor în diferite scenarii și identificați mijloacele de rezervă. Luați în considerare faptul că, în cazul urgențelor, ar putea fi util să aveți indicații clare privind ceea ce (și ceea ce să nu) comunicați, când să comunicați, ce canale de comunicare să folosiți și cu cine să comunicați. De asemenea, luați în considerare cum un incident ar putea afecta reputația organizației dvs. și fiți pregătiți să răspundeți adecvat. Asigurați-vă că responsabilul pentru comunicare din cadrul organizației dvs. (în anumite organizații, acesta ar putea fi persoana care administrează pagina de Facebook sau contul de Twitter) a fost informat cu privire la incident și poate urmări rețelele sociale sau alte medii pentru a un potențial impact. De asemenea, acesta trebuie să fie pregătit să răspundă la posibilele întrebări despre adresate de public sau de media, dacă este cazul. Acest lucru este îndeosebi important pentru a împiedica răspândirea de povești care v-a putea afecta negativ sau distruge reputația. Cu toate că fiecare incident și context este diferit, comunicările oneste și transparente ajută adesea la construirea încrederii în urma unui incident.

Crearea unui sistem de alertare timpurie și de răspuns

Luați în considerare crearea unui sistem de alertare timpurie și de răspuns. Un astfel de sistem sună pretențios, însă este, de fapt, doar un document centralizat (electronic sau de alt tip) pe care să-l deschideți în eventualitatea unei urgențe. În document, trebui să înregistrați toate detaliile despre indicatorii și incidentele de securitate care au survenit într-o axă de timp, să furnizați o descriere clară a acțiunilor și ordinii răspunsului plănuit și să indicați ce nevoie trebuie îndeplinite pentru a indica faptul că riscul a scăzut din nou. Ar trebui, de asemenea, să includă acțiuni de urmat în urma unui incident, pentru a-i proteja pe cei implicați de alte probleme și pentru a-i ajuta să se recupereze fizic și emoțional. Un sistem de alertare timpurie și de răspuns poate oferi documente utile pe care să le predați autorităților de aplicare a legii (dacă este cazul), o analiză ulterioară a ceea ce s-a întâmplat și indicații pentru îmbunătățirea tacticilor de prevenție și răspuns la amenințări pe viitor.

Pe lângă aceste concepte importante de răspuns la incidente, organizația dvs. trebuie să se pregătească și pentru orice răspuns **tehnic** specific. În unele cazuri, un răspuns tehnic poate fi gestionat de personalul IT intern sau administratorii de sistem. De exemplu, dacă un cont de e-mail pare să fi fost atacat de hackeri, administratorul de cont trebuie să fie pregătit și capabil să închidă sau să dezactiveze contul afectat. Însă unele incidente tehnice ar putea necesita abilități pe care personalul dvs. intern nu le deține. În astfel de situații, este important să identificați o listă de încredere de experți tehnici externi care vă pot ajuta să răspundeți la incidente. În anumite cazuri, vă recomandăm că prenegociați termenii cu furnizorii de servicii (precum gazda site-ului dvs. web sau un consultant IT), pentru a vă asigura că aceștia sunt disponibili (și nu vor percepe costuri suplimentare) pentru răspunsul la incidente tehnice.

Nu în ultimul rând, ar trebui să luați în considerare și pașii **legali**. Este important să înțelegeți protecția legală de care beneficiați, precum și obligațiile sau consecințele legale asupra organizației dvs. ca rezultat al unei breșe de date sau al unui alt incident de securitate. Un prim pas ar putea fi identificarea unui consilier juridic de încredere care să înțeleagă legile și reglementările țării sau ale zonei dvs. Discutați posibilele incidente cu consilierul juridic relevant dacă este necesar și concepeți un plan de acțiune pentru răspuns. O idee bună este să semnați un contract cu acest consilier de încredere care să vă reprezinte pe dvs. și interesele dvs. în urma unui incident, dacă este nevoie. Ca parte a acestei pregătiri legale, asigurați-vă că înțelegeți obligațiile legale ale tuturor furnizorilor sau partenerilor. Au obligația să vă informeze în cazul în care se confruntă cu o breșă de date? Ce sprijin (dacă este cazul) sunt obligați să vă ofere în cazul unui incident? Atunci când redactați contracte și acorduri cu furnizorii externi, luați în considerare posibilitatea unei breșe de date sau altui incident.

Cu toate că nu există o abordare universală pentru răspunsul la incidente, este esențială stabilirea unor planuri operaționale, de comunicare, tehnice și legale. În procesul de concepere a planului dvs. de răspuns la incidente, vă încurajăm cu tărie să faceți uz de câteva resurse excelente create pentru a ajuta organizațiile societății civile și alte grupuri de risc să răspundă la incidente. Aceste resurse includ Trusa de prim ajutor digital dezvoltată de RaReNet și CiviCERT, Manualul de apărare contra hărțuirii cibernetice creat de PEN America, Manualul securității cibernetice pentru campanii și Șablon de plan de comunicare pentru incidente cibernetice ale Centrului Belfer, cât și Linia de asistență pentru securitate digitală de pe Access Now.

Răspunsul la incidente

- **Dezvoltați un plan de răspuns la incidente la nivelul organizației și exersați-l.**
  - Faceți brainstorming despre posibilele incidente și pregătiți-vă răspunsul înainte ca incidentul să survină.
- **Asigurați-vă că toți membrii organizației dvs. cunosc metodele de comunicare și ce pași tehnici vor fi urmați în cazul unui incident.**
- **Însușiți-vă cunoștințe despre protecțiile și obligațiile legale.**
- **Pregătiți-vă să oferiți personalului organizației sprijinul emoțional și social de care au nevoie în urma unui incident.**

Anexa A:
Resurse recomandate

- Manualul securității holistice - Tactical Tech ; Licență internațională de atribuire-partajare în condiții identice 4.0 oferită de Creative Commons
  - Capitolul 2.4 - Înțelegerea și catalogarea informațiilor noastre
  - Capitolul 1.5 - Comunicarea cu privire la amenințări în cadrul echipelor și organizațiilor
  - Capitolul 3.4 - Securitatea în cadrul grupurilor și organizațiilor
- Partener în învățarea securității - Electronic Frontier Foundation ; Licență SUA de atribuire 3.0 oferită de Creative Commons
  - Model de amenințare pentru activități practice
- Ghidul de prevenire a phishingului și de igienă a e-mailului - Freedom of the Press Foundation ; Licență internațională de atribuire 4.0 oferită de Creative Commons
- Ghidul de folosire al aplicației Signal - Freedom of the Press Foundation ; Licență internațională de atribuire 4.0 oferită de Creative Commons
- Ghid de autoapărare contra supravegherii (SSD) - Electronic Frontier Foundation ; Licență SUA de atribuire 3.0 oferită de Creative Commons
  - Ce ar trebui să știu despre criptare
  - Comunicarea cu ceilalți
  - Alegerea unui VPN potrivit pentru dvs.
- Ghidul instrumentelor sigure pentru conversații de grup și conferințe - Frontline Defenders
- Data Detox Kit oferit de Tactical Tech
  - Permite accesul doar persoanelor dorite: Creează o parolă mai puternică
  - Blochează-ți ecranul mai bine
- Ghidul privind securitatea parolelor în timpul alegerilor - Center for Democracy and Technology ; Licență internațională de atribuire 4.0 oferită de Creative Commons
- Ghidul privind securitatea autentificării cu doi factori - Center for Democracy and Technology ; Licență internațională de atribuire 4.0 oferită de Creative Commons
- Autentificarea cu doi factori pentru începători - Martin Shelton ; Licență internațională de atribuire 4.0 oferită de Creative Commons
- Security-in-a-Box - Tactical Tech și Frontline Defender ; Licență neportată de atribuire-partajare în condiții identice 3.0 oferită de Creative Commons
  - Protejați-vă dispozitivul împotriva software-urilor rău intenționate și atacurilor de tip phishing
  - Protejați-vă informațiile împotriva amenințărilor fizice
- Buletinul informativ SANS: Oprește software-ul rău intenționat
- Accesul la dispozitiv și la date în cazul în care siguranța personală este în pericol - Apple
- Igiena de securitate cibernetică pentru organizații bazate pe misiuni - Global Cyber Alliance

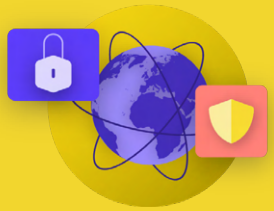
Anexa B:
Starter kit pentru planul de securitate

Folosiți următorul starter kit pentru a lua notiție pe măsură ce dvs. și organizația dvs. parcurgeți acest Îndrumar și digerați materialul și dezbateți întrebările însoțitoare cu colegii, pentru a isca o discuție productivă.
Faceți referință la „blocurile componente" din fiecare secțiune a Îndrumarului pentru a vă asigura că ați acoperit subiectele importante atunci când vă stabiliți planul de securitate. Până la finalul Îndrumarului, blocurile componente, răspunsurile la aceste discuții și notițele dvs. ar trebui să formeze fundația unui plan de securitate de succes!

Construirea unei culturi a securității

O fundație solidă: Securizarea conturilor și dispozitivelor

Comunicarea și stocarea securizată a datelor



Siguranța pe internet

Protejarea securității fizice

Ce trebuie să facem când lucrurile merg prost

Construirea unei culturi a securității

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Când puteți programa o conversație pentru a revizui planul de securitate cu întreaga organizație?
- Ce zile și ore ar fi potrivite pentru programarea de conversații regulate și cursuri de instruire despre securitate?
- Ce pași pot urma liderii pentru a modela un bun comportament de securitate și un angajament la un plan de securitate? Cum pot contribui alți membri ai organizației la securitate?

NOTIȚELE ȘI IDEILE DVS.:

O fundație solidă: Securizarea conturilor și dispozitivelor

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Cum veți implementa măsuri de securitate ale conturilor - printr-un manager de parole sau 2FA, de exemplu - la nivelul organizației dvs.? Ce obstacole ați putea întâlni în timpul implementării?
- Cum se va asigura organizația dvs. că dispozitivele sunt securizate și actualizate? Ca parte a acestui proces, va avea nevoie organizația dvs. de un plan de acțiune pentru software-urile sau computerele fără licență?
- Când este momentul oportun să organizați cursuri de instruire pentru tot personalul cu privire la cele mai bune practici pentru phishing, software-uri rău intenționate și securitatea dispozitivelor?

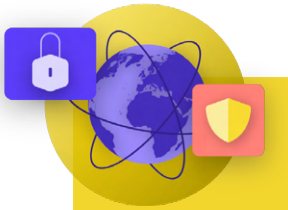
NOTIȚELE ȘI IDEILE DVS.:

Comunicarea și stocarea securizată a datelor

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Cum va implementa organizația dvs. criptarea de la un capăt la altul a mesajelor pentru o comunicare sigură? Ce obstacole ați putea întâlni în timpul implementării?
- Cum va impune organizația dvs. o soluție de partajare sigură a fișierelor, atât la nivel intern, cât și la nivel extern? Ce obstacole ați putea întâlni în timpul implementării?
- Cum va implementa organizația dvs. o soluție de stocare și de copiere de rezervă securizată a datelor? Ce obstacole ați putea întâlni în timpul implementării?

NOTIȚELE ȘI IDEILE DVS.:



Siguranța pe internet

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Cum va implementa organizația dvs. cerințe de navigate sigură pe web precum HTTPS, un browser de încredere și, dacă este cazul, un VPN pentru personal?
- Care vor fi elementele cheie ale politicii organizației dvs. privind rețelele sociale? Cum va fi aplicată aceasta?
- Cum își va proteja organizația dvs. site-urile și proprietățile web?

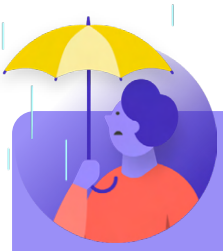
NOTIȚELE ȘI IDEILE DVS.:

Protejarea securității fizice

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Cum va distribui și aplica organizația dvs. politica privind vizitatorii și accesul în birouri?
- Cine se face responsabil pentru pregătirea personalului pentru provocările de securitate fizică și digitală cu care s-ar putea confrunta cât călătoresc în interes de serviciu?
- Ce pași poate urma personalul pentru a asigura siguranța dispozitivelor atât la birou, cât și în timpul călătoriilor?

NOTIȚELE ȘI IDEILE DVS.:



Ce trebuie să facem când lucrurile merg prost

ÎNTREBĂRI DE LUAT ÎN CONSIDERARE:

- Cum va distribui și pune în practică organizația dvs. politica de răspuns la incidente?
- Există resurse pentru personalul care ar putea avea nevoie de sprijin emoțional și social în urma unui incident? Dacă răspunsul este negativ, cum ar putea organizația să ofere aceste resurse în cazul unui incident?

NOTIȚELE ȘI IDEILE DVS.:

Anexa C:
Sursele imaginilor

Pagină 17: CNP Collection, “Security Protection Anti-Virus Software cms”, 2014, digital image, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.

Pagină 24: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

Pagină 26: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.

Pagină 29: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.

Pagină 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

Pagină 33: Crete-Nishihata, "Process For a Phishing Email Sent in 2016," digital image, University of Toronto, January 30, 2017, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/.

Pagină 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.

Pagină 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Pagină 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.

Pagină 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Pagină 50: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

Pagină 55: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.

Pagină 60: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

Pagină 62: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

Pagină 64: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.

Pagină 69: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE