NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Manual për sigurinë kibernetike

për

Parlamente

Një udhëzues për parlamentin që kërkon të fillojë me një plan të sigurisë kibernetike

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID FROM THE AMERICAN PEOPLE

Manual për sigurinë kibernetike

për

Parlamente

Një udhëzues për parlamentin që kërkon të fillojë me një plan të sigurisë kibernetike

Përmbajtjes

Legjenda vizuale

Përgjatë Manualit, përveç tekstit kryesor, do të gjeni disa elementë të ndryshëm të përsëritur dhe të theksuar. Këtu është një "legjenda" e shkurtër për t'ju ndihmuar të kuptoni elementët kryesorë:

Rast studimi

Tregon rastet e studimit që nxjerrin në pah ndikimin në jetën reale të një teme të caktuar në parlamentet globale ose të një vendi të caktuar

Këshilla shtesë

Thekson disa këshilla dhe informacione shtesë qe ndimon për të kushtuar vëmendje kur lexoni Manualin

Bota reale

Tregon shembuj të zakonshëm të mjeteve të taktikave të sigurisë kibernetike të përdorura në "botën reale", si për mirë ashtu edhe për keq.

E avancuar

Tregon një temë të avancuar - informacion që është i rëndësishëm për t'u marrë në konsideratë nga organizata juaj, por që mund të jetë pak më teknike ose më e ndërlikuar.

Blloqe ndërtimi të planit të sigurisë

Tregon "Blloqet e Ndërtimit të Planit të Sigurisë", të cilat janë pikat kryesore të marra nga secili seksion i Manualit.

Top 10

Këto 10 elemente janë kritike për planin e sigurisë së parlamentit tuaj. Nëse jeni duke kërkuar ndonjë pikë për të filluar, shikoni këtu së pari.

1. **Kryeni trajnime të rregullta për siguri, brenda parlamentit tuaj**
2. **Jini vigjilent ndaj phishing-ut dhe zhvilloni sistem raportimi.**
3. **Përdorni enkriptimin për të gjithë komunikimin - nga fundi në fund, kur është e mundur.**
4. **Kërkoni fjalëkalime të forta dhe zbatoni menaxher fjalëkalimesh në parlamentin tuaj.**
5. **Kërkoni vërtetim me dy faktorë kudo që të jetë e mundur.**
6. **Sigurohuni që të gjitha pajisjet dhe softueri i stafit të mbahen të përditësuara.**
7. **Përdorni ruajtje të sigurt në renë kompjuterike.**
8. **Përdorni HTTPS dhe, nëse është e përshtatshme, VPN, për të hyrë në internet.**
9. **Mbroni asetet fizike të parlamentit tuaj.**
10. **Zhvilloni një plan organizativ për reagim ndaj incidenteve.**

1

Ndërtimi i një kulture sigurie

2

Themel i fortë: Sigurimi i llogarive dhe pajisjeve

3

Komunikimi dhe ruajtja e të dhënave në mënyrë të sigurt

4

Qëndroni të sigurt në internet

5

Mbrojtja e sigurisë fizike

6

Çfarë të bëni kur gjërat shkojnë keq

Autorët dhe mirënjohjet

Ky udhëzues është hartuar nga Instituti Kombëtar Demokratik (NDI) dhe Partneriteti për Demokraci në Dhomën e Përfaqësuesve (HDP).

Autori kryesor: **Evan Summers (NDI)**
Autorë kontribues: **Sarah Moulton (NDI); Chris Doten (NDI)**

Duam të falënderojmë recensuesit tanë që si ekspertë të jashtëm na dhanë komente, redaktime dhe sugjerime të vlefshme gjatë përgatitjes së përmbajtjes së këtij Doracaku, veçanërisht: Fiona Krakenburger, Open Technology Fund; Bill Budington dhe Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Fondacioni për Lirinë e Shtypit; Dave Leichtman, Microsoft; Stephen Boyce, Fondacioni Ndërkombëtar për Sisteme Zgjedhore; Amy Studdart, Instituti Ndërkombëtar Republikan; Emma Hollingsworth, Aleanca Globale Kibernetike; Caroline Sinders, Design Convocation + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; Frieda Arenos, NDI; Anthony DeAngelo, NDI; Whitney Pfeifer, NDI; dhe Derek Luyten, Partneriteti për Demokraci në Dhomën e Përfaqësuesve. Dëshirojmë gjithashtu të falënderojmë Paul Kollie nga Shërbimet e Informacionit Legjislativ në Liberi; Nihad Bahram dhe Fuad Ahmed nga Parlamenti i Kurdistanit në Irak; Diana Plata nga Senati i Kolumbisë; Ayad Abbas dhe Majid Khudhur nga Këshilli i Përfaqësuesve të Irakut; dhe Tanja Danailovska nga Kuvendi i Maqedonisë së Veriut për njohuritë dhe kontributet e tyre të vlefshme.

Duam gjithashtu të shprehim mirënjohjen për të gjithë doracakët, udhëzuesit, librat e punës, modulet e trajnimit dhe materialet e tjera të përgatitura dhe të mirëmbajtura nga Komuniteti i Sigurisë Organizative (OrgSec). Ky Doracak është krijuar për të plotësuar ato materiale më të thelluara, duke kombinuar leksionet kryesore në një burim të vetëm dhe të lehtë për t'u lexuar për parlamentet që kërkojnë të fillojnë me një plan të sigurisë kibernetike.

Përveç frymëzimit indirekt nga shumë burime të mrekullueshme të përpiluara nga komuniteti, gjithashtu kemi kopjuar drejtpërdrejt gjuhë të dobishme nga një pjesë e vogël e burimeve ekzistuese në të gjithë Doracakun, veçanërisht nga Udhëzuesi i Vetëmbrojtjes së Mbikëqyrjes nga Electronic Frontier Foundation, Doracaku Holistik i Sigurisë nga (Tactical Tech), dhe një sërë shpjeguesish nga Center for Democracy and Technology dhe Freedom of the Press Foundation. Mund të gjeni citate specifike për këto burime në pjesët e mëposhtme, si dhe lidhje të plota, informacione për autorin dhe licencën brenda Shtojca A.

Kush jemi ne?

Instituti Kombëtar Demokratik për Çështje Ndërkombëtare **(NDI) është organizatë jofitimprurëse, jopartiake, me seli në Uashington D.C., që punon në partneritet në mbarë botën për të forcuar dhe mbrojtur institucionet, proceset, normat dhe vlerat demokratike dhe për të siguruar një cilësi më të mirë jete për të gjithë. NDI beson se të gjithë njerëzit kanë të drejtë të jetojnë në një botë që respekton dinjitetin, sigurinë dhe të drejtat e tyre politike – dhe se bota digjitale nuk bën përjashtim nga kjo.**

Në kuadër të NDI-së, ekipi i Demokracisë dhe Teknologjisë synon të nxisë një ekosistem global digjital në të cilin vlerat demokratike mbrohen, promovohen dhe mund të lulëzojnë; qeveritë janë më transparente dhe gjithëpërfshirëse; dhe të gjithë qytetarët janë të autorizuar të mbajnë qeverinë e tyre përgjegjëse. Ne e bëjmë këtë punë duke mbështetur një rrjet global aktivistësh të përkushtuar ndaj qëndrueshmërisë digjitale dhe nëpërmjet bashkëpunimit me partnerët për mjete dhe burime si ky Doracak. Mund të lexoni më shumë mbi punën tonë në uebfaqen, duke na ndjekur në Twitter, ose duke na kontaktuar drejtpërdrejt në cyberhandbook@ndi.org. Gjithmonë jemi të gatshëm të dëgjojmë nga ju ose t'ju përgjigjemi pyetjeve tuaja mbi ekipin dhe punën tonë në sigurinë kibernetike, teknologjinë dhe demokracinë.

Partneriteti për Demokraci në Dhomën e Përfaqësuesve (HDP) punon me legjislaturat në mbarë botën për të promovuar qeverisje të përgjegjshme, efektive dhe për të forcuar institucionet demokratike. Në qendër të punës sonë është bashkëpunimi "peer-to-peer" për të ndërtuar ekspertizë teknike në legjislaturat partnere që do të rrisin llogaridhënien, transparencën, pavarësinë legjislative, qasjen në informacione dhe mbikëqyrjen e qeverisë. HDP aktualisht ka partneritet me më shumë se 20 legjislatura kombëtare në mbarë botën. Fushat e bashkëpunimit me parlamentet partnere të HDP-së përfshijnë adresimin e çështjeve buxhetore, sigurimin e operacioneve më efektive të komitetit, përmirësimin e shërbimeve për votuesit, sigurimin e mjeteve për mbikëqyrje më të fortë, forcimin e etikës legjislative dhe përmirësimin e TI-së, bibliotekës dhe kërkimit, si dhe proceseve dhe procedurave legjislative. Programet e HDP-së zbatohen nga Instituti Kombëtar Demokratik (NDI) dhe nga Instituti Republikan Ndërkombëtar (IRI) nëpërmjet një marrëveshjeje bashkëpunuese financimi me Agjencisë së Shteteve të Bashkuara për Zhvillim Ndërkombëtar (USAID).

Kush menaxhon Sigurinë Kibernetike Parlamentare?

Një parlament efektiv dhe i sigurt kërkon staf me aftësi dhe autoritet të duhur për të zbatuar rekomandimet e përfshira në këtë Doracak. Me këtë, ata që janë përgjegjës për sigurinë kibernetike në parlamente mund të ndryshojnë shumë, dhe nuk ka një model "të duhur" se kush duhet të merret me sigurinë kibernetike. Në disa raste, mund të jetë ekip i përkushtuar për sigurinë kibernetike brenda njësisë suaj të TI-së, dhe në të tjera një grup stafi të ndryshëm administrativ dhe të anëtarëve. Sidoqoftë, mbani në mend se ndërkohë që është e rëndësishme të keni ekip të mirë në krye të sigurisë kibernetike të parlamentit tuaj, është gjithashtu përgjegjësi e të gjithëve brenda dhe rreth parlamentit të respektojnë politikat dhe procedurat e nevojshme për të mbajtur parlamentin të sigurt. Më poshtë janë disa shembuj të modeleve të ndryshme të personelit për menaxhimin e sigurisë kibernetike parlamentare:

Dhoma e Përfaqësuesve e Shteteve të Bashkuara
Në **Dhomën e Përfaqësuesve të Shteteve të Bashkuara**, zyra të anëtarëve individual angazhojnë **administrator sistemesh** që është përgjegjës për menaxhimin e të gjithë sistemeve kompjuterike të harduerit dhe softuerit të përdorur nga zyra - përfshirë menaxhimin e konsideratave të sigurisë kibernetike - dhe trajnon anëtarët e stafit për praktikat më të mira. Në nivel institucional, zyrtari kryesor administrativ i Dhomës së Përfaqësuesve angazhon ekip të burimeve të informacioneve, që përfshin një **departament përkushtuar sigurisë së informacioneve**.

Asambleja Kombëtare e Zambisë
Asambleja Kombëtare e Zambisë mbështetet në departamentin e teknologjisë së informacionit dhe komunikimit (TIK) për një sërë funksionesh, përfshirë menaxhimin e softuerit, harduerit dhe infrastrukturës së informacionit të parlamentit, trajnimin e anëtarëve ose parlamentit dhe stafit mbi sistemet e teknologjisë dhe sigurimin e infrastrukturës së informative të parlamentit nga kërcënimet kibernetike të brendshme dhe të jashtme.

Parlamenti i Malajzisë
Parlamenti i Malajzisë ka departamentin e teknologjisë së informacionit nën kryeadministratorin e parlamentit, i cili e lejon t'i shërbejë të dy dhomave të parlamentit. Kjo ndarje përfshin një post specifik për sigurinë e rrjetit, i cili e lejon atë të sigurojë që sistemet e rrjetit, qendrat e të dhënave dhe infrastruktura TIK janë të përditësuara dhe sa më të sigurta që të jetë e mundur.

Për kë është ky doracak?

Ky doracak është përpiluar me një qëllim të thjeshtë: të ndihmojë parlamentin tuaj që të zhvillojë një plan të kuptueshëm dhe të zbatueshëm të sigurisë kibernetike. Ndërsa bota po lëviz gjithnjë e më shumë në internet, siguria kibernetike nuk është vetëm fjalë kryesore, por paraqet një koncept kritik për suksesin e parlamenteve, dhe siguria e informacionit (si në internet ashtu edhe jashtë internetit) është një sfidë që kërkon fokus, investim dhe vigjilencë.

Parlamenti juaj ka gjasa ta gjejë veten – nëse nuk e ka bërë tashmë – si objektiv i një sulmi të sigurisë kibernetike. Qëllimi kësaj nuk është të duket alarmante; por paraqet realitet edhe për parlamentet që nuk e konsiderojnë veten si objektiva të veçantë.

Në një vit mesatar, Qendra për Studime Strategjike dhe Ndërkombëtare, e cila mban një **listë të vazhdueshme** të asaj që ata i quajnë "Incidente të rëndësishme kibernetike", katalogon qindra sulme serioze kibernetike, shumica prej të cilave synojnë dhjetëra, nëse jo qindra organizata në të njëjtën kohë. Përveç sulmeve të tilla të raportuara, ka gjasa të ketë qindra sulme të tjera më të vogla çdo vit që nuk zbulohen ose nuk raportohen, shumica prej tyre synojnë institucione qeveritare, organe legjislative dhe organizata politike.

Sulmet kibernetike si këto kanë pasoja të rëndësishme. Nëse qëllimi i tyre është të prishin operacionet parlamentare, të dëmtojnë reputacionin tuaj, apo edhe të vjedhin informacione që mund të çojnë në dëmtim psikologjik ose fizik për anëtarët ose stafin tuaj, kërcënimet e tilla duhet të merren seriozisht.

E mira është se nuk keni nevojë të bëheni kodues apo teknolog për të mbrojtur veten dhe parlamentin tuaj kundër kërcënimeve të zakonshme. Megjithatë, duhet të jeni të përgatitur për të investuar përpjekje, energji dhe kohë në zhvillimin dhe zbatimin e një plani të fortë parlamentar të sigurisë.

Nëse kurrë nuk keni menduar mbi sigurinë kibernetike të parlamentit tuaj, nuk keni pasur kohë të përqendroheni në të, ose dini disa informata themelore për këtë temë, por mendoni se parlamenti juaj mund të përmirësojë sigurinë e vet kibernetike, ky Doracak është për ju. **Pavarësisht se nga vini, ky Doracak synon t'i japë parlamentit tuaj informacione thelbësore që i nevojiten për të vendosur një plan të fortë sigurie - një plan që shkon thjesht përtej vendosjes së fjalëve në letër dhe që ju mundëson juve të vini në veprim praktikat më të mira.**

Çfarë është plani i sigurisë dhe pse parlamenti im duhet ta ketë një të tillë?

Plani i sigurisë është grupi i politikave, procedurave dhe udhëzimeve të shkruara për të cilat parlamenti juaj ka rënë dakord për të arritur nivelin e sigurisë që ju dhe ekipi juaj mendoni se është i përshtatshëm për të mbajtur njerëzit, partnerët dhe informacionin tuaj të sigurt. Një plan sigurie organizative i hartuar mirë dhe i përditësuar mund t'ju mbajë të sigurt dhe t'ju bëjë më efektiv, duke ofruar qetësinë e nevojshme për t'u fokusuar në punën e rëndësishme të përditshme të parlamentit tuaj. Pa menduar për një plan gjithëpërfshirës, është shumë e lehtë të jeni të verbër ndaj disa lloje kërcënimesh, duke u fokusuar shumë në një rrezik ose duke injoruar sigurinë kibernetike derisa të paraqitet ndonjë krizë.

Kur filloni të zhvilloni një plan sigurie, ka disa pyetje të rëndësishme që duhet t'ia parashtroni vetes, dhe këto pyetje formojnë një proces të quajtur vlerësim të rrezikut. Përgjigjja e këtyre pyetjeve ndihmon parlamentin tuaj të kuptojë kërcënimet unike me të cilat përballeni dhe ju lejon të tërhiqeni dhe të mendoni në mënyrë gjithëpërfshirëse për atë që duhet të mbroni dhe nga kush duhet ta mbroni. Vlerësues të trajnuar, të ndihmuar me sisteme si **SAFETAG** nga Internews, për kornizë revizioni, mund të ndihmojë në udhëheqjen e parlamentit tuaj nëpërmjet një procesi të tillë. Nëse mund të keni qasje në atë nivel të ekspertizës profesionale, ia vlen, por edhe nëse nuk mund t'i nënshtroheni një vlerësimi të plotë, duhet të takoheni me palët e interesuara në të gjithë parlamentin për të shqyrtuar me kujdes këto pyetje kyçe:

1 Çfarë asetesh ka parlamenti juaj dhe çfarë dëshironi të mbroni?

Mund të filloni t'u përgjigjeni këtyre pyetjeve **duke krijuar një katalog të të gjitha aseteve të parlamentit tuaj**. Informacione të tilla si mesazhet, postat elektronike, kontaktet, dokumentet, kalendarët dhe vendndodhjet janë të gjitha pasuritë e mundshme. Telefonat, kompjuterët dhe pajisjet e tjera mund të jenë asete. Edhe njerëzit, lidhjet dhe marrëdhëniet mund të jenë gjithashtu asete. Përpiloni një **listë të aseteve tuaja** dhe përpiquni t'i katalogoni sipas rëndësisë së tyre për organizatën, ku i mbani ato (ndoshta vende të shumta digjitale ose fizike) dhe çfarë i pengon të tjerët që t'i qasen, t'i dëmtojnë ose t'i prishin ato. Mbani në mend se jo gjithçka është njëlloj e rëndësishme. Nëse disa nga të dhënat e parlamentit janë çështje publike ose informacione që ju tashmë i publikoni, ato nuk janë sekrete që ju duhet t'i mbroni.

2 Cilët janë kundërshtarët tuaj dhe cilat janë aftësitë dhe motivet e tyre?

"Kundërshtar" është një term që përdoret shpesh në sigurinë organizative. Me fjalë të thjeshta, kundërshtarët janë aktorët (individët ose grupet) që janë të interesuar të synojnë parlamentin tuaj, të prishin punën tuaj dhe të kenë qasje ose të shkatërrojnë informacionin tuaj: të këqijtë. Shembuj të kundërshtarëve të mundshëm mund të përfshijnë mashtrues financiarë, qeveri kundërshtare ose hakerë të motivuar ideologjikisht ose politikisht. Është e rëndësishme të përpiloni një listë të kundërshtarëve tuaj dhe të mendoni në mënyrë kritike se kush mund të dëshirojë të ndikojë negativisht në parlamentin dhe stafin tuaj. Ndërsa është e lehtë të përfytyrosh aktorë të jashtëm (si një qeveri e huaj ose një grup i caktuar politik) si kundërshtarë, mbani në mend gjithashtu se kundërshtarë mund të jenë njerëz që ju i njihni, si p.sh. punonjësit e pakënaqur, ish-stafi dhe anëtarët ose partnerët që nuk ju mbështesin.

Kundërshtarë të ndryshëm paraqesin kërcënime të ndryshme dhe kanë burime dhe aftësi të ndryshme për të ndërprerë operacionet tuaja dhe për të fituar qasje ose për të shkatërruar informacionin tuaj. Për shembull, qeveritë shpesh kanë shumë para dhe aftësi të fuqishme, përfshirë mbylljen e internetit ose përdorimin e teknologjisë së shtrenjtë të mbikëqyrjes; rrjetet celulare dhe ofruesit e internetit ka gjasa të kenë qasje në regjistrimet e thirrjeve dhe historitë e shfletimit; Hakerat e aftë në rrjetet publike Wi-Fi kanë aftësinë të përgjojnë komunikime ose transaksione financiare dobët të siguruara. Ju madje mund të bëheni kundërshtari i vetes, për shembull, duke fshirë aksidentalisht skedarë të rëndësishëm ose duke dërguar mesazhe private te personi i gabuar.

Motivet e kundërshtarëve ka gjasa të ndryshojnë së bashku me kapacitetin, interesat dhe strategjitë e tyre. A janë të interesuar të diskreditojnë parlamentin tuaj? Ndoshta ata synojnë të heshtin mesazhin tuaj ose të pengojnë punën e parlamentit? Është e rëndësishme të kuptoni motivimin e një kundërshtari, sepse duke vepruar kështu mund ta ndihmoni parlamentin tuaj të vlerësojë më mirë kërcënimet që mund të paraqiten.

3 Me çfarë kërcënimesh përballet parlamenti juaj? Dhe sa të mundshme dhe me ndikim të lartë janë ato?

Ndërsa identifikoni kërcënimet e mundshme, ka gjasa të përfundoni me një listë të gjatë e cila mund të jetë dërrmuese. Ndoshta do mendoni se çdo përpjekje do të ishte e kotë, ose nuk dini se ku të filloni. Për të ndihmuar fuqizimin e parlamentit tuaj për të ndërmarrë hapa të ardhshëm produktiv, është e dobishme të analizoni çdo kërcënim bazuar në dy faktorë: gjasat që kërcënimi të ndodhë; dhe ndikimi nëse ndodh.

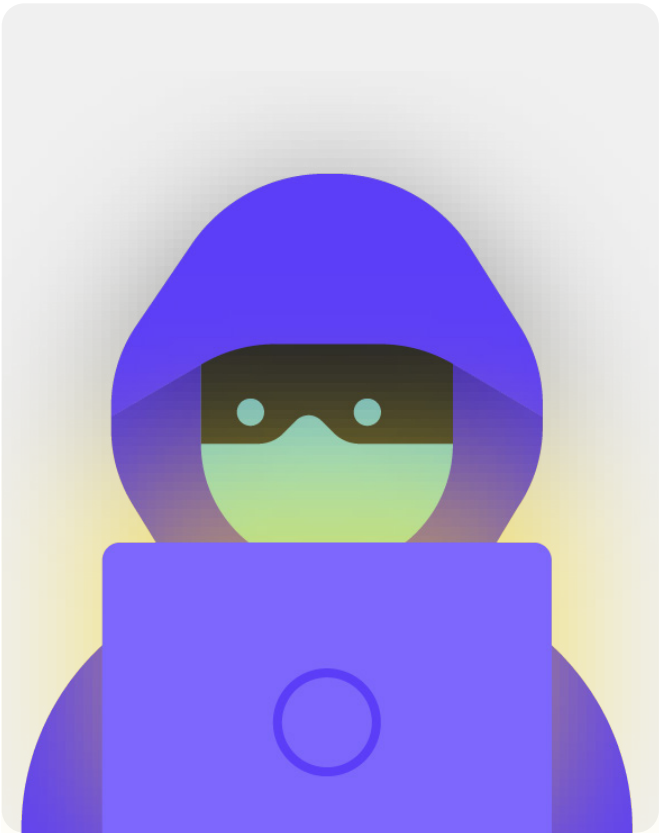
Për të matur mundësinë e një kërcënimi (ndoshta "i ulët, i mesëm ose i lartë", bazuar në faktin nëse një ngjarje e caktuar nuk ka gjasa të ndodhë, mund të ndodhë ose ndodh shpesh), mund të përdorni informacionin që dini për kapacitetin dhe motivimin e kundërshtarëve tuaj, analizën e incidenteve të kaluara të sigurisë, përvojat tjera të ngjashme të parlamenteve dhe sigurisht praninë e ndonjë strategjie zbutëse ekzistuese që keni vendosur.

Për të matur ndikimin e një kërcënimi, mendoni se si do të dukej bota juaj nëse kërcënimi do të ndodhte në të vërtetë. Bëni pyetje të tipit: "Si na ka dëmtuar kërcënimi si parlament dhe si njerëz, fizikisht dhe mendërisht?", "Sa i gjatë është efekti?", "A krijon kjo situata të tjera të dëmshme?", dhe "Si e pengon kjo aftësinë tonë për të arritur qëllimet tona tani dhe në të ardhmen?". Derisa u përgjigjeni këtyre pyetjeve, kini parasysh nëse kërcënimi është me ndikim të ulët, mesatar ose të lartë.

Për t'ju ndihmuar të menaxhoni këtë proces të vlerësimit të rrezikut, merrni parasysh përdorimin e një flete pune, si kjo e zhvilluar nga Electronic Frontier Foundation. Mbani në mend se informacioni që zhvilloni si pjesë e këtij procesi (si një listë e kundërshtarëve tuaj dhe kërcënimet që ata paraqesin) vetvetiu mund të paraqesin informacione të ndjeshme, prandaj është e rëndësishme t'i mbani të sigurt.

Pasi të keni kategorizuar kërcënimet tuaja sipas gjasave dhe ndikimit, mund të filloni të bëni një plan veprimi më të informuar. Duke u fokusuar në ato kërcënime që kanë më shumë gjasa të ndodhin DHE që do të kenë ndikime të rëndësishme negative, ju do të kanalizoni burimet tuaja të kufizuara në mënyrën më efikase dhe efektive të mundshme. Qëllimi juaj është gjithmonë të zbusni sa më shumë rrezikun, aq sa të jetë e mundur, por askush – as qeveria apo kompania me burime më të mira në tokë – nuk mund ta eliminojë plotësisht rrezikun. Dhe kjo është në rregull: Mund të bëni shumë për të mbrojtur veten, kolegët dhe parlamentin tuaj duke u kujdesur për kërcënimet më të mëdha

Për t'ju ndihmuar të menaxhoni këtë proces të vlerësimit të rrezikut, merrni parasysh përdorimin e një flete pune, si kjo e zhvilluar nga Electronic Frontier Foundation. Mbani në mend se informacioni që zhvilloni si pjesë e këtij procesi (si një listë e kundërshtarëve tuaj dhe kërcënimet që ata paraqesin) vetvetiu mund të paraqesin informacione të ndjeshme, prandaj është e rëndësishme t'i mbani të sigurt.

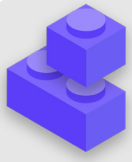


Krijimi i planit të sigurisë kibernetike të parlamentit tuaj

Plani i sigurisë i çdo parlamenti do të duket paksa i ndryshëm, bazuar në vlerësimin e rrezikut dhe dinamikën organizative, por disa koncepte thelbësore janë pothuajse universale. Ky doracak trajton këto koncepte thelbësore në një mënyrë që do të ndihmojë parlamentin tuaj të ndërtojë një plan konkret sigurie të bazuar në zgjidhje praktike dhe zbatime të botës së vërtetë.

Ky doracak përpiqet të ofrojë opsione dhe sugjerime që janë falas ose me kosto shumë të ulët. Mbani në mend se kostoja më e rëndësishme që lidhet me zbatimin e një plani efektiv sigurie do të jetë koha që ju dhe stafi, anëtarët dhe ekipet në të gjithë parlamentin duhet të flisni, të mësoni dhe të zbatoni planin tuaj të ri. Megjithatë, duke pasur parasysh rreziqet me të cilat ka gjasa të përballet parlamenti juaj, ky investim do të jetë më se i vlefshëm.

Në çdo pjesë, do të gjeni shpjegim të një teme kyçe për të cilën parlamenti juaj dhe stafi i tij duhet të jenë të vetëdijshëm - çfarë paraqet dhe pse është e rëndësishme. Çdo temë shoqërohet me strategji thelbësore, qasje dhe mjete të rekomanduara për të kufizuar rrezikun tuaj dhe këshilla dhe lidhje me burime shtesë që mund t'ju ndihmojnë të zbatoni rekomandimet e tilla në parlamentin tuaj.



Kompleti fillestar i planit të sigurisë

Që të ndihmoni parlamentin tuaj të përpunojë leksionet e Doracakut dhe t'i kthejë ato në një plan të vërtetë, përdorni këtë komplet fillestar. Mund ta printoni kompletin ose ta plotësoni në mënyrë digjitale ndërsa lexoni Doracakun në internet. Ndërsa mbani shënime dhe filloni të përditësoni ose hartoni planin tuaj të sigurisë, sigurohuni që t'u referoheni "Blloqeve të ndërtimit të planit të sigurisë" të detajuara në çdo pjesë. Asnjë plan sigurie nuk është i plotë pa adresuar së paku këto elemente thelbësore.

Përfitoni nga burime të tjera që mund t'ju ndihmojnë të ndërtoni dhe zbatoni gjithashtu planin tuaj. Përdorni burimet e trajnimit falas si Raportet e Konsumatorit të Security Planner, Umbrella aplikacioni nga Security First, Totem Project nga Free Press Unlimited dhe Greenhost, dhe Global Cyber Alliance Cybersecurity Toolkit for Mission Based-Organizations, të cilat përfshijnë burime për shumë nga praktikat më të mira të përmendura në këtë doracak dhe lidhje me dhjetëra mjete trajnimi që do t'ju ndihmojnë të zbatoni shumë baza themelore.

Ndërtimi i një kulture sigurie

Siguria ka të bëjë vetëm me njerëzit dhe për të mbrojtur parlamentin tuaj duhet të siguroheni që të gjithë të përfshirët - duke përfshirë anëtarët e parlamentit (deputetët), stafin mbështetës legjislativ dhe personelin e shërbimit kërkimor, dhe personelin administrativ në financa, burime njerëzore dhe TI, ndër shumë të tjerë - e merr seriozisht sigurinë kibernetike. Ndryshimi i kulturës është i vështirë, por disa hapa të thjeshtë dhe biseda të rëndësishme mund të ndihmojnë shumë në krijimin e një atmosfere që do të ndërtojë qëndrueshmërinë e stafit dhe parlamentit tuaj përballë kërcënimeve të sigurisë. Një nga hapat më të thjeshtë, por më të rëndësishëm që duhet ndërmarrë për të ndërtuar këtë kulturë parlamentare të sigurisë është të komunikoni për të, brenda dhe në të gjithë parlamentin tuaj, dhe që liderët të modelojnë dhe investojnë gjithmonë në sjellje të mirë.

Ndërtimi i një kulture sigurie në parlamente

Në shkurt 2019, Australia pësoi një sulm kibernetik që kompromentoi rrjetet e parlamentit kombëtar australian dhe të tre partive kryesore politike. Sulmuesit ishin në gjendje të fitojnë qasje në dokumentet e politikave dhe korrespondencën private me postë elektronike midis deputetëve, stafit të tyre dhe zgjedhësve. Sulmi ndodhi vetëm tre muaj para se të mbaheshin zgjedhjet, duke theksuar cenueshmërinë e rrjeteve të pasigurta gjatë zgjedhjeve.

Në përgjigje të këtij sulmi të rëndësishëm dhe të suksesshëm, parlamenti bëri përpjekje për të rritur gatishmërinë për sigurinë kibernetike. Një investim i tillë përfshinte hetimin e Komitetit të Përbashkët të Llogarive Publike dhe Revizioneve mbi qëndrueshmërinë kibernetike të Commonwealth-it. Hetimi **u bazua në gjetjet nga revizionet** e kryera gjatë disa viteve që zbuluan se proceset e zbutjes së rrezikut të sigurisë kibernetike mungojnë brenda parlamentit dhe agjencive të tjera qeveritare. Për shembull, Zyra Kombëtare e Revizionit të Australisë theksoi një dështim të parlamentit për t'u fokusuar në objektivat strategjike afatgjata dhe për të zhvilluar një qasje të bazuar në rrezik kur bëhej fjalë për sigurinë kibernetike. Dhe ndërsa hetimi dhe revizionet nuk ishin lajkatare, gatishmëria e parlamentit për të identifikuar problemet e sigurisë kibernetike dhe për të investuar në adresimin e tyre është një shembull i krijimit të një kulture të favorshme për sigurinë kibernetike parlamentare efektive. Një shembull që fillon me njohjen e problemeve dhe investimin në zgjidhje teknike dhe njerëzore, ku siguria nuk shmanget, por i jepet prioritet. Për shembull, nëpërmjet rekrutimit të një ekipi të "ngritjes së sigurisë kibernetike" dhe investimit buxhetor për një **"Fond të Përgjigjes për Sigurinë Kibernetike"**, parlamenti (dhe organet tjera qeveritare) duhet të jenë më mirë të përgatitur për të zbutur sulmet e ardhshme, nëse këto burime shpërndahen, mirëmbahen siç duhet dhe fokusi në sigurinë kibernetike si një element i rregullt i operacioneve parlamentare vazhdon të mbetet. Me këtë, sigurisht që është më mirë të ndërtoni këtë angazhim për siguri brenda parlamentit tuaj përpara se të ndodhë një shkelje e konsiderueshme e sigurisë.

Integroni sigurinë në strukturën tuaj të rregullt operative

Siç përshkruhet në detaje në Tactical Tech's Holistic Security Guide, është thelbësore të krijohen hapësira të rregullta dhe të sigurta për të folur për aspekte të ndryshme të sigurisë. Në këtë mënyrë, nëse stafi dhe anëtarët kanë shqetësime rreth sigurisë, ata do të jenë më pak të shqetësuar për t'u dukur paranojakë ose se janë duke ua humbur kohën të tjerëve. **Planifikimi i bisedave të rregullta rreth sigurisë** gjithashtu normalizon frekuencën e ndërveprimit dhe reflektimit për çështjet që kanë të bëjnë me sigurinë, që çështjet të mos harrohen dhe stafi nëpër ekipe të ndryshme, të ketë më shumë gjasa të sjellë të paktën një ndërgjegjësim pasiv mbi sigurinë në punën e tyre të vazhdueshme. Nuk ka nevojë kjo të ndodhë çdo javë, por caktojeni si takim që duhet përsëritur periodikisht. Këto diskutime nuk duhet të lënë hapësirë vetëm për temat e sigurisë teknike, por edhe çështjet që ndikojnë në komoditetin dhe sigurinë e stafit, si ngacmimet në internet (dhe offline), ose çështjet me përdorimin dhe zbatimin e mjeteve digjitale brenda zyrave parlamentare. Bisedat mund të përfshijnë edhe tema si zakonet e ndarjes së informacionit jashtë linje dhe mënyrat se si stafi siguron ose nuk siguron informacione jashtë parlamentit. Në fund të fundit, është e rëndësishme të mbani mend se siguria e një parlamenti është po aq e fortë sa që është hallka e tij më e dobët.

Një mënyrë për të arritur angazhim të qëndrueshëm është duke shtuar sigurinë në agjendën e një takimi të rregullt. Gjithashtu mund të ndërroni përgjegjësinë për organizimin dhe lehtësimin e diskutimit mbi sigurinë midis stafit të ndryshëm, gjë që mund të ndihmojë në zhvillimin e idesë se siguria është përgjegjësi e të gjithëve dhe jo vetëm e disa të përzgjedhurve ose "Ekipi i TI-së". Ndërsa filloni të zyrtarizoni diskutimin rreth sigurisë, stafi ka gjasa të ndihet më rehat duke diskutuar këto çështje të rëndësishme mes tyre, si dhe në mjedise më pak formale.

Është gjithashtu e rëndësishme që të përfshihen elemente sigurie në funksionimin normal të parlamentit, si p.sh. gjatë hyrjes së anëtarëve dhe stafit – dhe të mendoni mbi ndërprerjen e qasjes në sisteme gjatë fillimit të procesit për largim nga vendi i punës. Siguria nuk duhet të jetë një "gjë shtesë" për t'u shqetësuar, por një ***pjesë integrale e strategjisë dhe operacioneve tuaja.***

Mos harroni se të gjitha planet e sigurisë duhet të konsiderohen si dokumente të gjalla dhe duhet të rivlerësohen dhe diskutohen rregullisht, veçanërisht kur punonjës ose vullnetarë të rinj i bashkohen organizatës ose ndryshon konteksti juaj i sigurisë.

Planifikoni të rishikoni strategjinë tuaj dhe të bëni përditësime çdo vit, ose në rast se ka ndryshime të mëdha në strategji, mjete ose kërcënime me të cilat përballeni në ndonjë çast.

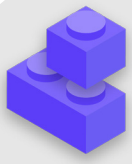
Siguroni mbështetjen e gjithë organizatës

Pjesë e një kulture të suksesshme sigurie është gjithashtu **të siguroni se keni mbështetje nga i gjithë parlamenti** për planin tuaj të sigurisë. Në mënyrë kritike, kjo duhet të përfshijë mbështetjen dhe udhëzimin e fortë e të zëshëm nga udhëheqësit, të cilët, në shumë raste, do të jenë ata që marrin vendimin përfundimtar për të ndarë kohën, burimet dhe energjinë drejt zhvillimit dhe zbatimit të një plani efektiv sigurie. Nëse ata nuk e marrin seriozisht, askush tjetër nuk do ta marrë. Për të arritur këtë mbështetje, mendoni me kujdes se kur dhe si ta prezantoni planin tuaj, bëjeni këtë në një mënyrë të qartë, sigurohuni që udhëheqja të përforcojë mesazhet dhe kaloni së bashku nëpër të gjitha elementet dhe hapat e planit në mënyrë që të mos ketë mistere ose konfuzione mbi atë që po përpiqeni të arrini. Sigurohuni që të buxhetoni siç duhet edhe për sigurinë kibernetike në të gjithë parlamentin. Megjithëse financat mund të jenë të kufizuara, është thelbësore të investohet siç duhet në sigurinë kibernetike, përndryshe, investimet e tjera ka gjasa të vihen në rrezik. Kur flisni për sigurinë, shmangni taktikat e frikësimit. Ndonjëherë kërcënimet me të cilat përballet parlamenti dhe stafi juaj mund të jenë të frikshme, por përpiquni të përqendroheni në ndarjen e fakteve dhe krijimin e një hapësire të qetë për pyetje dhe shqetësime. Nëse i prezantoni rreziqet të duken si shumë kërcënuese mund të ndodh që njerëzit t'ju hedhin poshtë si sensacionalistë ose thjesht të heqin dorë nga kjo, duke menduar se asgjë nuk ka rëndësi - dhe asgjë nuk mund të jetë më larg nga e vërteta

Vendosni një plan trajnimi

Pasi të keni zhvilluar dhe të jeni përkushtuar ndaj një plani, mendoni se si do t'i trajnoni të gjithë anëtarët, stafin dhe vullnetarët për këto praktika të reja më të mira. Parashtrimi i trajnimit të rregullt si kusht - dhe shënimi i pjesëmarrjes në trajnime të detyrueshme - mund të jetë një taktikë e dobishme. Shmangni krijimin e pasojave të ashpra dhe negative për stafin që lufton me konceptet e sigurisë. Mbani në mend se një staf i caktuar mund të përshtatet dhe të mësojë rreth teknologjisë ndryshe nga të tjerët, bazuar në nivele të ndryshme familjariteti me mjetet digjitale dhe internetin. Frika e dështimit vetëm sa e dekurajon më tej stafin nga raportimi i problemeve ose kërkimi i ndihmës. Megjithatë, krijimi i llogaridhënies dhe shpërblimeve pozitive për trajnimin dhe miratimin e suksesshëm të politikave mund të ndihmojë në nxitjen e përmirësimit në të gjithë parlamentin. Mund të gjeni mbështetje shtesë të vlefshme nëpërmjet rrjeteve lokale ose ndërkombëtare të trajnimit të sigurisë digjitale dhe burimeve të trajnimit falas si p.sh **Umbrella app from Security First**, **Totem Project** nga Free Press Unlimited dhe Greenhost, dhe Global Cyber Alliance **Learning Portal**.

Merrni parasysh se si plani juaj i trajnimit mund të arrijë tek deputetët, stafi i parlamentit si dhe administrata parlamentare. Mbani në mend se anëtarët e shquar shpesh kërkojnë edhe më shumë trajnim dhe vëmendje kur bëhet fjalë për sigurinë për shkak të profilit të tyre të lartë. Sigurohuni që plani juaj i trajnimit dhe plani i sigurisë të zbatohen për të gjithë këta lloje të ndryshëm individësh dhe çdo aset që ata mund të kenë brenda dhe jashtë parlamentit.



Blloqet e ndërtimit të planit të sigurisë:
Ndërtimi i një kulture sigurie

- **Caktoni biseda dhe trajnime të rregullta rreth sigurisë dhe planit tuaj të sigurisë.**
- **Përfshini të gjithë - shpërndani përgjegjësinë për zbatimin e planit tuaj të sigurisë në të gjithë parlamentin.**
- **Siguroni modele udhëheqësie për sjellje të mirë të sigurisë dhe përkushtimi ndaj planit tuaj.**
- **Shmangni taktikat e frikës ose ndëshkimit - shpërblejeni përmirësimin dhe krijoni hapësirë të rehatshme për stafin, që të raportojë problemet dhe të kërkojë ndihmë.**
- **Përditësoni planin tuaj të sigurisë çdo vit ose pas ndryshimeve të mëdha në personelin parlamentar, strukturën ose mjedisin operativ.**

Themel i fortë: Sigurimi i llogarive dhe pajisjeve

Pse fokusi vihet te llogaritë dhe pajisjet? Sepse ato përbëjnë themelin e gjithçkaje që parlamenti juaj bën në mënyrë digjitale. Ju pothuajse me siguri keni qasje në informacione të ndjeshme, komunikoni brenda dhe jashtë dhe ruani informacione private në to. Thjesht merrni parasysh pjesëmarrjen e anëtarëve në seancat plenare, votimin (përfshirë virtual), proceset e hartimit të legjislacionit dhe komunikimin me anëtarët e stafit dhe publikun e gjerë. Pa llogari dhe pajisje të sigurta, këto operacione të rëndësishme parlamentare dhe të tjera mund të vihen në rrezik.

Për shembull, nëse hakerët shikojnë goditjet e tasteve ose dëgjojnë mikrofonin tuaj, bisedat private me kolegët do të regjistrohen pavarësisht se sa të sigurta janë aplikacionet tuaja të mesazheve. Ose, nëse ndonjë kundërshtar fiton qasje në llogaritë e mediave sociale të parlamentit tuaj, mund të dëmtojnë lehtësisht reputacionin dhe besueshmërinë tuaj, duke minuar besimin me publikun. Prandaj, është thelbësore si parlament të sigurohet që të gjithë të ndërmarrin disa hapa të thjeshtë por efektivë për t'i mbajtur pajisjet dhe llogaritë e tyre të sigurta. Është e rëndësishme të theksohet se këto rekomandime përfshijnë gjithashtu llogaritë dhe pajisjet personale, pasi ato janë shpesh objektiva të lehta për kundërshtarët. Hakerët me kënaqësi do të ndjekin objektivin më të lehtë dhe do të hyjnë në një llogari personale ose kompjuter shtëpiak nëse anëtarët dhe stafi juaj i përdorin ato për të komunikuar dhe për të qasur në informacione të rëndësishme.

Siguroni llogaritë dhe parlamentet

Hakimi i përhapur gjerësisht i SolarWinds i zbuluar në fund të vitit 2020, i cili komprometoi mbi 250 organizata, duke përfshirë shumicën e departamenteve të qeverisë së Shteteve të Bashkuara, shitësit e teknologjisë si Microsoft dhe Cisco, dhe OJQ-të, ishte pjesërisht rezultat i **hakerëve që hamendësuan fjalëkalime** të dobëta që përdoreshin në llogari të rëndësishme administratorësh. Në përgjithësi, rreth 80 për qind e të gjitha shkeljeve të lidhura me hakerimin ndodhin për shkak të fjalëkalimeve të dobëta ose të ripërdorura.

Me përhapjen në rritje të shkeljeve të fjalëkalimeve si kjo dhe qasjen më të lehtë për të gjitha llojet e kundërshtarëve në mjetet e sofistikuara të hakerimit të fjalëkalimeve, praktikat më të mira të fjalëkalimit dhe vërtetimi me dy faktorë janë domosdoshmëri sigurie për të gjitha organizatat, përfshirë parlamentet. Asnjë incident nuk e ilustron më qartë këtë se sa **sulmi në vitin 2017** kundër sistemit të postës elektronike të Parlamentit britanik. Në këtë incident, praktikat e dobëta të fjalëkalimeve nga një numër i vogël, por domethënës deputetësh, çuan në ekspozimin e llogarive dhe bisedave të postës elektronike, mijëra kredencialeve të zbuluara dhe ndërprerje të jashtëzakonshme të operacioneve parlamentare. **Sipas** zyrës për shtyp të Parlamentit britanik, llogaritë e shkelura ishin "kompromentuar si rezultat i fjalëkalimeve të dobëta që nuk ishin në përputhje me udhëzimet e lëshuara nga Shërbimi Digjital Parlamentar".

Llogaritë e sigurta: Fjalëkalimet dhe vërtetimi me dy faktorë

Në botën e sotme, ka gjasa që parlamenti juaj dhe stafi i tij të kenë dhjetëra, nëse jo qindra llogari që, nëse shkelen, mund të ekspozojnë informacione të ndjeshme apo edhe të lëndojnë individë të rrezikuar. Mendoni për llogaritë e ndryshme që mund të ketë personeli individual dhe parlamenti në tërësi: postë elektronike, aplikacione bisede, media sociale, llogari bankare në internet, ruajtja e të dhënave në re, si dhe dyqane të veshjeve, restorante, lokale, gazeta dhe shumë faqe interneti ose aplikacione të tjera që ju i qasni. Siguria cilësore në botën e sotme kërkon një qasje të zellshme për të mbrojtur të gjitha këto llogari nga sulmet. Kjo fillon me sigurimin e higjienës së mirë të fjalëkalimit dhe përdorimin e vërtetimit me dy faktorë nga të gjithë.

ÇFARË E BËN NJË FJALËKALIM TË MIRË?

Ekzistojnë tre çelësa për një fjalëkalim të mirë dhe të fortë: gjatësia, rastësia dhe të qenit unik.

GJATËSIA:	Edhe nëse një fjalëkalim është i gjatë, nuk është shumë i mirë nëse është diçka që një kundërshtar mund ta hamendësojë lehtësisht për ju. Shmangni përfshirjen e informacioneve si ditëlindja juaj, vendlindja, aktivitetet e preferuara ose fakte të tjera që dikush mund të mësojë për ju nga një kërkim i shpejtë në internet.
RASTËSIA:	Ndoshta “praktika më e keqe” më e zakonshme e fjalëkalimit është përdorimi i të njëjtit fjalëkalim për shumë sajte. Përsëritja e fjalëkalimeve është një problem i madh sepse do të thotë që kur vetëm një nga ato llogari rrezikohet, çdo llogari tjetër që përdor të njëjtin fjalëkalim është gjithashtu e cenueshme. Nëse përdorni të njëjtën frazë kalimi në shumë sajte, mund të rrisë ndjeshëm ndikimin e një gabimi ose shkeljeje të të dhënave. Ndonëse mund të mos ju interesojë fjalëkalimi juaj për bibliotekën lokale, nëse ai hakerohet dhe përdorni të njëjtin fjalëkalim në një llogari më të ndjeshme, mund të vidhen informacione të rëndësishme.
TË QENIT UNIK:	Ndoshta “praktika më e keqe” më e zakonshme e fjalëkalimit është përdorimi i të njëjtit fjalëkalim për shumë sajte. Përsëritja e fjalëkalimeve është një problem i madh sepse do të thotë që kur vetëm një nga ato llogari rrezikohet, çdo llogari tjetër që përdor të njëjtin fjalëkalim është gjithashtu e cenueshme. Nëse përdorni të njëjtën frazë kalimi në shumë sajte, mund të rrisë ndjeshëm ndikimin e një gabimi ose shkeljeje të të dhënave. Ndonëse mund të mos ju interesojë fjalëkalimi juaj për bibliotekën lokale, nëse ai hakerohet dhe përdorni të njëjtin fjalëkalim në një llogari më të ndjeshme, mund të vidhen informacione të rëndësishme.

Një mënyrë e thjeshtë për të arritur këto qëllime të gjatësisë, rastësisë dhe veçantisë është zgjedhja e tri ose katër fjalëve të zakonshme, por të rastësishme. Për shembull, fjalëkalimi juaj mund të jetë "ariu jeshil me llambë lulesh", i cili është i lehtë për t'u mbajtur mend, por i vështirë për t'u marrë me mend. Ju mund t'i hidhni një sy **kësaj ueb-faqeje** nga Better Buys për të parë një vlerësim se sa shpejt mund të kapen fjalëkalimet e këqija.

PËRDORNI NJË MENAXHER FJALËKALIMI PËR T'JU NDIHMUAR

Pra, e dini se është e rëndësishme që të gjithë në parlament të përdorin një fjalëkalim të gjatë, të rastësishëm dhe të ndryshëm për secilën prej llogarive të tyre personale dhe parlamentare, por si e bëni këtë? Memorizimi i një fjalëkalimi të mirë për dhjetëra (nëse jo qindra) llogari është i pamundur, kështu që të gjithë duhet të mashtrojnë. Mënyra e gabuar për ta bërë këtë është ripërdorimi i fjalëkalimeve. Për fat të mirë, ne mund t'u drejtohemi menaxherëve të fjalëkalimeve digjitale për ta bërë jetën tonë shumë më të lehtë (dhe praktikat tona të fjalëkalimeve shumë më të sigurta). Këto aplikacione, shumë prej të cilave mund të qasen nëpërmjet kompjuterit ose pajisjes celulare, mund të krijojnë, ruajnë dhe menaxhojnë fjalëkalime për ju dhe të gjithë organizatën tuaj. Miratimi i një menaxheri të sigurt fjalëkalimesh do të thotë që do t'ju duhet të mbani mend vetëm një fjalëkalim shumë të fortë dhe të gjatë të quajtur fjalëkalimi kryesor (historikisht i referuar si fjalëkalimi "master"), ndërkohë që jeni në gjendje të merrni përfitimet e sigurisë nga përdorimi i fjalëkalimeve të mira dhe unike në të gjitha llogaritë tuaja. Ju do të përdorni këtë fjalëkalim kryesor (dhe në mënyrë ideale një faktor të dytë të vërtetimit (2FA), i cili do të diskutohet në pjesën tjetër) për të hapur menaxherin tuaj të fjalëkalimeve dhe për të zhbllokuar qasjen në të gjitha fjalëkalimet tuaja të tjera. Menaxherët e fjalëkalimeve gjithashtu mund të ndahen nëpër llogari të shumta për të lehtësuar ndarjen e sigurt të fjalëkalimit në të gjithë parlamentin.

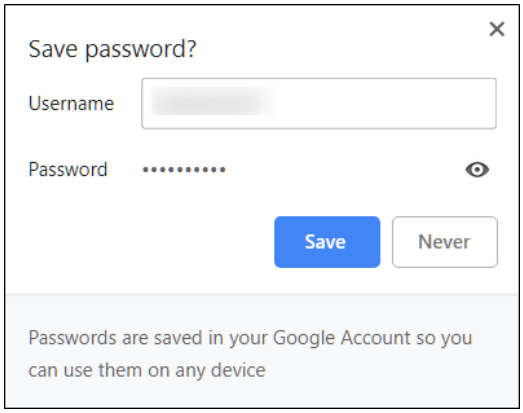
Pse duhet të përdorim diçka të re? A nuk mund t'i shkruajmë ato vetëm në letër ose në një fletëllogaritëse në kompjuter??

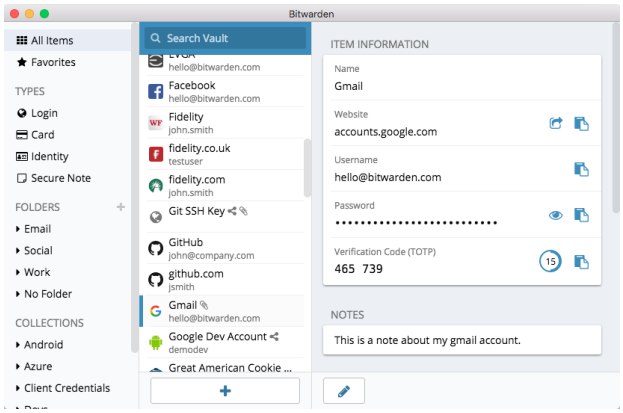
Fatkeqësisht, ka shumë qasje të zakonshme për menaxhimin e fjalëkalimeve që nuk janë të sigurta. Ruajtja e fjalëkalimeve në fletë letre (nëse nuk i mbani të mbyllura në një kasafortë) mund t'i ekspozojë ato ndaj vjedhjes fizike, syve kureshtarë dhe humbjes dhe dëmtimit të lehtë. Ruajtja e fjalëkalimeve në një dokument në kompjuterin tuaj e bën shumë më të lehtë për një haker që të ketë qasje - ose që dikush që vjedh kompjuterin tuaj të ketë jo vetëm pajisjen tuaj, por edhe qasje në të gjitha llogaritë tuaja. Përdorimi i një menaxheri të mirë fjalëkalimesh është po aq i lehtë sa ai dokument, por shumë më i sigurt.

Pse duhet t'i besojmë një menaxheri të fjalëkalimeve?

Menaxherët cilësorë të fjalëkalimeve bëjnë përpjekje të jashtëzakonshme (dhe punësojnë ekipe të shkëlqyera sigurie) për të mbajtur sistemet e tyre të sigurta. Aplikacionet e mira të menaxhimit të fjalëkalimeve (disa janë të rekomanduara më poshtë) janë gjithashtu të konfiguruara në mënyrë që të mos kenë aftësinë për të "zhbllokuar" llogaritë tuaja. Kjo do të thotë se në shumicën e rasteve, edhe nëse ata do të hakeroheshin ose do të detyroheshin ligjërisht të dorëzonin informacionin, ata nuk do të mund të humbnin ose të hiqnin dorë nga fjalëkalimet tuaja. Është gjithashtu e rëndësishme të mbani mend se ka pafundësisht më shumë gjasa që një kundërshtar të hamendësojë një nga fjalëkalimet tuaja të dobëta ose të përsëritura, ose ta gjejë një në ndonjë **shkelje të të dhënave** publike, sesa që një menaxher i mirë i fjalëkalimeve t'i prishë sistemet e tij të sigurisë. Është e rëndësishme të jesh skeptik dhe definitivisht nuk duhet t'u besosh verbërisht të gjithë programeve dhe aplikacioneve, por menaxherët me reputacion të fjalëkalimeve kanë të gjitha stimujt e duhur për të bërë gjënë e duhur.

Në vend që të përdorni shfletuesin tuaj (siç është Chrome, i treguar majtas) për të ruajtur fjalëkalimet tuaja, përdorni një menaxher të dedikuar të fjalëkalimeve (si Bitwarden, i treguar në të djathtë). Menaxherët e fjalëkalimeve kanë veçori që e bëjnë jetën më të sigurt dhe më të përshtatshme për parlamentin tuaj.





Po nëse ruajmë fjalëkalimet në shfletues?

Ruajtja e fjalëkalimeve në shfletuesin tuaj nuk është e njëjtë me përdorimin e një menaxheri të sigurt fjalëkalimesh. Me pak fjalë, nuk duhet të përdorni Chrome, Firefox, Safari ose ndonjë shfletues tjetër si menaxher të fjalëkalimit tuaj. Megjithëse është padyshim një përmirësim në krahasim me shkrimin e tyre në letër ose ruajtjen e tyre në një fletëllogaritëse, veçoritë themelore të kursimit të fjalëkalimit të shfletuesit tuaj të internetit nuk është i fortë nga këndvështrimi i sigurisë. Këto mangësi ju heqin gjithashtu shumë nga komoditeti që sjell një menaxher i mirë i fjalëkalimeve. Humbja e këtij komoditeti i bën më shumë gjasa që njerëzit në të gjithë parlamentin të vazhdojnë praktikat e dobëta të krijimit dhe ndarjes së fjalëkalimeve.

Për shembull, ndryshe nga menaxherët e dedikuar të fjalëkalimeve, veçoritë e integruara të shfletuesve "ruaj këtë fjalëkalim" ose "mbaje mend këtë fjalëkalim" nuk ofrojnë përputhshmëri të thjeshtë celulare, funksionalitet ndër-shfletues dhe mjete të forta gjenerimi dhe revizioni të fjalëkalimeve. Këto veçori janë një pjesë e madhe e asaj që e bën një menaxher të dedikuar fjalëkalimi kaq të dobishëm dhe të dobishëm për sigurinë e parlamentit tuaj. Menaxherët e fjalëkalimeve përfshijnë gjithashtu veçori specifike të organizatës (siç është ndarja e fjalëkalimit) që ofrojnë jo vetëm vlerë sigurie individuale, por vlerë për parlamentin tuaj në tërësi.

Nëse keni ruajtur fjalëkalime me shfletuesin tuaj (me dashje ose pa dashje), duhet t'i hiqni.

Çfarë menaxheri fjalëkalimi duhet të përdorim?

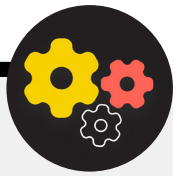
Ekzistojnë shumë mjete të mira të menaxhimit të fjalëkalimeve që mund të konfigurohen në më pak se 30 minuta. Nëse jeni duke kërkuar opsion të besuar në internet për parlamentin tuaj, të cilit njerëzit mund t'i qasen nga shumë pajisje në çdo kohë, 1Password (nis nga $2.99 USD për përdorues në muaj) ose opsionin falas, me burim të hapur Bitwarden, të dyja janë mirë të mbështetura dhe të rekomanduara.

Një online opsion si Bitwarden mund të jetë i dobishëm edhe për sigurinë edhe për komoditet. Bitwarden, për shembull, do t'ju ndihmojë të krijoni fjalëkalime unike të forta dhe të përdorni fjalëkalime nga shumë pajisje përmes shtesave të shfletuesit dhe një aplikacioni celular. Me versionin e paguar ($10 USD për një vit të plotë) Bitwarden ofron gjithashtu raporte për fjalëkalime të ripërdorura, të dobëta dhe ndoshta të shkelura për t'ju ndihmuar të qëndroni në krye të gjërave. Pasi të konfiguroni fjalëkalimin tuaj kryesor (të referuar si fjalëkalim kryesor), duhet të aktivizoni gjithashtu vërtetimin me dy faktorë për të mbajtur sa më të sigurt kasafortën e menaxherit të fjalëkalimit tuaj.

Është thelbësore të praktikoni siguri të mirë edhe kur përdorni menaxherin tuaj të fjalëkalimeve. Për shembull, nëse përdorni shtesën e shfletuesit të menaxherit të fjalëkalimit ose hyni në Bitwarden (ose ndonjë menaxher tjetër fjalëkalimi) në një pajisje, mos harroni të dilni pas përdorimit nëse e ndani atë pajisje ose mendoni se mund të jeni në rrezik të shtuar të dëmtimit fizik si vjedhje e pajisjes. Kjo nënkupton edhe daljen nga menaxheri i fjalëkalimit nëse lini kompjuterin ose pajisjen celulare pa mbikëqyrje. Nëse ndani fjalëkalime ndërmjet ekipeve ose parlamentit në tërësi, sigurohuni gjithashtu të revokoni qasjen në fjalëkalime (dhe të ndryshoni vetë fjalëkalimet) kur njerëzit largohen. Nuk doni që një ish-punonjës të ketë qasje në fjalëkalimin e parlamentit tuaj në Facebook, për shembull.

Çfarë ndodh nëse dikush harron fjalëkalimin e tij kryesor?

Është thelbësore të mbani mend fjalëkalimin tuaj kryesor. Sistemet e mira të menaxhimit të fjalëkalimeve, si ato të rekomanduara më sipër, nuk do ta mbajnë mend fjalëkalimin tuaj kryesor për ju ose nuk do t'ju lejojnë ta rivendosni atë drejtpërdrejt me postë elektronike, ashtu siç mund të jeni në gjendje ta bëni në faqet e internetit. Kjo është një veçori e mirë sigurie, por gjithashtu e bën thelbësore vendosjen e fjalëkalimit tuaj kryesor në memorie kur konfiguroni për herë të parë menaxherin tuaj të fjalëkalimit. Që ta keni më lehtë, merrni parasysh konfigurimin e një rikujtuesi ditor për të rikujtuar fjalëkalimin tuaj kryesor kur krijoni për herë të parë një llogari të menaxherit të fjalëkalimeve.



Nivel i avancuar: Përdorimi i një menaxheri të fjalëkalimeve për parlamentin tuaj

Mund të forconi praktikat e fjalëkalimeve të parlamentit tuaj dhe të siguroni që i gjithë stafi individual të ketë qasje (dhe të përdorë) menaxher fjalëkalimi duke zbatuar një të tillë në të gjithë organizatën. Në vend që secili anëtar i stafit të krijojë të vetin, konsideroni nëse mund të investoni në një plan për "ekip" ose "biznes". Për shembull, plani për "ekipe të organizatave" të Bitwarden-it kushton $3 për përdorues, në muaj. Me të (ose plane të tjera ekipore nga menaxherët e fjalëkalimeve si 1Password), keni mundësinë të menaxhoni të gjitha fjalëkalimet e përbashkëta në të gjithë "organizatën". Veçoritë e një menaxheri të fjalëkalimeve të parlamentit ose ekipit jo vetëm që ofron siguri më të madhe, por edhe komoditet për stafin. Mund të ndani në mënyrë të sigurt kredencialet brenda vetë menaxherit të fjalëkalimeve në llogari të ndryshme përdoruesish. Dhe Bitwarden, për shembull, ofron gjithashtu një veçori të përshtatshme të enkriptuar nga fundi në fund dhe ndarjen e skedarëve të quajtur "Bitwarden Send" brenda planit të tij për ekipe. Të dyja këto veçori i japin parlamentit tuaj më shumë kontroll mbi atë se kush mund të shohë dhe të ndajë cilat fjalëkalime, dhe ofrojnë mundësi më të sigurt për ndarjen e kredencialeve për llogaritë në të gjithë ekipin ose në grup. Nëse krijoni një menaxher të fjalëkalimeve në të gjithë parlamentin, sigurohuni që dikush të jetë veçanërisht përgjegjës për heqjen e llogarive të stafit dhe ndryshimin e çdo fjalëkalimi të përbashkët kur dikush largohet nga ekipi.

ÇFARË ËSHTË VËRTETIMI ME DY FAKTORË?

Sado e mirë të jetë higjiena juaj e fjalëkalimit, është shumë e zakonshme që hakerët t'i shmangin fjalëkalimet. Mbajtja e llogarive tuaja të sigurta nga disa aktorë të zakonshëm të kërcënimit në botën e sotme kërkon një shtresë tjetër mbrojtjeje. Këtu hyn në lojë vërtetimi me shumë faktorë ose me dy faktorë - i referuar si MFA ose 2FA.

Ka shumë udhëzues dhe burime të shkëlqyera që shpjegojnë vërtetimin me dy faktorë, duke përfshirë artikullin e Martin Shelton-it Two-Factor Authentication for Beginners dhe Election Cybersecurity 101 Field Guide nga Center for Democracy & Technology. Kjo pjesë huazon shumë nga të dyja këto burime për të ndihmuar në shpjegimin se pse 2FA është kaq e rëndësishme për t'u zbatuar në të gjithë parlamentin.

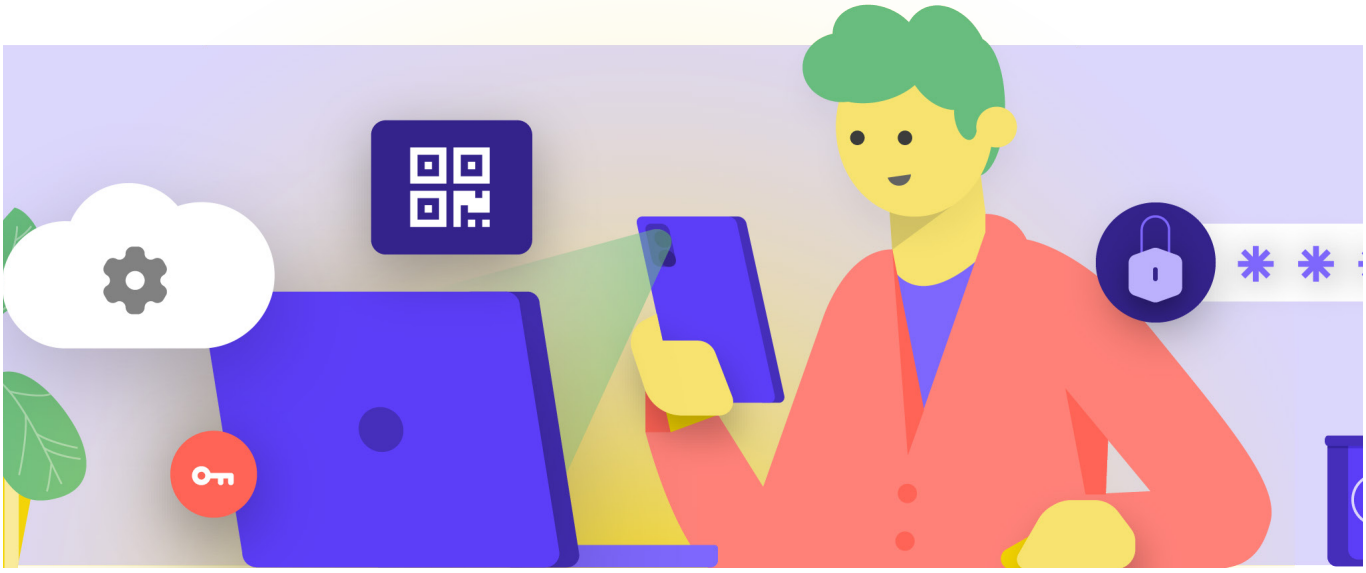
Me pak fjalë, 2FA forcon sigurinë e llogarisë duke kërkuar një informacion të dytë – diçka më shumë se thjesht një fjalëkalim – për të fituar qasje. Pjesa e dytë e informacionit është zakonisht diçka që keni, si një kod nga një aplikacion në telefonin tuaj ose një shenjë ose çelës fizik. Kjo pjesë e dytë e informacionit vepron si një shtresë e dytë e mbrojtjes. Nëse një haker vjedh fjalëkalimin tuaj ose fiton qasje në të, nëpërmjet një grumbullimi të fjalëkalimeve nga një shkelje e madhe e të dhënave, 2FA efektive mund t'i pengojë ata të hyjnë në llogarinë tuaj (dhe si pasojë i mban larg informacioneve private dhe të ndjeshme). Është jashtëzakonisht e rëndësishme të sigurohet që të gjithë në parlament të vendosin 2FA në llogaritë e tyre.

SI MUND TË VENDOSIM VËRTETIMIN ME DY FAKTORË?

Ekzistojnë tri metoda të zakonshme për 2FA: çelësat e sigurisë, aplikacionet e vërtetimit dhe kodet SMS për një herë.

Çelësat e sigurisë

Çelësat e sigurisë janë opsioni më i mirë, pjesërisht nga shkaku se ata janë pothuajse plotësisht rezistentë ndaj phishing. Këta "çelësa" janë shenja harduerike (paramendoni mini disqet USB) që mund të lidhen me zinxhirin tuaj të çelësave (ose të qëndrojnë në kompjuterin tuaj) për qasje dhe ruajtje të lehtë. Kur është koha për të përdorur çelësin për të zhbllokuar një llogari të caktuar, thjesht e futni atë në pajisjen tuaj dhe e prekni fizikisht kur ju kërkohet gjatë identifikimit. Ka një gamë të gjerë modelesh që mund t'i blini në internet ($20-50 USD), duke përfshirë shumë të vlerësuarat YubiKeys. Wirecutter-i i The New York Times' ka një udhëzues të dobishëm me disa rekomandime se cilat çelësa duhet të blini. Mbani në mend se i njëjti çelës sigurie mund të përdoret për aq llogari sa dëshironi.



Aplikacionet e vërtetimit

Opsioni i dytë më i mirë për 2FA janë aplikacionet e vërtetimit. Këto shërbime ju lejojnë të merrni një kod të përkohshëm hyrjeje me dy faktorë përmes një aplikacioni celular ose njoftimit push në telefonin tuaj të mençur. Disa opsione të njohura dhe të besuara përfshijnë **Google Authenticator**, **Authy**, dhe **Duo Mobile**. Aplikacionet e vërtetuesit janë gjithashtu të shkëlqyera sepse funksionojnë kur nuk keni qasje në rrjetin tuaj celular dhe janë falas për t'u përdorur për individët. Sidoqoftë, aplikacionet e vërtetuesit janë më të ndjeshëm ndaj phishing sesa çelësat e sigurisë, sepse përdoruesit mund të mashtrohen për të futur kodet e sigurisë nga një aplikacion vërtetimi në një faqe interneti të rreme. Kujdesuni që të futni kodet e hyrjes vetëm në faqet e ligjshme të internetit. Dhe mos "pranoni" njoftimet e dërguara të hyrjes nëse nuk jeni të sigurt se jeni ju ai që keni bërë kërkesën për hyrje. Është gjithashtu thelbësore që kur përdorni një aplikacion vërtetues të përgatiteni me kode rezervë (të diskutuar më poshtë) në rast se telefoni juaj humbet ose vidhet.

Kodet me SMSS

Forma më pak e sigurt, por fatkeqësisht ende më e zakonshme e 2FA janë kodet e dërguara me SMS. Për shkak se SMS-të mund të përgjohen dhe numrat e telefonit mund të mashtrohen ose hakohen nëpërmjet operatorit tuaj celular, SMS lë shumë hapësirë për veprim si një metodë për të kërkuar kode 2FA. Është më mirë sesa të përdorni vetëm një fjalëkalim, por aplikacionet e vërtetimit ose një çelës sigurie fizike rekomandohen kur ekziston mundësia. Një kundërshtar i vendosur mund të ketë qasje në kodet SMS 2FA, zakonisht thjesht duke **telefonuar kompaninë telefonike** dhe duke shkëmbyer kartën tuaj SIM.

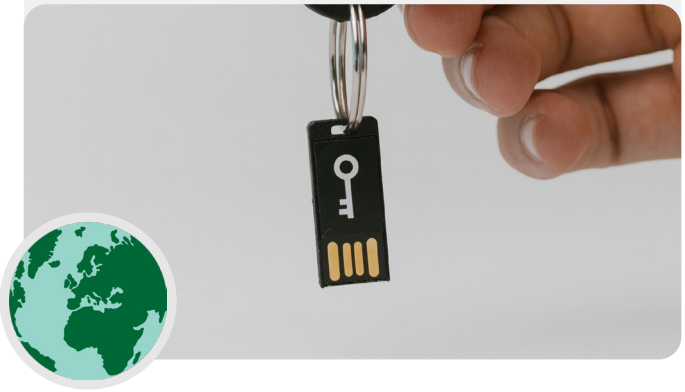
Kur të jeni gati të filloni të aktivizoni 2FA për të gjitha llogaritë e ndryshme të parlamentit tuaj, përdorni këtë faqe interneti (**https://2fa.directory/**) për të kërkuar me shpejtësi informacione dhe udhëzime për shërbime specifike (si Gmail, Office 365, Facebook, Twitter, etj.) dhe për të parë se cilat shërbime lejojnë cilat lloje të 2FA.

2FA dhe parlamentet

Sipas raporteve të lëshuara në vitin 2020, **hakerët depërtuan në sistemin e postës elektronike parlamentare të Norvegjisë** duke kompromentuar llogaritë e postës elektronike që u përkisnin disa zyrtarëve parlamentarë dhe madje duke shkarkuar informacione nga sistemet parlamentare. Ndërsa detajet e plota të hakimit nuk u publikuan, Norvegjia ia atribuoi ndërhyrjen APT28, një grup hakerimi i lidhur me shërbimet e sigurisë ruse. Ndërsa shumë të sofistikuara, APT28 dhe hakerët e tjerë shpesh përdorin taktika më pak komplekse si "sulmet me forcë brutale" (ku sulmuesi përdor mjete për të provuar shumë fjalëkalime me shpresën për të gjetur përfundimisht atë të duhurin) për të fituar qasje në llogari. Kjo taktikë i lejon hakerët të hamendësojnë edhe fjalëkalime të forta – siç besohej se ishte rasti në Norvegji. Lajmi i mirë? Llojet e sulmeve kanë shumë më pak gjasa të kenë sukses me vërtetimin e duhur me dy faktorë të bazuar në çelës ose aplikacion!

Çelësat e sigurisë në botën reale

Duke ofruar çelësa të sigurisë fizike për vërtetimin me dy faktorë për të gjithë 85,000+ punonjësit e tij, Google (një organizatë me rrezik shumë të lartë, shumë e shënjestruar) në mënyrë efektive **eliminoi çfarëdo sulmi të suksesshëm phishing** kundër organizatës. Ky rast tregon se sa efektivë mund të jenë çelësat e sigurisë edhe për organizatat më të rrezikuara.



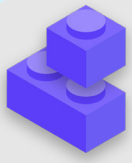
ÇFARË NDODH NËSE DIKUSH HUMBET NJË PAJISJE 2FA?

Nëse përdorni çelës sigurie, trajtojeni atë në të njëjtën mënyrë që do të trajtonit çelësin për shtëpinë ose banesën tuaj, nëse keni një të tillë. Me pak fjalë, mos e humbni. Ashtu si çelësat e shtëpisë tuaj, megjithatë, është gjithmonë ide e mirë që të keni një çelës rezervë të regjistruar në llogarinë tuaj, i cili do të qëndrojë i mbyllur në një vend të sigurt (si kasaforta në shtëpi ose ndonjë kasafortë) vetëm në rast humbjeje ose vjedhjeje.
Përndryshe, duhet të krijoni kode rezervë për llogaritë që e lejojnë atë. Duhet t'i mbani këto kode të ruajtura në një vend shumë të sigurt, si menaxheri i fjalëkalimit ose një kasafortë fizike. Kode të tilla rezervë mund të prodhohen brenda cilësimeve 2FA të shumicës së sajteve (në të njëjtin vend ku aktivizoni 2FA në radhë të parë) dhe mund të veprojnë si një çelës rezervë në rast urgjence. Fatkeqësia më e zakonshme 2FA ndodh kur njerëzit zëvendësojnë ose humbasin telefonat që përdorin për aplikacionet e vërtetimit. Nëse përdorni Google Authenticator, nuk keni fat nëse telefoni juaj është vjedhur, përveç nëse ruani kodet rezervë që krijohen në momentin që lidhni një llogari me Google Authenticator. Prandaj, nëse përdorni Google Authenticator si aplikacion 2FA, sigurohuni që të ruani kodet rezervë për të gjitha llogaritë që lidheni në një vend të sigurt. Nëse përdorni Authy ose Duo, të dy aplikacionet kanë veçori të integruara rezervë me cilësime të forta sigurie që mund t'i aktivizoni. Nëse zgjidhni njërën nga ato aplikacione, mund t'i konfiguroni ato opsione rezervë në rast të prishjes, humbjes ose vjedhjes së pajisjes. Shihni udhëzimet e Authy-t **këtu**, dhe të Duo-s **këtu**. Sigurohuni që të gjithë të jenë të vetëdijshëm për këta hapa pasi fillojnë të aktivizojnë 2FA në të gjitha llogaritë e tyre.

Nivel i avancuar: Zbatimi i 2FA në të gjithë parlamentin tuaj

Nëse parlamenti juaj ofron llogari të postës elektronike të gjithë stafit përmes Google Workspace (i njohur më parë si GSuite) ose Microsoft 365 duke përdorur domenin tuaj (për shembull, @ndi.org), ju mund të zbatoni 2FA dhe cilësime të forta sigurie për të gjitha llogaritë.
Një zbatim i tillë jo vetëm që ndihmon në mbrojtjen e këtyre llogarive, por gjithashtu vepron si mënyrë për të prezantuar dhe normalizuar 2FA për anëtarët dhe stafin tuaj, në mënyrë që ata të jenë më të kënaqur me adoptimin e tij edhe për llogaritë personale. Si administrator i Google Workspace, mund të ndiqni **këto udhëzime** për të zbatuar 2FA për domenin tuaj. Mund të bëni diçka të ngjashme në Microsoft 365 duke ndjekur **këta hapa** si administrator domeni.

Konsideroni gjithashtu regjistrimin e llogarive të parlamentit tuaj në **Advanced Protection Program** (Google) ose **AccountGuard** (Microsoft) për të zbatuar kontrolle shtesë të sigurisë dhe për të kërkuar çelësa fizikë të sigurisë për vërtetimin me dy faktorë.



Blloqet e ndërtimit të planit të sigurisë: Llogaritë e sigurta

- **Kërkoni fjalëkalime të forta për të gjitha llogaritë parlamentare; inkurajoni të njëjtën gjë për llogaritë personale të anëtarëve, stafit dhe vullnetarëve.**
- **Zbatoni një menaxher të besueshëm të fjalëkalimeve për parlamentin (dhe inkurajoni përdorimin edhe në jetën personale të stafit).**
  - Kërkoni fjalëkalim të fortë primar dhe 2FA për të gjitha llogaritë e menaxherit të fjalëkalimeve.
  - Përkujtojuni të gjithëve që të dalin nga menaxheri i fjalëkalimeve në pajisjet e përbashkëta ose kur janë në rrezik të shtuar të vjedhjes ose konfiskimit të pajisjes.
- **Ndryshoni fjalëkalimet e përbashkëta kur stafi dhe anëtarët largohen nga parlamenti.**
- **Ndani fjalëkalimet vetëm në mënyrë të sigurt, si p.sh. nëpërmjet menaxherit të fjalëkalimeve të parlamentit tuaj ose aplikacioneve të enkriptuara nga fundi në fundi.**
- **Kërkoni 2FA për të gjitha llogaritë e parlamentit dhe inkurajoni stafin të krijojë 2FA për të gjitha llogaritë personale gjithashtu.**
  - Nëse është e mundur, jepni çelësat e sigurisë fizike për të gjithë anëtarët dhe stafin.
  - Nëse nuk keni buxhet për çelësat e sigurisë, inkurajoni përdorimin e aplikacioneve të vërtetuesit në vend të SMS-ve ose telefonatave për 2FA.
- **Mbani trajnime të rregullta për t'u siguruar që të gjithë janë të vetëdijshëm për fjalëkalimin dhe praktikat më të mira 2FA, duke përfshirë atë që e bën një fjalëkalim të fortë dhe rëndësinë që kurrë, në çfarëdo kushte, të mos përdorin fjalëkalimet e kaluara, të pranojnë vetëm kërkesa legjitime 2FA dhe gjenerim të kodeve rezervë 2FA.**

Pajisje të sigurta

Përveç llogarive, është thelbësore që të gjitha pajisjet – kompjuterët, telefonat, USB-të, disqet e ngurtë të jashtme, etj. – të mbrohen mirë. Një mbrojtje e tillë fillon me të qenit të kujdesshëm për llojin e pajisjeve që blejnë dhe përdorin parlamenti dhe stafi juaj. Çdo shitës ose prodhues që ju zgjidhni duhet të ketë një histori të demonstruar të respektimit të standardeve globale në lidhje me zhvillimin e sigurt të pajisjeve harduerike (si telefonat dhe kompjuterët). Çdo pajisje që blini duhet të prodhohet nga kompani të besuara që nuk kanë një nxitje për t'i dorëzuar të dhënat dhe informacionin një kundërshtari të mundshëm. Është e rëndësishme të theksohet se qeveria kineze kërkon që kompanitë kineze t'i japin të dhëna qeverisë qendrore.

Prandaj, pavarësisht pranisë së kudogjendur dhe të lirë të telefonave inteligjentë si Huawei ose ZTE, ato duhen shmangur. Megjithëse kostoja e pajisjeve të lira mund të jetë shumë tërheqëse, rreziqet e mundshme të sigurisë për parlamentet duhet t'ju orientojnë drejt opsioneve të tjera të aparateve dhe pajisjeve.

Kundërshtarët tuaj mund të kompromet ojnë sigurinë e pajisjeve tuaja - dhe gjithçka që bëni nga ato pajisje - ose duke fituar qasje fizike ose qasje "në distancë" në pajisjen tuaj.

Siguria e pajisjeve dhe parlamentet

Disa nga softuerët më keqdashës të avancuar në botë janë zhvilluar dhe shpërndarë në të gjithë globin për të synuar deputetë, zyrtarë të tjerë qeveritarë dhe stafin e tyre. Në Indi, për shembull, një konsorcium gazetarësh zbuloi se shumë deputetë dhe ministra të qeverisë ishin shënjestruar nga softuer spiunimi (spyware) Pegasus, një lloj softueri keqdashës që kapi titujt kryesorë në vitin 2020. Pegasus është famëkeq për aftësinë e tij për të infektuar pajisjet celulare dhe për t'i dhënë autorit aftësinë për të regjistruar audio, për të përgjuar tastierë dhe mesazhe, dhe në fakt për ta vënë viktimën nën mbikëqyrje të plotë, pa kërkuar ndërveprimin e viktimës. Megjithatë, shumica dërrmuese e softuerit spyware ka sukses për shkak të praktikave të dobëta të sigurisë së pajisjes, të tilla si pakujdesia ndaj phishing ose mungesa e zbatimit të politikave të përmendura në këtë pjesë të Doracakut.

QASJA FIZIKE E PAJISJES NËPËRMJET HUMBJES OSE VJEDHJES

Për të parandaluar kompromisin fizik, është thelbësore t'i mbani pajisjet tuaja të sigurta fizikisht. Me pak fjalë, mos ia lehtësoni një kundërshtari vjedhjen apo edhe marrjen e përkohshme të pajisjes tuaj nga ju. Mbajini të mbyllura pajisjet nëse lihen në shtëpi ose në zyrë. Ose nëse mendoni se është më e sigurt, mbajini ato me vete. Kjo sigurisht do të thotë se një pjesë e sigurisë së pajisjes është siguria fizike e hapësirave tuaja të punës (qoftë në një mjedis zyre ose në shtëpi). Do t'ju duhet të instaloni bravë të fortë, kamera sigurie ose sisteme të tjera monitorimi. Kujtojuni personelit që t'i trajtojë pajisjet në të njëjtën mënyrë që do të trajtonte një grumbull të madh parash - mos i lini të shtrira përreth pa mbikëqyrje ose të pambrojtur.

Çfarë ndodh nëse një pajisje vidhet?

Për të kufizuar ndikimin nëse dikush arrin të vjedhë një pajisje - ose edhe nëse thjesht fiton qasje në të, për një periudhë të shkurtër kohore - **sigurohuni që të detyroni përdorimin e fjalëkalimeve ose kodeve të forta në kompjuterët dhe telefonat e të gjithëve**. Të njëjtat këshilla për fjalëkalimin nga pjesa mbi **Fjalëkalimet e këtij** Doracaku zbatohen për një fjalëkalim të mirë për kompjuter ose laptopë. Kur bëhet fjalë për kyçjen e telefonit tuaj, përdorni kode që kanë të paktën gjashtë deri në tetë shifra dhe shmangni përdorimin e "modeleve të rrëshqitjes" për të shkyçur ekranin. Për këshilla shtesë mbi kyçjet e ekranit, shikoni **Data Detox Ki**t nga Tactical Tech. Përdorimi i fjalëkalimeve të mira të pajisjes e bën shumë më të vështirë që një kundërshtar të qas shpejt informacionin në pajisjen tuaj në rast vjedhjeje ose konfiskimi.

Sigurohuni që çdo pajisje e lëshuar nga parlamenti është gjithashtu e regjistruar **në një pajisje celulare ose në një sistem të menaxhimit të pikës fundore**. Edhe pse nuk janë të lira, këto sisteme lejojnë parlamentin tuaj të zbatojë politikat e sigurisë në të gjitha pajisjet dhe të gjejë një të tillë dhe të fshijë përmbajtjet e tij potencialisht të ndjeshme, nëse vidhet, humbet ose konfiskohet. Ndërsa ekzistojnë shumë zgjidhje të ndryshme për menaxhimin e pajisjeve celulare, disa opsione të besuara që funksionojnë nëpër platforma (iPhones, Android, Mac dhe Windows) përfshijnë **Hexnode**, **Meraki Systems Manager** nga Cisco, **IBMs MDM**, dhe funksionin e integruar të Google Workspace **Mobile Device Management**. Nëse kostoja është faktor kufizues, të paktën inkurajoni anëtarët dhe stafin që të përdorin veçoritë e integruara "Gjeni pajisjen time" në telefonat e tyre të mençur të lëshuar nga parlamenti dhe në ato personal, si p.sh. Find My iPhone në iPhone dhe Find My Device në Android.

Po enkriptimi i pajisjes?

Është e rëndësishme të përdoret enkriptimi, gërvishtja e të dhënave në mënyrë që të jenë të palexueshme dhe të papërdorshme, në të gjitha pajisjet, veçanërisht kompjuterët dhe telefonat inteligjentë. Nëse është e mundur, duhet t'i konfiguroni të gjitha pajisjet në të gjithë parlamentin me diçka që quhet **enkriptim në diskun e plotë**. Enkriptimi i plotë i diskut do të thotë që tërësia e një pajisjeje është e enkriptuar në mënyrë që një kundërshtar, nëse do ta vidhte fizikisht, nuk do të ishte në gjendje të nxirrte përmbajtjen e një pajisjeje pa ditur fjalëkalimin ose çelësin që keni përdorur për ta enkriptuar.

Shumë telefona të mençur dhe kompjuterë modernë ofrojnë enkriptim të plotë të diskut. Pajisjet Apple si iPhone dhe iPad, në mënyrë mjaft të përshtatshme, aktivizojnë enkriptimin në diskun e plotë kur vendosni një kodkalim normal të pajisjes. Kompjuterët Apple që përdorin macOS ofrojnë një veçori të quajtur FileVault që mund ta aktivizoni për enkriptim të plotë të diskut.

Kompjuterët Windows që përdorin licenca pro, për ndërmarrje ose arsim, ofrojnë një veçori të quajtur BitLocker që mund ta aktivizoni për enkriptim të plotë të diskut. Mund të aktivizoni BitLocker duke ndjekur **këto udhëzime** nga Microsoft, të cilat mund të duhet së pari të aktivizohen nga administratori i organizatës suaj. Nëse stafi ka vetëm një licencë shtëpiake për kompjuterët e tyre Windows, BitLocker nuk është në dispozicion. Megjithatë, ende mund të aktivizojnë enkriptimin në diskun e plotë duke shkuar te "Përditësimi dhe Siguria" > "Enkriptimi i pajisjes" nën cilësimet e Windows OS.
Pajisjet Android, që nga versioni 9.0 e më vonë, dërgohen me enkriptim të bazuar në skedarë të aktivizuar si parazgjedhje. Enkriptimi i bazuar në skedarë i Android funksionon ndryshe nga enkriptimi në diskun e plotë, por gjithsesi ofron siguri të fortë. Nëse jeni duke përdorur telefon relativisht të ri Android dhe keni vendosur një kod kalimi, duhet të aktivizohet enkriptimi i bazuar në skedarë. Megjithatë, është mirë të kontrolloni cilësimet tuaja vetëm për t'u siguruar, veçanërisht nëse telefoni juaj është më i vjetër se disa vjet. Për të kontrolluar, shkoni te Cilësimet > Siguria në pajisjen tuaj Android. Brenda cilësimeve të sigurisë, duhet të shihni një nënseksion për "enkriptim" ose "enkriptimi dhe kredencialet", i cili do të tregojë nëse telefoni juaj është i enkriptuar dhe, nëse jo, do t'ju lejojë të aktivizoni enkriptimin.

Për kompjuterët (qoftë Windows ose Mac), është veçanërisht e rëndësishme të ruani çdo çelës enkriptimi (të referuar si çelësa rikuperimi) në një vend të sigurt. Këta "çelësat e rikuperimit" janë, në shumicën e rasteve, fjalëkalime ose fraza kalimi në thelb të gjata.
Në rast se harroni fjalëkalimin normal të pajisjes ose ndodh diçka e papritur (si dështimi i pajisjes), çelësat e rikuperimit janë mënyra e vetme për të rikuperuar të dhënat tuaja të enkriptuara dhe, nëse është e nevojshme, për t'i zhvendosur ato në një pajisje të re. Prandaj, kur aktivizoni enkriptimin në diskun e plotë, sigurohuni që t'i ruani këto çelësa ose fjalëkalime në një vend të sigurt, si një llogari e sigurt në re ose tek menaxheri i fjalëkalimeve të parlamentit tuaj.

QASJA NË DISTANCË NË PAJISJE – E NJOHUR GJITHASHTU SI HAKERIM

Përveç mbajtjes së pajisjeve fizikisht të sigurta, është e rëndësishme t'i mbani ato të lira nga softuerët keqdashës. Security-in-a-Box nga Tactical Tech, jep një përshkrim të dobishëm të asaj që paraqet softuer keqdashës dhe pse është e rëndësishme të shmanget, që është përshtatur pak në pjesën tjetër të këtij seksioni.

Kuptimi dhe shmangia e softuerëve keqdashës (malware)

Ka shumë mënyra për të klasifikuar malware (term që do të thotë softuer me qëllim të keq ose keqdashës). Viruset, softuerët për spiunim (spyware), kërmijtë (worms), trojanët (trojans), rootkits, ransomware dhe cryptojackers janë të gjitha llojet e softuerëve keqdashës. Disa lloje të softuerëve keqdashës përhapen në internet nëpërmjet postës elektronike, mesazheve me tekst, faqeve të internetit me qëllim të keq dhe mjeteve të tjera. Disa përhapen nëpërmjet pajisjeve si USB memorie që përdoren për të shkëmbyer dhe vjedhur të dhëna. Dhe, ndërsa disa softuerë keqdashës kërkojnë objektiv që nuk dyshon për të bërë një gabim, të tjerët mund të infektojnë në heshtje sistemet e cenueshme pa bërë asgjë të gabuar fare.

Përveç softuerëve keqdashës të përgjithshëm, që lëshohen gjerësisht dhe synojnë publikun e gjerë, softueri keqdashës i synuar zakonisht përdoret për të ndërhyrë ose për të spiunuar një individ, organizatë ose rrjet të caktuar. Kriminelët e rregullt i përdorin këto teknika, por po ashtu i përdorin shërbimet ushtarake dhe kundër-zbuluese, terroristët, ngacmuesit në internet, bashkëshortët abuzues dhe aktorët politikë të dyshimtë.

Sido që të quhen, sido që të shpërndahen, softuerët keqdashës mund të shkatërrojnë kompjuterët, të vjedhin dhe shkatërrojnë të dhënat, të prishin operacionet parlamentare, të pushtojnë privatësinë dhe t'i vënë përdoruesit në rrezik. Me pak fjalë, softueri keqdashës është vërtet i rrezikshëm. Megjithatë, ka disa hapa të thjeshtë që parlamenti juaj mund të marrë për t'u mbrojtur kundër këtij kërcënimi të përbashkët.

A do të na mbrojë një mjet kundër softuerëve keqdashës?

Mjetet kundër softuerëve keqdashës për fat të keq nuk janë një zgjidhje e plotë. Sidoqoftë, është një ide shumë e mirë të përdorni disa mjete bazë, falas si bazë. Softuerët keqdashës ndryshojnë kaq shpejt, me rreziqe të reja që paraqiten në botën reale kaq shpesh, saqë mbështetja në ndonjë mjet të tillë nuk mund të jetë mbrojtja juaj e vetme. Nëse jeni duke përdorur Windows, duhet të hidhni një sy Windows Defender-it të integruar. Kompjuterët Mac dhe Linux nuk vijnë me softuer të integruar kundër softuerëve keqdashës, as pajisjet Android dhe iOS. Mund të instaloni një mjet me reputacion dhe pa pagesë për përdorim si p.sh Bitdefender ose Malwarebytes për ato pajisje (dhe kompjuterët Windows gjithashtu). Por **mos u mbështetni në atë si linjën tuaj të vetme të mbrojtjes**, pasi ata me siguri do të humbasin disa nga sulmet e reja më të synuara dhe të rrezikshme.

Për më tepër, jini shumë të kujdesshëm që të shkarkoni vetëm mjete me reputacion kundër softuerëve keqdashës ose anti-virus nga burime legjitime (si faqet e internetit të lidhura më lart). Fatkeqësisht, ekzistojnë shumë versione të rreme ose të kompromentuara të mjeteve kundër softuerëve keqdashës që bëjnë më shumë dëm sesa mirë.

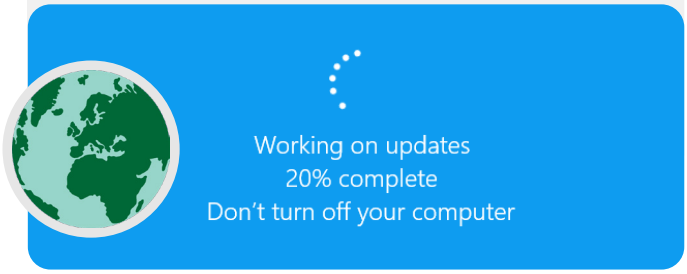
Nëse përdorni Bitdefender ose ndonjë mjet tjetër kundër softuerëve keqdashës në parlamentin tuaj, sigurohuni që të mos përdorni dy në të njëjtën kohë. Shumë prej tyre do të identifikojnë sjelljen e një programi tjetër kundër softuerëve keqdashës si të dyshimtë dhe do ta ndalojnë atë të funksionojë, duke i lënë të dy keqfunksionimet. Bitdefender ose programe të tjera me reputacion kundër softuerëve keqdashës mund të përditësohen falas dhe Windows Defender-i i integruar merr përditësime së bashku me kompjuterin tuaj. Sigurohuni që softueri juaj kundër softuerëve keqdashës përditësohet rregullisht (disa versione provë të softuerit komercial që dërgohen me një kompjuter do të çaktivizohen pas skadimit të periudhës së provës, duke e lënë atë më të rrezikshëm sesa të dobishëm.) Softueri keqdashës i ri shkruhet dhe shpërndahet çdo ditë, dhe kompjuteri do të bëhet shpejt edhe më i prekshëm nëse nuk vazhdoni me përkufizimet e reja të softuerëve keqdashës dhe teknikave kundër tyre. Nëse është e mundur, duhet të konfiguroni softuerin tuaj që të instalojë përditësimet automatikisht. Nëse mjeti juaj kundër softuerëve keqdashës ka një veçori opsionale "gjithmonë ndezur", duhet ta aktivizoni atë dhe të merrni parasysh herë pas here të skanoni të gjithë skedarët në kompjuterin tuaj.

Mbajini pajisjet të përditësuara

Përditësimet janë thelbësore. Përdorni versionin më të fundit të çdo sistemi operativ që funksionon në një pajisje (Windows, Mac, Android, iOS, etj.) dhe mbajeni atë sistem operativ të përditësuar. Mbani të përditësuar softuerin tjetër, shfletuesin dhe çdo shtojcë të shfletuesit. Instaloni përditësimet sapo të vihen në dispozicion, në mënyrë ideale duke aktivizuar përditësimet automatike. Sa më i përditësuar të jetë sistemi operativ i një pajisjeje, aq më pak dobësi do të keni. Mendoni për përditësimet sikur të vendosni një fashë në një prerje të hapur: mbyll një lëndim dhe redukton shumë mundësinë për infektime. Gjithashtu çinstaloni softuerin që nuk e përdorni më. Softueri i vjetërsuar shpesh ka probleme sigurie dhe mund të keni instaluar ndonjë mjet që nuk përditësohet më nga zhvilluesi, duke e lënë atë më të prekshëm ndaj hakerëve

Softuerët keqdashës në botën reale: Përditësimet janë thelbësore

Në vitin 2017, sulmet WannaCry ransomware infektuan miliona pajisje në mbarë botën, duke mbyllur spitale, organe qeveritare, organizata dhe biznese të mëdha dhe të vogla në dhjetëra vende. Pse sulmi ishte kaq efektiv? Për shkak të sistemeve operative të vjetërsuara, "të pa-patchuara" të Windows-it, shumë prej të cilave fillimisht ishin piratuar. Pjesa më e madhe e dëmit – njerëzor dhe financiar – mund të ishte shmangur me praktika më të mira të përditësimit të automatizuar dhe përdorimin e sistemeve operative legjitime.



Kini kujdes me USB-të

Jini të kujdesshëm kur hapni skedarë që ju dërgohen si bashkëngjitje, përmes lidhjeve të shkarkimit ose me çdo mjet tjetër. Gjithashtu **mendoni dy herë përpara se të futni media të lëvizshme si USB**, kartat e memories flash, DVD dhe CD në kompjuterin tuaj, pasi ato mund të jenë një vektor për softuerë keqdashës. USB-të që janë përdorur nga më shumë persona për një kohë më të gjatë ka shumë gjasa të kenë viruse në to. Për opsione alternative për të ndarë skedarët në mënyrë të sigurt në parlamentin tuaj, hidhini një sy seksionit File Sharing të Doracakut.

Jini të kujdesshëm edhe për pajisjet e tjera me të cilat lidheni përmes Bluetooth-it. Është mirë të sinkronizoni telefonin ose kompjuterin tuaj me një altoparlant të njohur dhe të besuar Bluetooth për të luajtur muzikën tuaj të preferuar, por kini kujdes me lidhjen ose pranimin e kërkesave nga çdo pajisje që nuk e njihni. Lejoni lidhjet vetëm me pajisje të besueshme dhe mos harroni të çaktivizoni Bluetooth-in kur nuk është në përdorim.

Tregohuni të zgjuar gjatë shfletimit

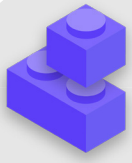
Asnjëherë mos pranoni dhe mos ekzekutoni aplikacione që vijnë nga faqe interneti që nuk i njihni dhe nuk i besoni. Në vend që të pranoni një "përditësim" të ofruar në një dritare kërcyese të shfletuesit, për shembull, kontrolloni për përditësime në faqen zyrtare të aplikacionit përkatës. Siç është diskutuar në pjesën mbi mashtrimin (Phishing) të Doracakut, është thelbësore të qëndroni vigjilent kur shfletoni faqet e internetit. Kontrolloni destinacionin e një lidhjeje (duke qëndruar pezull mbi të) përpara se të klikoni dhe hidhini një sy adresës së faqes së internetit pasi të ndiqni një lidhje dhe sigurohuni që të duket e përshtatshme përpara se të futni informacione të ndjeshme si fjalëkalimi juaj. Mos klikoni nëpër mesazhe gabimi ose paralajmërime, shikoni dritaret e shfletuesit që shfaqen automatikisht dhe lexojini ato me kujdes në vend që thjesht të klikoni Po ose OK.

Softuerët keqdashës në botën reale: Aplikacione celulare me qëllim të keq

Hakerët në shumë vende kanë përdorur aplikacione të rreme në dyqanin Google Play për të shpërndarë softuerë keqdashës për vite me radhë. Një rast i veçantë që ka synuar përdoruesit në Vietnam doli në dritë në prill 2020. Kjo fushatë spiunimi përdorte aplikacione të rreme, të cilat supozohet se i ndihmonin përdoruesit të gjenin lokalet e afërta ose të gjenin informacione për kishat lokale. Pasi u instaluan nga përdorues të padashur të Android, aplikacionet keqdashëse mblodhën regjistrat e thirrjeve, të dhënat e vendndodhjes dhe informacione rreth kontakteve dhe mesazheve me tekst. Kjo është vetëm një nga arsyet e shumta për të qenë të kujdesshëm se cilat aplikacione i shkarkoni në pajisjet tuaja.

Po në lidhje me telefonat e mençur?

Ashtu si me kompjuterët, mbani të përditësuar sistemin operativ dhe aplikacionet e telefonit tuaj dhe aktivizoni përditësimet automatike. Instaloni vetëm nga burime zyrtare ose të besueshme si Play Store në Google dhe App Store në Apple (ose F-droid, një dyqan aplikacionesh falas me burim të hapur për Android). Aplikacionet mund të kenë të futur softuerë keqdashës në to dhe ende duket se funksionojnë normalisht, kështu që nuk do ta dini gjithmonë nëse është keqdashës ose jo. Sigurohuni që shkarkoni versionin legjitim të një aplikacioni. Sidomos në Android, ekzistojnë versione "të rreme" të aplikacioneve të njohura. Pra, sigurohuni që një aplikacion është krijuar nga kompania ose zhvilluesi i duhur, ka vlerësime të mira dhe ka numrin e pritur të shkarkimeve (për shembull, një version i rremë i WhatsApp mund të ketë vetëm disa mijëra shkarkime, por versioni i vërtetë ka mbi pesë miliardë). Kushtojini vëmendje lejeve që kërkojnë aplikacionet tuaja. Nëse ato duken të tepërta (si një makinë llogaritëse që kërkon qasje në kamerën tuaj ose Angry Birds që kërkon qasje në vendndodhjen tuaj, për shembull) mohoni kërkesën ose çinstaloni aplikacionin. Çinstalimi i aplikacioneve që nuk i përdorni më, mund të ndihmojë gjithashtu në mbrojtjen e telefonit tuaj të mençur ose tabletit tuaj. Zhvilluesit ndonjëherë ua shesin pronësinë e aplikacioneve të tyre njerëzve të tjerë. Këta pronarë të rinj mund të përpiqen të fitojnë para duke shtuar kode me qëllim të keq

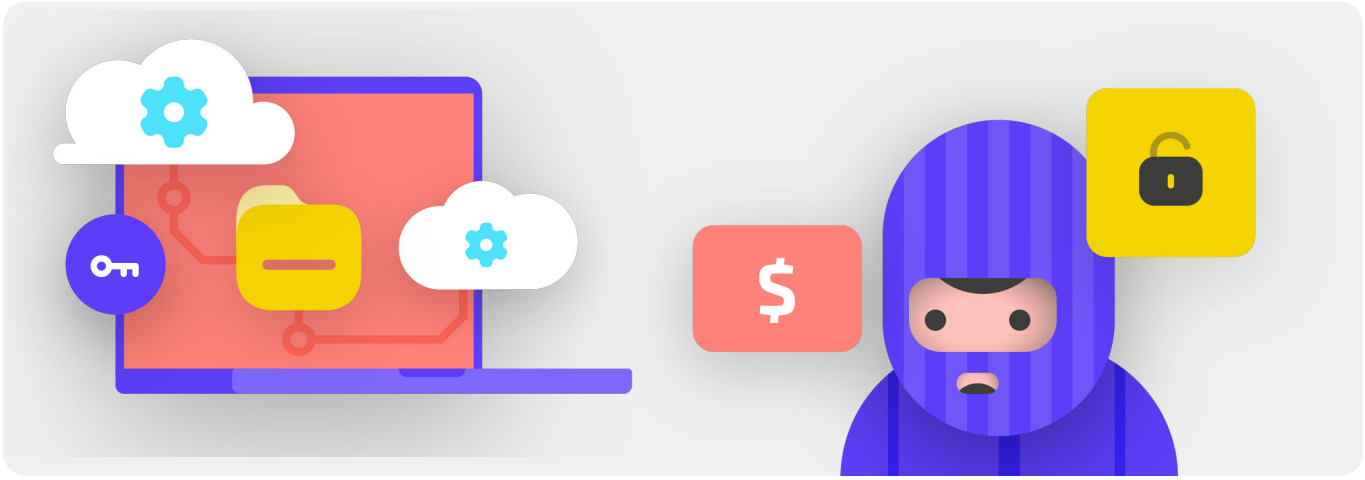


Mbajtja e pajisjeve të sigurta

- **Trajnoni anëtarët dhe stafin mbi rreziqet e softuerëve keqdashës dhe praktikat më të mira për t'i shmangur.**
  - Siguroni politika për lidhje të pajisjeve të jashtme, klikime në lidhje, shkarkime të skedarëve dhe aplikacioneve dhe kontrollim të lejes së softuerit dhe aplikacionit.
- **Urdhëroni që pajisjet, softueri dhe aplikacionet të mbahen plotësisht të përditësuara.**
- **Aktivizoni përditësimet automatike aty ku është e mundur.**
- **Regjistroni të gjitha pajisjet parlamentare në një pajisje celulare ose në një sistem të menaxhimit të pikës fundore.**
- **Sigurohuni që të gjitha pajisjet të përdorin softuer të licencuar.**
- **Kërkoni mbrojtje me fjalëkalim për të gjitha pajisje parlamentare, duke përfshirë pajisjet personale celulare që përdoren për komunikime të lidhura me parlamentin.**
- **Aktivizoni enkriptimin në diskun e plotë në pajisje.**
- **Kujtojuni shpesh anëtarëve dhe stafit që t'i mbajnë pajisjet e tyre fizikisht të sigurta - dhe menaxhoni sigurinë e zyrës tuaj me bravë dhe mënyra të përshtatshme për të siguruar kompjuterët.**
- **Mos ndani skedarë duke përdorur USB ose mos lidhni USB në kompjuterët tuaj.**
  - Përdorni opsione alternative të sigurta për ndarjen e skedarëve.

Phishing: Kërcënim i zakonshëm për pajisjet dhe llogaritë

Phishing është sulmi më i zakonshëm dhe më efektiv ndaj organizatave, përfshirë parlamentet, në mbarë botën. Teknika përdoret nga ushtritë më të sofistikuara të shteteve kombëtare, si dhe nga mashtruesit e vegjël. Phishing, thënë thjesht, është vendi ku një kundërshtar përpiqet t'ju mashtrojë për të shkëmbyer informacione që mund të përdoren kundër jush ose organizatës suaj. Phishing mund të ndodhë nëpërmjet postës elektronike, mesazheve me tekst/SMS (shpesh të referuara si SMS phishing ose "smishing"), aplikacioneve të mesazheve si WhatsApp, mesazheve ose postimeve të mediave sociale ose telefonatave (shpesh të referuara si phishing zanor ose "vishing"). Mesazhet e phishing mund të përpiqen t'ju bëjnë të shkruani informacione të ndjeshme (si fjalëkalimet) në një faqe interneti të rreme, në mënyrë që të keni qasje në një llogari, t'ju kërkojnë të ndani informacione private (si numri i kartës së kreditit) përmes zërit ose tekstit, ose t'ju bindin për të shkarkuar malware (softuer keqdashës) që mund të infektojnë pajisjen tuaj. Për një shembull jo teknik, çdo ditë miliona njerëz marrin telefonata të rreme automatike duke u thënë atyre se llogaria e tyre bankare është kompromentuar ose se identiteti i tyre është vjedhur - të gjitha këto janë krijuar për të mashtruar të pavetëdijshmit me qëllim që të ndajnë informacione të ndjeshme.



SI MUND TA IDENTIFIKOJMË PHISHING?

Phishing mund të duket i frikshëm dhe i pamundur për t'u kapur, por ka disa hapa të thjeshtë që të gjithë në parlament mund të ndërmarrin për t'u mbrojtur nga shumica e sulmeve. Këshillat e mëposhtme për mbrojtjen nga phishing janë modifikuar dhe zgjeruar nga udhëzuesi i thelluar i phishing i zhvilluar nga Freedom of the Press Foundation, dhe duhet të ndahet me të gjithë brenda dhe rreth parlamentit dhe të integrohet në planin tuaj të sigurisë:

Ndonjëherë, fusha "nga" ju gënjen

Kini parasysh se fusha "nga" në postat tuaja elektronike mund të jetë e falsifikuar për t'ju mashtruar. Është e zakonshme që phisher-ët të vendosin një adresë poste elektronike që duket shumë si një adresë legjitime me të cilën jeni njohur, e shkruar gabimisht vetëm për t'ju mashtruar. Për shembull, mund të merrni një poste elektronike nga dikush me adresën "john@goooogle.com" në krahasim me "john@google.com". Vini re O-të shtesë në google. gjithashtu mund të njihni dikë me një adresë poste elektronike "john@gmail.com", por merrni një poste elektronike phishing nga një imitues që krijoi "johm@gmail.com" - i vetmi ndryshim është një ndryshim delikat i shkronjave në fund. Gjithmonë sigurohuni që të kontrolloni dy herë nëse e dini adresën e dërgimit të një poste elektronike përpara se të vazhdoni. Një koncept i ngjashëm zbatohet për phishing nëpërmjet tekstit, telefonatave ose aplikacioneve të mesazheve. Nëse merrni një mesazh nga një numër i panjohur, mendoni dy herë përpara se t'i përgjigjeni ose të ndërveproni me mesazhin.

Phishing-u dhe parlamentet


Thu 4/8/2021 8:48 AM

[redacted] <[redacted]@aop.gov.af>

Kindlty mention this email Most Urgent.

To [redacted]@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page.
Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards | [redacted]

[redacted]

Press office | Spokesman

Presidential Palace (ARG) | Islamic Republic of Afghanistan

Mobile: [redacted] | ocs.gov.af

Mail: [redacted]

Sulmet e sofistikuara dhe të personalizuara të phishing synojnë rregullisht parlamente dhe aktorë të tjerë qeveritarë në mbarë botën.

Zyrtarët parlamentar federalë dhe lokalë në **Gjermani** u shënjestruan nga postat elektronike të phishing-ut në prag të zgjedhjeve në vjeshtën e vitit 2021. Vetëm disa muaj më parë në Afganistan, një grup hakerimi përdori **phishing teknika** për të depërtuar me sukses në ish-Këshillin e Sigurisë Kombëtare duke marrë përsipër identitetin e zëdhënësit të shtypit të ish-presidentit afgan Ashraf Ghani. Hakerët dërguan posta elektronike phishing (treguar më sipër) që u kërkonin viktimave të hapnin një skedar të bashkangjitur që "zëdhënësi" pretendonte se përmbante një gabim. Kur viktimat shkarkuan dhe hapën skedarin për të "konfirmuar gabimin", bashkëngjitja me qëllim të keq vendosi softuerë keqdashës që u jepte hakerëve qasje të qëndrueshme në kompjuterë. Një qasje e tillë u mundësoi hakerëve të ngarkonin dhe shkarkonin skedarë, të ekzekutonin komandat në pajisjet sipas dëshirës dhe të vidhnin të dhëna shumë të ndjeshme të qeverisë.

Kini kujdes nga bashkëngjitjet

Bashkëngjitjet mund të përmbajnë softuerë keqdashës dhe viruse, dhe zakonisht shoqërojnë phishing postat elektronike. **Mënyra më e mirë për të shmangur softuerët keqdashës nga bashkëngjitjet është të mos i shkarkoni kurrë ato**. Si rregull, mos hapni asnjë bashkëngjitje menjëherë, veçanërisht nëse ato vijnë nga njerëz që nuk i njihni. Nëse është e mundur, kërkoni nga personi që ju ka dërguar dokumentin të kopjojë-ngjisë tekstin në një poste elektronike ose ta ndajë dokumentin nëpërmjet një shërbimi si Google Drive ose Microsoft OneDrive, të cilat kanë skanim të integruar të viruseve të shumicës së dokumenteve të ngarkuara në platformat e tyre. Ndërtoni një kulturë organizative ku dekurajohen lidhjet
Nëse absolutisht duhet të hapni bashkëngjitjen, duhet të hapet vetëm në një mjedis të sigurt (shih seksionin e avancuar më poshtë) ku softueri keqdashës i mundshëm nuk mund të vendoset në pajisjen tuaj.
Nëse përdorni Gmail dhe pranoni bashkëngjitje në një poste elektronike, në vend që ta shkarkoni dhe ta hapni në kompjuterin tuaj, thjesht klikoni në skedarin e bashkangjitur dhe lexoni atë në "para-pamje" (preview) brenda shfletuesit tuaj. Ky hap ju lejon të shikoni tekstin dhe përmbajtjen e një skedari pa e shkarkuar atë ose pa e lejuar atë të ngarkojë softuer keqdashës të mundshëm në kompjuterin tuaj. Kjo funksionon mirë për dokumente në Word, PDF dhe madje edhe prezantime në diapozitiv (slide-show/PPT). Nëse keni nevojë të redaktoni dokumentin, merrni parasysh hapjen e skedarit në një program re (cloud) si Google Drive dhe konvertimin e skedarit në një Google Doc ose Google Slides.
Nëse përdorni Outlook, mund të shikoni paraprakisht bashkëngjitjet pa i shkarkuar ato nga klienti i uebit i Outlook-ut. Nëse keni nevojë të modifikoni bashkëngjitjen, merrni parasysh ta hapni atë në OneDrive nëse është në dispozicion për ju. Nëse përdorni Yahoo Mail, zbatohet i njëjti koncept. Mos shkarkoni bashkëngjitjet, por shikoni paraprakisht ato brenda shfletuesit të internetit.

Pavarësisht nga mjetet që keni në dispozicion, qasja më e mirë është thjesht të mos shkarkoni kurrë bashkëngjitje që nuk i njihni ose i besoni, dhe pavarësisht se sa e rëndësishme mund të duket një bashkëngjitje, mos hapni kurrë diçka me ndonjë lloj skedari që nuk e njihni ose nuk synoni ta përdorni ndonjëherë.

Nivel i avancuar: Mbrojtja nga phishing për parlamentin tuaj

Nëse parlamenti juaj përdor Microsoft 365 të ndërmarrjes për postë elektronike dhe aplikacione të tjera, administratori i domenit tuaj duhet të konfigurojë Politikën e bashkëngjitjeve të sigurta për t'u mbrojtur nga bashkëngjitjet e rrezikshme. Nëse përdorni Google Workspace të ndërmarrjes (i njohur më parë si GSuite), ekziston një opsion po aq efektiv që duhet të konfigurojë administratori juaj i quajtur Google Security Sandbox. Përdoruesit individualë më të avancuar mund të marrin në konsideratë vendosjen e programeve të sofistikuara të sandbox, të tilla si Dangerzone ose, për ata me versionin Pro ose Enterprise të Windows 10, Windows Sandbox.

Një tjetër opsion i avancuar për të konsideruar për zbatim në të gjithë parlamentin është një shërbim filtrimi i sistemit të emrave me domain të sigurt (DNS). Parlamentet mund ta përdorin këtë teknologji për të bllokuar personelin nga qasja ose ndërveprimi aksidental i përmbajtjeve me qëllim të keq, duke ofruar një shtresë shtesë mbrojtjeje kundër phishing. Shërbime të reja si Cloudflare's Gateway ofrojnë aftësi të tilla për organizatat pa kërkuar shuma të mëdha parash. Mjete shtesë falas, duke përfshirë Quad9 nga Global Cyber Alliance Toolkit, do t'ju ndihmojë të bllokoni hyrjen në faqet e njohura që kanë viruse ose softuerë keqdashës të tjerë dhe mund të zbatohen në më pak se pesë minuta.

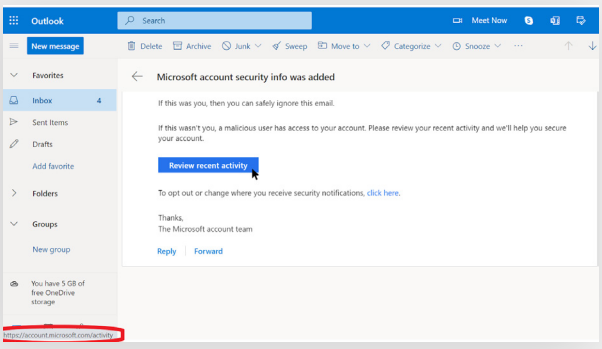
Klikoni me kujdes

Jini skeptik ndaj lidhjeve në poste elektronike ose mesazhe të tjera me tekst. Lidhjet mund të maskohen për të shkarkuar skedarë me qëllim të keq ose për t'ju çuar në sajte të rreme që mund t'ju kërkojnë të jepni fjalëkalime ose informacione të tjera të ndjeshme. Kur jeni në një kompjuter, ekziston një truk i thjeshtë për t'u siguruar që një lidhje në një poste elektronike ose mesazh do t'ju dërgojë atje ku supozohet: Përdorni miun për të lëvizur mbi çdo lidhje përpara se të klikoni mbi të dhe shikoni në fund të dritares në shfletuesit tuaj për të parë se cila është URL-ja aktuale (shih imazhin më poshtë).

Është më e vështirë të kontrolloni lidhjet në një poste elektronike në një pajisje celulare pa klikuar aksidentalisht mbi to - prandaj kini kujdes. Mund të kontrolloni destinacionin e një lidhjeje në shumicën e telefonave të mençur duke shtypur gjatë (duke mbajtur të shtypur) një lidhje derisa të shfaqet URL-ja e plotë.

Në phishing nëpërmjet SMS-ve dhe aplikacioneve të mesazheve, lidhjet e shkurtuara janë praktikë shumë e zakonshme që përdoret për të maskuar destinacionin e një URL-je. Nëse shihni një lidhje të shkurtër (p.sh., bit.ly ose tinyurl.com) në vend të URL-së së plotë, mos klikoni mbi të. Nëse lidhja është e rëndësishme, kopjojeni atë në një zgjerues të URL-së, si p.sh https://www.expandurl.net/, për të parë destinacionin aktual të një URL-je të shkurtuar. Për më tepër, mos klikoni në lidhjet e faqeve të internetit me të cilat nuk jeni të njohur. Nëse keni dyshime, kryeni një kërkim për faqen, me emrin e sajtit në thonjëza (p.sh. "www.badwebsite.com") për të parë nëse është një faqe interneti legjitime. Gjithashtu mund të kontrolloni lidhje potencialisht të dyshimta nëpërmjet skanerit të URL-së VirusTotal. Edhe pse kjo nuk është 100 për qind e saktë, është një masë e mirë kujdesi për t'u marrë.

Së fundi, nëse klikoni në lidhje nga ndonjë mesazh dhe ju kërkohet të identifikoheni në diçka, mos e bëni nëse nuk jeni



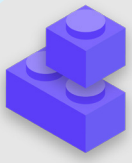
100 për qind i sigurt se posta elektronike është e ligjshme dhe ju dërgon në faqen e duhur. Shumë sulme phishing do të ofrojnë lidhje që ju dërgojnë në faqe të rreme të hyrjes për Gmail, Facebook ose sajte të tjera të njohura. Mos u mashtroni. Gjithmonë mund të hapni një shfletues të ri dhe të shkoni drejtpërdrejt në një sajt të njohur si Gmail.com, Facebook.com, etj., nëse dëshironi ose duhet të identifikoheni. Kjo gjithashtu do t'ju çojë te përmbajtja, në mënyrë të sigurt - nëse ajo ishte e ligjshme në radhë të parë.

Çfarë duhet të bëjmë kur marrim një mesazh phishing?

Nëse dikush brenda parlamentit pranon ndonjë bashkëngjitje, lidhje, imazh të pakërkuar ose ndonjë mesazh ose telefonatë të dyshimtë, është e rëndësishme që ata t'ia raportojnë menjëherë personit ose ekipit të sigurisë së TI-së. Nëse nuk keni një individ ose ekip të tillë, duhet t'i identifikoni ata si pjesë e zhvillimit të planit tuaj të sigurisë. Stafi dhe anëtarët mund të raportojnë gjithashtu postën elektronike si postë të padëshiruar ose phishing drejtpërdrejtë në Gmail ose Outlook.

Është thelbësore të keni një plan se si duhet të veprojë stafi, anëtarët ose vullnetarët nëse/kur marrin një mesazh të mundshëm phishing. Për më tepër, rekomandojmë të përdorni këto praktika më të mira për phishing - të mos klikoni në lidhje të dyshimta, të shmangni bashkëngjitjet dhe të kontrolloni adresën "nga" ju vjen posta - dhe t'i ndani ato me kolegët me të cilët punoni, mundësisht përmes një kanali komunikimi të përdorur gjerësisht. Kjo ilustron që ju kujdeseni për njerëzit me të cilët jeni në komunikim dhe inkurajon një kulturë në rrjetet tuaja që është vigjilente dhe e vetëdijshme për rreziqet e phishing-ut. Siguria juaj varet nga ato organizata që ju besoni, dhe anasjelltas. Praktikat më të mira mbrojnë të gjithë.

Përveç ndarjes së këshillave të mësipërme me të gjithë, ju gjithashtu mund të praktikoni identifikimin e phishing-ut me Google Phishing Quiz. Gjithashtu rekomandojmë fuqimisht caktimin e trajnimit të rregullt për phishing-un me stafin për të testuar ndërgjegjësimin dhe për t'i mbajtur njerëzit vigjilentë. Një trajnim i tillë mund të zyrtarizohet si pjesë e takimeve të rregullta të ekipit dhe takimeve parlamentare, ose të mbahet në mënyrë joformale. Ajo që është e rëndësishme është që të gjithë personat e përfshirë në operacionet parlamentare, të ndihen rehat duke bërë pyetje në lidhje me phishing-un, të raportojnë phishing (edhe nëse mendojnë se mund të kenë bërë një gabim, si p.sh. duke klikuar ndonjë lidhje), dhe se të gjithë janë të autorizuar të ndihmojnë në mbrojtjen e parlamentit kundër këtij kërcënimi me nivel të lartë ndikimi dhe gjasa të larta.



Blloqet e ndërtimit të planit të sigurisë: Phishing-u

- **Trajnoni rregullisht anëtarët dhe stafin se çfarë është phishing-u, si ta dallojnë dhe të mbrohen kundër tij, duke përfshirë phishing në mesazhe me tekst, aplikacione të mesazheve dhe telefonata, jo vetëm me postë elektronike.**
- **Kujtojini shpesh anëtarëve dhe stafit praktikat më të mira si p.sh:**
  - Mos shkarkoni bashkëngjitje të panjohura ose potencialisht të dyshimta.
  - Kontrolloni URL-në e një lidhjeje përpara se të klikoni. Mos klikoni lidhje të panjohura ose potencialisht të dyshimta.
  - Mos jepni informacione të ndjeshme ose private me postë elektronike, tekst ose telefonatë për adresa ose njerëz të panjohur ose të pakonfirmuar.
- **Inkurajoni raportimin e phishing-ut.**
  - Krijoni mekanizëm raportimi dhe një person të caktuar për phishing brenda parlamentit.
  - Shpërblejeni raportimin dhe mos e ndëshkoni dështimin.

Komunikimi dhe ruajtja e të dhënave në mënyrë të sigurt

Komunikimi dhe ndarja e të dhënave

Si parlament, është gjithashtu e rëndësishme të sigurohet që komunikimet zyrtare qeveritare të anëtarëve dhe stafit të jenë në përputhje me të gjitha detyrimet përkatëse të qeverisë së hapur (siç janë kërkesat për qasje të lirë në informacione) dhe angazhimet për sigurinë e të dhënave. Prandaj, kur hartoni dhe zbatoni sisteme dhe politika të sigurta të komunikimit në të gjithë parlamentin, sigurohuni që t'i mbani parasysh këta faktorë në mënyrë që mesazhet përkatëse të mund të sigurohen siç duhet dhe, kur është e nevojshme sipas ligjit, të ruhen.

Për të marrë vendimet më të mira për parlamentin tuaj mbi mënyrën e komunikimit, është thelbësore të kuptoni llojet e ndryshme të mbrojtjes që mund të kenë komunikimet tona dhe pse një mbrojtje e tillë është e rëndësishme. Një nga elementët më të rëndësishëm të sigurisë së komunikimit lidhet me ruajtjen e privatësisë të komunikimeve private - për të cilat në epokën moderne kujdeset kryesisht enkriptimi. Pa enkriptim të duhur, komunikimet e brendshme parlamentare do mund të shiheshin nga një numër i madh kundërshtarësh. Komunikimet e pasigurta mund të ekspozojnë informacione dhe mesazhe të ndjeshme ose të sikletshme, të zbulojnë fjalëkalime ose të dhëna të tjera private dhe ndoshta të vënë në rrezik anëtarët ose stafin tuaj në varësi të natyrës së komunikimit dhe përmbajtjes që ndani.

Komunikime dhe parlamente të sigurta

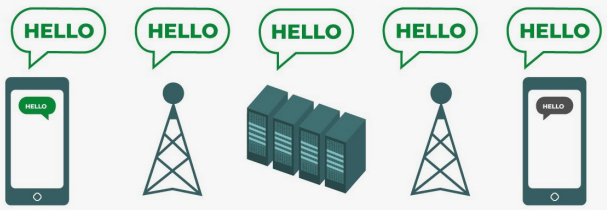
Vitet e fundit ka pasur shumë incidente në të cilat sistemet e komunikimit të parlamenteve dhe llogaritë e deputetëve dhe stafit të tyre janë kompromentuar, duke çuar në ndërprerje të funksionimit parlamentar dhe në disa raste në vjedhje të komunikimeve të ndjeshme. Në korrik 2021, për shembull, autoritetet polake njoftuan se llogaritë e postës elektronike të gati një duzinë deputetësh vendas ishin hakuar, përfshirë një llogari personale të ndihmësit të lartë të kryeministrit dhe llogari të anëtarëve nga pothuajse çdo grup opozitar parlamentar. Ky raport erdhi vetëm disa muaj pasi lajme të ngjashme dolën në dritë për një sulm kibernetik kundër sistemeve të informacionit dhe komunikimit në parlamentin finlandez. Autoritetet në Finlandë përshkruan sulmin si "spiunazh të rënduar dhe përgjim të mesazheve" që synonte parlamentin e saj.

ÇFARË ËSHTË ENKRIPTIMI DHE PSE ËSHTË I RËNDËSISHËM?

Enkriptimi është një proces matematikor që përdoret për të përzier një mesazh ose një skedar në mënyrë që vetëm një person ose ent me çelësin e duhur të mund ta "deshifrojë" dhe ta lexojë atë. Pa enkriptim, mesazhet tona lihen të hapura për t'u lexuar nga kundërshtarët e mundshëm, duke përfshirë qeveritë e huaja jomiqësore ose hakerët në ueb. Një enkriptim i tillë është i rëndësishëm jo vetëm për komunikimet e brendshme parlamentare, por edhe për komunikimet e jashtme në të cilat privatësia dhe integriteti duhet të mbrohen. [Udhëzuesi i vetëmbrojtjes për mbikëqyrje] i Fondacionit Electronic Frontier ofron një shpjegim praktik, me grafikë, se çfarë do të thotë

Mesazhe të pa-enkriptuara

Pa enkriptim, mesazhet tona lihen të hapura për t'u lexuar nga kundërshtarët e mundshëm, duke përfshirë qeveritë e huaja jomiqësore ose hakerët në ueb. Një enkriptim i tillë është i rëndësishëm jo vetëm për komunikimet e brendshme parlamentare, por edhe për komunikimet e jashtme në të cilat privatësia dhe integriteti duhet të mbrohen.



Siç mund ta shihni në imazhin e mësipërm, një telefon i mençur dërgon mesazh me tekst të gjelbër, të pa-enkriptuar ("përshëndetje") në një telefon tjetër të mençur në skajin e djathtë. Gjatë rrugës, një kullë celulare (ose në rastin e diçkaje të dërguar përmes internetit, ofruesi juaj i shërbimit të internetit, i njohur si një ISP) ua kalon mesazhin serverëve të kompanisë. Prej aty kalon nëpërmjet rrjetit në një kullë tjetër celulare, e cila mund të shohë mesazhin e pa-enkriptuar "përshëndetje" dhe më në fund dërgohet në destinacion. Është e rëndësishme të theksohet se pa ndonjë enkriptim, të gjithë të përfshirë në transmetimin e mesazhit dhe kushdo që mund të shikojë vjedhurazi ndërsa kalon, mund të lexojë përmbajtjen e tij. Kjo mund të mos ketë shumë rëndësi nëse gjithçka që po thoni është një "përshëndetje", por mund të jetë punë e madhe nëse komunikoni diçka më private ose të ndjeshme që nuk dëshironi që telekomi juaj, ISP, një qeveri jomiqësore ose ndonjë kundërshtar tjetër ta shohë. Andaj, është thelbësore që të shmangni përdorimin e mjeteve të pa-enkriptuara për të dërguar mesazhe të ndjeshme (dhe idealisht për të gjitha mesazhet.) Mbani në mend se disa nga metodat më të njohura të komunikimit - si SMS dhe thirrjet telefonike - praktikisht funksionojnë pa asnjë enkriptim (si në imazhin e mësipërm).

Ekzistojnë dy mënyra për të enkriptuar të dhënat gjatë lëvizjes: **enkriptimi i shtresës së transportit dhe enkriptimi nga fundi në fund**. Është e rëndësishme të dihet lloji i enkriptimit që mbështet një ofrues shërbimi pasi parlamenti juaj bën zgjedhje për të miratuar praktika dhe sisteme më të sigurta komunikimi. Dallimet e tilla përshkruhen mirë nga [Udhëzuesi i vetëmbrojtjes nga mbikëqyrja], i cili është përshtatur sërish këtu:

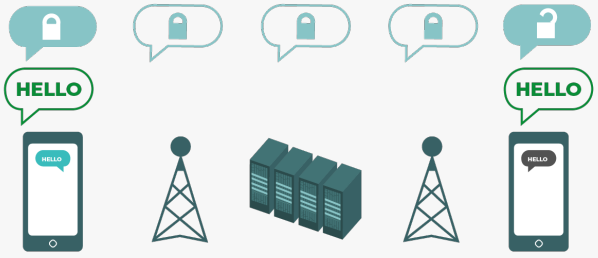
Enkriptimi i shtresës së transportit

Enkriptimi i shtresës së transportit, i njohur gjithashtu si siguria e shtresës së transportit (TLS), mbron mesazhet ndërsa ato udhëtojnë nga pajisja juaj në serverët e aplikacionit/shërbimit të mesazheve dhe prej andej në pajisjen e marrësit tuaj. Kjo i mbron nga sytë kureshtarë të hakerëve të ulur në rrjetin tuaj ose ofruesit tuaj të internetit ose të shërbimeve të telekomunikacionit. Megjithatë, në mes, ofruesi juaj i shërbimit të mesazheve/ postave elektronike, faqja e internetit që po shfletoni ose aplikacioni që po përdorni mund të shohin kopje të pa-enkriptuara të mesazheve tuaja. Për shkak se mesazhet tuaja mund të shihen dhe ruhen shpesh në serverët e kompanisë, ato mund të jenë të cenueshme ndaj kërkesave të zbatimit të ligjit ose vjedhjes nëse serverët e kompanisë janë kompromet uar.

Imazhi i mësipërm tregon një shembull të enkriptimit të shtresës së transportit. Në të majtë, një telefon i mençur dërgon një mesazh të gjelbër, të pa-enkriptuar: "Përshëndetje". Ky mesazh është i enkriptuar dhe më pas kalon në një kullë celulare. Në mes, serverët e kompanisë janë në gjendje të deshifrojnë mesazhin, të lexojnë përmbajtjen, të vendosin se ku ta dërgojnë, ta ri-enkriptojnë dhe ta dërgojnë së bashku në kullën tjetër të celularit drejt destinacionit të tij. Në fund, telefoni tjetër i mençur merr mesazhin e enkriptuar dhe e deshifron atë për të lexuar "Përshëndetje".

Enkriptimi nga fundi në fund

Enkriptimi nga fundi në fund mbron mesazhet në tranzit nga dërguesi te marrësi. Siguron që informacioni të kthehet në një mesazh sekret nga dërguesi i tij origjinal ("fundi" i parë) dhe të deshifrohet vetëm nga marrësi i tij përfundimtar ("fundi" i dytë). Askush, duke përfshirë aplikacionin ose shërbimin që po përdorni, nuk mund të "dëgjojë" dhe të përgjojë aktivitetin tuaj.



Imazhi i mësipërm tregon një shembull të enkriptimit nga fundi në fund. Në të majtë, një telefon i mençur dërgon mesazh të gjelbër, të pa-enkriptuar: "Përshëndetje". Ai mesazh është i enkriptuar dhe më pas kalon në një kullë celulari dhe pastaj në serverët e aplikacionit/shërbimit, të cilët nuk mund ta lexojnë përmbajtjen, por do ta kalojnë mesazhin sekret në destinacionin e tij. Në fund, telefoni tjetër i mençur e pranon mesazhin e enkriptuar dhe e deshifron për të lexuar "Përshëndetje". Ndryshe nga enkriptimi i shtresës së transportit, ISP-ja juaj ose nikoqiri i mesazheve nuk është në gjendje të deshifrojë mesazhin. Vetëm pikat përfundimtare (pajisjet origjinale që dërgojnë dhe marrin mesazhe të enkriptuara) kanë çelësat për të deshifruar dhe lexuar mesazhin.

ÇFARË LLOJ ENKRIPTIMI NA NEVOJITET?

Kur vendosni nëse parlamenti juaj ka nevojë për enkriptim të shtresës së transportit ose enkriptim nga fundi në fund për komunikimet tuaja (ose ndonjë kombinim i të dyjave për sisteme dhe aktivitete të ndryshme), pyetja e madhe që duhet ta parashtroni përfshin besimin. Për shembull, a i besoni aplikacionit ose shërbimit që po përdorni? A keni besim në infrastrukturën e saj teknike? A jeni i shqetësuar për mundësinë që një qeveri e huaj jo-miqësore mund ta detyrojë kompaninë të dorëzojë mesazhet tuaja - dhe nëse po, a i besoni politikave të kompanisë për t'u mbrojtur nga kërkesat e huaja të zbatimit të ligjit?

Nëse i përgjigjeni "jo" ndonjërës prej këtyre pyetjeve, atëherë keni nevojë për enkriptim nga fundi në fund. Nëse përgjigjeni me "po", atëherë mund të mjaftojë një shërbim që mbështet vetëm enkriptimin e shtresës së transportit - por në përgjithësi është më mirë të shkoni me shërbime që mbështesin enkriptimin nga fundi në fund kurdo që është e mundur.

Një grup tjetër pyetjesh për t'u marrë në konsideratë është nëse juve si parlament ju kërkohet me ligj të mbani qasjen e vetëm në çdo komunikim parlamentar, nëse ka ndonjë kërkesë për lokalizimin e të dhënave në vendin tuaj dhe/ose nëse disa komunikime duhet të ruhen (p.sh. jo-përgjithmonë të fshihen nga stafi) në mënyrë që të jetë në përputhje me ligjet dhe angazhimet e qeverisë së hapur. Nëse po, mund të konsideroni një sistem komunikimi të nivelit të ndërmarrjes me enkriptim nga fundi në fund, në të cilin ju, si parlament, jeni në gjendje të kontrolloni vetë çelësat e enkriptimit. Sistemet e tilla (të cilat do të diskutohen më në detaje në pjesën e Doracakut mbi **"Ruajtja e të dhënave në mënyrë të sigurt"**) mund të jenë të fuqishme, por kërkojnë aftësi të avancuara teknike për t'u zbatuar.

Gjithashtu, kur dërgoni mesazhe me grupe, mbani në mend se siguria e mesazheve tuaja është po aq e mirë sa siguria e të gjithëve që pranojnë mesazhet. Përveç zgjedhjes me kujdes të aplikacioneve dhe sistemeve të sigurta, është e rëndësishme që të gjithë në grup të ndjekin praktikat e tjera më të mira në lidhje me sigurinë e llogarisë dhe sigurinë e pajisjes. Mjafton që një person ose një pajisje e infektuar për të nxjerrë në pah përmbajtjen e një bisede ose telefonate të tërë grupit.

ÇFARË DUHET TË BËJMË ME POSTËN ELEKTRONIKE?

Në përgjithësi, posta elektronike nuk është alternativa më e mirë kur bëhet fjalë për sigurinë. Edhe opsionet më të mira të postës elektronike të enkriptuar nga fundi në fund zakonisht lënë hapësirë të zbrazët nga këndvështrimi i sigurisë, për shembull, mos-enkriptimi i linjave të subjektit të postave elektronike dhe mos-mbrojtja e meta të dhënave (një koncept i rëndësishëm që do të përshkruhet më poshtë). Nëse keni nevojë të komunikoni informacione shumë të ndjeshme që nuk kanë nevojë të ruhen për regjistrim publik, mbani në mend se posta elektronike (si sistemi i parlamentit dhe veçanërisht llogaria personale e dikujt) është më mirë të shmanget në favor të opsioneve të sigurta të mesazheve (të cilat do të theksohen në pjesën tjetër).

Megjithatë, si parlament, ndoshta doni ose keni nevojë që anëtarët dhe stafi të komunikojnë përmbajtje të ndjeshme ose private nëpërmjet një sistemi që menaxhohet nga qendra si pjesë e operacioneve të tyre të përditshme. Këtu mund të jetë i dobishëm një sistem për postë elektronike në të gjithë parlamentin, me kontrollet e duhura të llogarisë. Nëse, sipas analizës suaj më sipër, enkriptimi i shtresës së transportit do të mjaftojë, atëherë ofertat standarde të biznesit nga ofruesit e postës elektronike si Google Workspace (Gmail) dhe Microsoft 365 (Outlook) mund të jenë opsione solide për parlamentin tuaj. Megjithatë, nëse shqetësoheni se ofruesit tuaj të postës elektronike mund t'i kërkohet ligjërisht t'i ofrojë informacione në lidhje me komunikimet tuaja një qeverie të huaj ose ndonjë kundërshtari, ose nëse kërkesat lokale për rezidencën e të dhënave mund të paraqesin shqetësim, mund të konsideroni përdorimin e një lidhjeje nga fundi në fund si opsion për postë elektronike të enkriptuar. Disa opsione të tilla përfshijnë shtimin e menaxhimit tuaj me çelësin e enkriptimit në Google Workspace ose Microsoft 365 (siç përshkruhet në pjesën e Doracakut mbi **"Ruajtja e të dhënave në mënyrë të sigurt"**), ose përdorimi i shërbimeve të enkriptuara të postës elektronike nga fundi në fund të krijuara për organizata të mëdha si p.sh **ProtonMail** Business ose **Tutanota** Business.

ÇFARË JANË META TË DHËNAT DHE A DUHET TË SHQETËSOHEMI PËR TO?

Who you and your staff, members, and teams talk to and when and where you talk to them can often be just as sensitive as what you talk about. It is important to remember that end-to-end encryption only protects the contents (the "what") of your communications. This is where metadata comes into play. EFF's Surveillance Self-Defense Guide provides an overview of metadata and why it matters (including an illustration of what metadata looks like):

Meta të dhënat shpesh përshkruhen si gjithçka përveç përmbajtjes së komunikimeve tuaja. Ju mund të mendoni për meta të dhënat si ekuivalentin digjital të një zarfi. Ashtu si një zarf përmban informacione për dërguesin, marrësin dhe destinacionin e një mesazhi, po ashtu edhe meta të dhënat. Meta të dhënat janë informacione rreth komunikimeve digjitale që dërgoni dhe merrni.

Shembuj të meta të dhënave përfshijnë:
- me kë komunikoni
- linja e subjektit të postave elektronike të juaja
- kohëzgjatja e bisedave tuaja
- koha në të cilën është zhvilluar biseda
- vendndodhja juaj kur komunikoni

Ndërsa transparenca e operacioneve të zbatueshme parlamentare është thelbësore, kufizimi i qasjes së paautorizuar në meta të dhëna (përveç mbrojtjes së përmbajtjes së komunikimeve) është gjithashtu i rëndësishëm. Në fund të fundit, meta të dhënat mund t'u zbulojnë informacione të ndjeshme hakerëve, qeverive të huaja, kompanive ose palëve të tjera, për të cilët ju mund të mos dëshironi të keni qasje në ato informacione. Disa shembuj se si mund të jenë zbuluese meta të dhënat:

Kur e dinë se një deputet ose punonjës i stafit e ka thirrur një gazetar dhe ka folur me të për një orë përpara se ai gazetar të publikonte një artikull me një citim anonim. Megjithatë, ata nuk e dinë se për çfarë keni folur.

Kur e dinë që keni pranuar një postë elektronike nga një shërbim testimi për COVID, më pas keni thirrur mjekun tuaj dhe më pas keni vizituar faqen e internetit të Organizatës Botërore të Shëndetësisë në të njëjtën orë. Megjithatë, ata nuk e dinë se çfarë ka përmbajtur posta elektronike ose për çfarë keni folur në telefon.

Mjetet e rekomanduara të komunikimit të enkriptuar nga fundi në fund

MESAZHE ME TEKST (INDIVIDUALE OSE GRUPORE)	• **Signal** • **WhatsApp (vetëm me konfigurime specifike të cilësimeve të detajuara më poshtë)**
THIRRJET AUDIO DHE VIDEO	• **Signal (deri në 40 persona)** • **WhatsApp (deri në 32 persona në audio, 8 në video)**
NDARJA E SKEDARËVE	• **Signal** • **Keybase / Keybase Teams** • **Tresorit**

CILAT MJETE PËR MESAZHE TË ENKRIPTUARA NGA FUNDI NË FUND DUHET TË PËRDORIM (PREJ 2022)?

Nëse keni nevojë të përdorni enkriptim nga fundi në fund, ose thjesht doni të miratoni praktikën më të mirë, pavarësisht nga konteksti i kërcënimit ndaj parlamentit tuaj, kemi disa shembuj të besueshëm të shërbimeve që, prej vitit 2022, ofrojnë mesazhe dhe telefonata të enkriptuara nga fundi në fund. Kjo pjesë e Doracakut do të përditësohet rregullisht në internet, por ju lutemi të vini re se gjërat ndryshojnë shpejt në botën e mesazheve të sigurta, kështu që këto rekomandime mund të mos jenë të përditësuara në kohën kur ju do ta lexoni këtë pjesë. Mbani në mend se komunikimet tuaja janë po aq të sigurta sa që është edhe vetë pajisja juaj. Pra, përveç zbatimit të praktikave të sigurta të mesazheve, është thelbësore të zbatohen praktikat më të mira të përshkruara në pjesën mbi "Pajisjet e sigurta" të këtij Doracaku.

Meta të dhënat nuk mbrohen nga enkriptimi i ofruar nga shumica e shërbimeve të mesazheve. Nëse dërgoni mesazh në WhatsApp, për shembull, mbani në mend se ndërsa përmbajtja e mesazhit tuaj është e enkriptuar nga fundi në fund, është ende e mundur që të tjerët të dinë se kujt po i dërgoni mesazhe, sa shpesh, kurse me thirrjet, edhe për sa kohë. Si rezultat, duhet të keni parasysh se cilat rreziqe ekzistojnë (nëse ka) nëse keni kundërshtarë që janë në gjendje të zbulojnë se me kë flisni, kur keni biseduar me ta dhe (në rastin e postës elektronike) temat e përgjithshme të komunikimeve të parlamentit tuaj.

Një nga arsyet që **Signal** rekomandohet kaq shumë është se, përveç ofrimit të enkriptimit nga fundi në fund, është se **ka prezantuar veçori dhe ka marrë zotime për të zvogëluar sasinë e meta të dhënave që regjistron dhe ruan**. Për shembull, veçoria e

Signal's Sealed Sender është të kodojë meta të dhënat se kush po flet me kë, në mënyrë që Signal-i të njohë vetëm marrësin e një mesazhi, por jo dërguesin. Si parazgjedhje, kjo veçori funksionon vetëm kur komunikoni me kontaktet ose profilet ekzistuese (njerëzit) me të cilët keni komunikuar tashmë ose të cilët i keni ruajtur në listën e kontakteve. Megjithatë, mund ta aktivizoni këtë cilësim "Dërguesi i vulosur" në "Lejo nga kushdo" nëse është e rëndësishme për ju që të eliminoni këto meta të dhëna në të gjitha bisedat e Signal-it, madje edhe ato me njerëz të panjohur për ju. Kjo mund të mos jetë kritike për shumicën e komunikimeve parlamentare, por është e rëndësishme të jemi të vetëdijshëm për rreziqet që sjellin meta të dhënat dhe të zgjidhen mjetet dhe politikat e duhura të komunikimit në përputhje me rrethanat.

A MUND T'I BESOJMË VËRTET WHATSAPP-IT?

WhatsApp-i është një zgjedhje popullore për mesazhe të sigurta dhe mund të jetë një opsion i mirë duke pasur parasysh përhapjen e tij. Disa njerëz janë të shqetësuar se ai është në pronësi dhe kontroll të Facebook-ut, që ka punuar për ta integruar atë me sistemet e tjera të veta. Njerëzit janë gjithashtu të shqetësuar për sasinë e meta të dhënave (d.m.th., informacione se me kë komunikoni dhe kur) që mbledh WhatsApp-i. Nëse zgjidhni të përdorni WhatsApp-in si opsion i sigurt të mesazheve, sigurohuni që të lexoni pjesën e mësipërme mbi meta të dhënat. Ekzistojnë gjithashtu disa cilësime që duhet të siguroheni se janë konfiguruar siç duhet. Më e rëndësishmja, sigurohuni që të çaktivizoni kopjet rezervë të resë ose, të paktën, të aktivizoni risinë e WhatsApp-it, tiparin e kopjeve rezervë të enkriptuara nga fundi në fund duke përdorur çelës enkriptimi 64 shifror ose fjalëkalim të gjatë, të rastësishëm dhe unik, të ruajtur në vend të sigurt (si menaxheri i fjalëkalimit). Sigurohuni gjithashtu që të shfaqni njoftimet e sigurisë dhe të verifikoni kodet e sigurisë. Mund të gjeni udhëzime të thjeshta për konfigurimin e këtyre cilësimeve për telefonat Android **këtu** dhe për iPhone-t **këtu**. **Nëse stafi juaj *dhe ata me të cilët ju të gjithë komunikoni* nuk i konfigurojnë siç duhet këto opsione, atëherë nuk duhet ta konsideroni WhatsApp-in si opsion të mirë për komunikime të ndjeshme që kërkojnë enkriptim nga fundi në fund**. Sinjali mbetet opsioni më i mirë për nevoja të tilla të mesazheve të enkriptuara nga fundi në fund duke pasur parasysh cilësimet e tij të sigurta të paracaktuara dhe mbrojtjen e meta të dhënave.

PO NË LIDHJE ME DËRGIMIN E MESAZHEVE?

Mesazhet me tekst bazë janë shumë të pasigurta (SMS standard janë efektivisht të pa-enkriptuar) dhe duhet t'i shmangni për çdo gjë që nuk është e paraparë për publikun e gjerë. Ndërsa mesazhet iPhone-në-iPhone të Apple (të njohura si iMessages) janë të enkriptuara nga fundi në fund, por nëse në bisedë kemi një telefon jo-iPhone, mesazhet nuk janë të sigurta. Është më mirë të jesh i sigurt dhe të **shmangni mesazhet me tekst për çdo gjë që mund të vlerësohet sadopak e ndjeshme, private ose e fshehtë**.

PSE NUK REKOMANDOHEN TELEGRAM-I, FACEBOOK MESSENGER-I OSE VIBER-I PËR BISEDA TË SIGURTA?

Disa shërbime, si Facebook Messenger dhe Telegram, ofrojnë enkriptim nga fundi në fund vetëm nëse e aktivizoni qëllimisht (dhe vetëm për biseda një me një), kështu që nuk janë opsione të mira për mesazhe të ndjeshme ose private, veçanërisht për ekipe. Mos u mbështetni në këto mjete nëse keni nevojë të përdorni enkriptim nga fundi në fund, sepse është mjaft e lehtë të harroni të ndryshoni cilësimet e paracaktuara dhe më pak të sigurta. Viber-i pretendon se ofron enkriptim nga fundi në fund, por nuk e ka vënë kodin e tij metadat të disponueshëm për shqyrtim për studiuesit e jashtëm të sigurisë. Kodi i Telegram-it gjithashtu nuk është vënë në dispozicion për një revizion publik. Si rezultat, shumë ekspertë kanë frikë se enkriptimi i Viber-it (ose "bisedat sekrete" të Telegramit) mund të jetë nën standard dhe për këtë arsye jo të përshtatshëm për komunikime që kërkojnë enkriptim të vërtetë nga fundi në fund.

KOLEGËT TANË PARLAMENTARË DHE ZGJEDHËSIT PËRDORIN APLIKACIONE DHE SISTEME TË TJERA MESAZHESH PËR KOMUNIKIM - SI MUND T'I BINDIM ATA TË SHKARKOJNË NJË APLIKACION TË RI PËR TË KOMUNIKUAR ME NE?

Ndonjëherë ka shkëmbim midis sigurisë dhe komoditetit, por ia vlen pak përpjekje shtesë për komunikime të ndjeshme. Jepni një shembull të mirë për kontaktet tuaja – qofshin ato në agjenci të tjera qeveritare, institucione, në të gjithë parlamentin apo votues të jashtëm. Nëse duhet të përdorni sisteme të tjera më pak të sigurta, jini shumë të vetëdijshëm për atë që po thoni. Shmangni diskutimin e temave të ndjeshme. Disa parlamente mund të kenë protokolle të ndryshme për bisedat e përgjithshme ose komunikimet me publikun, krahasuar me diskutimet e fshehta me udhëheqësinë, për shembull. Klasifikoni komunikimet tuaja parlamentare (të brendshme dhe të jashtme) në bazë të ndjeshmërisë dhe sigurohuni që anëtarët dhe stafi të përdorin mekanizmat e duhur të komunikimit në përputhje me rrethanat! Natyrisht, është shumë më e thjeshtë nëse gjithçka kodohet automatikisht gjatë gjithë kohës - asgjë për të kujtuar ose menduar fort.

Fatmirësisht, aplikacionet e enkriptuara nga fundi në fund si Signal po bëhen gjithnjë e më të njohura dhe miqësore për përdoruesit – nuk ka nevojë madje të përmendim që edhe janë lokalizuar në dhjetëra gjuhë për përdorim global. Nëse partnerët tuaj ose kontaktet e tjera kanë nevojë për ndihmë për të kaluar komunikimet në ndonjë opsion të enkriptuar nga fundi në fund si Signal, rezervoni pak kohë për t'u folur atyre përse është kaq e rëndësishme t'i mbroni siç duhet komunikimet tuaja. Kur të gjithë e kuptojnë rëndësinë, minutat e pakta të nevojshme për të shkarkuar një aplikacion të ri dhe dy ditët që mund të duhen për t'u mësuar me përdorimin e tij nuk do të duken si punë e madhe.

A KA CILËSIME TË TJERA PËR APLIKACIONET E ENKRIPTUARA NGA FUNDI NË FUND PËR TË CILAT DUHET TË JEMI TË VETËDIJSHËM?

Në aplikacionin "Signal", verifikimi i kodeve të sigurisë (të cilave u referohen si Numrat e Sigurisë) është gjithashtu i rëndësishëm. Për të parë një numër sigurie dhe për ta verifikuar atë në "Signal", mund të hapni bisedën tuaj me një kontakt, trokitni lehtë mbi emrin e tij në krye të ekranit tuaj dhe lëvizni poshtë për të trokitur "Shiko numrin e sigurisë". Nëse numri juaj i sigurisë përputhet me kontaktin tuaj, mund t'i shënoni si "të verifikuar" nga i njëjti ekran. Është veçanërisht e rëndësishme t'u kushtoni vëmendje këtyre numrave të sigurisë dhe të verifikoni kontaktet tuaja nëse pranoni ndonjë njoftim në bisedë se numri juaj i sigurisë me një kontakt të caktuar ka ndryshuar. Nëse ju ose personeli tjetër keni nevojë për ndihmë për konfigurimin e këtyre cilësimeve, vetë Signal-i **siguron udhëzime të dobishme**. Nëse përdorni Signal, i cili konsiderohet gjerësisht si opsioni më i përshtatshëm për përdoruesit për mesazhe të sigurta dhe telefonata një-për-një, sigurohuni që të vendosni PIN të fortë. Përdorni të paktën gjashtë shifra, dhe mos të jetë diçka e lehtë për t'u hamendësuar si data juaj e lindjes.
Për më shumë këshilla se si të konfiguroni **Signal-in** dhe **WhatsApp-in**, mund të kontrolloni **udhëzuesit e veglave** për të dyja, të zhvilluara nga EFF në **Udhëzues për vetëmbrojtje nga mbikëqyrja**.

PO TELEFONATAT ME VIDEO NË GRUPE MË TË MËDHA? A KA OPSIONE TË ENKRIPTUARA NGA FUNDI NË FUND?

Me rritjen e punës në distancë, është e rëndësishme të keni një opsion të sigurt për video-telefonatat e mëdha të zyrës suaj në grup ose komunat virtuale për deputetët. Fatkeqësisht, aktualisht nuk ekzistojnë opsione të shkëlqyera që plotësojnë të gjitha kushtet: të jenë miqësore për përdoruesit, të mbështesin një numër të madh pjesëmarrësish dhe veçori të bashkëpunimit

dhe të mundësojnë enkriptimin nga fundi në fund si parazgjedhje.

Nevojat specifike të seancave plenare dhe mbledhjeve të komisioneve do të diskutohen më vonë në këtë doracak, por për takimet tuaja të tjera më të përgjithshme që nuk kërkojnë veçori të avancuara bashkëpunimi si dhomat e veçanta, rekomandohet shumë përdorimi i Signal-it. Video thirrjeve grupore në Signal mund t'u bashkohen deri në 40 pjesëmarrës, me telefon të mençur ose nga desktop aplikacioni i Signal për në kompjuter, i cili lejon ndarjen e ekranit. Kini parasysh, megjithatë, se vetëm kontaktet tuaja që përdorin tashmë Signal-in mund të shtohen në një grup të Signal-it.

Nëse jeni duke kërkuar opsione tjera, një platformë që së fundi ka shtuar opsion të enkriptuar nga fundi në fund është Jitsi Meet. **Jitsi Meet** është një zgjidhje për audio dhe video konferenca, e bazuar në ueb që mund të funksionojë për audiencë të madhe (deri në 100 persona) dhe nuk kërkon shkarkim të aplikacionit ose softuer të veçantë. Vini re se nëse e përdorni këtë veçori me grupe të mëdha (më shumë se 15-20 persona), cilësia e telefonatës mund të ulet. Për të konfiguruar një takim në Jitsi Meet, mund të shkoni te **meet.jit.si**, shkruani kod takimi dhe ndajeni atë lidhje (nëpërmjet një kanali të sigurt siç është Signal-i) me pjesëmarrësit tuaj të dëshiruar. Për të përdorur enkriptimin nga fundi në fund, hidhini një sy këtyre **instruksioneve** të përshkruara nga Jitsi. Vini re se të gjithë përdoruesit individualë do të duhet të aktivizojnë vetë enkriptimin nga fundi në fund në mënyrë që të funksionojë. Kur përdorni Jitsi, sigurohuni që të krijoni emra të rastësishëm të dhomave të mbledhjeve dhe të përdorni kode kalimi të forta për të mbrojtur telefonatat tuaja.

Nëse kjo nuk funksionon për ekipet tuaja, mund të konsideroni përdorimin e opsionit të njohur komercial si Webex ose Zoom me enkriptim të aktivizuar nga fundi në fund. Webex ka lejuar prej kohësh enkriptimin nga fundi në fund; megjithatë, ky opsion nuk është i aktivizuar si parazgjedhje dhe kërkon që pjesëmarrësit të shkarkojnë Webex-in për t'iu bashkuar takimit tuaj. Për të marrë opsionin e enkriptuar nga fundi në fund për Webex llogarinë tuaj, duhet të hapni Webex rast mbështetjeje dhe të ndiqni **këto udhëzime** që të siguroni konfigurimin e enkriptimit nga fundi në fund. Vetëm nikoqiri i takimit duhet të aktivizojë enkriptimin nga fundi në fund. Nëse e bëjnë këtë, i gjithë takimi do të jetë i enkriptuar nga fundi në fund. Nëse përdorni Webex për takime dhe seminare të sigurta në grup, sigurohuni që të aktivizoni edhe kodkalime të forta në telefonatat tuaja.

Pas disa muaj kritikash negative, Zoom zhvilloi një **opsion enkriptimi prej fundi në fund** për thirrjet e veta. Megjithatë, ky opsion nuk aktivizohet si parazgjedhje, kërkon që nikoqiri i telefonatave të lidh llogarinë e tij me një numër telefoni dhe funksionon vetëm nëse të gjithë pjesëmarrësit bashkohen nëpërmjet Zoom aplikacionit të desktopit ose celularit, në vend që të telefonojnë. Për shkak se është e lehtë të konfigurohen gabimisht këto cilësime, nuk është ideale të mbështetesh te Zoom-i si opsion i enkriptuar nga fundi në fund. Megjithatë, nëse kërkohet enkriptim nga fundi në fund dhe Zoom-i është opsioni juaj i vetëm, mund të ndiqni **udhëzimet** e Zoom-it për ta konfirguruar. Vetëm sigurohuni që të kontrolloni çdo telefonatë përpara se të fillojë, për t'u siguruar që është vërtet e enkriptuar nga fundi në fund, duke klikuar bravën e gjelbër në këndin e sipërm majtas ekranit të Zmadhimit dhe duke parë opsionin "nga fundi në fund" pranë rregullimeve për enkriptim. Duhet të vendosni gjithashtu kodkalim të fortë për çdo takim në Zoom.

Sidoqoftë, vlen të përmendet se disa veçori të njohura të mjeteve të mësipërme funksionojnë vetëm me enkriptim të shtresës së transportit. Për shembull, aktivizimi i enkriptimit nga fundi në fund në Zoom çaktivizon dhomat e veçanta, mundësinë e votimit dhe regjistrimin në renë kompjuterike. Në Jitsi Meet, dhomat e veçanta mund të çaktivizojnë funksionin e enkriptimit nga fundi në fund, duke çuar në një ulje të padashur të sigurisë.

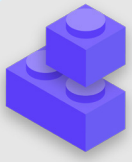
NJË SHËNIM PËR NDARJEN E SKEDARËVE

Përveç faktit që mesazhet do t'i keni të sigurta gjatë dërgimit dhe pranimit, ndarja e sigurt e skedarëve paraqet pjesë e rëndësishme e planit të sigurisë së parlamentit tuaj. Shumica e opsioneve të ndarjes së skedarëve janë të integruara në aplikacionet ose shërbimet e mesazheve që tashmë mund të përdorni. Për shembull, ndarja e skedarëve nëpërmjet Signal-it është një opsion i shkëlqyeshëm nëse nevojitet enkriptim nga fundi në fund. Nëse enkriptimi i shtresës së transportit është i mjaftueshëm, përdorimi i Google Drive ose Microsoft SharePoint mund të jetë opsion i mirë për parlamentin tuaj. Vetëm sigurohuni që të konfiguroni siç duhet cilësimet e ndarjes, që vetëm njerëzit e duhur të kenë qasje në një dokument ose dosje të caktuar dhe sigurohuni që këto shërbime të jenë të lidhura me llogaritë organizative (jo personale) të postës elektronike të stafit. Nëse mundeni, ndaloni ndarjen e skedarëve të ndjeshëm nëpërmjet bashkëngjitjeve të postës elektronike ose fizikisht me USB. Përdorimi i pajisjeve si USB brenda parlamentit tuaj rrit shumë gjasat e softuerëve keqdashës ose vjedhjeve dhe mbështetja në postë elektronike ose forma të tjera të bashkëngjitjeve dobëson mbrojtjen e parlamentit tuaj kundër sulmeve të phishing-ut.

PO SIKUR VËRTET TË MOS KEMI NEVOJË PËR ENKRIPTIM NGA FUNDI NË FUND PËR TË GJITHA KOMUNIKIMET TONA?

Nëse enkriptimi nga fundi në fund nuk nevojitet për të gjitha komunikimet e parlamentit tuaj bazuar në vlerësimin e rrezikut, mund të konsideroni përdorimin e aplikacioneve të mbrojtura nga enkriptimi i shtresës së transportit. Mos harroni, ky lloj enkriptimi kërkon që t'i besoni ofruesit të shërbimit, si Google për Gmail, Microsoft për Outlook/Exchange ose Facebook për Messenger, sepse ata (dhe kushdo me të cilin mund të detyrohet të ndajë informacionin) mund të shohë/dëgjojë komunikimet. Edhe një herë, opsionet më të mira do të varen nga modeli juaj i kërcënimit (për shembull, nëse nuk i besoni Google-it ose nëse qeveria e SHBA-ve është kundërshtari juaj, atëherë Gmail-i nuk është opsion i mirë), por disa opsione të njohura dhe përgjithësisht të besueshme përfshijnë:

POSTË ELEKTRONIKE	• **Gmail (nëpërmjet Google Workspace)** • **Outlook (nëpërmjet Office 365)** • Mos strehoni serverin tuaj Microsoft Exchange për postën elektronike të parlamentit tuaj. Nëse jeni duke e bërë këtë aktualisht, duhet **të migroni** në Office 365..
MESAZHE ME TEKST (INDIVIDUALE OSE GRUPORE)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
KONFERENCA NË GRUP, AUDIO DHE VIDEO THIRRJE	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
NDARJA E SKEDARËVE	• **Google Drive** • **Microsoft SharePoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Blloqet e ndërtimit të planit të sigurisë: Komunikimi i të dhënave në mënyrë të sigurt

- **Klasifikoni komunikimet bazuar në ndjeshmërinë e tyre.**
  - Përcaktoni sistemet dhe mjetet e duhura për komunikim në përputhje me rrethanat.
  - Vendosni politikë mbi afatin e ruajtjes së mesazheve në përputhje me rrethanat, duke pasur parasysh sigurinë dhe angazhimet ndaj transparencës parlamentare.
- **Kërkoni përdorimin e shërbimeve të besueshme të mesazheve të enkriptuara nga fundi në fund për komunikimet e ndjeshme të parlamentit tuaj.**
  - Ndani kohë për t'i shpjeguar stafit dhe partnerëve të jashtëm pse komunikimet e sigurta janë kaq të rëndësishme; pasi kjo do të rrisë suksesin e planit tuaj.
- **Sigurohuni që janë vendosur cilësimet e duhura për aplikacionet e komunikimit të sigurt, duke mos harruar:**
  - Të siguroheni që i gjithë stafi t'u kushtojë vëmendje njoftimeve të sigurisë dhe, nëse përdorni WhatsApp, të mos mban kopje të bisedave.
  - Të sigurohuni që përdoruesit e kërkuar të kenë aktivizuar cilësimet e duhura në fillim të çdo telefonate ose takimi nëse përdorni aplikacion ku enkriptimi nga fundi në fund nuk është aktivizuar si parazgjedhje (p.sh., Zoom ose Webex),.
- **Mos u përpiqni të strehoni serverin tuaj të postës elektronike - përdorni si alternativa të shërbimeve të postës elektronike të bazuara në re, si Office 365 ose Google Workspace.**
  - Mos lejoni personelin të përdorë llogaritë personale të postës elektronike për punë.
- **Kujtojini shpesh stafit dhe anëtarëvë mbi praktikat më të mira të sigurisë në lidhje me mesazhet në grup dhe meta të dhënat.**
  - Jini të vetëdijshëm se kush përfshihet në mesazhet grupore, bisedat dhe temat e postës elektronike.

Parlamentet digjitale (e-Parlament)

Si parlament, është e rëndësishme t'i kushtoni vëmendje të veçantë politikave të komunikimit dhe sigurisë operacionale të funksioneve tuaja më thelbësore, përfshirë ato në internet dhe në hapësirën digjitale. Pa marr parasysh nëse parlamenti juaj shqyrton sistem të plotë "e-Parlament" që mund të digjitalizojë gjithçka nga hartimi i projektligjeve nëpërmjet debatit dhe votimit elektronik (siç janë **Nextsense**, **Propylon**, ose **Granicus** për të përmendur disa shembuj), ose jeni duke përdorur mjete më të thjeshta, më pak të shtrenjta për të lehtësuar operacionet tuaja parlamentare, është thelbësore që të merrni parasysh se si çdo mjet (ose mjete) dhe proces (ose procese) merr parasysh sigurinë, integritetin dhe disponueshmërinë e informacionit.

Siguria dhe parlamentet digjitale

Siç dëshmohet nga një **sërë incidentesh** në Afrikën e Jugut, tranzicioni i operacioneve parlamentare në botën digjitale kërkon vëmendje ndaj sigurisë kibernetike për të shmangur jo vetëm humbjen ose vjedhjen e të dhënave të ndjeshme, por edhe sikletin, fyerjen dhe dëmin e mundshëm të anëtarëve dhe stafit. Në maj 2020, imazhe pornografike u shfaqën disa minuta para fillimit të një takimi virtual të Asamblesë Kombëtare të vendit. Pas shfaqjes së imazheve fyese, "hakeri" ose "bombarduesi i zmadhimit" më pas shfaqi fyerje seksiste dhe raciste ndaj kryetarit të asamblesë që udhëhiqte seancën, duke e detyruar mbledhjen të shtyhej. Një incident i ngjashëm ndodhi edhe një muaj më parë kur një takim i kryesuar nga ministrja e grave, rinisë dhe personave me aftësi të kufizuara u ndërpre me imazhe pornografike.

SEANCAT PLENARE DHE MBLEDHJET E KOMISIONEVE NË DISTANCË

Kryesore ndër këto procese janë seancat plenare dhe mbledhjet e komisioneve. Këto seanca si dhe bisedat, vendimet dhe votat që ndodhin brenda tyre janë thelbi i pjesës më të madhe të punës së parlamentit tuaj dhe si të tilla mund të jenë një objektiv i veçantë për kundërshtarët. Në një botë moderne, të ndikuar nga pandemia, seanca dhe takime të tilla zhvillohen në mënyra gjithnjë e më të larmishme në varësi të kontekstit të vendit tuaj, si personalisht, plotësisht në internet dhe në mënyrë "hibride".

Siç është përshkruar në udhëzuesin e fundit të Partneritetit për Demokracinë e Dhomës, me titull **Përgjigjja e parlamenteve ndaj pandemisë**, struktura tipike e debatit parlamentar është e ndryshme nga një diskutim normal gjatë konferencës ose ndonjë takim standard organizativ. Nevojat për votim në distancë, paraqitje të propozimeve dhe amendamenteve zyrtare, debati i strukturuar dhe madje interpretimi i njëkohshëm për të siguruar përfshirjen e të gjitha zonave zgjedhore shpesh kërkojnë veçori shtesë që nuk gjenden në shumicën e zgjidhjeve standarde teknologjike. Si rezultat, kur organizoni seancë virtuale ose hibride, ka gjasa që parlamenti juaj të ketë nevojë që të zhvillojë (ose tashmë ka zhvilluar) softuer të personalizuar, ose të blejë zgjidhje të shtrenjta, të ndërmarrjeve (si p.sh. **Cisco's Webex Legislate**) krijuar posaçërisht për të menaxhuar seancat parlamentare nga distanca. Çfarëdo opsioni që të zgjedhë parlamenti juaj, është e rëndësishme të vlerësoni, siç përshkruhet në udhëzuesin **Përgjigjja e parlamenteve ndaj pandemisë**, se si të gjithë anëtarët dhe stafi do të jenë në gjendje të qasin në një sistem të tillë. Është gjithashtu e rëndësishme të sigurohet që sistemi i tillë të jetë i siguruar siç duhet.

Gjatë ndërtimit dhe zbatimit të zgjidhjeve teknike për seancat parlamentare, është e rëndësishme të sigurohet që bazat themelore të sigurisë janë në vend. Këto përfshijnë hapa për të siguruar që të dhënat të jenë të siguruara "në qetësi" brenda vetë sistemit, të enkriptuara siç duhet gjatë tranzitit dhe që vetëm përdoruesit e autorizuar të mund të hyjnë në sistem. Ka shumë qasje që mund të merren për të garantuar një siguri të tillë, duke përfshirë shumë nga bazat e përshkruara në pjesën tjetër të këtij doracaku. Enkriptimi nga fundi në fund në çdo sistem të përdorur të shkëmbimit të të dhënave dhe komunikimit, fjalëkalimi i fortë dhe kërkesat e vërtetimit me dy faktorë dhe/ose kufizimi i adresës IP për përdoruesit për të hyrë në sisteme të tilla (përveç nëse ato synohen të jenë të hapura për publikun), kërkesa e rrjeteve private virtuale (të cilat do të diskutohen më vonë në Doracak) dhe kufizimi i qasjes vetëm në pajisjet e besueshme dhe të pastra paraqesin disa nga hapat e dobishme.

VOTIM NË DISTANCË

Nevoja për siguri të fuqishme është ndoshta më e rëndësishmja kur kemi të bëjmë me votimin në distancë. Siç theksohet në pikat kryesore të udhëzuesit **Përgjigjja e parlamenteve ndaj pandemisë**, deputetët zgjidhen në parlament për qëllimin specifik të votimit në emër të zgjedhësve të tyre. Aftësia për të besuar dhe verifikuar këto vota është thelbësore jo vetëm për funksionimin e vetë parlamentit tuaj, por edhe për sistemin demokratik në tërësi. Vota të tilla verifikohen relativisht lehtë kur një deputet voton personalisht, por kur merr pjesë virtualisht, vërtetimi teknik shndërrohet në sfidë të madhe që kërkon kujdes dhe fokus të konsiderueshëm. Siç theksohet në **dëshminë** e ekspertëve dhënë Komisionit të Përhershëm të Dhomës së Komunave kanadeze për Procedurat dhe Çështjet e Dhomës, parlamentet zakonisht zgjedhin një nga katër opsionet për votim në distancë:

- Votimi me postë elektronike: ku anëtarët marrin një formular të fletëvotimit në mënyrë elektronike dhe dorëzojnë votën e tyre me postë elektronike. Ky opsion përgjithësisht konsiderohet i pasigurt, pjesërisht për shkak të mungesës së enkriptimit nga fundi në fund dhe duhet të shmanget.
- Votimi i bazuar në ueb: ku anëtarët qasin dhe hedhin votat nëpërmjet një faqe interneti ose në një kompjuter ose telefon celular. Kjo qasje kërkon investime në infrastrukturë të sigurt, përfshirë pajisje të sigurta me kontrolle të forta vërtetimi siç u përmend më lart.
- Votimi i bazuar në aplikacion: ku anëtarët shkarkojnë aplikacion për të hyrë dhe për të hedhur votat. Ngjashëm me votimin e bazuar në ueb, por përdor aplikacion specifik, i cili mund të shkarkohet në një telefon ose tablet, në vend që të qaset nëpërmjet shfletuesit.
- Votimi me video: ku anëtarët votojnë në ekran me ngritjen e duarve ose me votë me zë. Për votim jo-anonim, kjo mund të jetë teknikisht më pak e komplikuar dhe teknikisht më pak e sofistikuar për t'u vendosur dhe siguruar. Por sidoqoftë nevojiten sisteme të fuqishme enkriptimi dhe vërtetimi, për të shmangur imitimin ose ndërprerjen gjatë seancave të votimit.

Çfarëdo opsioni që parlamenti juaj zgjedh të zbatojë për votimin në distancë - nëse përdor fare votimin në distancë - është e rëndësishme të adresohen edhe bazat e sigurisë kibernetike gjatë gjithë procesit të votimit. Bazat e tilla përfshijnë sigurimin që pajisjet, që deputetët përdorin për të votuar, të jenë të siguruara siç duhet fizikisht dhe të mos kenë programe të dëmshme, që qasja në internet e anëtarëve të sigurohet siç duhet kur votojnë (dhe gjithashtu kur kryejnë punë të tjera parlamentare), dhe që anëtarët të kenë lidhje të qëndrueshme interneti dhe të jenë në gjendje të votojnë kur thirren. Siç është përshkruar në udhëzuesin **Përgjigjja e parlamenteve ndaj pandemisë**, kur miratohet votimi në distancë, duhet të kryhet testimi i gjerë i sistemit përpara

se ai të fillojë të funksionojë si dhe të ofrohet mbështetje dhe trajnim për deputetët, për t'u siguruar që ata të mund ta përdorin sistemin në mënyrë efektive. Është e rëndësishme të mbani mend se një pjesë e sigurisë është disponueshmëria. Gjithashtu duhet të siguroheni që gratë deputete dhe stafi të jenë në gjendje të përdorin sistemet online në mënyrë të sigurt, duke përfshirë votimin në distancë, dhe të kenë qasje në teknologji për ta bërë këtë. Kur gratë, veçanërisht gratë e zgjedhura, hyjnë në internet, ato përballen me nivele më të mëdha frikësimi dhe ngacmimi, dhe ky faktor duhet të merret parasysh kur zhvillohet dhe përdoret teknologjia si votimi në distancë për të siguruar që të gjithë deputetët të jenë në gjendje të përmbushin funksionet e tyre në mënyrë efektive. Për më tepër, është thelbësore të sigurohet qasje e përshtatshme shumëgjuhëshe në distancë në vendet ku fliten gjuhë të shumta zyrtare nga anëtarët dhe stafi.

SHITËSI DHE SIGURIA E SOFTUERIT TË E-PARLAMENT-IT

Çdo softuer që ju prokuroni – pa marr parasysh nëse përdoret për votim në distancë ose për gamë më të gjerë nevojash parlamentare - **duhet të vijë nga një burim i sigurt dhe i akreditуar, të kalojë kontrollin për siguri nga ekipe të pavarura dhe të marrë certifikatat e duhura.** Është e rëndësishme të mbani mend se zhvilluesit e softuerit, ata që punësoni për të ndërtuar një aplikacion ose mjet, nuk janë gjithmonë vetë ekspertë të sigurisë. Prandaj, angazhimi i ekspertëve të sigurisë për të testuar aplikacionin për boshllëqe të mundshme të sigurisë nëpërmjet revizionit / kontrollit është kritike për të reduktuar rrezikun që platforma, mjeti ose aplikacioni juaj të hakerohet ose komprometohet. Edhe zhvilluesit më të mirë të softuerit bëjnë gabime nëse një ekspert i dytë (ose i tretë) nuk e kontrollon punën e tyre!

Votimi në distancë në botën reale

Parlamente të ndryshme kanë zbatuar sisteme të votimit në distancë dhe, duke e bërë këtë, kanë ndërmarrë hapa të konsiderueshëm për të garantuar sigurinë dhe integritetin e votave të anëtarëve. Një element në këtë proces, ndër të tjerat e përmendura më lart, është sigurimi i vërtetimit të duhur. Disa shembuj përfshijnë Dhoma e Poshtme e Parlamentit Britanik ku anëtarët përdorin proces të vetëm identifikimi për t'u identifikuar në llogaritë e tyre parlamentare përpara se të votojnë, gjë që kërkon fjalëkalim për t'u përdorur në një pajisje specifike, të caktuar. Në Spanjë, deputetëve u jepen kode personale që duhet të futen nëpërmjet një aplikacioni për telefona të mençur përpara se një votim të mund të regjistrohet nga distanca. Në Kili, senatorët që votojnë nga distanca nëpërmjet aplikacionit të votimit në distancë të dizajnuar me kujdes të dhomës duhet të jenë të dukshëm në ekran për të hedhur një votë

Ruajtja e të dhënave në mënyrë të sigurt

Për shumicën e parlamenteve, një nga vendimet më të rëndësishme për t'u marrë është se ku të ruhen të dhënat e tyre. A është "më e sigurt" ruajtja e të dhënave në kompjuterët e stafit, në një server lokal, në pajisjet e jashtme të ruajtjes ose në re? Në 99 për qind të situatave, opsioni më i lehtë dhe më i sigurt është mbajtja e të dhënave të ruajtura në shërbimet e besuara të ruajtjes në retë kompjuterike. Ndoshta shembujt më të zakonshëm përfshijnë Microsoft 365 dhe Google Drive. Pa një plan gjithëpërfshirës të ruajtjes në retë kompjuterike, ka gjasa që të dhënat e parlamentit tuaj të ruhen në vende të ndryshme - përfshirë kompjuterët e stafit dhe deputetëve, disqet e jashtme të ngurtë dhe madje edhe disa serverë lokalë. Ndërsa është e mundur të sigurohen të dhëna në të gjitha këto pajisje, është shumë e vështirë ta bësh këtë me sukses pa shpenzuar shumë para dhe pa punësuar staf të konsiderueshëm të TI-së.

Ruajtja e të dhënave dhe parlamentet

Shpikja e ruajtjes së të dhënave për shuma të përballueshme (ndonjëherë falas) të bazuara në retë kompjuterike e ka bërë jetën më të lehtë dhe më të sigurt për shumë parlamente dhe organizata të tjera. Për fat të keq, numër i madh i parlamenteve ende përpiqen të strehojnë (host) serverët e tyre me buxhet relativisht të kufizuar për TI, personel dhe mbështetje. Në mars të vitit 2021, kërcënimi i një infrastrukture të tillë organizative u bë i vërtetë për dhjetëra mijëra organizata, duke përfshirë parlamentet, në të gjithë botën kur një aktor kërcënimi i lidhur me qeverinë kineze, i quajtur Hafnium, shkaktoi një katastrofë globale të sigurisë kibernetike me sulm të sofistikuar ndaj palëve që vetë strehojnë serverët e tyre Microsoft Exchange. Sulmi komprometoi serverët lokalë, përfshirë atë të parlamentit të Norvegjisë, duke u mundësuar hakerëve të kenë qasje në llogaritë e postës elektronike parlamentare, të instalojnë softuerë keqdashës shtesë në serverët e viktimave dhe sistemet e lidhura, dhe në fund **të nxjerrin të dhëna të ndjeshme.**

Ndërsa Microsoft publikoi shpejt një përditësim dhe udhëzime për të identifikuar dhe hequr ndërhyrës të mundshëm sapo hakimet të bëheshin publike, shumë organizata nuk kishin kapacitet të TI-së për të zbatuar shpejt përditësime të tilla, duke i lënë të ekspozuar për periudha të gjata kohore. Shtrirja dhe ndikimi i këtij hakimi global zbulon rrezikun e parlamenteve dhe organizatave të tjera që zgjedhin të vetë-strehojnë serverët e postës elektronike dhe lloje të tjera të dhënash të ndjeshme, veçanërisht pa investime të konsiderueshme në stafin përkushtuar sigurisë kibernetike.

PËRFITIMET E RUAJTJES SË TË DHËNAVE NË RE KOMPJUTERIKE(ICLOUD)

Edhe nëse ndërmerrni të gjitha hapat e duhur për të mbrojtur kompjuterët tuaj kundër softuerëve keqdashës dhe vjedhjeve fizike, është ende e mundur që një kundërshtar i vendosur ta hakojë kompjuterin tuaj ose serverin lokal parlamentar. Është shumë më e vështirë për ta, të mposhtin mbrojtjen e sigurisë së, për shembull, Google ose Microsoft. Kompanitë cilësore për ruajtje të të dhënave në re kanë burime të pashembullta sigurie dhe kanë një nxitje të fortë biznesi për të ofruar siguri maksimale për përdoruesit e tyre. Shkurtimisht: një strategji e besueshme e ruajtjes së të dhënave në re do të jetë shumë më e lehtë për t'u zbatuar dhe mbajtur e sigurt me kalimin e kohës. Pra, në vend që të përpiqeni të identifikoni (dhe të ruani) numrin e stafit të përkushtuar dhe shumë të aftë të sigurisë kibernetike, që kërkohet për të mbrojtur serverët lokalë në parlamentin tuaj, përqendroni energjinë tuaj në një sërë detyrash më të thjeshta. Këto përfshijnë zgjedhjen e opsionit të duhur të ruajtjes në Re kompjuterike për nevojat tuaja të privatësisë dhe lokalizimit të të dhënave, zbatimin e sigurisë së mirë të llogarisë, trajnimin e stafit për të shpërndarë (dhe për të mos-shpërndarë) dosjet dhe dokumentet siç duhet (në përgjithësi, duhet të konfiguroni dosje brenda diskut tuaj të ruajtjes në re që kufizon qasjen vetëm tek stafi që ka nevojë për skedarë të caktuar), dhe revizioni rutinë i sistemit tuaj për t'u siguruar që stafi dhe anëtarët nuk "shpërndajnë" ndonjë skedar (si p.sh. aktivizimi i ndarjes universale të lidhjeve për skedarë që duhet të kufizohen vetëm në pak njerëz).

Mbajtja e pjesës më të madhe të informacionit tuaj në Re kompjuterike ndihmon me një sërë rreziqesh të zakonshme. A ka mbetur kompjuteri i dikujt në ndonjë restorant apo telefoni në autobus? Mos ka derdhur fëmija juaj gotë me lëng në tastierë, duke e prishur pajisjen tuaj? Ose keni nevojë të ndani të dhënat që i përkasin një deputetes nga informacionet që i prodhon për parlamentin ajo deputete? A ka një punonjës softuer keqdashës dhe duhet të fshijë kompjuterin e tij dhe të fillojë nga e para? Nëse shumica e dokumenteve dhe të dhënave ruhen në Re kompjuterike, është e lehtë të risinkronizohen dhe të shkarkohen të reja në një kompjuter të pastruar ose krejtësisht të ri. Gjithashtu nëse softueri keqdashës futet në një kompjuter ose nëse ndonjë hajdut skanon një disk të ngurtë, nuk do të ketë asgjë për të vjedhur nëse shumica e dokumenteve qasen përmes shfletuesit të internetit.

A MUND T'I BESOJMË VËRTET RUAJTJES NË RE KOMPJUTERIKE?

Me pak fjalë, nuk ka asgjë në thelb të pabesueshme në lidhje me ruajtjen e të dhënave në re. Siç u përmend më lart, shumica e ofruesve kryesorë të ruajtjes në Re kompjuterike kanë ekipe të inxhinierëve më të mirë të sigurisë në botë që punojnë për të mbrojtur produktet e tyre çdo ditë dhe ofrojnë mbështetje sigurie për klientët e tyre përtej asaj që shumica e departamenteve të vogla të TI-së mund të jenë në gjendje të ofrojnë vetë. Sidoqoftë, mbani në mend se shërbimet tradicionale të ruajtjes në re zakonisht kërkojnë dhënie të qasjes në të dhëna të ndjeshme për kompani të palës së tretë që ofron shërbimin. **Me këtë, çdo parlament individual do të ketë konsideratat e veta politike dhe kërkesat ligjore (si mandatet e lokalizimit të të dhënave) për t'i marrë parasysh kur bën zgjidhjen nëse mund t'i besojë dhe të përdorë një ofrues të caktuar të ruajtjes së dhënave në Re kompjuterike.**

CILIN OFRUES PËR RUAJTJE TË TË DHËNAVE NË RE KOMPJUTERIKE DUHET TË ZGJEDHIM?

Nëse parlamenti juaj nuk duhet të marrë në konsideratë ndonjë kërkesë për lokalizimin e të dhënave dhe nuk ka asnjë problem me kompani të besuar të palës së tretë që ndan qasjen në të dhëna, dy opsionet më të njohura të ruajtjes së të dhënave në Re kompjuterike janë Google Workspace (më parë i njohur si GSuite) dhe Microsoft 365. Nëse parlamenti juaj tashmë përdor Gmail, regjistrimi i tij për Google Workspace dhe ruajtja e të dhënave në Google Drive me aplikacionet e integruara të Google Docs, Sheets dhe Slides për përpunimin e tekstit, fletëllogaritësit dhe prezantimet paraqesin një zgjidhje të logjikshme. Ngjashëm, nëse parlamenti juaj mbështetet në Excel dhe Word, zgjedhja më e lehtë është të regjistroheni në Microsoft 365, i cili jep qasje në Outlook për postë elektronike dhe versionet e licencuara të Microsoft Word, Excel, PowerPoint dhe Teams.

PO SIKUR TË NA DUHET TË KONTROLLOJMË TË DHËNAT TONA OSE TË RESPEKTOJMË LIGJET E LOKALIZIMIT TË TË DHËNAVE?

Për shumë parlamente, një opsion kaq i thjeshtë mund të mos jetë i realizueshëm, duke pasur parasysh kërkesat për lokalizimin e të dhënave ose pritshmëritë specifike që kërkojnë kontroll ekskluziv parlamentar mbi të dhënat e veta. Lajm i mirë është se kohët e fundit, ofruesit e sigurt të ruajtjes së të dhënave në re kanë zhvilluar opsione që lejojnë klientët e ndërmarrjeve ose të zgjedhin vendndodhjen e të dhënave të tyre (mbani në mend se kjo është kryesisht e kufizuar për klientët evropianë për momentin), ose të kontrollojnë çelësat e tyre të enkriptimit. **Në praktikë, kjo do të thotë që parlamenti juaj ka opsione për të kontrolluar të dhënat e veta, ndërkohë që ende përfiton nga infrastruktura dhe siguria e ruajtjes së të dhënave në re.**

Nëse parlamenti juaj aktualisht përdor ose është i interesuar të përdor Google Workspace për ruajtjen dhe ndarjen e të dhënave në Re kompjuterike, Google prezantoi një veçori që mundëson **Enkriptim nga ana e klientit** për pakon për organizata Enterprise Plus. Edhe pse për momentin është në fazë testimi dhe në dispozicion vetëm për pakot më të shtrenjta të Google Workspace, kjo veçori ofron një mundësi për të përfituar nga paketa e plotë e funksioneve të ruajtjes dhe ndarjes së të dhënave në Google Drive - dhe veçorive të sigurisë të integruara në to - duke kufizuar aftësinë e Google për të qasur informacionin delikat ose privat të parlamentit tuaj. Me enkriptimin nga ana e klientit, ju mund të zgjidhni të integroni një shërbim shtesë të menaxhimit të çelësave, siç është Virtru, dhe t'i lejoni përdoruesit të menaxhojnë çelësat e tyre të enkriptimit pa lejuar qasjen në vetë Google. Një shërbim i tillë kërkon që të gjithë të kenë kujdes të madh në mbrojtjen e atyre çelësave për të mbrojtur siç duhet qasjen në cilindo sistem të menaxhimit të çelësave që zgjidhni të integroni në Google Workspace. Administratorët e llogarisë mund të mësojnë më shumë se si të aktivizojnë enkriptimin nga ana e klientit në **faqen e mbështetjes** për Google Workspace.

Nëse parlamenti juaj aktualisht përdor ose është i interesuar të përdor Microsoft 365 për ruajtjen dhe ndarjen e të dhënave në Re kompjuterike, ofrohet edhe një opsion pak më i ndërlikuar, por mirë i vendosur për menaxhimin e çelësave tuaj të enkriptimit të njohur si **Microsoft 365 Double Key Encryption**. Ky opsion sigurie kërkon **Microsoft 365 E5**, por ju lejon të mbani kontrollin e të dhënave të ndjeshme ose private parlamentare dhe të kufizoni qasjen edhe në vetë Microsoft.

Tresorit është një tjetër opsion që është më i thjeshtë për t'u zbatuar nëse parlamenti juaj është i shqetësuar për lejimin e një pale të tretë që të ketë qasje në informacionin tuaj të brendshëm. Tresorit ofron enkriptim nga fundi në fund për ruajtjen e të dhënave në re, ndarjen e skedarëve dhe ofron një gamë të **opsioneve për mbajtjen e të dhënave**.

PO SIKUR TË MOS MUND T'I BESOJMË ASNJË ZGJIDHJEJE TË RUAJTJES SË TË DHËNAVE NË RE KOMPJUTERIKE?

Nëse vendosni të veproni vetëm dhe të mbështeteni në serverët lokalë për të ruajtur të dhënat e parlamentit tuaj, është thelbësore që të investoni kohë dhe burime të konsiderueshme për të forcuar mbrojtjen digjitale të pajisjeve të parlamentit tuaj dhe të siguroheni që serverët e tillë të konfigurohen dhe kodohen siç duhet, si dhe të mirëmbahen fizikisht të sigurt. Siç u tha më lart, qasja e tillë kërkon identifikimin, punësimin dhe mbajtjen e një numri të stafit të përkushtuar dhe shumë të aftë për siguri kibernetike për të ruajtur sigurinë e infrastrukturës së serverit tuaj lokal.

Nivel i avancuar: Rritja e sigurisë së llogarive parlamentare në Re kompjuterike

Nëse parlamenti juaj zgjedh të krijojë një domen në Google Workspace ose Microsoft 365, kini parasysh se të dyja kompanitë ofrojnë nivele më të larta sigurie për llogaritë në rrezik. **Google Advanced Protection Program** dhe **Microsoft AccountGuard** ofrojnë siguri edhe më të fuqishme për llogaritë në re të organizatave të përshtatshme dhe ju ndihmon të reduktoni shumë gjasat e phishing-ut efektiv dhe kompromentimit të llogarisë. Nëse besoni se parlamenti juaj kualifikohet dhe jeni i interesuar të regjistroni anëtarët dhe stafin tuaj në cilindo plan, vizitoni faqet e internetit të lidhura më sipër ose kontaktoni cyberhandbook@ndi.org për ndihmë të mëtejshme.

KOPJET REZERVË TË TË DHËNAVE (BACK UP)

Pavarësisht nëse parlamenti juaj ruan të dhëna në pajisje fizike dhe serverë ose në re, është e rëndësishme të keni kopje rezervë. Mbani në mend se nëse mbështeteni në ruajtjen fizike të të dhënave në pajisje, është mjaft e lehtë të humbni qasjen në të dhënat tuaja. Mund t'ju derdhet kafja mbi kompjuter dhe të shkatërroni diskun e ngurtë. Kompjuterët e stafit mund të hakohen dhe të gjithë skedarët lokalë të kyçen me ransomware. Dikush mund të humbasë pajisje në tren ose t'i vidhet së bashku me çantën e tyre. Siç u përmend më lart, kjo është një arsye shtesë pse ruajtja e të dhënave në re mund të jetë përfitim, sepse nuk është i lidhur me pajisje specifike që mund të infektohet, humbet ose vidhet. Mac-et vijnë me softuer të integruar për kopje rezervë të quajtur **Time Machine** që përdoret së bashku me pajisje për ruajtje të jashtme të të dhënave; për pajisjet Windows, **File History** ofron funksionalitetin e njëjtë. Telefonat e mençur iPhone dhe Android munden automatikisht të bëjnë kopje rezervë të përmbajtjes së tyre më të rëndësishme në re sipas

rregullimeve të telefonit tuaj.
Nëse parlamenti juaj përdor Re kompjuterike për të ruajtur të dhënat (si Google Drive), rreziku që Google të bie ose të shkatërrohen të dhënat tuaja në ndonjë fatkeqësi është mjaft i ulët, por gabimi njerëzor (si fshirja e rastësishme e skedarëve të rëndësishëm) vazhdon të jetë mundësi. Hulumtimi për një zgjidhje rezervë në re si **Backupify** ose **SpinOne Backup** mund t'ia vlejë.

Nëse të dhënat ruhen në një server lokal dhe/ose pajisje lokale, kopja rezervë e sigurt bëhet edhe më kritike. Mund të rezervoni të dhënat e parlamentit tuaj në një disk të ngurtë të jashtëm ose një seri disqesh, por sigurohuni që të enkriptoni disqe të tillë me fjalëkalim të fortë. Time Machine mund të enkriptojë disqet e ngurtë për ju, ose mund të përdorni mjete të besuara të enkriptimit për të gjithë diskun e ngurtë si VeraCrypt ose BitLocker. Sigurohuni që të mbani çdo pajisje rezervë në një vend të ndryshëm nga pajisjet dhe skedarët tuaj të tjerë. Mos harroni, nevojitet një zjarr që mund të shkatërrojë kompjuterët tuaj dhe kopjet rezervë të tyre, që do të thotë që nuk keni fare kopje rezervë. Konsideroni të mbani kopje në vend shumë të sigurt, siç është kasaforta.

Blloqet e ndërtimit të planit të sigurisë: Ruajtja e të dhënave në mënyrë të sigurt

- **Ruani të dhënat e ndjeshme ekskluzivisht në një shërbim të besuar për ruajtje në Re kompjuterike.**
  - Sigurohuni që çdo llogari e lidhur që përdoret për të hyrë në një shërbim të tillë të ketë fjalëkalime të forta dhe 2FA.
- **Vendosni dhe zbatoni politikë për të kufizuar cilësimet e ndarjes brenda reve kompjuterike.**
  - Trajnoni të gjithë anëtarët dhe stafin se si të ndajnë siç duhet dokumentet (dhe jo t'i tej-shpërndajnë).
- **Nëse parlamenti juaj vendos të ruajë të dhënat në nivel lokal, investoni në staf të aftë të TI-së.**
- **Mbani të sigurta kopjet rezervë të të dhënave - enkriptoni disqet e ngurta rezervë ose pajisje të tjera rezervë.**

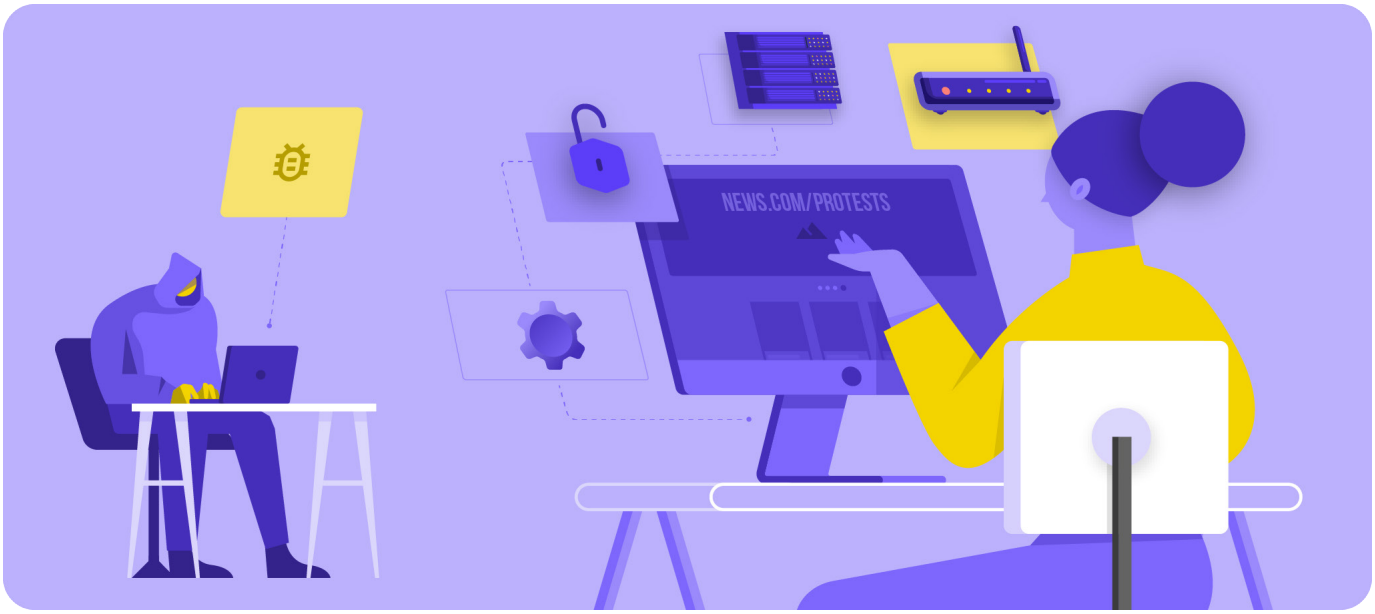
Qëndroni të sigurt në internet

Kur përdorni internetin në telefonin ose kompjuterin tuaj, aktiviteti juaj mund të tregojë shumë për ju. Është e rëndësishme të mbani informacione të ndjeshme – si emrat e përdoruesve dhe fjalëkalimet që i shkruani në faqe interneti, postimet tuaja në mediat sociale, ose në kontekste të caktuara edhe emrat e faqeve të internetit që i vizitoni – larg syve kureshtarë. Bllokimi ose kufizimi i qasjes suaj në sajte ose aplikacione të caktuara është gjithashtu një shqetësim i zakonshëm. Këto dy probleme – mbikëqyrja e internetit dhe censura e internetit – shkojnë paralelisht, por edhe strategjitë për të reduktuar ndikimet e tyre janë të ngjashme.

Shfletimi i sigurt

PËRDORIMI I HTTPS-SË

Hapi më i rëndësishëm për të kufizuar aftësinë e një kundërshtari për të vëzhguar parlamentin tuaj në internet është të minimizoni sasinë e informacionit në dispozicion për ju dhe aktivitetin e kolegëve tuaj në internet. Gjithmonë sigurohuni që jeni duke u lidhur me faqet e internetit në mënyrë të sigurt: sigurohuni që URL-ja (vendndodhja) fillon me “https” dhe shfaq një ikonë të vogël bllokimi në shiritin e adresave të shfletuesit tuaj. Kur shfletoni internetin **pa enkriptim**, informacioni që shkruani në një sajt (si fjalëkalimet, numrat e llogarisë ose mesazhet) dhe detajet e sajtit dhe faqeve që vizitoni ekspozohen të gjitha. Kjo do të thotë që (1) çdo haker në rrjetin tuaj, (2) administratori i rrjetit tuaj, (3) ISP-ja juaj dhe çdo ent me të cilin mund të ndajnë të dhëna (si autoritetet qeveritare), (4) ISP-ja e sajtit që po vizitoni dhe çdo entitet me të cilin mund të ndajnë të dhëna, dhe sigurisht, (5) vetë faqja që po vizitoni, të gjithë kanë qasje në mjaft informacione potencialisht të ndjeshme. Le të marrim një shembull të botës reale se si duket shfletimi pa enkriptim:



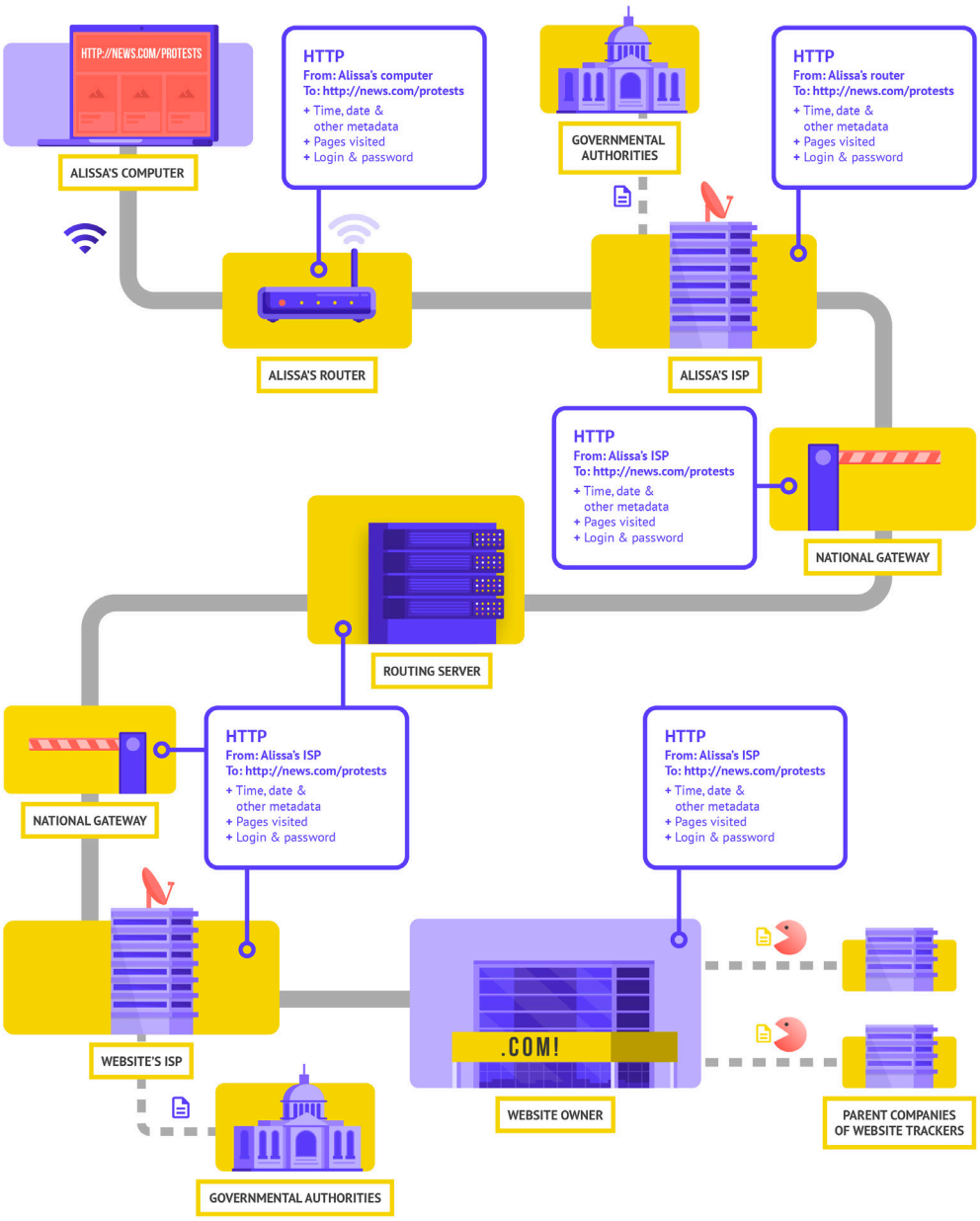
Mbikëqyrja, censura dhe parlamentet

Qeveritë jomiqësore dhe aktorë të tjerë kërcënimi anembanë globit përdorin teknologjinë e mbikëqyrjes gjithnjë e më të qasshme, dhe në disa raste hakerimin e thjeshtë Wi-Fi, për të monitoruar aktivitetin online të deputetëve dhe të punësuarve të tjerë në parlament. Për shembull, hakerët vodhën të dhëna nga stafi i parlamentit evropian dhe vizitorët **duke e mashtruar Wi-Fi rrjetin publik të Parlamentit** në vitin 2013. Një paralajmërim të sulmeve shumë më të sofistikuara që do të ndodhin në vitet në vijim.

Përveç rrëmbimit të trafikut të internetit dhe vjedhjes së të dhënave, kundërshtarët pengojnë gjithashtu operacionet kritike parlamentare, duke bllokuar qasjen dhe sistemet e internetit. Në Bruksel, parlamenti i Belgjikës u hoq jashtë linje nga një **sulm masiv i mohimit të shërbimit** në maj 2021. Sulmi detyroi shtyrjen e disa debateve dhe mbledhjeve të komisioneve, pasi përdoruesit nuk mund të qasnin shërbimet virtuale të nevojshme për të marrë pjesë në seancë.

Frekuenca në rritje e sulmeve të tilla ndaj qasjes dhe lirisë së informacioneve në internet nxjerr në pah se sa thelbësore është që parlamentet t'i kuptojnë rreziqet e funksionimit në internet dhe të zhvillojnë plane se si të lidhen kur ndikohet lidhja.

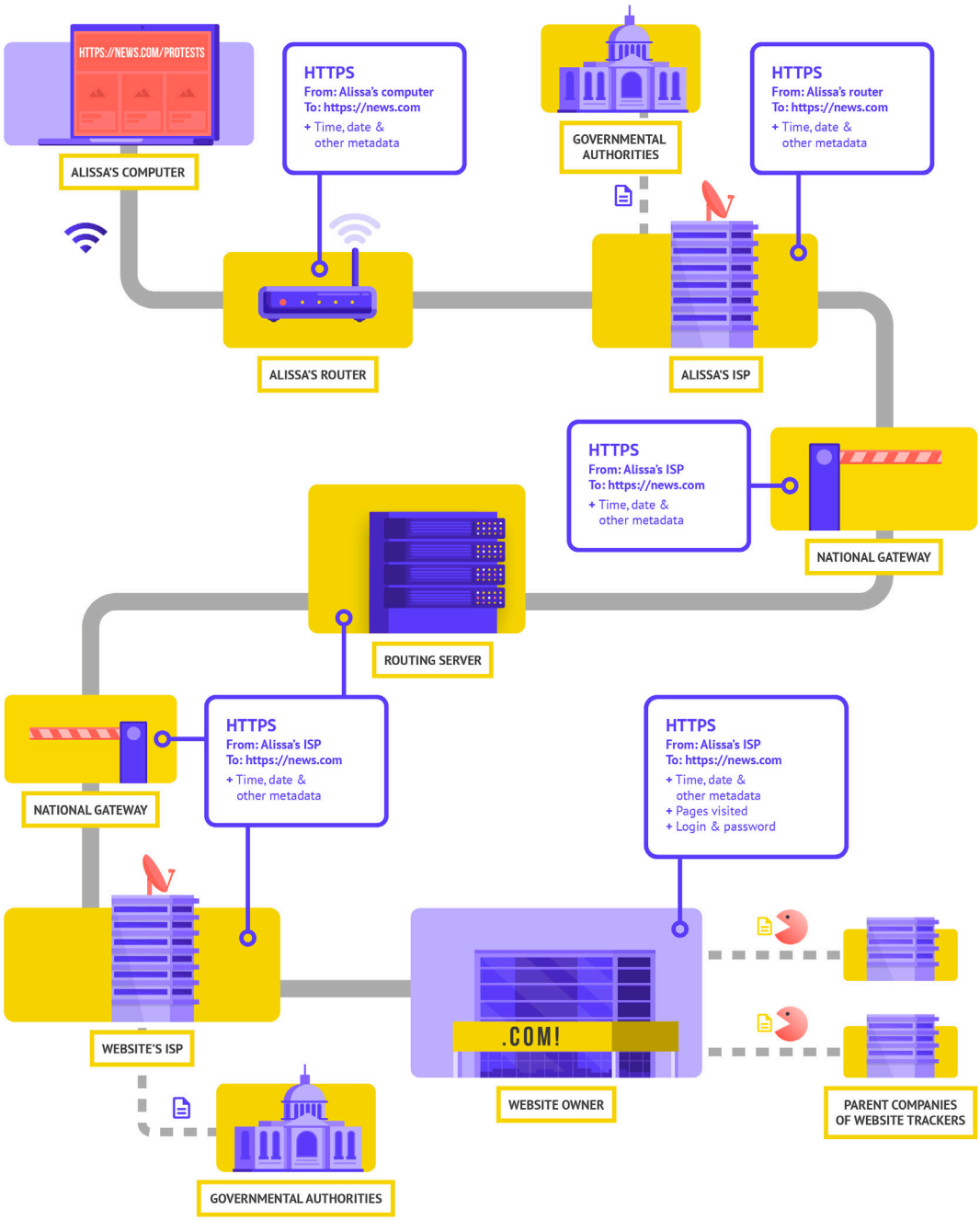
Le të marrim një shembull të botës reale se si duket shfletimi pa kriptim:



Përshtatur nga Projekti Totem [How the Internet Works](#) (CC–BY–NC–SA)

Kur shfletoni pa enkriptim, të gjitha të dhënat tuaja ekspozohen. Siç u tregua më lart, ndonjë kundërshtar mund të shohë se ku jeni, se po shkoni te news.com, duke parë në mënyrë specifike faqen e protestave në vendin tuaj, dhe ndoshta më e rëndësishmja si deputet ose anëtar i stafit parlamentar, të shohë fjalëkalimin tuaj që ju e ndani për të hyrë në vetë sajtin. Një informacion i tillë në duar të gabuara jo vetëm që ekspozon llogarinë tuaj, por gjithashtu u jep kundërshtarëve të mundshëm, kudo që të jenë në botë, pasqyrë të mirë të asaj që mund të bëni ose mendoni.

Përdorimi i HTTPS-së (“s” shënon sigurt) do të thotë që enkriptimi është në vend. Kjo ju ofron shumë më tepër mbrojtje. Të vështrojmë se si duket shfletimi me HTTPS (gjegjësisht me enkriptim):



Përshtatur nga Projekti Totem [How the Internet Works](#) (CC–BY–NC–SA)

Me HTTPS në vend, kundërshtari i mundshëm nuk mund të shohë më fjalëkalimin tuaj ose informacione të tjera të ndjeshme që mund të ndani në një faqe interneti. Megjithatë, ende mund të shohin se cilat domene (për shembull, news.com) vizitoni. Dhe ndërsa HTTPS gjithashtu kodon informacionin për faqet individuale brenda një sajti (për shembull, website.com/protests) që vizitoni, kundërshtarët e sofistikuar mund ta shohin këtë informacion duke inspektuar trafikun tuaj të internetit. Me HTTPS në vend, kundërshtari mund të dijë që ju shkoni te news.com, por nuk do të jetë në gjendje të shohë fjalëkalimin tuaj dhe do të ishte më e vështirë (por jo e pamundur) për ata që të shihnin se kërkoni informacione rreth protestave (për të përdorur si shembull). Ky është një ndryshim i rëndësishëm. Gjithmonë kontrolloni nëse HTTPS është në vend përpara se të lundroni nëpër një faqe interneti ose të futni informacione të ndjeshme. Ju gjithashtu mund të përdorni **HTTPS Everywhere browser extension** për t'u siguruar që përdorni HTTPS gjatë gjithë kohës, ose nëse përdorni Firefox, kyçni **HTTPS only mode** në shfletues.

Nëse ju paraqitet paralajmërim nga shfletuesi juaj se një faqe interneti mund të jetë e pasigurt, mos e injoroni atë. Diçka nuk është në rregull. Mund të jetë beninj – si faqja mund të ketë certifikatë sigurie të skaduar – ose mund të jetë e falsifikuar ose e falsifikuar me qëllim të keq. Sido që të jetë, është e rëndësishme t'i kushtoni vëmendje paralajmërimit dhe të mos shkoni në atë faqe.

Nivel i avancuar: Përdorimi i DNS-së së enkriptuar

Nëse dëshironi ta bëni më të vështirë (por jo të pamundur) që një ISP të dijë detajet e faqeve të internetit që vizitoni, mund të përdorni DNS të enkriptuar.

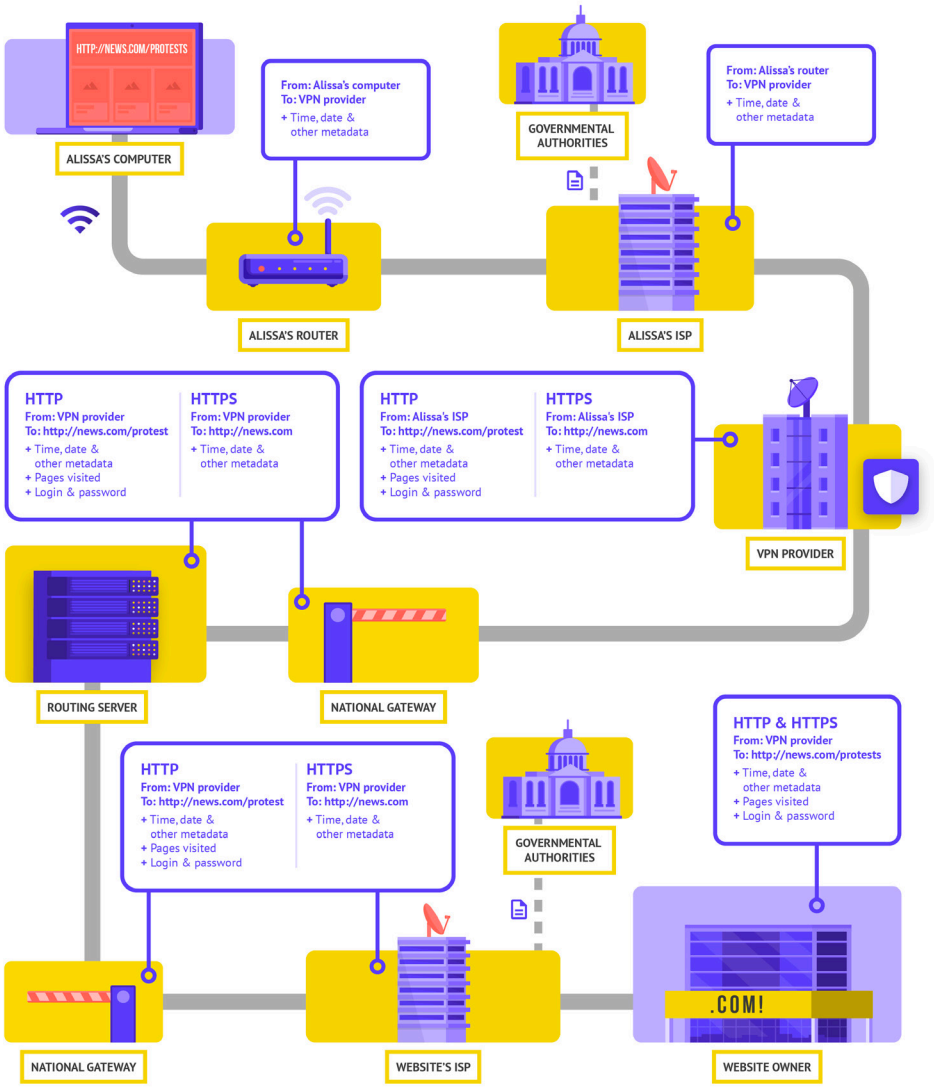
Nëse ju **intereson**, DNS qëndron për Domain Name System. Në thelb është libri i telefonave të internetit, duke përkthyer emra domenesh miqësore për njerëzit (si ndi.org) në adresa miqësore të protokollit të internetit (IP) me ueb. Kjo i lejon njerëzit të përdorin shfletues uebi për të kërkuar dhe ngarkuar me lehtësi burimet e internetit dhe për të vizituar faqet e internetit. Sidoqoftë, si parazgjedhje, DNS nuk është i enkriptuar.

Për të përdorur DNS të enkriptuar dhe për të shtuar pak mbrojtje në trafikun tuaj të internetit në të njëjtën kohë, një opsion i thjeshtë është të shkarkoni dhe aktivizoni **Cloudflare's 1.1.1.1 app** në kompjuterin dhe pajisjen tuaj celulare. Opsione të tjera të enkriptuara DNS, duke përfshirë 8.8.8.8 të Google, janë në dispozicion, por kërkohen **hapa më teknik** për ta konfiguruar. Nëse përdorni shfletuesin Firefox, DNS i enkriptuar tani është i aktivizuar si parazgjedhje. Përdoruesit e shfletuesve Chrome ose Edge munden **të kyçin DNS-në e enkriptuar** nëpërmjet cilësimeve të avancuara të sigurisë së shfletuesit duke aktivizuar "përdor DNS të sigurt" dhe duke zgjedhur "Me: Cloudflare (1.1.1.1)" ose ofruesin e zgjedhjes së tyre.

1.1.1.1 i Cloudflare me WARP enkripton DNS-në tuaj dhe enkripton të dhënat tuaja të shfletimit, duke ofruar shërbim të ngjashëm me një VPN tradicionale. Ndërsa WARP-i nuk e mbron plotësisht vendndodhjen tuaj nga të gjitha faqet e internetit që vizitoni, është një veçori e lehtë për t'u përdorur që mund të ndihmojë stafin e parlamentit tuaj të përfitojë nga DNS-ja e enkriptuar dhe nga mbrojtja shtesë nga ISP-ja juaj në situata kur një VPN e plotë ose nuk është funksionale ose është e nevojshme, duke pasur parasysh kontekstin e kërcënimit. Në 1.1.1.1 me cilësimet e avancuara të DNS WARP, stafi mund të aktivizojë gjithashtu 1.1.1.1 për Familjet për të ofruar mbrojtje shtesë kundër softuerëve keqdashës gjatë qasjes në internet.

ÇFARË ËSHTË VPN?

Një VPN është në thelb tunel që mbron nga mbikëqyrja dhe bllokimi i trafikut tuaj të internetit nga hakerët në rrjetin tuaj, administratori i rrjetit tuaj, ISP-ja juaj dhe kushdo me të cilin mund të ndajnë të dhëna. Në një organizatë të madhe - si parlamenti - VPN-të "biznes" ose "korporativ" shpesh përdoren për të ndihmuar mbrojtjen e integritetit të qasjes në sistemet dhe aplikacionet e brendshme (si ato që përdoren për votim në distancë). Qoftë duke përdorur një VPN personale ose një të krijuar për qëllime biznesi, koncepti i mbrojtjes së trafikut tuaj të internetit kundër përgjimit funksionon përgjithësisht njëjtë dhe mbetet thelbësore të vazhdoni të përdorni HTTPS (madje edhe me VPN në vend.) Është gjithashtu e rëndësishme të sigurohet që ju i besoni VPN-së që përdor parlamenti juaj. Këtu kemi shembull se si duket shfletimi me një VPN:



Përshtatur nga Projekti Totem [How the Internet Works](#) (CC–BY–NC–SA)

Për të përshkruar VPN-të më thellë, ky seksion i referohet [Udhëzuesit për vetëmbrojtje nga mbikëqyrja](#) të EFF-së:

VPN-të tradicionale janë krijuar për të maskuar adresën tuaj aktuale IP të rrjetit dhe për të krijuar tunel të enkriptuar për trafikun e internetit midis kompjuterit tuaj (ose telefonit ose ndonjë pajisjeje "të zgjuar" të lidhur në rrjet) dhe serverit të VPN-së. Për shkak se trafiku në tunel është i enkriptuar dhe dërguar në VPN-në tuaj, është shumë më e vështirë për palët e treta si ISP-të ose hakerat në Wi-Fi publik të monitorojnë, modifikojnë ose bllokojnë trafikun tuaj. Pasi kalon nëpërmjet tunelit nga ju në VPN, trafiku juaj më pas e lë VPN-në në destinacionin e tij përfundimtar, duke maskuar adresën tuaj origjinale IP. Kjo ndihmon për të maskuar vendndodhjen tuaj fizike për këdo që shikon trafikun pasi të largohet nga VPN-ja. Kjo ju ofron më shumë privatësi dhe siguri, por përdorimi i një VPN-së nuk ju bën plotësisht anonim në internet: trafiku juaj është ende i dukshëm për operatorin e VPN-së. ISP-ja juaj do të dijë gjithashtu se po përdorni një VPN, gjë që mund të rrisë profilin tuaj të rrezikut.

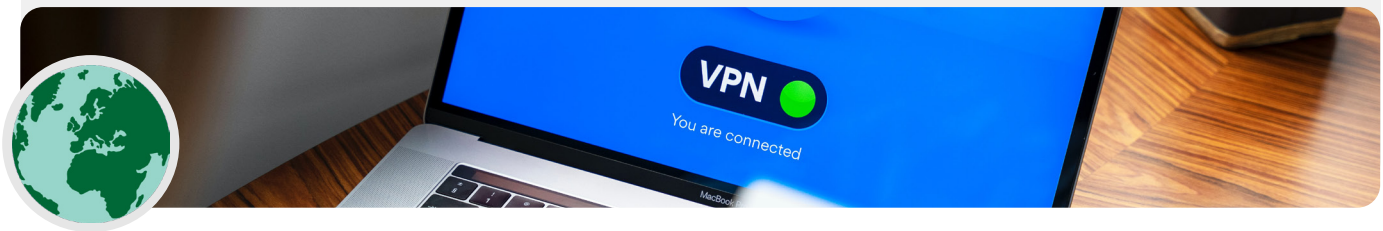
Kjo do të thotë që **zgjedhja e një ofruesi të besueshëm** VPN është thelbësore. Në disa vende si Irani, qeveritë armiqësore në fakt kanë krijuar VPN-të e tyre për të qenë në gjendje të gjurmojnë se çfarë bëjnë qytetarët. Për të gjetur VPN-në e duhur për parlamentin dhe stafin tuaj, mund të vlerësoni VPN-të bazuar në modelin dhe reputacionin e tyre të biznesit, çfarë të dhënash mbledhin ose nuk mbledhin, dhe sigurisht, sigurinë e vetë mjetit.

Pse të mos përdorni thjesht një VPN falas? Përgjigjja e shkurtër është se shumica e VPN-ve falas, përfshirë ato që vijnë të para-instaluara në disa telefona të mençur, vijnë me një kusht të madh. Ashtu si të gjitha bizneset dhe ofruesit e shërbimeve, VPN-të duhet të mbajnë veten disi. Nëse VPN-ja nuk shet shërbim, si po e mban në këmbë biznesin e vet? A kërkon donacione? A paguan për shërbimet premium? A mbështetet nga organizata bamirëse apo nga financues? Fatkeqësisht, shumë VPN falas fitojnë para duke mbledhur dhe më pas duke shitur të dhënat tuaja.
Një ofrues VPN që nuk mbledh të dhëna në radhë të parë është zgjidhja më e mirë. Nëse të dhënat nuk mblidhen, as nuk mund të shiten ose t'i dorëzohen një qeverie të huaj nëse kërkohet. Kur shikoni politikën e privatësisë së një ofruesi të VPN-së, shikoni nëse VPN-ja mbledh në të vërtetë të dhënat e përdoruesit. Nëse nuk thotë në mënyrë eksplicite se të dhënat e lidhjes së përdoruesit nuk regjistrohen, ka shumë mundësi që të jetë ashtu. Edhe nëse një kompani pretendon se nuk regjistron të dhënat e lidhjes, kjo mund të mos jetë gjithmonë garanci e sjelljes së mirë.

Ia vlen të bëni një kërkim për kompaninë që qëndron pas VPN-së. A miratohet nga profesionistë të pavarur të sigurisë? A ka VPN-ja artikuj të shkruar në lidhje me të? A është kapur ndonjëherë duke mashtruar apo gënjyer klientët e vet? Nëse VPN-ja është krijuar nga njerëz të njohur në komunitetin e sigurisë së informacionit, ka më shumë gjasa të jetë i besueshëm. Jini skeptik ndaj një VPN-je që ofron shërbim për të cilin askush nuk dëshiron të rrezikojë reputacionin e vet, ose nëse drejtohet nga një kompani për të cilën askush nuk ka informata.

VPN të rreme në botën reale

Në fund të vitit 2017, pas një rritje të protestave në vend, [iranianët filluan të zbulojnë një version "falas" (por të rremë) të një VPN popullore që shpërndahej përmes mesazheve me tekst](#). VPN-ja falas, që në fakt nuk funksionoi, premtoi të jepte qasje në Telegram, që në atë kohë ishte i bllokuar në nivel lokal. Fatkeqësisht, aplikacioni i rremë nuk ishte gjë tjetër veçse softuer keqdashës që i lejonte autoritetet të gjurmon lëvizjen dhe të monitoronin komunikimet e personave që e shkarkonin atë.



Pra, çfarë VPN duhet të përdorim?

Nëse, përveç garantimit të sigurisë së trafikut të internetit në parlament, gjithashtu ju nevojitet zgjidhje për të kufizuar në mënyrë të sigurt qasjen vetëm në anëtarët në rrjetin tuaj parlamentar (edhe kur punoni në distancë) në sistemet dhe aplikacionet e brendshme parlamentare, mund të zbatoni VPN " biznes" ose VPN "korporativ". Ka një sërë opsionesh që përdorin teknologji të ndryshme që mund t'i merrni parasysh, duke përfshirë **AnyConnect** nga Cisco, **Global Protect** nga PaloAlto, ose **Access** nga Cloudflare (teknikisht Zero Trust Access System, jo VPN) vetëm për të përmendur disa. Sido që të jetë, sisteme të tilla kërkojnë staf të aftë të TI-së për t'i zbatuar dhe menaxhuar në mënyrë efektive.

Nëse një VPN sistem i avancuar "korporativ" është ose jashtë buxhetit ose i ndërlikuar në mënyrë të panevojshme për parlamentin tuaj, mund të konsideroni gjithashtu përdorimin e opsioneve personale VPN si p.sh. **ProtonVPN** ose **TunnelBear** (i cili ofron gjithashtu plan për ekipe për ta bërë më të thjeshtë menaxhimin e llogarisë) për të gjithë anëtarët dhe stafin e parlamentit. Opsion tjetër i besueshëm është të konfiguroni serverin tuaj duke përdorur **Outline** nga Jigsaw, ku nuk ka kompani që menaxhon llogarinë tuaj, por në këmbim, ju duhet të konfiguroni serverin tuaj.

Megjithëse shumica e VPN-ve moderne janë përmirësuar në lidhje me performancën dhe shpejtësinë, ia vlen të keni parasysh faktin se përdorimi i një VPN-je mund të ngadalësojë shpejtësinë tuaj të shfletimit nëse jeni në rrjet me gjerësi shumë të ulët të brezit, vuani nga vonesa të larta të transferit, vonesa në rrjet, ose keni ndërprerjet të kohëpaskohshme të internetit. Nëse jeni në rrjet më të shpejtë, duhet të përdorni një VPN gjatë gjithë kohës. Nëse rekomandoni që stafi të përdorë një VPN, është gjithashtu e rëndësishme të siguroheni që njerëzit ta mbajnë VPN-në të ndezur. Mund të duket si mjaftë e qartë, por një VPN që është instaluar por nuk funksionon nuk ofron asnjë mbrojtje.

Nivel i avancuar: Anonimiteti nëpërmjet Tor-it

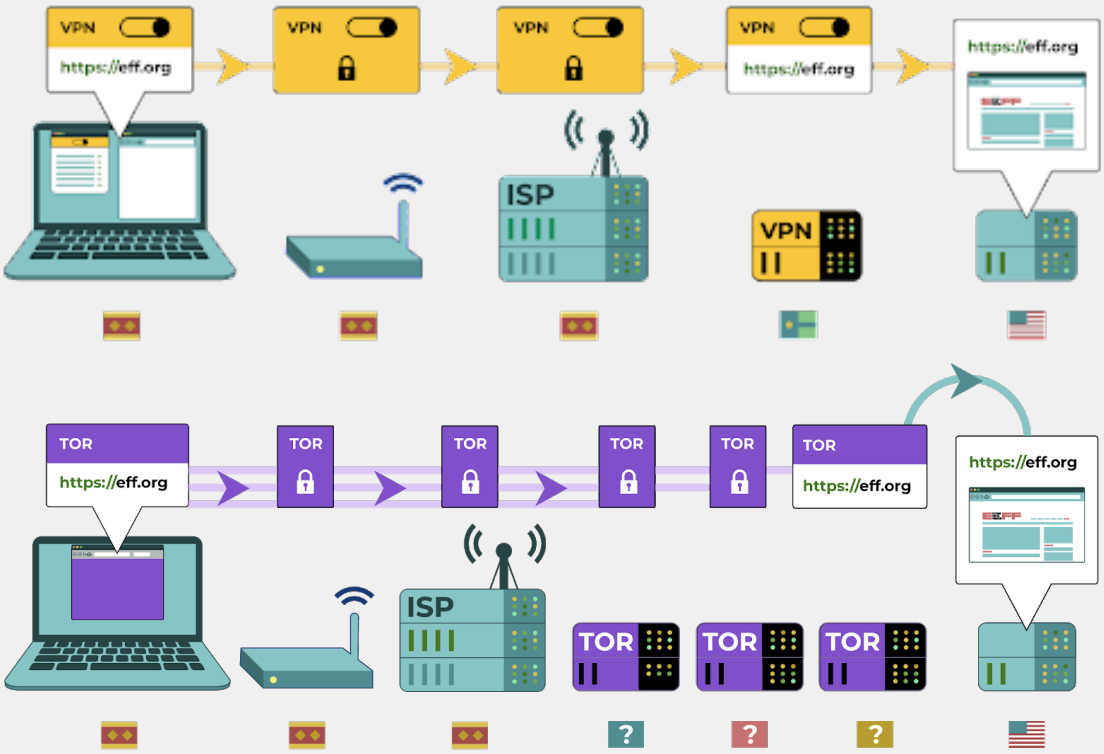
Përveç VPN-ve, mund të keni dëgjuar për Tor-in si një mjet tjetër për përdorim më të sigurt të internetit. Është e rëndësishme të kuptoni se çfarë janë të dyja dhe pse mund të përdorni njërën ose tjetrën.

Tor-i është një protokoll për transmetimin e të dhënave në mënyrë anonime nëpërmjet internetit, duke kursyer mesazhe ose të dhëna nëpërmjet një rrjeti të decentralizuar. Mund të mësoni më shumë se si Tor-i funksionon **këtu**, por me pak fjalë, drejton trafikun tuaj nëpër pika të shumta përgjatë rrugës për në destinacionin e tij, në mënyrë që asnjë pikë e vetme të mos ketë informacion të mjaftueshëm për të ekspozuar se kush jeni dhe çfarë po bëni në internet menjëherë.

Tor-i është i ndryshëm nga një VPN në disa mënyra. Në thelb, ai ndryshon sepse nuk mbështetet në besimin e ndonjë pike specifike (si një ofrues VPN). Kjo grafikë, e zhvilluar nga EFF, tregon ndryshimin midis një VPN tradicionale dhe Tor.

Mënyra më e lehtë për të përdorur Tor është nëpërmjet **Tor shfletuesin e internetit**. Funksionon si çdo shfletues normal, përveç që drejton trafikun tuaj nëpërmjet rrjetit Tor. Mund të shkarkoni shfletuesin Tor në pajisjet Windows, Mac, Linux ose Android. Mbani në mend se kur përdorni Tor Browser, ju mbroni vetëm informacionin në të cilin keni qasje ndërsa jeni në shfletues. Tor-i nuk ofron asnjë mbrojtje për aplikacionet e tjera ose skedarët e shkarkuar që mund t'i hapni veçmas në pajisjen tuaj. Gjithashtu, mbani në mend se Tor-i nuk e enkripton trafikun tuaj, kështu që - njësoj si kur përdorni një VPN - është ende thelbësore të përdorni praktikat më të mira si HTTPS gjatë shfletimit.

Nëse dëshironi të zgjeroni mbrojtjen e anonimitetit të Tor-it në të gjithë kompjuterin tuaj, përdoruesit më të zgjuar të teknologjisë mund të instalojnë Tor-in si një lidhje interneti në të gjithë sistemin ose të marrin në konsideratë përdorimin e sistemit operativ **Tails**, i cili drejton të gjithë trafikun nëpërmjet Tor-it si parazgjedhje. Përdoruesit e Android-it mund të përdorin gjithashtu aplikacionin **Orbot** për të përdorur Tor-in për të gjithë trafikun e internetit dhe aplikacionet në pajisjen e tyre. Pavarësisht se si e përdorni Tor-in, është e rëndësishme të dini se kur e përdorni, ofruesi



juaj i shërbimit të internetit nuk mund të shohë se cilat faqe interneti vizitoni, por ata *mund* të shohin që ju po përdorni vetë Tor. Ashtu si kur përdorni një VPN, kjo mund të rrisë ndjeshëm profilin tuaj të rrezikut, sepse Tor nuk është një mjet shumë i zakonshëm dhe për këtë arsye dallohet nga kundërshtarët që mund të monitorojnë trafikun tuaj të internetit.

Pra, ndërsa ka shumë pak raste kur Tor-i do të ishte i nevojshëm për t'u përdorur brenda një konteksti parlamentar, nëse nuk mund të përballoni një VPN të besueshme ose e kuptoni parlamenti juaj funksionon në një mjedis ku VPN-të bllokohen në mënyrë rutinore, Tor-i mund të jetë opsion i mirë, nëse është e ligjshme, për kufizimin e ndikimit të mbikëqyrjes dhe shmangien e censurës në internet.

A ka ndonjë arsye pse nuk duhet të përdorim VPN ose Tor?

Përveç shqetësimeve rreth shërbimeve VPN që nuk kanë reputacion, faktori më i madh që duhet marrë parasysh është nëse përdorimi i një VPN-së ose Tor-it mund të tërheqë vëmendje të padëshiruar ose, në nivel lokal, të jetë kundër ligjit. Megjithëse ISP-ja juaj nuk do të dijë se cilat faqe i vizitoni gjatë përdorimit të këtyre shërbimeve, ata mund të shohin që jeni lidhur me Tor ose VPN. Nëse kjo është e paligjshme në vendin tuaj, parlamenti dhe stafi juaj mund të shkaktojë më shumë vëmendje ose rrezik sesa thjesht të lundron në ueb me HTTPS standarde dhe DNS të enkriptuar, ndoshta një VPN ose veçanërisht Tor (i cili përdoret shumë më rrallë dhe për këtë arsye paraqet "flamur të kuq" më të madh) nuk është zgjedhja e duhur.

ÇFARË SHFLETUESI DUHET TË PËRDORIM?

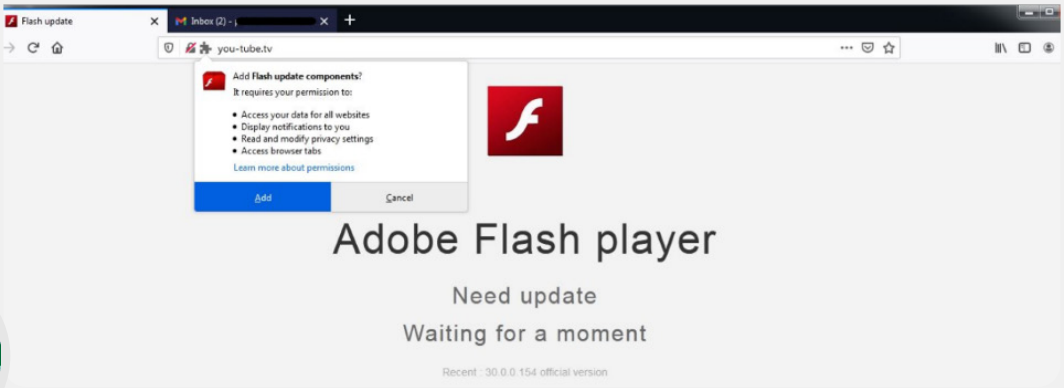
Përdorni një shfletues me reputacion si Chrome, Firefox, Brave, Safari, Edge ose Tor Browser. Si Chrome ashtu edhe Firefox përdoren shumë gjerësisht dhe janë të shkëlqyer me sigurinë. Disa njerëz preferojnë Firefox-in duke pasur parasysh fokusin e tij në privatësi. Sido që të jetë, është e rëndësishme që t'i rinisni ato dhe kompjuterin tuaj relativisht shpesh për ta mbajtur shfletuesin tuaj të përditësuar. Nëse jeni të interesuar të krahasoni veçoritë e shfletuesit, shikoni këtë resurs nga Fondacioni për Liri të Shtypit.

Pavarësisht nga shfletuesi, është gjithashtu një ide e mirë të përdorni një (extension) ose shtesë (add-on) si Privacy Badger, uBlock Origin, ose DuckDuckGo's Privacy Essentials që i ndalon reklamuesit dhe gjurmuesit e tjerë të palëve të treta të gjurmojnë se ku shkoni dhe cilat faqe vizitoni. Dhe kur shfletoni internetin, merrni parasysh të largoni kërkimet tuaja të paracaktuara në ueb prej Google në DuckDuckGo, Startpage, ose një motor tjetër kërkimi për mbrojtjen e privatësisë. Një ndërrim i tillë do të ndihmojë gjithashtu në kufizimin e reklamuesve dhe gjurmuesve të palëve të treta.

Siguria e shfletuesit në botën reale

Zgjatjet e shfletuesit ose sulmet e shtesave mund të jenë po aq të dëmshme sa softueri keqdashës që ndahet drejtpërdrejt nëpërmjet shkarkimeve të phishing ose softuerëve të tjerë. Për shembull, një shtesë me qëllim të keq e dizajnuar me zgjuarsi me titullin "Përbërësit e përditësimit të Flash-it" synonin organizatat politike tibetiane në fillim të vitit 2021. Shtesa iu prezantua përdoruesve që vizitonin faqet e internetit të lidhura me phishing postat elektronike dhe kur u instalua, u mundësoi hakerëve të vidhnin postat elektronike dhe të dhënat e shfletimit.

Shtesat e shfletuesit mund të jenë gjithashtu vektor për infektimin e burimeve parlamentare si faqet e internetit, të cilat nga ana e tyre mund të përhapin softuer keqdashës në një gamë të gjerë vizitorësh të faqes (përfshirë publikun e gjerë, stafin parlamentar dhe vetë anëtarët). Merrni, për shembull, shfrytëzimin e hakerëve të shtesës popullore të shfletuesit Browsealoud (tani e njohur si ReachDeck), një program që konverton tekstin e faqes në internet në audio për përdoruesit me shikim të dëmtuar. Në vitin 2018, hakerët futën kodin keqdashës në shtesën e shfletuesit, i cili kishte qenë në përdorim në faqet e internetit të entiteteve të ndryshme qeveritare, duke përfshirë Parlamentin e Viktorias në Australi.
Me shtojcën e infektuar të shfletuesit në vend dhe të konfiguruar në mënyrë jo të duhur, pajisjet e vizitorëve të faqes në internet u infektuan me softuer keqdashës gjatë vizitës së sajtit. Në këtë rast, softueri keqdashës u përdor për të shfrytëzuar pajisjet për të minuar kriptomonedhë, por taktika të tilla mund të përdoren nga hakerët për të përhapur softuerë keqdashës për qëllime të vjedhjes së të dhënave ose gjithashtu edhe spiunazhit.



Siguria e mediave sociale

Stafi parlamentar dhe deputetët mund të shpalosin shumë informata – dhe ndonjëherë më shumë sesa synojnë – duke postuar dhe komentuar në mediat sociale. Pavarësisht nëse janë në Facebook, Twitter, Instagram, YouTube ose sajte të mediave sociale specifike për rajonin, si VKontakte dhe Odnoklassniki, duhet gjithmonë të mendoni me kujdes për atë që postoni dhe të konfiguroni siç duhet çdo cilësim privatësie që mund të jetë në dispozicion. Kjo është e vërtetë jo vetëm për faqet zyrtare të parlamenteve, por në disa raste edhe për llogaritë personale të stafit dhe ato të familjes dhe miqve të tyre.

Siguria e mediave sociale dhe parlamentet

Edhe organizatat me rrezik të ulët mund të shënjestrohen dhe ngacmohen në mediat sociale nëse nuk vendosin politikat e duhura të sigurisë. Në **këtë shembull** nga viti 2018, një strehimore jofitimprurëse e kafshëve humbi mijëra dollarë dhe i tjetërsoi mbështetësit pasi një administrator i paautorizuar i llogarisë ngriti një përpjekje të rreme për mbledhjen e fondeve si dhe llogari të rreme që imitonin punonjësit, që u shfaqën në platformë. Nëse hakerët do të punonin kaq shumë për të fituar disa mijëra dollarë nga një strehimore e kafshëve, mund të imagjinoni dëmin që kundërshtarët e sofistikuar mund të shkaktojnë nëse do të kishin qasje në llogaritë e parlamentit tuaj ose do të imitonin, online, me sukses një deputet ose personel të shquar të stafit.

Përveç hakerimit të llogarive të mediave sociale, faqet e internetit të parlamentit janë gjithashtu objektiva të zakonshëm, duke pasur parasysh dukshmërinë e tyre publike dhe rëndësinë e reputacionit. Në një shembull nga viti 2017, faqja e internetit e parlamentit të Austrisë u **rrëzua nga një grup hakerësh** që supozohej se ishte i zemëruar nga acarimi i marrëdhënieve të vendit me Turqinë në atë kohë.

ZHVILLONI POLITIKË PARLAMENTARE PËR MEDIE SOCIALE

Supozoni se çdo gjë e postuar në mediat sociale mund të bëhet e njohur për publikun dhe krijoni politikë parlamentare për medie sociale në përputhje me rrethanat. Duke pasur parasysh natyrën publike të pjesës më të madhe të punës parlamentare, ka gjasa që ju të dëshironi të ndani publikisht shumicën e postimeve dhe mesazheve, por është ende thelbësore të bëni dhe t'u përgjigjeni pyetjeve si: Kush ka qasje në llogaritë tuaja të mediave sociale? Kujt i lejohet të postojë dhe kush duhet të miratojë postimet? Po komentet dhe përgjigjet? Çfarë informacioni duhet/nuk duhet të ndahet në mediat sociale? Nëse postoni foto, informacione për vendndodhjen ose informacione të tjera identifikuese për stafin, anëtarët ose partnerët tuaj, a keni kërkuar lejen e tyre dhe a kanë konsideruar ata ndonjë rrezik të mundshëm? Pyetjet e tilla janë veçanërisht të rëndësishme nëse parlamenti juaj angazhohet publikisht me qytetarët nëpërmjet mediave sociale ose online portaleve të ngjashme për angazhim publik.

Përveç zhvillimit të politikës suaj dhe marrëveshjes së qartë me stafin, sigurohuni që të konfiguroni siç duhet cilësimet e privatësisë dhe sigurisë (shpesh të referuara si "siguri"). Disa pyetje kyçe për t'i bërë vetes ndërsa vendosni se cilat cilësime të privatësisë dhe sigurisë kanë më shumë kuptim për llogaritë parlamentare dhe personale, përfshijnë:

- A doni t'i ndani postimet tuaja me publikun, apo vetëm me një grup të caktuar njerëzish brenda apo jashtë?
- A duhet dikush të jetë në gjendje të komentojë, të përgjigjet ose të ndërveprojë me mesazhet ose postimet tuaja?
- A duhet persona të ndryshëm të jenë në gjendje t'ju gjejnë duke përdorur adresën tuaj të postës elektronike ose numrin e telefonit (personal ose të punës)?
- A doni që vendndodhja juaj të ndahet automatikisht kur postoni?
- A doni të bllokoni apo të heshtni llogaritë armiqësore?
- A doni të bllokoni fjalë ose hashtag specifike?

Çdo faqe e mediave sociale do të ketë cilësime të ndryshme të privatësisë dhe sigurisë, por këto koncepte të përgjithshme zbatohen në mënyrë universale. Ndërsa shqyrtoni këto pyetje, përfitoni nga udhëzuesit e dobishëm të privatësisë nga platformat kryesore: **Facebook**, **Twitter**, **Instagram** dhe **YouTube**. Për Facebook në veçanti, jini të kujdesshëm në lidhje me zgjedhjet tuaja të privatësisë në lidhje me Grupet. Grupet e Facebook-ut janë një vend i njohur për angazhim, avokim dhe shkëmbim informacioni, por në grupet e pakufizuara mund të bashkëngjitet kushdo. Nuk është e pazakontë që llogaritë "e rreme" të paraqiten si njerëz të vërtetë në përpjekje që të depërtojnë në grupe apo faqe private të mediave sociale. Prandaj, pranoni me kujdes kërkesat për "miqësi" dhe "ndjekje". Mos harroni se llogaritë e mediave sociale të parlamentit tuaj janë po aq të sigurta sa llogaritë e "lidhura" me të. Kjo është veçanërisht e rëndësishme të mbahet mend për Facebook-un, ku faqet mund të menaxhohen nga llogaria personale e lidhur e dikujt.

NGACMIMI NË INTERNET

Fatkeqësisht, shumë parlamente dhe grupe të lidhura përballen me ngacmime të konsiderueshme në internet, veçanërisht në mediat sociale. Ngacmimet e tilla shpesh drejtohet me intensitet edhe më të madh ndaj grave dhe popullatave të margjinalizuara. Dhuna në internet kundër grave në veçanti mund të krijojë një mjedis armiqësor që çon në autocensurë ose tërheqje nga diskursi politik ose qytetar. Siç është identifikuar nga raporti i ekipit të NDI-së për Gjini, Gra dhe Demokraci **Tweets That Chill**, kur sulmet kundër grave aktive politike kanalizohen në internet, shtrirja e gjerë e mediave sociale mund të zmadhojë efektin e ngacmimit dhe abuzimit psikologjik, duke minuar ndjenjën e sigurisë personale të grave në mënyra që nuk përjetohen nga burrat.

Derisa parlamenti juaj zhvillon politikën e mediave sociale, është e rëndësishme të jeni të vetëdijshëm për këto dinamika. Në planin tuaj të sigurisë duhet të ndërtoni mbështetje të strukturuar për anëtarët dhe stafin që përballen me mesazhe negative, fyerje dhe kërcënime në mediat sociale, si pjesë e punës së tyre ashtu edhe në jetën e tyre personale. Zhvilloni infrastrukturë kundër ngacmimit brenda parlamentit, përfshirë anketimin e stafit tuaj për të kuptuar se si ngacmimi në internet ndikon tek ata dhe krijoni ekip për reagim të shpejtë për të ndihmuar stafin që të përballet me situata sfiduese. **Doracaku i ngacmimit në teren në internet** nga PEN America ofron rekomandime të hollësishme se si mund të mbështesni stafin që përballet me ngacmime të tilla. Mund të konsideroni opsionin, sigurisht që nëse stafi juaj është i gatshëm të veprojë në këtë mënyrë, për **raportim të incidenteve** të ngacmimeve dhe/ose llogarive problematike gjithashtu edhe direkt në platforma.

Kur angazhoheni me anëtarë ose staf që kanë qenë viktimë të ngacmimeve në internet (dhe në botën fizike gjithashtu), është e rëndësishme të jeni të kujdesshëm. Siç është përshkruar nga Programi për të Drejtat e Grave të Shoqatës për Komunikim Progresiv **Take Back the Tech**, kuptoni se personi që ka kaluar përvojë të tillë mund të jetë duke u përballur me traumë dhe pranoni se dhuna, online ose offline, nuk është kurrë faji i të mbijetuarit. Sigurohuni që çështje të tilla të mund të ngrihen dhe diskutohen (nëse stafi është i gatshëm ta bëjë këtë) në një mjedis të fshehtë dhe të sigurt, me opsion për anonimitet. Dhe përfshini në planin e sigurisë të parlamentit tuaj një listë të profesionistëve, organizatave dhe agjencive të zbatimit të ligjit të vendit me të cilët mund të lidhni stafin për ndihmë ligjore, mjekësore, mendore dhe teknike nëse është e nevojshme. Për ide shtesë, kontrolloni **Udhëzuesin e Sigurisë në internet** nga Feminist Frequency.

Mbani faqet tuaja të internetit Online

Përveç mbrojtjes së aftësisë suaj për të hyrë në internet në mënyrë të sigurt, është gjithashtu e rëndësishme të bëni atë që mundeni për të siguruar që edhe të tjerët të mund të hyjnë në faqet e internetit të parlamentit tuaj ose në pronat e internetit. Për faqet e mediave sociale, kjo nënkupton mbrojtjen e atyre llogarive me fjalëkalime të forta, unike dhe vërtetim me dy faktorë. Për faqen tuaj të internetit, kjo do të thotë ta mbroni atë kundër sulmeve të hakimit dhe mohimit të shërbimit. Sulmet e Shpërndara të Mohimit të Shërbimit (DDoS) paraqesin sulme të një grupi të madh kompjuterësh që njëkohësisht mbytin serverin tuaj në trafik me qëllim të keq. Disa opsione për mbrojtjen DDoS - gjë që e bën shumë më të vështirë për një kundërshtar që të heqë faqen tuaj të internetit - përfshinë **Cloudflare**, **AWS Shield** nga Amazon-i ose shërbimi **Deflect** nga eQualitie.

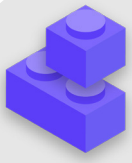
Nivel i avancuar: Hostimi i sigurt i faqes së internetit të Parlamentit tuaj

Uebsajtet strehohen në kompjuterë - dhe ato janë të cenueshme ndaj hakerimit ashtu si edhe pajisjet tuaja. Nëse është e mundur, parlamenti juaj duhet të shfrytëzojë nga shërbimet ekzistuese të hostimit si WordPress, Wix ose të tjera që menaxhojnë të gjithë sigurinë e faqes për ju. Nëse nevojat e faqes suaj të internetit janë më të ndërlikuara dhe/ose ju duhet ta organizoni vetë faqen tuaj të internetit, atëherë sigurohuni që të përqendroheni në mbajtjen e përditësuar të sistemit tuaj operativ dhe softuerit të mbajtjes së faqes në internet, ashtu si do të bëni për kompjuterin tuaj personal. Konsideroni përdorimin e ofruesve të mirë-vendosur të hostimit në Re kompjuterike siç janë Shërbimet e Uebit të Amazon-it (AWS), Microsoft Azure, ose **eclips.is** nga Greenhost, që ofrojnë mundësi të zgjeruara sigurie për faqet e internetit të hostuara. Pavarësisht nga mjetet që përdorni për të hostuar faqen e internetit, sigurohuni që çdo llogari e përdorur për të qasur cilësimet e modifikimit dhe konfigurimit të përmbajtjes është e mbrojtur me fjalëkalime të forta dhe vërtetim me dy faktorë.

Nëse parlamenti juaj ka njohuri teknike për të organizuar uebsajtin e vet, ju duhet të konsideroni zgjedhjen e një të ashtuquajture “faqe statike” ose faqe interneti të sheshtë. Në krahasim me faqet e internetit dinamike, këto lloj faqesh zvogëlojnë sipërfaqen e sulmit për hakerët dhe do ta bëjnë faqen tuaj më rezistente ndaj sulmeve.

Mbroni rrjetin tuaj WiFi

Të gjithë këta hapa për të mbrojtur trafikun e internetit nga mbikëqyrja dhe censura janë të rëndësishme, por ato nuk janë zëvendësim për sigurinë bazë të rrjetit në parlament dhe në shtëpi. Mos harroni bazat si përdorimi i një fjalëkalimi të fortë (jo fjalëkalimi të parazgjedhur) në ruterët tuaj për Wi-Fi, duke siguruar që vetëm përdoruesit e autorizuar të kenë qasje në rrjetin tuaj, duke ndryshuar shpesh fjalëkalimin, dhe duke aktivizuar mbrojtjen e integruar (fire-wall) të ruterëve tuaj pa tel. Gjithashtu konsideroni krijimin e një rrjeti për mysafirë në hapësirat e parlamentit nëse keni vizitorë që hyjnë dhe dalin nga ndërtesa dhe që përdorin internetin.



Blloqet e ndërtimit të planit të sigurisë: Qëndroni të sigurt në internet

- **Zhvilloni trajnime të rregullta për anëtarët dhe stafin mbi rëndësinë e ndjekjes së masave bazë të sigurisë në internet.**
- **Përkujtoni stafit që të shfletojë gjithmonë me HTTPS dhe DNS të enkriptuar.**
- **Kërkoni nga stafi që të rinisin rregullisht shfletuesit e tyre për të instaluar përditësime.**
- **Inkurajoni përdorimin e shfletuesve dhe shtesave për mbrojtjen e privatësisë.**
- **Nëse ndonjë VPN është e përshtatshme, zgjidhni një me reputacion, trajnoni stafin për ta përdorur dhe sigurohuni që të përdoret vazhdimisht.**
- **Zhvilloni dhe shpërndani politikë të qartë parlamentare për përdorimin e mediave sociale.**
- **Aktivizoni cilësimet e privatësisë dhe sigurisë në të gjitha llogaritë e mediave sociale.**
- **Kuptoni ndikimet e ngacmimit në internet dhe jini të përgatitur për të mbështetur anëtarët dhe stafin që preken nga to.**
- **Përpiloni një listë të profesionistëve, organizatave dhe agjencive të zbatimit të ligjit nga vendi, që të mund të lidhni anëtarët dhe stafin për asistencë ligjore, shëndetësore mendore dhe teknike në përgjigje të ngacmimeve në internet.**
- **Regjistrohuni për mbrojtjen DDOS për faqet tuaja të internetit.**
- **Përdorni ofrues të besueshëm të hostimit në ueb.**
- **Përdorni fjalëkalim të fortë dhe Wi-Fi rrjet për mysafirë në hapësirat tuaja.**

Mbrojtja e sigurisë fizike

Është thelbësore t'i mbani pajisjet tuaja të sigurta fizikisht. Mbani në mend se siguria fizike shkon përtej pajisjeve dhe duhet të përfshijë strategji për të mbrojtur gjithçka tjetër në botën tuaj. Kjo përfshin dokumente të shtypura; zyrat e parlamentit tuaj; dhomat, ose hapësirat e punës; dhe sigurisht ju, stafi juaj dhe anëtarët e parlamentit.

Siguria fizike dhe parlamenti

Fatkeqësisht, sulmet fizike ndaj parlamenteve dhe organeve të tjera legjislative nuk janë të pazakonta, dhe shpesh kanë implikime të rëndësishme si për sigurinë fizike ashtu edhe për atë të informacioneve. Më 6 janar 2021, kryengritës sulmuan ndërtesën e Kapitolit të Shteteve të Bashkuara - shtëpia e të dy dhomave të legjislaturës amerikane - në një përpjekje për të ndaluar certifikimin e rezultateve të zgjedhjeve presidenciale.

Sulmi fizik tragjikisht shkaktoi pesë vdekje si dhe shqetësime të konsiderueshme psikologjike për anëtarët dhe stafin e Kongresit. Megjithatë, ky nuk ishte ndikimi i vetëm negativ. Sulmuesit shkatërruan gjithashtu pajisjet e TI-së, fituan qasje në materiale të ndjeshme në zyrat e anëtarëve dhe ndoshta më e dëmshmja, vodhën kompjuterë dhe pajisje tjera me informacione potencialisht konfidenciale nga Kapitoli i SHBA.

Nivel i avancuar: Hapësira të dedikuara për informacione të ndjeshme (SCIF-et)

Për të zhvilluar biseda shumë të ndjeshme, disa parlamente kanë siguruar dhoma fizike të quajtura SCIF. Këto hapësira janë krijuar në mënyrë që informacionet e ndjeshme, si çështjet që lidhen me sigurinë kombëtare ose inteligjencën, të mund të shikohen dhe diskutohen midis deputetëve dhe stafit të tyre pa shqetësimin e mbikëqyrjes ose spiunimit nga jashtë. Përveç ndërtimit përkatës fizik, një SCIF i duhur kërkon që njerëzit të lënë pajisjet (si celularët e tyre) jashtë dhomës përpara se të hyjnë për të diskutuar.

Mbrojtja e aseteve fizike

Një komponent thelbësor i sigurisë së informacionit është siguria fizike e pajisjeve tuaja. Përveç zbutjes së ndikimit të një pajisjeje të vjedhur duke përdorur ekranet e kyçjes dhe fjalëkalimet, zbatimin e enkriptimit të plotë të diskut dhe aktivizimin e veçorive të fshirjes në distancë, gjithashtu, fillimisht duhet të konsideroni se si t'i ruani ato pajisje nga vjedhja. Për ta bërë vjedhjen më të vështirë, sigurohuni që të instaloni bravë të fortë (dhe t'i ndërroni sa herë që ndryshon stafi) në hapësirat e parlamentit dhe/ose në shtëpi. Përveç kësaj, merrni parasysh blerjen e një kasaforte laptopi ose një kabineti të kyçur për t'i mbajtur pajisjet të mbrojtura gjatë natës. Kamerat e sigurisë ose sistemet e sensorëve të lëvizjes rreth ambienteve mund të zbulojnë, dhe shpresojmë, të parandalojnë thyerjet fizike dhe vjedhjet. Kërkoni opsione në vendin tuaj që **respektojnë privatësinë**, dhe sigurohuni që të zgjidhni kamerat dhe sistemet e sigurisë të ofruara nga kompani të besuara që nuk kanë nxitje për t'i dorëzuar të dhënat dhe informacionet tek ndonjë kundërshtari të mundshëm.

Nëse pajisjet e vjetra kanë ende informacione të ruajtura në to, por nuk janë më në përdorim, merrni parasysh fshirjen e tyre – **ky udhëzues** nga Wirecutter është burim i shkëlqyer se si ta bëni këtë për shumicën e pajisjeve moderne. Nëse fshirja e pajisjeve tuaja nuk është e mundur, mund t'i shkatërroni ato fizikisht. Mënyra më e lehtë, edhe pse jo më e ndjeshme ndaj mjedisit jetësor, është prishja e pajisjeve dhe disqeve të tyre me çekiç. Ndonjëherë zgjidhjet më të vjetra vazhdojnë të funksionojnë më së miri!

Edhe përpara se të bëni këto hapa teknikë, përpiloni një inventar të të gjitha pajisjeve në të gjithë parlamentin. Pa listë të të gjitha pajisjeve, është shumë më vështirë të mbani gjurmët e asaj që mund të mungojë nëse ju vidhet.

ÇFARË TË BËJMË ME GJITHË KËTË LETËR?

Ka shumë gjasa që parlamenti juaj të ketë shumë informacione të shtypura në letër, të shkruara në fletore ose të shkarravitura në fletëza Post-it. Disa nga këto mund të jenë shumë të ndjeshme - shënime nga dëshmitë konfidenciale ose takime private, për shembull. Është thelbësore të mendoni edhe për sigurinë e këtyre informacioneve. Nëse domosdoërisht ju duhet të ruani kopje të forta të informacionit të ndjeshëm, sigurohuni që ai të ruhet në mënyrë të sigurt në një dollap të mbyllur ose në ndonjë vend tjetër të sigurt. Mos mbani asnjë informacion privat ose delikat (përfshirë fjalëkalimet) të vendosura në tavolinë ose të shkruar në tabelë të bardhë.

Mbani informacionet shumë të ndjeshme në vend më pak të synuar dhe mirë të mbrojtur.

Përpiquni, aq sa të jetë e mundur, të hidhni informacionin e panevojshëm të printuar. Mos harroni: nëse nuk e keni, nuk mund të vidhet. Vendosni një politikë parlamentare në lidhje me pronësinë e shënimeve të shtypura dhe sigurohuni që të merrni çdo shënim letre nga stafi nëse ata vendosin të largohen ose lirohen nga organizata, ashtu si do të merrnit një kompjuter ose telefon të lëshuar nga parlamenti. Për të hequr qafe letrën e ndjeshme, blini një grirës cilësor. Një aktivitet argëtues i fundjavës mund të jetë marrja e një pushimi 15-minutësh me ekipet tuaja për të copëtuar çdo mbetje, printime të ndjeshme ose shënime nga java e kaluar.

POLITIKA E ZYRËS PARLAMENTARE

Edhe pse për shumicën, realitetet e "zyrës" kanë ndryshuar ndjeshëm që nga fillimi i pandemisë COVID-19, ende është e rëndësishme që parlamenti juaj të vendosë një politikë të qartë në lidhje me qasjen në hapësirat e juaja. Një politikë e tillë duhet të adresojë çështjet kryesore, përfshirë se kush lejohet brenda hapësirave parlamentare (dhe kur), kush mund të hyjë në burimet e zyrës (si Wi-Fi rrjeti) dhe si veprohet me mysafirët.

Një pyetje e thjeshtë por e rëndësishme për t'iu përgjigjur është se kush merr çelës zyre ose një distinktiv qasjeje. Vetëm personeli i besuar duhet të ketë çelësa ose distinktivë dhe bravat duhet të ndërrohen kur stafi largohet dhe/ose në mënyrë gjysmë të rregullt. Gjatë ditës, çdo derë që lihet e hapur duhet të jetë vazhdimisht në sy të dikujt të besuar dhe/ose një roje sigurie. Për më tepër, sigurohuni që parlamenti juaj të ketë një marrëdhënie të besueshme me ofruesit e shërbimeve si p.sh. personeli i pastrimit dhe teknikët e jashtëm që kanë qasje në ambientet. Mendoni se në çfarë informacioni ose pajisjesh mund të kenë qasje njerëzit e tillë dhe sigurohuni që të jenë të mbrojtura, veçanërisht nëse nuk keni besim të mjaftueshëm në ta. Kushdo që ka qasje, gjithmonë duhet të caktohen persona të besuar për të mbyllur zyrat dhe ndërtesat dhe për të siguruar që pajisjet të jenë të siguruara siç duhet, përpara se të largohen në fund të ditës.

A lejohen zgjedhësit brenda parlamentit tuaj? Ndoshta publiku ka të drejtë të hyjë në një pjesë të ambienteve të parlamentit? Nëse po, sigurohuni që ata të mos kenë qasje (ose të paktën qasje të pambikëqyrur) në pajisje ose

të dhëna të ndjeshme të kopjuara. Nëse është një kërkesë ose pritshmëri që publiku ose të ftuarit që vizitojnë të kenë qasje në internet kur ata vizitojnë, ju duhet të krijoni një rrjet "për mysafirë" në mënyrë që të ftuarit e tillë të mos kenë aftësinë për të monitoruar trafikun tuaj të rregullt. Në përgjithësi, vetëm personeli i besuar duhet të jetë në gjendje të qas rrjetin dhe pajisjet e rrjetit si printerët. Zakonisht është gjithashtu ide e mirë të kërkohet regjistrimi i mysafirëve që të keni regjistër se kush ka vizituar parlamentin.

Derisa zhvilloni një politikë zyre, qëllimi duhet të jetë të lejoni vetëm personat e besuar të kenë qasje në pajisjet, dokumentet, hapësirat dhe sistemet e ndjeshme.

STAFI DHE VULLNETARËT MBËSHTETËS

Kërcënimet e sigurisë fizike ndaj parlamentit tuaj mund të ndikojnë edhe në stafin tuaj. Ngjashëm me ngacmimet në mediat sociale, këto kërcënime të sigurisë fizike shpesh ndikojnë në mënyrë disproporcionale te gratë dhe komunitetet e margjinalizuara. Nuk bëhet fjalë vetëm për xhama të thyer dhe laptopë të vjedhur. Frikësimi, kërcënimet ose rastet e dhunës fizike ose seksuale, abuzimi në familje dhe frika nga sulmi mund të kenë ndikim serioz negativ në jetën e anëtarëve dhe stafit. Mjeti i NDI-së për planifikim të sigurisë **#Think10** është burim i dobishëm për t'u ofruar grave politikisht aktive të cilat mund të jenë në rrezik të rritur personal si rezultat i pjesëmarrjes së tyre në parlament dhe politikë në përgjithësi.

Mirëqenia e stafit është padyshim një aset i rëndësishëm për ta si individë, por gjithashtu edhe element thelbësor për një parlament të shëndetshëm dhe mirë-funksional. Për këtë qëllim, merrni parasysh se çfarë burimesh shtesë mund t'i siguroni stafit për t'i mbajtur ata të mbrojtur dhe, në rast sulmi fizik ose digjital, t'i ndihmoni të rikuperohen. Siç u përmend më herët në Doracak, kjo do të thotë minimalisht të përpiloni një listë burimesh me të cilat mund të lidhni stafin për ndihmë ligjore, mjekësore, mendore dhe teknike nëse është e nevojshme. Përsëri, **Doracaku praktik i ngacmimit në internet** nga PEN America përfshin ide se si organizatat mund të mbështesin stafin gjatë dhe pas krizave.

SIGURIA GJATË UDHËTIMIT

Udhëtimi - qoftë në një vend tjetër, në qytet, në rrugë - shpesh intensifikon rreziqet fizike të sigurisë së informacionit. Në përgjithësi është e sigurt të supozohet se ju dhe pajisjet tuaja nuk keni të drejta privatësie kur kaloni kufij. Andaj, është ide e mirë të përfshini një politikë parlamentare të udhëtimit në planin tuaj të sigurisë, i cili do të përfshijë përkujtues për praktikat më të mira kryesore të sigurisë.

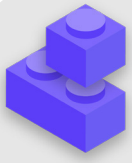
Politika e udhëtimit e parlamentit tuaj duhet të përfshijë shumë informacione të mbuluara në pjesët tjera të Doracakut, përfshirë përdorimin e sigurt të internetit dhe mbajtjen e pajisjeve dhe burimeve të tjera të informacionit fizikisht të sigurta dhe me vete gjatë gjithë kohës kur udhëtoni. Nëse është e mundur, lini pas informacionet tuaja të ndjeshme dhe thjesht përdorni një kompjuter të papërdorur e të fshirë, hyni në skedarët që ju nevojiten domosdomërisht nga retë dhe më pas fshijini kur të ktheheni në shtëpi përsëri. Përveç përgatitjes për udhëtime dhe minimizimit të të dhënave të shpërndara kur udhëtoni, ka disa këshilla thelbësore operacionale që duhet t'i mendoni dhe t'i përfshini në politikën parlamentare të udhëtimit.

Merrni parasysh përdorimin e laptopëve ose telefonave specifikë të udhëtimit që kanë pak ose aspak të dhëna të ndjeshme të ruajtura në to. Nëse shumica e punës së parlamentit tuaj kryhet në renë kompjuterike, një Chromebook relativisht i lirë mund të jetë opsion i mirë për pajisje të tillë. Rivendosni në gjendje fabrike ose "fshijini" këto pajisje pas kthimit të tyre përpara se të lidheni me Wi-Fi rrjetet e zakonshme në shtëpi ose në zyrë.Jepni personelit informacionin e kontaktit dhe plan veprimi për atë që duhet të bëjnë nëse diçka nuk shkon sipas planit në udhëtimin e tyre. Kjo përfshin informacione për spitalet, klinikat ose farmacitë lokale nëse kanë nevojë për ndihmë mjekësore gjatë udhëtimit.

Stafi gjithashtu duhet të mbajë të gjitha pajisjet me vete gjatë udhëtimit. Për shembull, mbajeni laptopin pranë këmbëve tuaja (jo në pjesën e sipërme ose në bagazhin e kontrolluar) kur jeni në autobus, tren ose aeroplan. Mos supozoni se dhoma e hotelit – apo edhe kasaforta e hotelit – është një "vend i sigurt" për të mbajtur pajisje dhe sende të ndjeshme. Mos u besoni portave publike të USB karikimit. Portat e USB karikimit në aeroporte, stacione dhe automjete bëhen një pamje gjithnjë e më e zakonshme dhe një mënyrë shumë e përshtatshme për të mbushur pajisjet. Megjithatë, mund të jenë një vektor i lehtë për marrjen e softuerëve keqdashës. Pra, sigurohuni që, ose të karikoni pajisjet në mënyrën tradicionale nëpërmjet një prize në mur, ose të blini **bllokues të të dhënave USB** për të lejuar personelin udhëtues të karikojë në mënyrë të sigurt pajisjet e tyre nëpërmjet USB-së.

Nivel i avancuar: Rezervoni udhëtime të sigurta për parlamentin tuaj

Kur hartoni një politikë udhëtimi, mbani në mend se çfarë informacioni mund të ekspozohet kur organizoni ose rezervoni ndonjë udhëtim. Kjo mund të jetë veçanërisht e rëndësishme nëse organizoni ngjarje ose konferenca të mëdha për të cilat trajtoni informacione të ndjeshme nga një shumëllojshmëri stafi, anëtarësh ose pjesëmarrësish. Mendoni me kujdes se si do të ndani dhe ruani në mënyrë të sigurt (nëse nevojitet) informacionet personale, siç janë detajet e pasaportës, itineraret e udhëtimit dhe të dhënat mjekësore.



Blloqet e ndërtimit të planit të sigurisë: Mbrojtja e sigurisë tuaj fizike

- **Kujtojuni anëtarëve dhe stafit që t'i mbajnë pajisjet të mbrojtura fizikisht gjatë gjithë kohës.**
- **Kontrolloni dhe siguroni të gjitha mënyrat se si njerëzit mund të hyjnë në ambientet tuaja.**
- **Zhvilloni politikë për mysafirë dhe për qasje.**
- **Përdorni bravë të fortë, sisteme ID/distinktivë dhe ndërroni/ndryshojini kur nevojitet.**
- **Merrni parasysh konfigurimin e kamerave ose sistemeve të tjera të sigurisë brenda objektit.**
- **Mbani dhe përdorni grirëse letre.**
  - Vendosni kohën e paraparë të stafit për të asgjësuar dokumentet e shtypura që përmbajnë informacione të ndjeshme.
- **Përpiloni listë profesionistësh, organizatash dhe agjencish të zbatimit të ligjit me të cilët mund të lidhni anëtarët dhe stafin për ndihmë ligjore, mjekësore dhe shëndetësore mendore në përgjigje të sulmeve fizike ose kërcënimeve.**
- **Zhvilloni politike parlamentare të udhëtimit.**
- **Sigurohuni që stafi të dijë se çfarë të bëjë në rast urgjence gjatë udhëtimit**
- **Kini parasysh të dhënat shtesë që krijohen dhe ndahen kur organizoni udhëtime ose ngjarje.**

Çfarë të bëni kur gjërat shkojnë keq

Pra, ju i dini gjërat e duhura që duhen bërë. Keni vendosur politikat dhe keni trajnuar të gjithë në parlament për të gjitha praktikat më të mira. Edhe me gjithë këtë punë të vështirë, ka shumë gjasa që përfundimisht diçka të shkojë keq. Gjërat ndodhin. Kur ndodhin, është thelbësore që të ketë një plan reagimi ndaj incidentit. Përgjigjja ndaj incidentit është pjesë thelbësore, dhe shpesh e nënvlerësuar, e planit të sigurisë së parlamentit tuaj, sepse mund të paraqesë dallimin midis një sulmi që shkatërron reputacionin tuaj ose thjeshtë një përplasje e pakëndshme në rrugë.

Mbani në mend se mund t'i përgjigjeni një incidenti vetëm nëse dini për të. Është shumë e rëndësishme të keni kulturë të fortë sigurie dhe të inkurajoni anëtarët dhe stafin për të raportuar problemet. Kjo është arsyeja pse është më mirë të shpërbleni sjelljen e mirë të sigurisë sesa të ndëshkoni gabimet ose gabimet e sigurisë. Është gjithashtu e rëndësishme të shprehni ndjeshmëri dhe të kontrolloni mirëqenien e stafit kur ata raportojnë ndonjë incident. Ju dëshironi që stafi të raportojë menjëherë një lidhje të klikuar në një mesazh phishing, telefon të vjedhur ose llogari të hakuar të mediave sociale – të mos hezitojnë nga frika e ndëshkimit ose mungesës së mbështetjes. Në fund të fundit, reagimi ndaj incidentit, ashtu si strategjitë zbutëse të përmendura në pjesët tjera të Doracakut, është një përpjekje e gjerë parlamentare.

Çfarë duhet të planifikoni? Me pak fjalë, çdo gjë që ka disi gjasa të ndodhë. Kjo do të jetë e ndryshme për çdo parlament, por pyetjet e zakonshme që plani i reagimit ndaj incidentit do të ndihmojë t'i përgjigjet përfshijnë:

- Çfarë të bëjmë nëse llogaritë ose faqet tona të internetit hakohen?
- Çfarë të bëjmë nëse dikush klikon në postë elektronike phishing ose nëse një pajisje vepron në mënyrë të dyshimtë?
- Çfarë bëjmë nëse postat tona elektronike ose dokumentet më të ndjeshme vidhen dhe zbulohen?
- Çfarë të bëjmë nëse një nga stafi ynë vihet në rrezik fizik? Apo po lufton me stres dhe ankth për shkak të kërcënimeve të tilla?
- Çfarë të bëjmë nëse zyra jonë dëmtohet nga zjarri, përmbytja ose fatkeqësia natyrore?
- Çfarë bëjmë nëse kompjuteri ose telefoni i një anëtari humbet ose vidhet?

Përgjigjet e këtyre pyetjeve dhe të pyetjeve tjerave do të ndryshojnë nga parlamenti në parlament, por është e rëndësishme t'i mendojmë së bashku dhe të artikulojmë dhe ndajmë qartë një plan në mënyrë që të gjithë të jenë të përgatitur që të ndërmarrin veprime menjëherë për të kufizuar dëmin.

Duke huazuar nga **Udhëzuesi Holistik** i Sigurisë, i Tactical Tech, vend i mirë për të filluar me një plan reagimi ndaj incidentit është **përkufizimi i incidentit ose emergjencës** në kontekstin e parlamentit tuaj. Vendosni se çfarë është një "emergjencë" - d.m.th., pika në të cilën duhet të fillojmë të zbatojmë aktivitetet dhe masat e planifikuara për situatat e paparashikuara. Kjo është e rëndësishme pasi ndonjëherë do të jetë e paqartë – nëse imagjinoni një skenar si humbja e kontaktit me ndonjë koleg në mision në terren; sa kohë do të prisnit përpara se të shpallni emergjencë? Dikush nuk dëshiron të alarmon shumë herët, por të presësh shumë gjatë në disa rrethana mund të jetë katastrofike.

Është gjithashtu e rëndësishme të mendoni edhe për çdo hap të **operacionit**. Çdo personi caktojini një rol të qartë për të cilin janë të vetëdijshëm dhe kanë rënë dakord paraprakisht - kjo do të reduktojë çorganizimin dhe panikun në rast të incidentit. Në çfarëdo rast kërcënimi, merrni parasysh rolet e ndryshme që mund t'ju duhet të merrni dhe praktikat e përfshira në reagimin ndaj një emergjence. Brenda kësaj strategjie të rëndësishme për emergjencat është aktivizimi i një rrjeti mbështetës – një rrjet i gjerë aleatësh, i cili mund të përfshijë degë të ndryshme të qeverisë suaj, qeveri të tjera miqësore, kompani teknologjike, shitës sigurie dhe institucione shumëpalëshe. Si mund t'ju mbështesin aleatët tuaj? A duhet t'i kontaktoni paraprakisht për të verifikuar se ata do të jenë të gatshëm t'ju ndihmojnë në rast urgjence dhe t'i tregoni se çfarë prisni prej tyre?

Kur reagoni ndaj një incidenti, **komunikimi** efektiv bëhet gjithnjë e më i rëndësishëm. Vendosni se cili është mjeti më i sigurt dhe efektiv i komunikimit me secilin aktor në skenarë të ndryshëm dhe identifikoni mjet rezervë. Kini parasysh se për raste urgjente, mund të jetë e dobishme të keni udhëzime të qarta se çfarë duhet (dhe çfarë nuk duhet) të komunikoni, kur të komunikoni, cilat kanale të përdorni për të komunikuar dhe me kë duhet të komunikoni. Gjithashtu, merrni parasysh ndikimin e reputacionit të një incidenti në parlamentin tuaj dhe përgatituni të përgjigjeni në përputhje me rrethanat. Sigurohuni që drejtuesi i komunikimit i parlamentit është i vetëdijshëm për incidentin dhe mund të shikojë mediat sociale ose media të tjera për ndikim të mundshëm. Ata gjithashtu duhet të jenë të përgatitur të zhvillojnë hetime të mundshme publike ose media në lidhje me ndonjë incident, nëse është e rëndësishme. Kjo është veçanërisht e rëndësishme për të dalë përpara çdo historie të mundshme negative ose dëmtimi të reputacionit. Ndërsa çdo incident dhe kontekst është i ndryshëm, komunikimet e ndershme dhe transparente shpesh ndihmojnë në ndërtimin e besimit pas një incidenti.

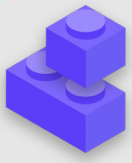
Nivel i avancuar: Krijimi i një sistemi të paralajmërimit dhe reagimit të hershëm

Konsideroni krijimin e një sistemi të paralajmërimit dhe reagimit të hershëm. Një sistem i tillë tingëllon si mjaft i ndërlikuar, por në thelb është thjesht një dokument i centralizuar (elektronik ose ndryshe) që duhet hapur në rast emergjence. Në dokument, duhet të regjistroni të gjitha detajet në lidhje me treguesit e sigurisë dhe incidentet që kanë ndodhur në një afat kohor, të jepni një përshkrim të qartë të veprimeve dhe sekuencës për reagimin e planifikuar dhe të tregoni se çfarë duhet të arrihet për të zvogëluar rrezikun. Gjithashtu duhet të përfshijë veprimet që duhet të ndërmerren pas një incidenti, në mënyrë që të mbrohen personat e përfshirë nga dëmtimi i mëtejshëm dhe t'i ndihmojë ata të shërohen fizikisht dhe emocionalisht. Një sistem alarmi dhe reagimi i hershëm mund të sigurojë dokumentacion të dobishëm për shpërndarje me organet e zbatimit të ligjit (nëse është e zbatueshme), analiza të mëvonshme të asaj që ka ndodhur dhe udhëzime se si të përmirësoni taktikat tuaja parandaluese dhe përgjigjet ndaj kërcënimeve në të ardhmen.

veç këtyre koncepteve të rëndësishme të reagimit ndaj incidenteve, parlamenti juaj duhet të përgatitet gjithashtu për çdo përgjigje teknike specifike. Në disa raste, një përgjigje teknike mund të menaxhohet nga stafi i brendshëm i TI-së ose administratorët e sistemit. Për shembull, nëse një llogari poste elektronike duket se është hakuar, administratori i llogarisë duhet të jetë i përgatitur dhe në gjendje të mbyllë ose çaktivizojë llogarinë e ndikuar. Megjithatë, disa incidente teknike mund të kërkojnë ekspertizë që ju nuk e keni brenda parlamentit tuaj. Për situata të tilla, është e rëndësishme të përpiloni listë të besuar të ekspertëve teknikë të jashtëm, të cilët mund t'ju ndihmojnë në reagimin tuaj ndaj incidentit. Në disa raste, mund të dëshironi të negocioni paraprakisht kushtet me ofruesit e shërbimeve (si p.sh. hosti i faqes suaj të internetit ose ndonjë firmë sigurie TI) për t'u siguruar që ata janë në dispozicion (dhe nuk do të kërkojnë pagesë shtesë) për një përgjigje të tillë gjatë ndonjë incidenti teknik.

E fundit, por sigurisht jo më pak e rëndësishme, është se duhet të keni parasysh hapat ligjorë. Të kuptuarit e mbrojtjeve ligjore që mund të keni, si dhe detyrimet ligjore ose pasojat me të cilat parlamenti juaj mund të përballet si rezultat i një shkeljeje të të dhënave ose incidentit tjetër të sigurisë, është e rëndësishme. Si parlament, jeni në një pozitë të fuqisë dhe rëndësisë së veçantë kur bëhet fjalë për mirëkuptimin dhe respektimin e rregullave lokale të sigurisë së të dhënave dhe të intimitetit. Rishikoni mirë opsionet për incidentet e mundshme me këshilltarin ligjor përkatës nëse është e nevojshme edhe përpiloni plan për atë se si do të vepronit si përgjigje. Ide e mirë është të përgatitni një marrëveshje me këtë këshillë për të përfaqësuar ju dhe interesat tuaja nëse do ishte e nevojshme si pasojë e ndonjë incidenti. Si pjesë e kësaj përgatitjeje ligjore, sigurohuni që të kuptoni detyrimet ligjore të ndonjë shitësi ose partneri. A u kërkohet t'ju njoftojnë në rastin e shkeljes së të dhënave të tyre? Çfarë mbështetje (nëse ka) u kërkohet atyre që t'ju ofrojnë në rastin e një incidenti? Ndërsa zhvilloni kontrata dhe marrëveshje me shitës të jashtëm, kini parasysh mundësinë e shkeljes së të dhënave ose ndonjë incidentit tjetër.

Ndërsa nuk ka një qasje të vetme për përgjigjen ndaj incidentit, është thelbësore të ketë plane të qarta operacionale, komunikuese, teknike dhe ligjore. Ndërsa hartoni planin tuaj të reagimit ndaj incidentit, fuqimisht ju inkurajojmë të përdorni disa burime ekzistuese të shkëlqyera, të krijuara për të ndihmuar organizatat të veprojnë në reagimin ndaj ndonjë incidenti. Edhe pse jo të gjitha këto burime janë krijuar posaçërisht për parlamente, përmbajtja e tyre vazhdon të jetë shumë e rëndësishme. Këto burime përfshijnë **Kompleti i ndihmës së parë digjitale** të zhvilluar nga Rarenet dhe CiviCERT, **Doracaku praktik i ngacmimit në internet** nga PEN America, **Libri i fushatës për sigurinë kibernetike** dhe **Modeli i planit të komunikimit për incidente kibernetike** nga Belfer Center dhe **Linja e ndihmës për sigurinë digjitale** nga Access Now.



Blloqet e ndërtimit të planit të sigurisë: Përgjigjja ndaj incidentit

- **Zhvilloni plan parlamentar për reagim ndaj incidenteve dhe praktikojeni atë.**
  - Mendoni për incidente të mundshme dhe përgatituni për përgjigjen tuaj përpara se të ndodhë.
- **Sigurohuni që të gjithë në parlament të jenë të vetëdijshëm se si do të komunikoni dhe çfarë hapash teknikë do të ndërmerren në rast të një incidenti.**
- **Përdorni kohën e duhur për të kuptuar mbrojtjen dhe detyrimet tuaja ligjore.**
- **Jini të përgatitur për t'u ofruar anëtarëve dhe stafit mbështetjen emocionale dhe sociale që u nevojitet pas një incidenti.**

Shtojca A: Burimet e rekomanduara

- Tactical Tech's Holistic Security Manual ; Creative Commons Attribution-ShareAlike 4.0 International License
  - Chapter 2.4 - Understanding and Cataloguing Our Information
  - Chapter 1.5 - Communicating About Threats in Teams and Organizations
  - Chapter 3.4 - Security in Groups and Organizations
- The Electronic Frontier Foundation's Security Education Companion ; Creative Commons Attribution 3.0 US License
  - Threat Modeling Activity Handout
- Freedom of the Press Foundation's Phishing Prevention and Email Hygiene Guide ; Creative Commons Attribution 4.0 International License
- Freedom of the Press Foundation's Locking Down Signal Guide ; Creative Commons Attribution 4.0 International License
- Electronic Frontier Foundation's Surveillance Self-Defense (SSD) Guide ; Creative Commons Attribution 3.0 US License
  - What Should I Know About Encryption
  - Communicating with Others
  - Choosing the VPN That's Right for You
- Front Line Defenders' Guide to Secure Group Chat and Conferencing Tools
- Tactical Tech's Data Detox Kit
  - Let the Right One In: Make Your Passwords Stronger
  - Strengthen Your Screen Locks
- Center for Democracy & Technology's Elections Security Guide on Passwords ; Creative Commons Attribution 4.0 International License
- Center for Democracy and Technology's Elections Security Guide on Two Factor Authentication ; Creative Commons Attribution 4.0 International License
- Martin Shelton's Two Factor Authentication for Beginners ; Creative Commons Attribution 4.0 International License
- Tactical Tech and Frontline Defender's Security in a Box ; Creative Commons Attribution-ShareAlike 3.0 Unported License
  - Protect your device from malware and phishing attacks
  - Protect against physical threats
- SANS' OUCH! Newsletter: Stop That Malware
- Apple's Device and Data Access When Personal Safety is at Risk
- Global Cyber Alliance Cybersecurity Toolkit for Mission-Based Organizations
- Ford Foundation's Cybersecurity Assessment Tool

Shtojca B: Kompleti fillestar i planit të sigurisë

Përdorni kompletin fillestar të mëposhtëm për të mbajtur shënime ndërsa ju dhe organizata juaj lexoni Doracakun dhe përpunoni materialin dhe merrni parasysh pyetjet shoqëruese me kolegët tuaj për të ndihmuar gjenerimin e diskutimit produktiv. Sigurohuni që t'i referoheni "blloqeve ndërtuese" kryesore në çdo pjesë të Doracakut për t'u siguruar që mbuloni temat e rëndësishme ndërsa ndërtoni planin tuaj të sigurisë. Deri në fund të Doracakut, blloqet e ndërtimit, përgjigjet e këtyre pyetjeve të diskutimit dhe shënimet tuaja duhet të përbëjnë themelin e një plani të suksesshëm sigurie.

Ndërtimi i një kulture sigurie

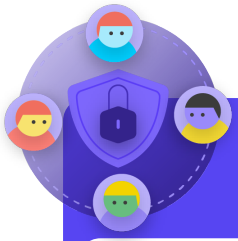
Themel i fortë: Sigurimi i llogarive dhe pajisjeve

Komunikimi dhe ruajtja e të dhënave në mënyrë të sigurt

Qëndroni të sigurt në internet

Mbrojtja e sigurisë fizike

Çfarë të bëni kur gjërat shkojnë keq



Ndërtimi i një kulture sigurie

PYETJE QË DUHET MARRË PARASYSH

- Kur mund të planifikoni një bisedë për të rishikuar planin tuaj të sigurisë me të gjithë organizatën?
- Cilat ditë ose orë ju konvenojnë që organizata të planifikojë biseda të rregullta dhe trajnime rreth sigurisë?
- Çfarë hapash mund të ndërmarrë udhëheqësia për të modeluar sjelljen e mirë të sigurisë dhe përkushtimin ndaj një plani sigurie? Si mund të luajnë të tjerët në organizatë rol në siguri?

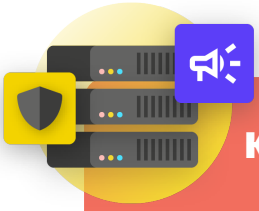
SHËNIMET DHE IDETË TUAJA

Një themel i fortë: Sigurimi i llogarive dhe pajisjeve

PYETJE QË DUHET MARRË PARASYSH

- Si do të zbatoni masat e sigurisë së llogarisë - si një menaxher fjalëkalimi dhe 2FA - në të gjithë organizatën? Çfarë pengesash mund të hasni gjatë zbatimit?
- Si do të sigurojë organizata juaj që pajisjet të mbahen të sigurta dhe të përditësuara? Si pjesë e kësaj, a do t'i duhet organizatës plan për të adresuar softuerët ose kompjuterët pa licenca?
- Kur është koha e duhur për të organizuar trajnime për të gjithë stafin mbi rreziqet e phishing, softuerëve keqdashës dhe praktikat më të mira të sigurisë së pajisjes?

SHËNIMET DHE IDETË TUAJA

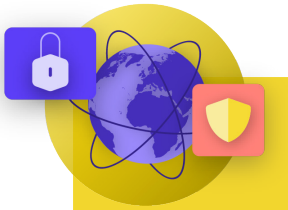


Komunikimi dhe ruajtja e të dhënave në mënyrë të sigurt

PYETJE QË DUHET MARRË PARASYSH

- Si do të zbatojë organizata juaj mesazhe të enkriptuara nga fundi në fund për komunikim të sigurt? Çfarë pengesash mund të hasni gjatë zbatimit?
- Si do të zbatojë organizata juaj një zgjidhje të sigurt për ndarjen e skedarëve si brenda ashtu edhe jashtë? Çfarë pengesash mund të hasni gjatë zbatimit?
- Si do të zbatojë organizata juaj një zgjidhje të sigurt të ruajtjes dhe rezervimit të të dhënave? Çfarë pengesash mund të hasni gjatë zbatimit?

SHËNIMET DHE IDETË TUAJA



Qëndroni të sigurt në internet

PYETJE QË DUHET MARRË PARASYSH

- Si do të zbatojë organizata juaj kërkesat e sigurta të shfletimit si HTTPS, një shfletues i besuar dhe, nëse është e përshtatshme, një VPN për stafin?
- Cilët do të jenë elementët kryesorë të politikës së mediave sociale të organizatës suaj? Si do të zbatohet?
- Si do t'i mbrojë organizata juaj faqet e internetit dhe pronat e saj në ueb?

SHËNIMET DHE IDETË TUAJA

Mbrojtja e sigurisë fizike

PYETJE QË DUHET MARRË PARASYSH

- Si do të shpërndajë dhe zbatojë organizata politikën e saj për mysafirë dhe qasjen në zyrë?
- Kush është përgjegjës për përgatitjen e stafit për sfidat e sigurisë fizike dhe digjitale me të cilat mund të përballen gjatë udhëtimit për punë?
- Çfarë hapash mund të ndërmarrë personeli për t'i mbajtur pajisjet e tyre të sigurta si në zyrë ashtu edhe gjatë udhëtimit?

SHËNIMET DHE IDETË TUAJA

Çfarë duhet të bëni kur gjërat shkojnë keq

PYETJE QË DUHET MARRË PARASYSH

- Si do ta shpërndajë dhe praktikojë organizata politikën e saj të reagimit ndaj incidenteve?
- A ka burime në dispozicion për stafin që mund të ketë nevojë për mbështetje emocionale dhe sociale pas një incidenti? Nëse jo, si mund të jetë në gjendje organizata t'i sigurojë ato burime në rast të një incidenti?

SHËNIMET DHE IDETË TUAJA

Shtojca C: Citimet e imazheve

Faqe 14: New York Times, "Australian Parliament Reports Cyberattack on Its Computer Network", 2019, digital image, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html.
Faqe 18: 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.
Faqe 24: Bleeping Computers, "Norway parliament data stolen in Microsoft Exchange attack", 2021, digital image, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
Faqe 25: 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.
Faqe 27: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Faqe 30: "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.
Faqe 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/.
Faqe 33: ZDNet, "Chinese hacking group impersonates Afghan president to infiltrate government agencies," 2021, digital image, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
Faqe 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Faqe 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.
Faqe 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.
Faqe 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Faqe 49: African News Agency, "Parliament meeting falls victim to hacking as MPs greeted by pornographic images," 2020, digital image, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120
Faqe 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Faqe 52: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Faqe 58: 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/.
Faqe 63: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Faqe 65: 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
Faqe 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Faqe 72: 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


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE