NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Прирачник за сајбер безбедност

за

парламенти

Водич за парламент кој сака да започне со план за сајбер безбедност

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID FROM THE AMERICAN PEOPLE

Прирачник за сајбер безбедност

за

Парламенти

Водич за парламент кој сака да започне план за сајбер безбедност

Содржина

Визуелна легенда

Низ прирачникот, покрај главниот текст, ќе најдете неколку различни повторливи, истакнати елементи. Еве една кратка „легенда“ која ќе ви помогне да ги разберете основните елементи:

Rast studimi

Укажува студии на случај кои го нагласуваат реалниот животен ефект на одредена тема врз парламентите на глобално ниво или во одредена земја

Këshilla shtesë

Истакнува некои дополнителни совети и информации на кои треба да обрнете внимание додека го читате прирачникот

Bota reale

Посочува вообичаени примери на алатки за тактика за сајбер-безбедност што се користат во „реалниот свет“, и за добро и за лошо.

E avancuar

Покажува напредна тема - информации што се важни за вашата организација да ги земе предвид, но тие може да бидат малку потехнички или комплицирани.

Blloqe ndërtimi të planit të sigurisë

Ги означува „Блокови за градење на безбедносниот план“, кои се клучните информации од секој дел од Прирачникот.

Најважните 10

Овие 10 елементи се клучни за планот за безбедност на вашиот парламент. Ако барате од каде да почнете, прво погледнете овде.

1. **Спроведувајте редовна обука за безбедност во вашиот парламент.**
2. **Внимавајте на лажно претставување („фишинг“) и имајте систем за известување.**
3. **Користете шифрирање за целата комуникација – од крај до крај - кога е можно.**
4. **Барајте силни лозинки и поставете апликација за управување со лозинки (password manager) во рамките на вашиот парламент.**
5. **Барајте автентикација со два фактора секогаш кога е можно.**
6. **Погрижете се сите уреди и софтвер на вработените да бидат ажурирани.**
7. **Користете безбедно складирање во облак.**
8. **Користете ХТТПС (HTTPS) и, доколку е соодветно, ВПН (VPN) за пристап на интернет.**
9. **Заштитете ги физичките средства на вашиот парламент.**
10. **Направете организациски план за одговор на инциденти.**

1

Градење култура на безбедност

2

Силна основа: Обезбедување на сметките и на уредите

3

Безбедно комуницирање и складирање податоци

4

Безбедност на интернет

5

Заштита на физичката безбедност

6

Што да направите кога работите ќе тргнат наопаку

Автори и изрази на благодарност

Овој водич е изготвен од Националниот демократски институт (НДИ) и од Комисијата за демократско партнерство на Претставничкиот дом (ХДП).

Главен автор: **Evan Summers (НДИ)**
Придружни автори: **Sarah Moulton (НДИ); Chris Doten (НДИ)**

За подготовката на овој прирачник би сакале особено да им се заблагодариме на нашите стручни надворешни рецензенти, кои ни помогнаа при уредувањето на текстот и ни дадоа значајни повратни информации и предлози, вклучувајќи ги: Фиона Кракенбургер, Фонд за отворена технологија; Бил Бадингтон и Ширин Мори, фондација Електронски граници; Џоселин Вулбрајт, Клаудфлер (Cloudflare); Мартин Шелтон, фондација Слобода на печатот; Дејв Лајхтмен, Мајкрософт; Стивен Бојс, Меѓународна фондација за изборни системи; Ејми Стадарт, Меѓународен републикански институт; Ема Холингсворт, Глобална сајбер алијанса; Каролајн Синдерс, Конвокејшн дизајн + Рисрч (Convocation Design + Research); Дита Катурани, Сандра Пепера, НДИ; Арон Азелтон, НДИ; Фрида Аренос, НДИ; Антони Деанџело, НДИ; Витни Фајфер, НДИ и Дерек Луј̄тен, Комисија за демократско партнерство на Претставничкиот дом. Исто така, би сакале да им се заблагодариме и на Пол Коли од Службата за законодавни информации во Либерија, Нихад Бахрам и Фуад Ахмед од Парламентот на Курдистан во Ирак, Диана Плата од Сенатот на Колумбија; Ајад Абас и Маџид Кхудур од Ирачкиот претставнички совет и на Тања Данаиловска од Собранието на Северна Македонија за нивните значајни согледувања и придонеси.

Исто така, сакаме да се заблагодариме за сите извонредни прирачници, водичи, работни книги, модули за обука и други материјали коишто се изготвени и одржувани од Заедницата за организациска безбедност (OrgSec). Овој прирачник е дизајниран како надополнување на тие подетални материјали, комбинирајќи ги клучните лекции на едно место како лесночитлив ресурс за парламентите што сакаат да воведат план за кибернетска безбедност.

Освен што имавме индиректна инспирација од многу прекрасни ресурси креирани од заедницата, во овој Прирачник директно копиравме и корисни формулации од неколку постојни ресурси, особено од Водичот за самоодбрана од надзор на Electronic Frontier Foundation, Холистичкиот прирачник за безбедност на Тактикал тек (Tactical Tech) и различни лица кои ни ги објаснуваат работите од Center for Democracy and Technology и Freedom of the Press. Можете да најдете конкретни цитати на овие ресурси во деловите подолу, како и комплетни врски, информации за авторите и за лиценците во Додаток А.

Кои сме ние?

National Democratic Institute for International Affairs (ХДП) е непрофитна, непартиска организација, со седиште во Вашингтон, којашто работи во партнерство насекаде низ светот за зајакнување и заштита на демократските институции, процеси, норми и вредности за да обезбеди подобар квалитет на животот за сите. НДИ верува дека сите луѓе имаат право да живеат во свет во кој се почитуваат нивното достоинство, безбедност и политички права – и дека дигиталниот свет не е исклучок.

Во рамките на НДИ постои тим за демократија и технологија кој се обидува да поттикне глобален дигитален екосистем во кој демократските вредности се заштитени, промовирани и може да напредуваат; владите се потранспарентни и поинклузивни, а сите граѓани имаат моќ да бараат отчет од нивната влада. Ние работиме на ова преку обезбедување поддршка на глобална мрежа на активисти посветени на дигиталната отпорност и преку соработка со партнери за креирање алатки и ресурси како овој прирачник. Можете да дознаете повеќе за нашата работа на нашата веб-страница, ако нè следите на Twitter или ако директно нè контактирате на cyberhandbook@ndi.org. Секогаш ни причинува задоволство да го слушнеме вашето мислење и да одговориме на прашањата за нашиот тим и за нашата работа посветена на кибернетската безбедност, технологијата и на демократијата.

Комисијата за демократско партнерство на Претставничкиот дом (ХДП) работи со законодавните власти од целиот свет на промовирање одговорна, ефективна влада и зајакнување на демократските институции. Од клучно значење за нашата работа е заемната соработка со цел да се изгради техничка експертиза во партнерските законодавни власти којашто ќе ги подобри отчетот, транспарентноста, независноста на законодавната власт, пристапот до информации и надзорот над владата. ХДП во моментов има партнерства со повеќе од 20 национални законодавни власти насекаде низ светот. Областите на соработка со партнерските парламенти на ХДП вклучуваат решавање буџетски прашања, обезбедување поефикасно работење на комисиите, подобрување на услугите за гласачите, обезбедување алатки за посилен надзор, зајакнување на законодавната етика, подобрување на информатичката технологија, библиотеките, истражувањата и законодавните процеси и процедури. Програмите на ХДП се спроведуваат од страна на Националниот демократски институт (НДИ) и Меѓународниот републикански институт (ИРИ) преку договор за соработка и финансирање со Агенцијата на САД за меѓународен развој (УСАИД).

Кој управува со кибернетската безбедност на парламентот?

За ефикасен и безбеден парламент се потребни вработени со вештини и соодветно овластување за спроведување на препораките содржани во овој прирачник. Имајќи го тоа предвид, одговорните лица за кибернетската безбедност во парламентите можат многу да се разликуваат и не постои еден вистински модел за тоа кој треба да управува со кибернетската безбедност. Во некои случаи тоа може да биде назначен тим за кибернетска безбедност во рамките на вашата служба за ИТ, а во други група од различен административен кадар и членови. Во секој случај, имајте предвид дека, иако е важно да имате добар тим задолжен за кибернетската безбедност на вашиот парламент, одговорност на сите во парламентот и околу него е да ги следат политиките и процедурите што се неопходни за парламентот да биде безбеден. Подолу се дадени неколку примери на различни модели на кадар за управување со кибернетската безбедност на парламентот:

Претставнички дом на Соединетите Американски Држави
Во **Претставничкиот дом на Соединетите Американски Држави** некои поединечни служби ангажираат **системски администратор** кој е одговорен за управување со сите компјутерски хардверски и софтверски системи што ги користи службата – вклучително и за управување со согледувањата за кибернетската безбедност – и ги обучува вработените за најдобрите практики. На институционално ниво, главниот административен директор на Претставничкиот дом има тим за информациски ресурси, кој вклучува **сектор посветен на безбедноста на информациите**.

Национално собрание на Замбија
Националното собрание на Замбија смета на својот Сектор за информациска и комуникациска технологија (ИКТ) за различни функции, вклучително и управување со софтверот, хардверот и информатичката инфраструктура на парламентот, обука на пратениците и на вработените за технолошките системи и обезбедување на информацискатa инфраструктура на парламентот од внатрешни и надворешни закани за кибернетската безбедност.

Парламент на Малезија
Во **Парламентот на Малезија** одделот за информатичка технологија се наоѓа под главниот администратор на парламентот што му овозможува да ги опслужува двата дома на парламентот. Во овој оддел има конкретна позиција за безбедност на мрежи, која му овозможува да осигури дека мрежните системи, податочните центри и инфраструктурата за ИКТ се ажурирани и што е можно побезбедни.

За кого е наменет овој прирачник?

Овој прирачник е напишан со едноставна цел: да му помогне на вашиот парламент да изготви разбирлив и спроведлив план за кибернетска безбедност. Како што светот е сè поприсутен на интернет, кибернетската безбедност не е само модерна фраза, туку концепт кој е од клучно значење за успехот на парламентите, а безбедноста на информациите (на интернет и надвор од интернет) е предизвик кој изискува фокус, инвестиции и внимание.

Вашиот парламент, најверојатно, ќе стане – ако веќе не е – цел на кибернетски напад. Намерата на ова не е да предизвика паника, туку тоа е реалност дури и за парламентите за коишто не се смета дека претставуваат одредена цел.

Во една просечна година Центарот за стратегиски и меѓународни студии, кој води **тековна листа** на она што тие го нарекуваат „Значајни кибернетски инциденти“, каталогизира стотици сериозни кибернетски напади, од кои повеќето се насочени кон десетици, ако не и стотици, организации одеднаш. Покрај ваквите пријавени напади, веројатно има стотици други помали напади секоја година кои остануваат неоткриени или непријавени, а многу од нив се насочени кон владини институции, законодавни тела и кон политички организации.

Ваквите кибернетски напади имаат значителни последици. Без разлика дали целта на таквите закани е да го нарушат работењето на парламентот, да ѝ нанесат штета на вашата репутација, па дури и да украдат информации кои може да доведат до психичка или физичка повреда на вашите членови или вработени, тие треба да се сфатат сериозно.

Добрата работа е во тоа што не мора да станете програмер или експерт за технологија за да се одбраните себеси и вашиот парламент од вообичаените закани. Сепак, треба да бидете подготвени да вложите напор, енергија и време за изработување и спроведување цврст парламентарен план за безбедност.

Ако никогаш не сте размислувале за кибернетската безбедност на вашиот парламент, не сте имале време да се фокусирате на тоа или имате некои основни познавање за темата, но сметате дека вашиот парламент би можел да ја подобри својата кибернетска безбедност, овој прирачник е за вас. **Без оглед на тоа од каде сте, овој прирачник има цел да му ги даде на вашиот парламент суштинските информации што му се потребни за да воспостави еден цврст план за безбедност – план кој не е само едноставно ставање зборови на хартија, туку ви овозможува да ги спроведете најдобрите практики на дело.**

Што претставува планот за безбедност и зошто секој парламент треба да има таков план?

Планот за безбедност е збир на пишани политики, процедури и упатства со кои вашиот парламент се согласил за да го постигнете нивото на безбедност кое вие и вашиот тим сметате дека е соодветно за да ги заштитите вашите луѓе, партнери и информации. Добро изработен и ажуриран план за организациска безбедност може да ве заштити и да ве направи поефективни со тоа што ќе ви даде чувство на смиреност кое ви е потребно за да се фокусирате на важната секојдневна работа на вашиот парламент. Без детално размислување за еден сеопфатен план, многу е лесно несвесно да се занемарат некои видови закани, фокусирајќи се премногу на еден ризик или игнорирајќи ја кибернетската безбедност додека не се случи криза.

Кога ќе почнете да подготвувате план за безбедност, треба да си поставите неколку важни прашања кои го формираат процесот наречен процена на ризик. Одговарањето на тие прашања му помага на вашиот парламент да ги разбере уникатните закани со кои се соочувате и ви овозможува да застанете и детално да размислите за тоа што треба да заштитите и од кого треба да го заштитите. Обучени проценувачи со помош на системи, како ревизорската рамка **SAFETAG** на „Интер њус“ (Internews), можат да помогнат во водењето на вашиот парламент низ еден таков процес. Навистина вреди ако можете да добиете пристап до тоа ниво на професионална експертиза, но дури и ако не можете да направите целосна процена, треба да се сретнете со засегнатите страни во рамките на парламентот за внимателно да ги разгледате овие клучни прашања:

1 Со какви средства располага вашиот парламент и што сакате да заштитите?

Можете да почнете да одговарате на овие прашања **со креирање каталог на сите средства на вашиот парламент**. Информациите како пораки, е-пошта, контакти, документи, календари и локации се можни средства. Телефоните, компјутерите и другите уреди може да бидат средства. И луѓето, врските и односите, исто така, можат да бидат средства. Направете **список на вашите средства** и обидете се да ги каталогизирате според нивната важност за организацијата, каде ги чувате (можеби на повеќе дигитални или физички места) и што ги спречува другите да им пристапат, да ги оштетат или да ги нарушат. Имајте предвид дека не е сè подеднакво важно. Ако некои од податоците на парламентот претставуваат јавна евиденција или информации што веќе ги објавувате, тие не се тајни што треба да ги заштитите.

2 Кои се вашите противници и кои се нивните способности и мотивации?

„Противник“ е поим кој често се користи во организациската безбедност. Едноставно кажано, противници се актери (поединци или групи) коишто се заинтересирани за вашиот парламент, да ја нарушат вашата работа и да добијат пристап до вашите информации или да ги уништат информациите: лошите момци. Примери на потенцијални противници може да бидат финансиски измамници, непријателски влади или идеолошки или политички мотивирани хакери. Важно е да направите список на вашите противници и да размислите критички за тоа кој би сакал негативно да влијае на вашиот парламент и на вработените. Иако е лесно да се предвидат надворешните актери (како странска влада или одредена политичка група) како противници, имајте предвид дека противници можат да бидат и луѓе што ги познавате, како што се незадоволни вработени, поранешен кадар и членови на семејството или партнери што не ве поддржуваат.

Различни противници претставуваат различни закани и имаат различни ресурси и способности да го нарушат вашето работење и да добијат пристап до вашите информации или да ги уништат. На пример, владите често имаат многу пари и моќни способности, вклучително и да го исклучат интернетот или да користат скапа технологија за надзор; давателите на услуги за мобилни мрежи и интернет веројатно имаат пристап до евиденцијата на повици и претходни пребарувања на интернет; вештите хакери на јавните безжични мрежи имаат способност да пресретнуваат слабо обезбедени комуникации или финансиски трансакции. Можете дури и да станете свој сопствен противник, на пример, со случајно бришење важни датотеки или испраќање приватни пораки на погрешна личност.

Мотивите на противниците, веројатно, ќе се разликуваат и според нивниот капацитет, интереси и стратегии. Дали се заинтересирани да го дискредитираат вашиот парламент? Можеби имаат намера да ја оневозможат вашата порака или да ја нарушат работата на парламентот? Важно е да се разбере мотивацијата на противникот бидејќи тоа може да му помогне на вашиот парламент подобро да ги процени заканите.

3 Со какви закани се соочува вашиот парламент? Колку тие закани се веројатни и колку е големо нивното влијание?

При идентификувањето на можните закани, најверојатно ќе добиете список кој може да биде огромен. Можеби сметате дека сите напори ќе бидат бесмислени или не знаете од каде да почнете. За да му помогнете на вашиот парламент да зајакне и да преземе продуктивни следни чекори, корисно е да се анализира секоја закана врз основа на два фактора: веројатноста дека заканата ќе се случи и влијанието доколку се случи.

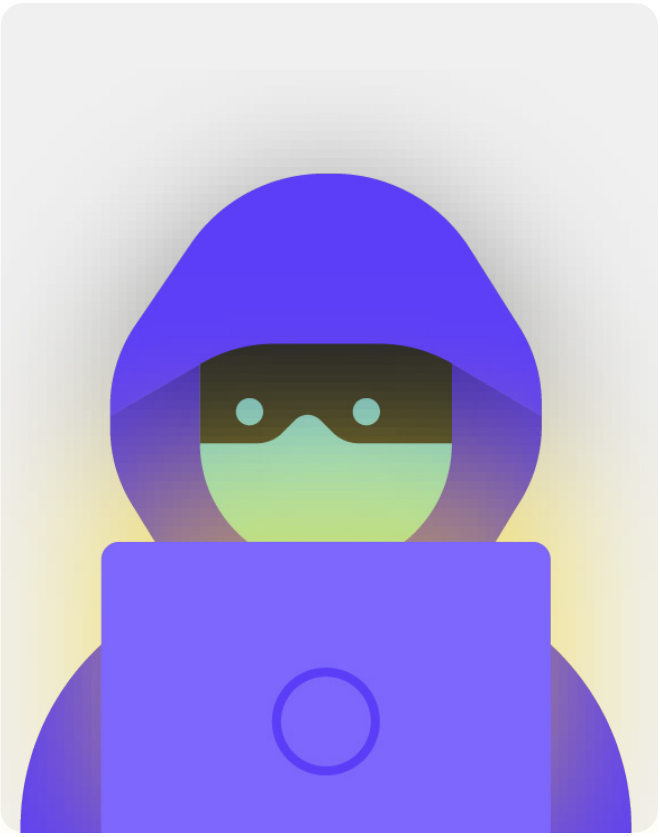
За да ја измерите веројатноста за закана (дали е можеби ниска, средна или висока, врз основа на тоа дали одреден настан веројатно нема да се случи, може да се случи или често се случува), можете да ги искористите информациите што ги знаете во однос на капацитетот и мотивацијата на вашите противници, анализата на минатите безбедносни инциденти, други слични искуства на парламентите и, секако, присуството на какви било постојни стратегии за ублажување што сте ги воспоставиле.

За да го измерите влијанието на заканата, размислете како би изгледал вашиот свет доколку заканата навистина се случи. Поставувајте прашања како, на пример, „Како заканата ни наштети како парламент и како луѓе, физички и психички?“, „Колку долго трае ефектот од заканата?“, „Дали заканата создава други штетни ситуации?“ и „Како ја попречува нашата способност да ги постигнеме нашите цели сега и во иднина?“ Додека одговарате на овие прашања, размислете дали влијанието од заканата е ниско, средно или високо.

За да ви помогне да управувате со овој процес на процена на ризикот, можете да користите работен лист, како овој изработен од фондацијата Електронски граници. Имајте предвид дека информациите што ги креиравте како дел од овој процес (како што е списокот на вашите противници и заканите од нив) може да бидат чувствителни, па затоа е важно да се погрижите да бидат безбедни.

Откако ќе ги категоризирате вашите закани според веројатноста и влијанието, можете да почнете да правите поинформативен план со активности. Со фокусирање на заканите кои најверојатно ќе се случат и ќе имаат значителни негативни влијанија, ќе ги канализирате вашите ограничени ресурси на најефикасен и најефективен можен начин. Вашата цел е секогаш да го ублажите ризикот колку што е можно повеќе, но никој – ниту владата или компанијата со најмногу ресурси на светот – никогаш не може целосно да го елиминира ризикот. И тоа е во ред: Можете да направите многу за да се заштитите себеси, вашите колеги и вашиот парламент со тоа што ќе се погрижите за најголемите закани

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 (siç është lista e kundërshtarëve tuaj dhe kërcënimet që ata paraqesin) mund të jenë vetë të ndjeshme, ndaj është e rëndësishme ta mbani të sigurt.

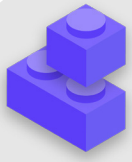


Креирање план за кибернетска безбедност на вашиот парламент

Иако планот за безбедност на секој парламент ќе изгледа малку поинаку врз основа на неговата процена на ризик и организациската динамика, одредени суштински концепти се речиси универзални. Овој прирачник се осврнува на тие суштински концепти на начин којшто ќе му помогне на вашиот парламент да направи конкретен план за безбедност заснован на практични решенија и апликации од реалниот свет.

Овој прирачник се обидува да обезбеди опции и предлози кои се бесплатни или со многу ниски трошоци. Имајте предвид дека најзначајниот трошок поврзан со спроведувањето ефективен план за безбедност ќе биде времето во текот на кое вие и вработените, членовите и тимовите во парламентот ќе треба да разговарате, да го научите и да го спроведете вашиот нов план. Меѓутоа, со оглед на ризиците со кои веројатно ќе се соочи вашиот парламент, оваа инвестиција ќе биде многу вредна.

Во секој дел ќе најдете објаснување за клучната тема со која треба да се запознаат вашиот парламент и вработените – што претставува таа и зошто е важна. Секоја тема е поврзана со суштински стратегии, пристапи и препорачани алатки за ограничување на вашиот ризик, како и совети и врски до дополнителни ресурси кои може да ви помогнат да ги спроведете тие препораки во вашиот парламент.



Комплет со почетни упатства за план за безбедност

За да му помогнете на вашиот парламент да ги обработи лекциите од прирачникот и да ги претвори во реален план, искористете го овој комплет со почетни упатства. Можете да го испечатите комплетот или да го пополните дигитално додека го читате прирачникот во електронска верзија. Додека правите белешки и почнувате да го ажурирате или изработувате вашиот план за безбедност, не заборавајте да се повикате на „Основните елементи на планот за безбедност“ кои се детално опишани во секој дел. Ниту еден план за безбедност не е комплетен без, минимално, осврнување на овие суштински елементи.

Искористете ги предностите на другите ресурси кои може да ви помогнат да го направите и спроведете вашиот план. Искористете ги бесплатните ресурси за обука, како Security Planner на „Консјумер рипортс“ (Consumer Reports), апликацијата Umbrella од „Секјурити фирст“ (Security First), проектот Totem од „Фри прес анлимитед“ (Free Press Unlimited) и „Гринхост“ (Greenhost), како и Комплет со почетни упатства за план за безбедност на Глобалната сајбер алијанса, кои содржат ресурси за многу од најдобрите практики споменати во овој прирачник и врски до десетици алатки за обука кои ќе ви помогнат да спроведете многу суштински основи.

Градење култура на безбедност

погрижите сите кои се вклучени – вклучително и пратениците, кадарот за законодавна поддршка, кадарот на службата за истражување и административните службеници во финансии, човечки ресурси и ИТ, меѓу многуте други – сериозно да ја сфаќаат кибернетската безбедност. Менувањето на културата е тешко, но неколку едноставни чекори и важни разговори можат многу да помогнат кон создавање атмосфера што ќе ги направи вашите вработени и парламентот отпорни при соочувањето со безбедносни закани. Еден од наједноставните, но најважни чекори што треба да се преземат за да се изгради оваа култура на безбедност во парламентот е да се комуницира за тоа во рамките на вашиот парламент, а лидерите секогаш треба да бидат пример и да инвестираат во добро однесување.

Градење култура на безбедност во парламентите

Во февруари 2019 година Австралија претрпе кибернетски напад кој ги компромитираше мрежите на австралискиот национален парламент и на три водечки политички партии. Напаѓачите добија пристап до документи за политики и кореспонденција по приватна е-пошта меѓу пратениците, нивниот кадар и нивните избирачи. Нападот се случи само три месеци пред да се одржат изборите, што ја истакна ранливоста на небезбедните мрежи за време на изборите.

Како одговор на овој значаен и успешен напад, парламентот презеде напори за да ја зајакне својата подготвеност за кибернетска безбедност. Таквата инвестиција вклучуваше истрага на Заедничкиот комитет за јавни сметки и ревизии на кибернетската отпорност на Комонвелтот. Истрагата **се засноваше на наодите од ревизиите** спроведени во текот на неколку години, кои утврдија дека недостигаат процеси за ублажување на ризикот за кибернетската безбедност во парламентот и во другите владини агенции. На пример, Националната ревизорска служба на Австралија го истакна неуспехот на парламентот да се фокусира на долгорочните стратегиски цели и да креира пристап заснован на ризик кога станува збор за кибернетската безбедност. И додека истрагата и ревизиите не беа поволни, подготвеноста на парламентот да ги идентификува проблемите со кибернетската безбедност и да инвестира во нивно решавање е пример за создавање култура соодветна за ефективна парламентарна кибернетска безбедност. Тоа е култура што почнува со препознавање на проблемите и инвестирање во технички и човечки решенија, каде што безбедноста не се избегнува, туку Ѝ се дава приоритет. На пример, преку ангажирање тим за подобрување на кибернетската безбедност и буџетска инвестиција за **„Фонд за одговор на кибернетската безбедност“**, парламентот (и другите владини субјекти) треба да биде подобро опремен за да ги ублажат идните напади доколку таквите ресурси се правилно распоредени, одржливи и ако фокусот остане на кибернетската безбедност како редовен елемент на парламентарното работење. Имајќи го предвид тоа, секако подобро е да ја изградите оваа посветеност на безбедноста во вашиот парламент пред да се случи значително нарушување на безбедноста.

Интегрирајте ја безбедноста во вашата редовна оперативна структура

Како што детално е опишано во Холистичкиот водич за безбедност на „Тактикал тек“ (Tactical Tech), од суштинска важност е да се создаде редовен, безбеден простор за да се зборува за различните аспекти на безбедноста. На тој начин, ако вработените и членовите се загрижени во врска со безбедноста, тие помалку ќе се грижат за тоа дали изгледаат параноични или дали им го трошат времето на другите луѓе. Закажувањето редовни дискусии за безбедноста, исто така, ја нормализира зачестеноста на интеракцијата и размислувањето за прашањата поврзани со безбедноста, така што прашањата не се забораваат, а кадарот во тимовите е поверојатно да внесе барем пасивна свесност за безбедноста во нивната тековна работа. Не мора да биде секоја недела, но нека биде повторлив потсетник. Овие дискусии не треба само да остават простор за теми од техничката безбедност, туку и за прашања кои влијаат врз удобноста и безбедноста на вработените, како што се вознемирувањето на интернет (и надвор од интернет), или прашања во однос на користењето и поставувањето дигитални алатки во канцелариите на парламентот.
Дискусиите дури може да вклучуваат и теми како навиките за споделување информации надвор од интернетот и начините на кои вработените ги прават или не ги прават безбедни информациите надвор од парламентот. На крајот, важно е да се запамети дека безбедноста на парламентот е исто толку силна колку и неговата најслаба алка.
Еден од начините за да се постигне доследен ангажман е со додавање на безбедноста на дневниот ред на некој редовен состанок. Исто така, можете да ја ротирате одговорноста за организирање и олеснување на дискусијата за безбедност помеѓу различни вработени, што може да помогне да се создаде идејата дека безбедноста е одговорност на сите, а не само на неколку избрани лица или на тимот за ИТ. Како што ќе почнувате да ја формализирате дискусијата за безбедноста, вработените, најверојатно, ќе се чувствуваат посигурни да дискутираат за овие важни прашања меѓу себе, како и во помалку формални услови.

Исто така, важно е да се вклучат безбедносни елементи во нормалното функционирање на парламентот, како, на пример, при приклучување на некој нов член и вработен – и да се размисли за прекинување на пристапот до системите кога некој ќе си замине од парламентот. Безбедноста не треба да биде некоја дополнителна работа за која треба да се грижите, туку **составен дел од вашата стратегија и работење**.

Запомнете дека сите **планови за безбедност треба да се сметаат за живи документи** и треба редовно да се врши нивно оценување и да се дискутираат, особено кога нови вработени или волонтери ќе се приклучат на организацијата или кога ќе се смени вашиот безбедносен контекст.

Планирајте повторно да ја разгледате вашата стратегија и да ја ажурирате на годишна основа, или ако има големи промени во стратегијата, алатките или заканите со кои се соочувате.

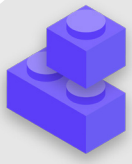
Обезбедете прифаќање на организациско ниво

Дел од успешната култура на безбедност, исто така, е да **се обезбеди прифаќање на вашиот план за безбедност во рамките на парламентот**. Од клучно значење е тоа да вклучува силна, гласна поддршка и насоки од лидерите, кои во многу случаи ќе ја донесат конечната одлука за издвојување време, ресурси и енергија за креирање и спроведување ефективен план за безбедност. Ако тие не го сфатат тоа сериозно, никој друг нема да го сфати. За да го постигнете ова прифаќање, внимателно размислете кога и како да го воведете вашиот план, направете го тоа на јасен начин, погрижете се раководството да ги зајакне пораките и секому објаснете му ги сите елементи и чекори од планот за да нема непознати работи или забуна во врска со тоа што се обидувате да постигнете. Исто така, погрижете се да обезбедите соодветен буџет за кибернетската безбедност во рамките на парламентот. Иако финансиските средства може да бидат ограничени, од суштинска важност е соодветно да се инвестира во кибернетската безбедност, во спротивно другите инвестиции, најверојатно, ќе бидат изложени на ризик. Кога зборувате за безбедност, избегнувајте тактики на заплашување. Понекогаш заканите со кои се соочуваат вашиот парламент и вработените може да бидат страшни, но обидете се да се фокусирате на споделување факти и да создадете мирен простор за прашања и работи што предизвикуваат загриженост. Правењето на опасностите да изгледаат премногу заканувачки може да доведе до тоа луѓето да ве сметаат за сензационалист или едноставно да се откажат мислејќи дека ништо од тоа што го прават не е важно – а тоа апсолутно не е точно.

Воспоставете план за обука

Откако ќе го направите и ќе се посветите на планот, размислете како ќе ги обучите сите членови, вработени и волонтери за новите најдобри практики. Барањето редовна обука – и задолжителното присуство на обуката – може да биде корисна тактика. Избегнувајте да создавате строги, негативни последици за вработените што имаат проблем со безбедносните концепти. Имајте предвид дека одредени вработени можат да се приспособат и да ја научат технологијата поинаку од другите врз основа на нивното ниво на познавање на дигиталните алатки и интернетот. Стравот од неуспех само дополнително ги обесхрабрува вработените да пријавуваат проблеми или да побараат помош. Меѓутоа, создавањето позитивна одговорност и награди за успешна обука и усвојување на политиките може да помогне да се поттикне подобрувањето на состојбата во рамките на парламентот. Може да најдете дополнителна вредна поддршка преку локални или меѓународни мрежи за обука за дигитална безбедност и бесплатни ресурси за обука, како **апликацијата Umbrella од „Секјурити фрст“ (Security First)**, **проектот Totem** од „Фри прес анлимитед“ (Free Press Unlimited) и „Гринхост“ (Greenhost), како и **Порталот за учење** на Глобалната сајбер алијанса.

Размислете како вашиот план за обука може да допре до пратениците, парламентарната служба, како и до парламентарната администрација. Имајте предвид дека истакнатите членови често бараат уште повеќе обука и внимание кога станува збор за безбедноста поради нивниот висок профил. Погрижете се вашиот план за обука и план за безбедност да важат за сите овие различни видови поединци и за сите средства што тие може да ги имаат во парламентот и надвор од него.



Основни елементи на планот за безбедност: Градење култура на безбедност

- **Закажете редовни дискусии и обука за безбедност и за вашиот план за безбедност.**
- **Вклучете ги сите – распределете ја одговорноста за спроведување на вашиот план за безбедност во рамките на целиот парламент.**
- **Осигурете добри примери на лидерство, добро безбедносно однесување и посветеност на вашиот план.**
- **Избегнувајте тактики на страв или казнување – наградете го подобрувањето и создадете комфорен простор за вработените да пријавуваат проблеми и да бараат помош.**
- **Ажурирајте го вашиот план за безбедност еднаш годишно или по големи промени во парламентарната служба, структурата или работното опкружување.**

Силна основа: Обезбедување на сметките и на

Зошто го ставаме фокусот на сметките и на уредите? Затоа што тие ја формираат основата на сето она што вашиот парламент го прави дигитално. Речиси сигурно пристапувате до чувствителни информации, комуницирате внатрешно и надворешно и зачувувате приватни информации на нив. Само размислете за учеството на членовите на пленарни седници, гласањето (вклучувајќи виртуелно), процесите на подготовка на законодавството и комуникацијата со вработените и со поширокатa јавност. Без безбедни сметки и уреди, овие клучни парламентарни активности и многу други активности може да бидат изложени на ризик.

На пример, ако хакерите го гледаат вашето работење на тастатурата или го слушаат вашиот микрофон, приватните разговори со колегите ќе бидат снимени без разлика колку се безбедни вашите апликации за пораки. Или, ако некој противник добие пристап до сметките на вашиот парламент на социјалните медиуми, тој лесно може да им наштети на вашиот углед и кредибилитет, како и да ја поткопа довербата кај јавноста. Затоа, од суштинска важност е како парламент да се осигурите дека сите преземаат некои едноставни, но ефективни чекори за одржување на безбедноста на своите уреди и сметки. Важно е да се спомне дека овие препораки се однесуваат и на личните сметки и уреди бидејќи тие често се лесни цели за противниците. Хакерите со задоволство ќе тргнат по најлесната цел и ќе упаднат во личната сметка или во домашниот компјутер доколку вашите членови и вработените ги користат за да комуницираат и да пристапат до важни информации.

Безбедни сметки и парламенти

Хакерскиот напад Соларвиндс (SolarWinds) со широк публицитет, кој беше откриен кон крајот на 2020 година и кој компромитираше над 250 организации, вклучувајќи ги и повеќето владини сектори на Соединетите Американски Држави, продавачи на технологија, како „Мајкрософт“ и „Циско“ (Cisco), и невладини организации, делумно беше резултат на тоа што **хакерите погодија слаби лозинки** што се користеле на важни администраторски сметки. Севкупно, околу 80 проценти од сите нарушувања на безбедноста поврзани со хакирање се случуваат поради слаби или повторно употребени лозинки. Со зголемената распространетост на ваквите пробивања на лозинките и полесниот пристап за сите видови противници до софистицираните алатки за хакирање лозинки, најдобрите практики за лозинки и автентикацијата со два фактора се безбедносни елементи кои мора да ги имаат сите организации, вклучително и парламентите. Ниту еден инцидент не го илустрира појасно ова од **нападот во 2017 година** врз системот за е-пошта на британскиот парламент. Во овој инцидент, практиките на употреба на слаби лозинки од мал, но значаен број пратеници доведоа до незаштитени сметки за е-пошта и разговори, илјадници неовластено откриени кориснички имиња и лозинки и огромно нарушување на парламентарното работење. **Според** прес-службата на британскиот парламент, пробиените сметки биле „компромитирани како резултат на слаби лозинки кои не биле во согласност со упатствата издадени од Парламентарната дигитална служба“.

Безбедни сметки: Лозинки и автентикација со два фактора

Во денешно време, најверојатно, вашиот парламент и неговите вработени имаат десетици, ако не и стотици, сметки кои, доколку се пробијат, би можеле да разоткријат чувствителни информации или дури и да повредат лица кои се изложени на ризик. Размислете за различните сметки што може да ги има поединечен вработен и парламентот како целина: е-пошта, апликации за разговори, социјални медиуми, електронско банкарство, складирање податоци во облак, како и продавници за облека, локални ресторани, весници и многу други веб-страници или апликации на кои се најавувате. Добрата безбедност во денешно време бара темелен пристап за заштита од напади на сите овие сметки. Тоа почнува со добра грижа за лозинките и со употреба на автентикација со два фактора од сите.

ШТО Е ОНА ШТО ЈА ПРАВИ ЛОЗИНКАТА ДОБРА?

Има три клучни работи за добра и силна лозинка: должина, случајност и уникатност.

ДОЛЖИНА:

Колку е подолга лозинката, толку е потешко противникот да ја погоди. Во последно време, повеќето хакирања на лозинките се вршат од компјутерски програми и на тие злобни програми не им треба долго време за да пробијат една кратка лозинка. Како резултат на тоа, од суштинска важност е вашите лозинки да имаат најмалку 16 карактери, или најмалку пет збора, а по можност да бидат и подолги

СЛУЧАЈНОСТ:

Дури и ако лозинката е долга, таа не е многу добра ако е поврзана со нешто во врска со вас што противникот лесно може да го погоди. Избегнувајте да внесувате информации како што се вашиот роденден, родниот град, омилените активности или други факти што некој би можел да ги дознае за вас од едно кратко пребарување на интернет.

УНИКАТНОСТ:

Можеби најчестата најлоша практика со лозинките е користењето иста лозинка за повеќе интернет-страници. Повторувањето на лозинките е голем проблем затоа што кога само една од тие сметки е компромитирана, сите други сметки што ја користат истата лозинка се исто така ранливи. Ако ја користите истата лозинка на повеќе интернет-страници, тоа значително може да го зголеми влијанието на една грешка или на нарушувањето на безбедноста на податоците. Иако можеби не се грижите за вашата лозинка за локалната библиотека, доколку таа е хакирана, а вие ја користите истата лозинка на почувствителна сметка, би можеле да бидат украдени важни информации.

Еден лесен начин да се постигнат целите за должина, случајност и за уникатност е да се изберат три или четири вообичаени, но случајни зборови. На пример, вашата лозинка може да биде „цветна ламба зелена мечка“ што е лесно да се запомни, но тешко да се погоди. Можете да ја погледнете **оваа веб-страница** на „Бетр бајс“ (Better Buys) за тоа колку брзо може да се пробијат лошите лозинки.

КОРИСТЕТЕ АПЛИКАЦИЈА ЗА УПРАВУВАЊЕ СО ЛОЗИНКИ ЗА ПОМОШ

Значи, знаете дека е важно секој во парламентот да користи долга, случајна и различна лозинка за секоја своја лична и парламентарна сметка, но како, всушност, да го направите тоа? Запомнувањето добра лозинка за десетици (ако не и стотици) сметки е невозможно, така што секој мора да мами. Погрешен начин да се прави тоа е повторно да се употребат истите лозинки. За среќа, наместо тоа, можеме да се обратиме до дигиталните менаџери на лозинки за да ни го направат животот многу полесен (и нашите практики на користење лозинки многу побезбедни). Овие апликации, до кои може да се пристапи преку компјутер или мобилен уред, може да креираат, складираат и да управуваат со лозинки за вас и за целата ваша организација. Користењето безбедна апликација за управување со лозинки значи дека ќе треба да запомните само една многу силна, долга лозинка наречена примарна лозинка (историски наречена главна лозинка), при што ќе добиете безбедносни придобивки од користењето добри, уникатни лозинки на сите ваши сметки. Ќе ја користите оваа примарна лозинка (и во најдобар случај, втор фактор на автентикација (2FA), за кој ќе се дискутира во следниот дел) за да ја отворите вашата апликација за управување со лозинки и да го отклучите пристапот до сите ваши други лозинки. Апликациите за управување со лозинки, исто така, може да се користат на повеќе сметки за да се олесни безбедното споделување лозинки низ парламентот.

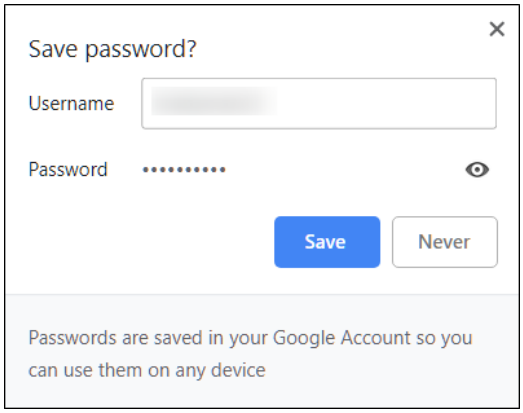
Зошто треба да користиме нешто ново? Не можеме ли само да ги запишеме на хартија или во табела на компјутерот?

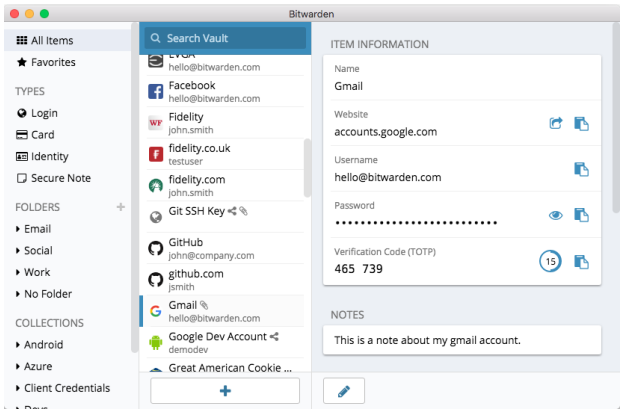
За жал, постојат многу вообичаени пристапи за управување со лозинки кои не се безбедни. Чувањето лозинки на листови хартија (освен ако не ги чувате заклучени во сеф) може да ги изложи на физичка кражба, љубопитни очи и лесно губење и оштетување. Зачувувањето на лозинките на документ на вашиот компјутер многу му го олеснува пристапот на хакерот – или на некој што ќе го украде вашиот компјутер, кој не само што ќе го има вашиот уред туку и ќе има пристап до сите ваши сметки. Користењето добра апликација за управување со лозинки е исто толку лесно како и користењето на тој документ, но многу побезбедно.

Зошто треба да веруваме на апликации за управување со лозинки?

Квалитетните апликации за управување со лозинки прават извонредни напори (и вработуваат одлични безбедносни тимови) за да ја одржуваат безбедноста на нивните системи. Исто така, добрите апликации за управување со лозинки (некои се препорачани подолу) се креирани на тој начин што не можат да ги „отклучат“ вашите сметки. Тоа значи дека во повеќето случаи, дури и ако биле хакирани или законски принудени да ги предадат информациите, нема да можат да ги изгубат или да ги откријат вашите лозинки. Исто така, важно е да се запомни дека е бескрајно поголема веројатноста противникот да погоди една од вашите слаби или повторени лозинки, или да најде некоја лозинка на **нарушување на безбедноста на јавни податоци**, отколку да ѝ се пробијат безбедносните системи на добра апликација за управување со лозинки. Важно е да се биде скептичен и дефинитивно не треба слепо да им се верува на сите софтвери и апликации, но реномираните апликации за управување со лозинки ги имаат сите вистински мотивации да ја направат вистинската работа.

Наместо да го користите вашиот веб-пребарувач (како Хром, прикажан лево) за зачувување на вашите лозинки, користете специјализирана апликација за управување со лозинки (како Битворден (Bitwarden), прикажан десно). Апликациите за управување со лозинки имаат функции што го прават работењето на вашиот парламент побезбедно и полесно.





Што е со складирањето лозинки во веб-пребарувачот?

Зачувувањето на лозинките во вашиот веб-пребарувач не е исто како и користењето безбедна апликација за управување со лозинки. Накратко, не треба да користите Хром, Фајрфокс, Сафари или кој било друг веб-пребарувач како менаџер на вашите лозинки. Иако тоа, дефинитивно, е подобро во однос на нивното пишување на хартија или зачувување во табела, основните функции за зачувување лозинка на вашиот веб-пребарувач не се многу добри од безбедносен аспект. Овие недостатоци, исто така, ви одземаат голем дел од погодноста што ја носи една добра апликација за управување со лозинки. Губењето на оваа погодност ја зголемува веројатноста дека луѓето во парламентот ќе продолжат со лошите практики на креирање и споделување лозинки.

На пример, за разлика од специјализираните апликации за управување со лозинки, вградените функции на веб-пребарувачите „зачувај ја оваа лозинка“ или „запомни ја оваа лозинка“ не обезбедуваат едноставна мобилна компатибилност, функционалност меѓу веб-пребарувачите и силни алатки за креирање и ревидирање на лозинките. Овие функции се голем дел од она што ја прави специјализираната апликација за управување со лозинки толку корисна и поволна за безбедноста на вашиот парламент. Апликациите за управување со лозинки, исто така, вклучуваат специфични функции за организацијата (како што е споделување лозинки) кои обезбедуваат не само вредност за поединци, туку и вредност за вашиот парламент како целина кога се работи за безбедноста.

Ако сте ги зачувувале лозинките во вашиот веб-пребарувач (намерно или ненамерно), одвојте малку време за да ги отстраните.

Кои апликации за управување со лозинки треба да ги користиме?

Постојат многу добри алатки за управување со лозинки кои може да се постават за помалку од 30 минути. Ако барате доверлива опција на интернет за вашиот парламент до која луѓето ќе можат да пристапат од повеќе уреди во секое време, добро поддржани и препорачани се 1Password (со почетна цена од 2,99 долари по корисник месечно) или бесплатниот Bitwarden со отворен код.

Интернет-опциите како Bitwarden се одлични и во однос на безбедноста и во однос на погодноста. Bitwarden,

на пример, ќе ви помогне да креирате силни уникатни лозинки и да пристапите до лозинките од повеќе уреди преку наставки на веб-пребарувачот и преку мобилна апликација. Платената верзија (10 долари за цела година) Bitwarden обезбедува и извештаи за повторно употребени, слаби и евентуално пробиени лозинки за да ви помогне да имате контрола врз работите. Откако ќе ја креирате вашата примарна лозинка (наречена главна лозинка), треба да вклучите и автентикација со два фактора за трезорот на вашата апликација за управување со лозинки да биде што е можно побезбеден.

Од суштинско значење е да **практикувате добра безбедност и кога ја користите вашата апликација за управување со лозинки**. На пример, ако користите наставка на веб-пребарувач на вашата апликација за управување со лозинки или се најавите на Bitwarden (или на која било друга апликација за управување со лозинки) на еден уред, не заборавајте да се одјавите откако ќе завршите со користењето на тој уред ако го делите уредот со некој друг или ако сметате дека, можеби, сте изложени на зголемен ризик од физичка кражба на уредот. Тоа вклучува одјавување од вашата апликација за управување со лозинки ако го оставите компјутерот или мобилниот уред без надзор. Ако споделувате лозинки меѓу тимовите или во рамките на парламентот како целина, не заборавајте да го поништите пристапот до лозинките (и да ги промените самите лозинки) кога ќе си заминат луѓето. Не сакате поранешен вработен да има пристап до лозинката на вашиот парламент на Фејсбук, на пример.

Што ако некој ја заборави својата примарна лозинка?

Од суштинска важност е да ја запомните вашата примарна лозинка. Добрите системи за управување со лозинки, како оние што се препорачани погоре, нема да ја запомнат вашата примарна лозинка или да ви овозможат да ја ресетирате директно преку е-пошта на начин кој е можен кај веб-страниците. Ова е добра безбедносна функција, но, исто така, го прави неопходно запомнувањето на вашата примарна лозинка кога првпат ќе ја поставите вашата апликација за управување со лозинки. За да си помогнете со ова, размислете да поставите дневен потсетник за да се потсетите на вашата примарна лозинка кога првпат ќе креирате сметка на апликацијата за управување со лозинки.

Напредно ниво: Користење апликација за управување со лозинки за вашиот парламент

Можете да ги зајакнете практиките за употреба на лозинки на вашиот парламент и да се осигурите дека секој вработен има пристап до (и користи) апликација за управување со лозинки со тоа што ќе поставите една таква апликација во рамките на целата организација. Наместо секој вработен да поставува своја апликација, размислете за инвестирање во план за „тим“ или за „бизнис“. На пример, планот „teams organization” (организација на тимови) на Bitwarden чини 3 долари по корисник месечно. Со него (или со други планови за тимови од апликации за управување со лозинки како 1Password) имате можност да управувате со сите споделени лозинки во рамките на „организацијата“. Функциите на апликацијата за управување со лозинки на ниво на парламент или на ниво на тим не само што обезбедуваат поголема безбедност туку и погодност за вработените. Можете безбедно да ги споделувате корисничкото име и лозинката во самата апликација за управување со лозинки со различни кориснички сметки. И Bitwarden, на пример, исто така, обезбедува погодна функција за целосно, од крај до крај, шифриран текст и споделување датотеки наречена „Bitwarden Send“ во рамките на својот план за тимови. Двете функции му даваат на вашиот парламент поголема контрола врз тоа кој кои лозинки може да ги види и сподели, и обезбедуваат побезбедна опција за споделување кориснички имиња и лозинки за сметките на ниво на тим или група. Ако поставите апликација за управување со лозинки на ниво на парламент, погрижете се некој да биде конкретно задолжен за отстранување на сметките на вработените и менување на сите споделени лозинки кога некој ќе го напушти тимот.

ШТО Е АВТЕНТИКАЦИЈА СО ДВА ФАКТОРА?

Колку и да е добра вашата грижа за лозинките, премногу често хакерите можат да ги заобиколат лозинките. За одржувањето на безбедноста на вашите сметки од некои актери што претставуваат вообичаена закана во денешно време, потребен е уште еден слој на заштита. Тука стапува на сцена автентикацијата со повеќе фактори или со два фактора – наречена MFA или 2FA.

Има многу одлични водичи и ресурси што ја објаснуваат автентикацијата со два фактора, вклучително и статијата **Автентикација со два фактора за почетници** на Мартин Шелтон и **Кибернетска безбедност на избори 101 Практичен водич** на Центарот за демократија и технологија. Овој дел содржи многу позајмени делови од двата ресурси за подобро да се објасни зошто е толку важно 2FA да се спроведе во рамките на парламентот.

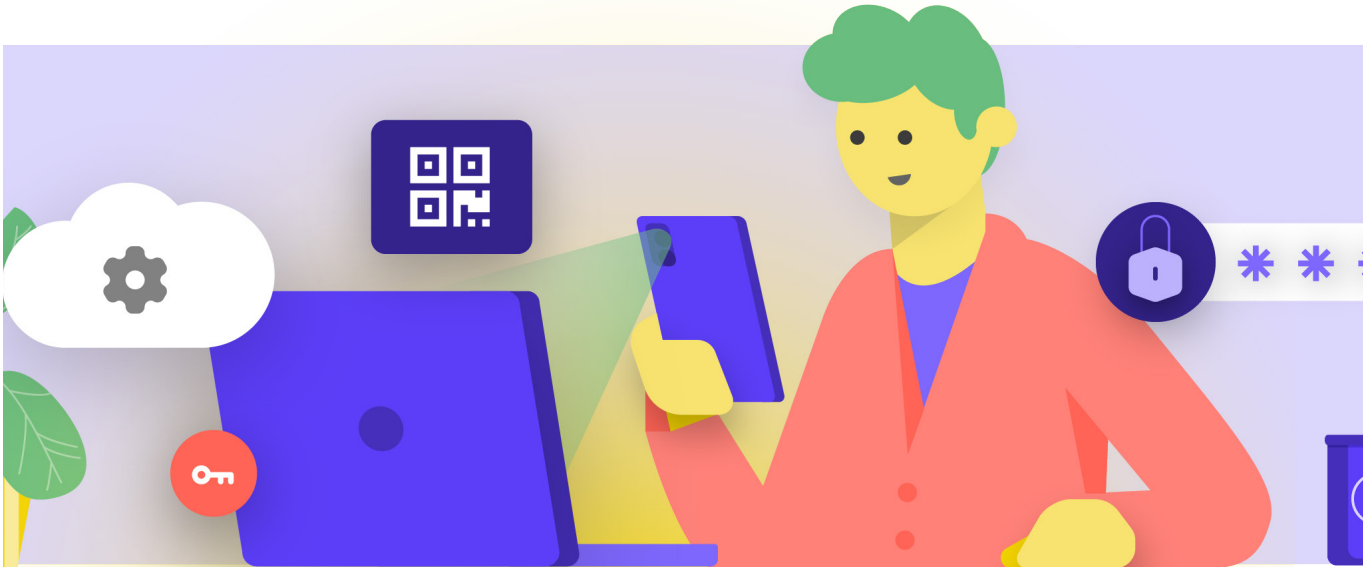
Накратко, 2FA ја зајакнува безбедноста на сметките со тоа што бара втора информација - нешто повеќе од само лозинка – за да се добие пристап. Втората информација обично е нешто што го имате, како код од апликација на вашиот телефон, физички токен или клуч. Оваа втора информација функционира како втор слој на одбрана. Ако некој хакер ја украде вашата лозинка или добие пристап до неа преку складиште на лозинки од големо нарушување на безбедноста на податоците, ефективната 2FA може да го спречи да пристапи до вашата сметка (а со тоа да го држи подалеку од приватните и од чувствителните информации). Од клучно значење е да се погрижите сите во парламентот да постават 2FA на нивните сметки.

КАКО МОЖЕМЕ ДА ПОСТАВИМЕ АВТЕНТИКАЦИЈА СО ДВА ФАКТОРА?

Постојат три вообичаени методи за 2FA: безбедносни клучеви, апликации за автентикација и еднократни СМС-кодови.

Безбедносни клучеви

Безбедносните клучеви се најдобрата опција, делумно затоа што тие се речиси целосно отпорни на „фишинг“. Овие „клучеви“ се хардверски токени (замислете си мини УСБ-дискови) кои може да се прикачат на вашиот приврзок со клучеви (или да останат во вашиот компјутер) за да ви бидат леснодостапни и лесни за чување. Кога треба да го искористите клучот за отклучување на одредена сметка, едноставно го вметнувате во вашиот уред и физички го активирате кога тоа ќе биде побарано за време на најавата. Има широк избор на модели кои можете да ги купите преку интернет (20-50 долари), вклучувајќи ги и високоценетите YubiKeys. Вајркатер (Wirecutter) на „Њујорк тајмс“ има **корисен водич** со неколку препораки за тоа кои клучеви да ги купите. Имајте предвид дека истиот безбедносен клуч може да се користи за онолку сметки колку што сакате.



Authentication Apps

Втората најдобра опција за 2FA се апликациите за автентикација. Овие услугите ви дозволуваат да добиете привремено најавување со два фактори код преку мобилна апликација или притисни известување на вашиот паметен телефон. Некои популарни и доверливи опции вклучуваат Google Authenticator, Authy и Duo Mobile. Апликациите за автентикација, исто така, се одлични бидејќи функционираат кога немате пристап до вашата мобилна мрежа и се бесплатни за користење за физички лица. Сепак, апликациите за автентикација се поподложни на „фишинг“ отколку безбедносните клучеви бидејќи корисниците може да бидат измамени за да внесат безбедносни кодови од апликација за автентикација во лажна веб-страница. Внимавајте да внесувате кодови за најава само на легитимни веб-страници. Ѝ не прифаќајте „пуш“ известувања за најава освен ако сте сигурни дека вие сте го направиле барањето за најава. Исто така, важно е кога користите апликација за автентикација да имате подготвено резервни кодови (за кои ќе се дискутира подолу) во случај вашиот телефон да биде изгубен или украден.

Codes Via SMS

Најмалку безбедна, но, за жал, сепак најчеста форма на 2FA се кодовите испратени преку СМС. Бидејќи СМС-пораките може да се пресретнат, а телефонските броеви може да се фалсификуваат или хакираат преку вашиот мобилен оператор, СМС-пораките не се многу добри како метод за барање 2FA кодови. Тоа е подобро отколку само да користите лозинка, но се препорачува да се користат апликации за автентикација или физички безбедносен клуч доколку е можно. Одлучниот противник може да добие пристап до 2FA кодовите испратени преку СМС-порака, обично само со **јавување во телефонската компанија** и со замена на вашата СИМ-картичка.

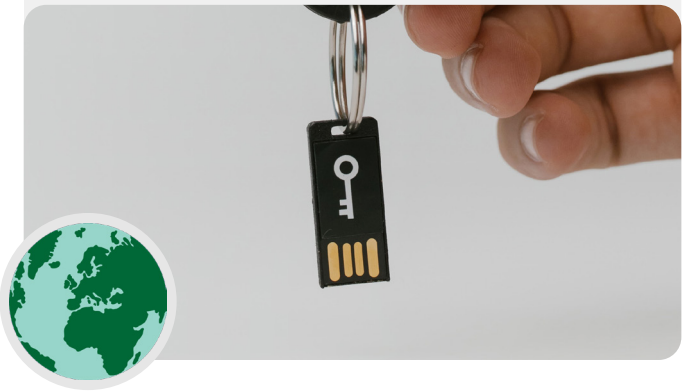
Кога ќе бидете подготвени да почнете со овозможување на 2FA за сите различни сметки на вашиот парламент, искористете ја оваа веб-страница (**https://2fa.directory/**) за брзо да пребарате информации и упатства за одредени услуги (како Џимеил, Офис 365, Фејсбук, Твитер, итн.) и за да видите кои услуги какви видови на 2FA овозможуваат.

2FA и парламентите

Според извештаите објавени во 2020 година, **хакери се инфилтрирале во парламентарниот систем за е-пошта на Норвешка** и ги компромитирале сметките за е-пошта на неколку парламентарни службеници, па дури и преземале некои информации од парламентарните системи. Иако не беа објавени во јавност целосните детали за хакирањето, Норвешка Ѝ го припиша упадот на APT28, хакерска група поврзана со руските безбедносни служби. Иако е многу софистицирана, APT28 и другите хакери често користат помалку сложени тактики, како што се „напади со брутална сила“ (при што напаѓачот користи алатки за да проба многу лозинки со надеж дека на крајот ќе ја погоди вистинската), за да добијат пристап до сметките. Оваа тактика им овозможува на хакерите да погодат дури и солидни лозинки – како што се сметаше дека е случај во Норвешка. Добрите вести? Овие видови напади имаат многу помала веројатност да успеат кога има соодветна автентикација со два фактора заснована на клуч или на апликација!

Безбедносни клучеви во реалниот свет

Со обезбедување физички безбедносни клучеви за автентикација со два фактора на сите 85.000+ вработени, „Гугл“(организација со многу висок ризик и висока цел на напади) ефективно **ги елиминираше сите успешни „фишинг“** напади против организацијата. Овој случај покажува колку ефикасни може да бидат безбедносните клучеви дури и за организациите што се најмногу изложени на ризик.



ШТО АКО НЕКОЈ ГО ИЗГУБИ УРЕДОТ СО 2FA?

Ако користите безбедносен клуч, постапувајте со него исто како што би постапиле со клучот од вашата куќа или стан, доколку го имате. Накратко, не губете го. Сепак, исто како и клучевите од вашата куќа, секогаш е добра идеја да имате регистриран резервен клуч на вашата сметка што ќе биде заклучен на безбедно место (како, на пример, во сеф дома или во сеф во банка) во случај на загуба или кражба.

Од друга страна, треба да креирате резервни кодови за сметките што го дозволуваат тоа. Треба да ги чувате овие кодови на многу безбедно место, какво што е вашата апликација за управување со лозинки или во физички сеф. Ваквите резервни кодови може да се креираат во поставките за 2FA на повеќето веб-страници (на истото место каде што првично ја овозможувате 2FA) и може да служат како резервен клуч при итни случаи.

Најчестиот проблем со 2FA се случува кога луѓето ќе ги заменат или изгубат телефоните што ги користат за апликации за автентикација. Ако користите Google Authenticator, нема да имате среќа ако ви биде украден телефонот, освен ако не ги зачувате резервните кодови што се креираат во моментот кога ќе ја поврзете сметката со Google Authenticator. Затоа, ако користите Google Authenticator како апликација за 2FA, погрижете се да ги зачувате на безбедно место резервните кодови за сите сметки што ги поврзувате со него.

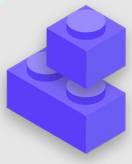
Ако користите Authy или Duo, двете апликации имаат вградени функции за креирање резервна копија со силни безбедносни поставки кои можете да ги вклучите. Ако изберете која било од тие апликации, можете да ги конфигурирате тие опции за креирање резервна копија во случај на кршење, губење или кражба на уредот. Видете ги упатствата на Authy **овде**, а на Duo **овде**.

Погрижете се сите да се запознаени со овие чекори кога ќе ја вклучат 2FA на сите нивни сметки. овде

Напредно ниво: Спроведување 2FA во рамките на вашиот парламент

Ако вашиот парламент обезбедува сметки за е-пошта за сите вработени преку Гугл воркспејс (Google Workspace, претходно познат како ЏиСјут (GSuite) или Мајкрософт 365 со користење сопствен домен (на пример, @ndi.org), можете да спроведете 2FA и силни безбедносни поставки за сите сметки. Нејзиното спроведување не само што помага да се заштитат овие сметки туку и функционира како начин за воведување и нормализирање на 2FA за вашите членови и вработени, така што ним ќе им биде полесно да ја прифатат и за нивните лични сметки. Како администратор на Гугл воркспејс, можете да ги следите **овие упатства** за да спроведете 2FA за вашиот домен. Можете да направите нешто слично во Мајкрософт 365 следејќи ги **овие чекори** како администратор на домен.

Размислете и за вклучување на сметките на вашиот парламент во **Програмата за напредна заштита** (Гугл) или **AccountGuard** (Мајкрософт) за да спроведете дополнителни безбедносни контроли и да барате физички безбедносни клучеви за автентикација со два фактора.



Основни елементи на планот за безбедност: Безбедни сметки

- **Барајте силни лозинки за сите парламентарни сметки; поттикнете го истото за личните сметки на членовите, вработените и на волонтерите.**
- **Поставете доверлива апликација за управување со лозинки за парламентот (и поттикнете ја нејзината употреба и во приватниот живот на вработените).**
  - Барајте силна примарна лозинка и 2FA за сите сметки на апликацијата за управување со лозинки.
  - Потсетете ги сите да се одјават од апликацијата за управување со лозинки на заедничките уреди или кога се изложени на зголемен ризик од кражба или заплена на уредот.
- **Променете ги споделените лозинки кога вработени и членови ќе го напуштат парламентот.**
- **Споделувајте ги лозинките само на безбеден начин, како, на пример, преку апликацијата за управување со лозинки на вашиот парламент или преку целосно, од крај до крај, шифрирани апликации.**
- **Барајте 2FA на сите сметки на парламентот и поттикнете ги вработените да постават 2FA и на сите лични сметки.**
  - Доколку е можно, обезбедете физички безбедносни клучеви за сите членови и вработени.
  - Ако безбедносните клучеви не се предвидени во вашиот буџет, поттикнете ја употребата на апликации за автентикација наместо СМС-пораки или телефонски повици за 2FA.
- **Одржувајте редовна обука за да се осигурите дека сите ги знаат лозинката и најдобрите практики за 2FA, вклучително и што е потребно за една лозинка да биде силна и зошто е важно никогаш повторно да не се користат истите лозинки, само да се прифаќаат легитимни барања за 2FA и да се креираат резервни кодови за 2FA**

Безбедни уреди

Покрај сметките, од суштинска важност е да бидат добро заштитени сите уреди – компјутери, телефони, УСБ-дискови, надворешни тврди дискови итн. Таквата заштита почнува со тоа што ќе внимавате каков тип уреди купуваат и користат вашиот парламент и вашите вработени. Секој продавач или производител што ќе го изберете треба да има докажана историја на деловно работење со придржување кон глобалните стандарди за безбедно изработување хардверски уреди (како телефони и компјутери). Сите уреди што ќе ги набавите треба да бидат произведени од компании од доверба кои немаат мотивација да ги предадат податоците и информациите на потенцијален противник. Важно е да се спомне дека кинеската влада бара од кинеските компании да доставуваат податоци до централната влада. Затоа, и покрај насекаде распространетите и евтини паметни телефони, како „хуавеи“ или „ЗТЕ“, тие треба да се избегнуваат. Иако цената на евтиниот хардвер може да биде многу привлечна, потенцијалните безбедносни ризици за парламентите треба да ве насочат кон други опции за уреди и за опрема.

Вашите противници можат да ја загрозат безбедноста на вашите уреди, и на сè што правите од тие уреди, со тоа што ќе добијат физички или „далечински“ пристап до нив.

Безбедност на уредите и на парламентите

Некои од најнапредните злонамерни софтвери во светот се развиени и распоредени низ целиот свет за да **таргетираат** пратеници, владини службеници и нивен кадар. Во Индија, на пример, конзорциум од новинари **откри** дека повеќе пратеници и владини министри биле цел на шпионскиот софтвер „Пегасус“, вид злонамерен софтвер кој беше главна тема во медиумите во 2020 година. „Пегасус“ е озлогласен поради својата способност да зарази мобилни уреди и да му овозможи на престапникот да снима аудио, да пресретнува кликнувања на тастатурата и пораки, и, всушност, да ја стави жртвата под целосен надзор без да бара интеракција од неа. Сепак, огромен дел од шпионските софтвери успеваат во својата намера поради слабите безбедносни практики на уредите, како што е невниманието што доведува до „фишинг“ или неспроведувањето на политиките споменати во овој дел од прирачникот.

ПРИСТАП ДО ФИЗИЧКИ УРЕД ПРИ ГУБЕЊЕ ИЛИ КРАЖБА

За да спречите физичко компромитирање, од суштинска важност е да се погрижите за физичката безбедност на вашите уреди. Накратко, не олеснувајте му на противникот да ви го украде или дури привремено да ви го одземе уредот. Чувајте ги уредите заклучени ако сте ги оставиле дома или во канцеларија. Или ако мислите дека е побезбедно, носете ги со себе. Тоа, секако, значи дека дел од безбедноста на уредот е физичката безбедност на вашите работни простории (без разлика дали во канцеларија или дома). Ќе треба да инсталирате силни брави, безбедносни камери или други системи за следење. Потсетете ги вработените да постапуваат со уредите на ист начин како што би постапувале со голем куп пари – не оставајте ги наоколу без надзор или заштита.

Што ако некој уред е украден?

За да го ограничите влијанието врз украден уред – или дури и ако само добие пристап до него за краток временски период – **барајте да се употребуваат силни лозинки или шифри на компјутерите и на телефоните на сите вработени**. Истите совети за лозинките од делот „Лозинки“ во овој прирачник важат за добра лозинка за компјутер или лаптоп. Кога станува збор за заклучување на вашиот телефон, користете шифри кои се состојат од најмалку шест до осум цифри и избегнувајте да користите „шеми со лизгање“ за отклучување на екранот. За дополнителни совети за заклучување на екранот, погледнете го Data Detox Kit на „Тактикал тек“ (Tactical Tech). Ако употребувате добри лозинки на уредот, на противникот ќе му биде многу потешко брзо да пристапи до информациите на вашиот уред во случај на кражба или заплена.

Исто така, погрижете се сите уреди издадени од парламентот да бидат пријавени во **систем за управување со мобилни уреди или систем за управување со уреди како крајни точки во мрежа (endpoint management system)**. Иако не се евтини, овие системи му овозможуваат на вашиот парламент да спроведува безбедносни политики за сите уреди, да ги лоцира и да ги избрише нивните потенцијално чувствителни содржини доколку бидат украдени, изгубени или запленети. Иако постојат многу различни решенија за управување со мобилни уреди, неколку доверливи опции кои работат на повеќе платформи (iPhones, Android, Mac и Windows) се Hexnode, Meraki Systems Manager на Циско, MDM на Ај-Би-Ем (IBM) и вградената функција за Управување со мобилни уреди на Гугл воркспејс. Ако цената е ограничувачки фактор, барем поттикнете ги членовите и вработените да ги користат вградените функции „Најди го мојот уред“ на нивните службени и приватни паметни телефони, како што се „Најди го мојот ајфон“ на Ајфон и „Најди го мојот уред“ на Андроид.

Што е со шифрирањето на уредите?

Важно е да се користи шифрирање, менување на податоците за да бидат нечитливи и неупотребливи на сите уреди, особено на компјутерите и на паметните телефони. Ако е можно, на сите уреди во рамките на парламентот треба да поставите нешто што се нарекува шифрирање на целиот диск. Шифрирање на целиот диск значи дека целиот уред е шифриран така што противникот, доколку физички го украде, нема да може да ја извлече содржината на уредот без да ја знае лозинката или клучот што сте го користеле за да го шифрирате.

Многу модерни паметни телефони и компјутери овозможуваат шифрирање на целиот диск. редите на „Епл“ (Apple), како што се ајфон (iPhone) и ајпад (iPad), многу погодно го вклучуваат шифрирањето на целиот диск кога ќе поставите вообичаена шифра на уредот. Компјутерите на „Епл“ користат оперативен систем Мек (Mac) и обезбедуваат функција наречена FileVault, која можете да ја вклучите за шифрирање на целиот диск.

Компјутерите со Виндоус (Windows) што работат со професионални лиценци, лиценци за претпријатија или образовни лиценци нудат функција наречена BitLocker, која можете да ја вклучите за шифрирање на целиот диск. Можете да го вклучите BitLocker следејќи ги овие упатства од „Мајкрософт“, што, можеби, прво ќе треба да го овозможи администраторот на вашата организација. Ако вработените имаат само домашна лиценца за нивните компјутери што користат Windows, BitLocker не е достапен. Сепак, тие ќе можат да го вклучат шифрирањето на целиот диск ако одат во Ажурирање и безбедност> Шифрирање на уред (‘Update & Security’ > ‘Device encryption’) во поставките за оперативниот систем Виндоус.

Уредите со Андроид, од верзијата 9.0 и понови верзии, се испорачуваат со стандардно вклучено шифрирање засновано на датотеки. Шифрирањето засновано на датотеки на Андроид работи поинаку од шифрирањето на целиот диск, но, сепак, обезбедува силна безбедност. Ако користите релативно нов телефон со Андроид и имате поставено шифра, шифрирањето засновано на датотеки треба да биде овозможено. Сепак, добро би било да ги проверите вашите поставки само за да бидете сигурни, особено ако вашиот телефон е купен пред повеќе години. За да проверите, одете во Поставки > Безбедност (Settings > Security) на вашиот уред со Андроид. Во рамките на безбедносните поставки, треба да видите дел за „шифрирање“ (encryption) или „шифрирање и корисничко име и лозинка“ (encryption and credentials), што ќе ви покаже дали вашиот телефон е шифриран и, доколку не е, ќе ви овозможи да го вклучите шифрирањето.

За компјутерите (без разлика дали се Виндоус или Мек) особено е важно сите клучеви за шифрирање (наречени клучеви за обновување) да се чуваат на безбедно место. Овие „клучеви за обновување“ во повеќето случаи, во суштина, се долги лозинки или фрази за пристап. Во случај ако ја заборавите вашата вообичаена лозинка на уредот или ако се случи нешто неочекувано (како што е дефект на уредот), клучевите за обновување се единствениот начин да ги вратите вашите шифрирани податоци и, доколку е потребно, да ги префрлите на нов уред. Затоа, кога го вклучувате шифрирањето на целиот диск, погрижете се да ги зачувате овие клучеви или лозинки на безбедно место, како, на пример, на безбедна сметка во облак или на апликацијата за управување со лозинки на вашиот парламент.

ДАЛЕЧИНСКИ ПРИСТАП ДО УРЕДИ – ИСТО ТАКА ПОЗНАТ КАКО ХАКИРАЊЕ

Освен тоа што уредите треба да бидат физички безбедни, важно е да се заштитат од злонамерен софтвер. Security-in-a-Box на „Тактикал тек“ (Tactical Tech) дава корисен опис на тоа што е злонамерен софтвер и зошто е важно да се избегнува, што е малку адаптирано во остатокот од овој дел.

Разбирање и избегнување злонамерен софтвер

Постојат многу начини за класификација на злонамерен софтвер. Вируси, шпионски софтвер, црви, тројанци, руткитови, уценувачки софтвер и криптоџекери, сите овие се видови злонамерен софтвер. Некои видови злонамерен софтвер се шират на интернет преку е-пошта, текстуални пораки, злонамерни веб-страници и на други начини. Некои се шират преку уреди како мемориски дискови (УСБ-меморија), кои се користат за размена и за кражба на податоци. И, додека некои злонамерни софтвери бараат некоја несвесна цел да направи грешка, други можат тивко да ги заразат ранливите системи без вие да направите нешто погрешно.

Покрај општиот злонамерен софтвер, кој е широко распространет и е насочен кон поширокатa јавност, целниот злонамерен софтвер обично се користи за попречување или за шпионирање одредено лице, организација или мрежа. Овие техники ги користат криминалци, но, исто така, и воени и разузнавачки служби, терористи, вознемирувачи на интернет, насилни сопружници и сомнителни политички актери.

Како и да се нарекуваат, како и да се дистрибуираат, злонамерните софтвери може да ги уништат компјутерите, да украдат и уништат податоци, да го нарушат работењето на парламентот, да ја нарушат приватноста и да ги доведат корисниците во опасност. Накратко, злонамерниот софтвер е навистина опасен. Сепак, постојат неколку едноставни чекори што може да ги преземе вашиот парламент за да се заштити од оваа вообичаена закана.

Дали алатка за заштита од злонамерен софтвер (антималвер) ќе нè заштити?

„Антималвер“ алатките, за жал, не се целосно решение. Сепак, многу добра идеја е да користите некои основни, бесплатни алатки како основа. Злонамерниот софтвер се менува толку брзо и со новите ризици во реалниот свет толку често, така што потпирањето на која било таква алатка не може да биде вашата единствена одбрана.

Ако користите Виндоус, треба да го земете предвид вградениот Windows Defender. Компјутерите со Мек и Линукс немаат вграден „антималвер“ софтвер, ниту, пак, уредите со Андроид и иОС. Можете да инсталирате реномирана, бесплатна алатка, како на пример Bitdefender или Malwarebytes, за тие уреди (и за компјутерите со Виндоус). Но, не се потпирајте на нив како ваша единствена одбранбена линија бидејќи тие сигурно ќе пропуштат некои од најтаргетираните, најопасни нови напади.

Освен тоа, бидете многу внимателни и преземајте реномирани „антималвер“ или антивирусни алатки само од легитимни извори (како што се веб-страниците дадени погоре). За жал, постојат многу лажни или компромитирани верзии на „антималвер“ алатки кои прават многу повеќе штета отколку корист.

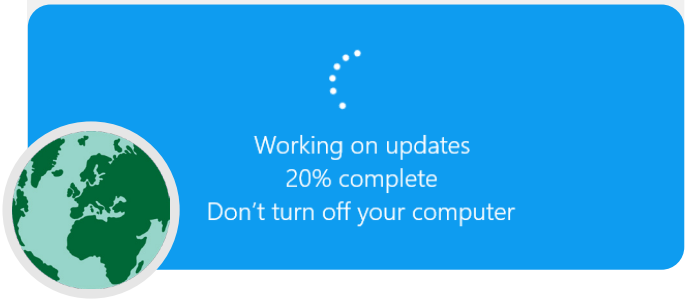
Доколку користите Bitdefender или друга „антималвер“ алатка во рамките на вашиот парламент, осигурете се да не користите две во исто време. Многу од нив ќе го идентификуваат однесувањето на другата „антималвер“ програма како сомнително и ќе ја спречат да работи, така што на крајот и двете ќе бидат неисправни. Bitdefender или други реномирани „антималвер“ програми може да се ажурираат бесплатно, а вградениот Windows Defender се ажурира заедно со вашиот компјутер. Осигурете се дека вашиот „антималвер“ софтвер се ажурира редовно (некои пробни верзии на комерцијален софтвер што се испорачуваат заедно со компјутерите ќе бидат оневозможени по истекот на пробниот период, по што ќе бидат повеќе опасни отколку корисни). Секој ден се пишува и дистрибуира нов злонамерен софтвер, а вашиот компјутер брзо ќе стане уште поранлив доколку не бидете во чекор со новите злонамерни софтвери и техниките за справување со нив. Ако е можно, треба да го конфигурирате вашиот софтвер за автоматски да инсталира ажурирања. Ако вашата „антималвер“ алатка има опционална функција секогаш да биде вклучена („always on“), треба да ја овозможите и повремено да ги скенирате сите датотеки на вашиот компјутер.

Ажурирајте ги уредите

Ажурирањата се од суштинска важност. Користете ја најновата верзија на кој било оперативен систем кој работи на уредот (Виндоус, Мек, Андроид, иОС итн.) и ажурирајте го тој оперативен систем. Ажурирајте ги и другите софтвери, веб-пребарувачи и сите дополнителни компоненти на веб-пребарувачот. Инсталирајте ги ажурирањата веднаш штом ќе станат достапни, најдобро со вклучување автоматски ажурирања. Колку е поажуриран оперативниот систем на уредот, толку помалку ранлив ќе биде. Замислете ги ажурирањата како да ставате фластер на отворена исеченица: ја запечатува ранливоста и во голема мера ја намалува можноста да се инфицира. Исто така, деинсталирајте го софтверот што веќе не го користите. Застарениот софтвер често има безбедносни проблеми, а можеби сте инсталирале алатка којашто веќе не се ажурира од страна на компанијата што ја развила, што, пак, ја прави поранлива на хакери.

Злонамерниот софтвер во реалниот свет: Ажурирањата се од суштинска важност

Во 2017 година **нападите со уценувачкиот софтвер WannaCry** заразија милиони уреди насекаде низ светот, при што беа затворени болници, владини субјекти, големи и мали организации и бизниси во десетици земји. Зошто нападот беше толку ефикасен? Поради застарени, „незакрпени“ оперативни системи на Виндоус, од кои повеќето првично беа пиратски. Голем дел од штетата – човечка и финансиска – можеше да се избегне со подобри автоматизирани практики за ажурирање и употреба на легитимни оперативни системи.



Внимавајте со УСБ-дисковите

Бидете внимателни кога отворате датотеки што ви се испраќаат како прилози, преку врски за преземање или на кој било друг начин. **Исто така, размислете двапати пред да вметнете пренослив медиум како УСБ-дискови**, флеш мемориски картички, дивидија и цедеа во вашиот компјутер, бидејќи тие може да бидат вектор за злонамерен софтвер. УСБ-дисковите што се споделувале одредено време е многу веројатно дека имаат вируси на нив. За алтернативни опции за безбедно споделување датотеки во рамките на вашиот парламент, погледнете го **делот Споделување датотеки** од овој прирачник.

Бидете внимателни и со кои други уреди се поврзувате преку Блутут (Bluetooth). Во ред е да го синхронизирате преку Блутут вашиот телефон или компјутер со познат и сигурен звучник за да си ја пуштите вашата омилена музика, но внимавајте со поврзувањето или прифаќањето барања од уреди што не ги препознавате. Дозволувајте поврзување преку Блутут само со сигурни уреди и не заборавајте да го исклучите кога не го користите.

Бидете паметни додека пребарувате на интернет

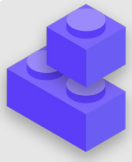
Никогаш не прифаќајте и не стартувајте апликации од веб-страници што не ги познавате и на кои не им верувате. Наместо да прифатите „ажурирање“ понудено во скок-прозорец на веб-пребарувачот, на пример, проверете дали има ажурирања на официјалната веб-страница на релевантната апликација. Како што беше дискутирано во **делот „Фишинг“**, од суштинско значење е да бидете внимателни кога пребарувате веб-страници. Проверете ја дестинацијата на врската (така што ќе поминете врз неа) пред да кликнете, погледнете ја адресата на веб-страницата откако ќе ја следите врската и проверете дали изгледа соодветно пред да внесете чувствителни информации, како, на пример, вашата лозинка. Не кликајте на пораки за грешки или предупредувања и внимавајте на прозорци на веб-пребарувачот што се појавуваат автоматски и внимателно читајте ги наместо само да кликнете „Да“ или „ОК“.

Злонамерниот софтвер во реалниот свет: Злонамерни мобилни апликации

Хакерите во повеќе земји со години користат лажни апликации во Google Play за да дистрибуираат злонамерен софтвер. Еден **конкретен случај**, кој како цел ги имал корисниците во Виетнам, излезе на виделина во април 2020 година. Оваа шпионска кампања користела лажни апликации, кои наводно им помагале на корисниците да најдат пабови во близина или да бараат информации за локални цркви. Откако несвесните корисници на Андроид ќе ги инсталирале, злонамерните апликации собирале евиденции на повици, податоци за локации и информации за контакти и текстуални пораки. Ова е само една од многуте причини да внимавате кои апликации ги преземате на вашите уреди.

Што е со паметните телефони?

Како и кај компјутерите, ажурирајте ги оперативниот систем и апликациите на телефонот и вклучете ги автоматските ажурирања. Инсталирајте ги само од официјални или сигурни извори, какви што се Play Store на „Гугл“ и App Store на „Епл“ (или F-droid, бесплатна продавница за апликации со отворен код за Андроид). Апликациите може да имаат вметнат злонамерен софтвер во нив и да изгледа дека работат нормално, така што нема секогаш да знаете дали некој софтвер е злонамерен. Исто така, погрижете се да преземете легитимна верзија на апликацијата. Особено на Андроид постојат „лажни“ верзии на популарни апликации. Затоа, осигурете се дека апликацијата е креирана од соодветната компанија или програмер, има добри критики и го има очекуваниот број преземања (на пример, лажна верзија на WhatsApp може да има само неколку илјади преземања, но вистинската верзија има над пет милијарди). Обрнете внимание на дозволите што ги бараат вашите апликации. Ако изгледаат претерано (како, на пример, калкулатор да бара пристап до вашата камера или Angry Birds да бара пристап до вашата локација), отфрлете го барањето или деинсталирајте ја апликацијата. Деинсталирањето на апликациите што веќе не ги користите, исто така, може да помогне да се заштитат вашиот паметен телефон или таблет. Програмерите понекогаш ја продаваат сопственоста на нивните апликации на други лица. Новите сопственици може да се обидат да заработат со додавање злонамерен код.



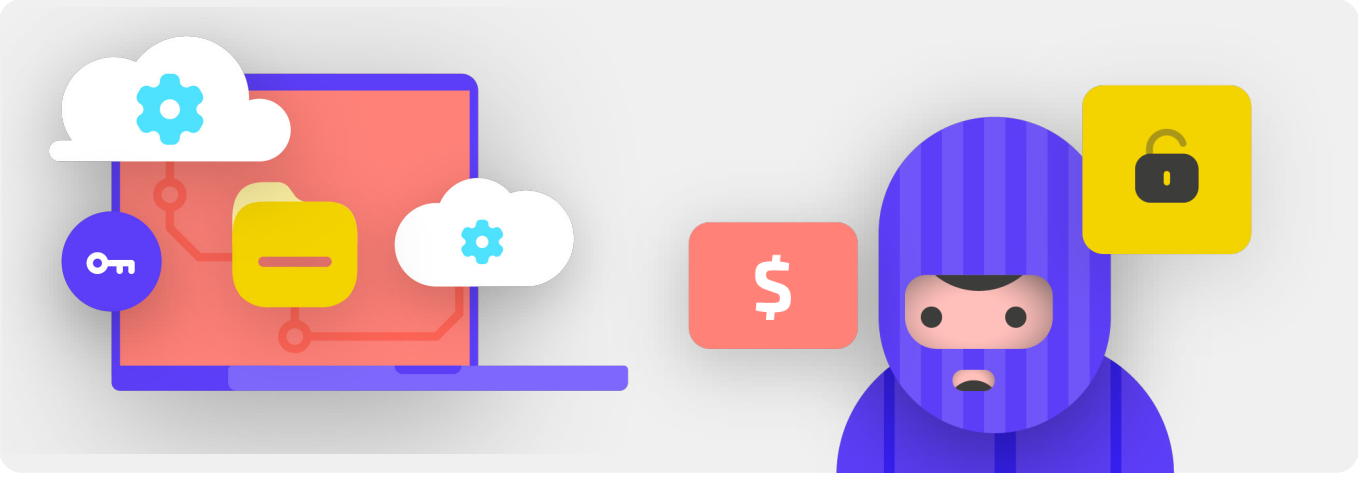
Основни елементи на планот за безбедност:

Одржување на безбедноста на уредите

- **Обучете ги членовите и вработените за ризиците од злонамерен софтвер и најдобрите практики за негово избегнување.**
  - Обезбедете политики за поврзување надворешни уреди, кликнување на врски, преземање датотеки и апликации и проверка на дозволите за софтвер и апликации.
- **Барајте уредите, софтверот и апликациите постојано да бидат целосно ажурирани.**
  - Вклучете ги автоматските ажурирања онаму каде што е можно.
- **Пријавете ги сите парламентарни уреди во систем за управување со мобилни уреди или систем за управување со уреди како крајни точки во мрежа (endpoint management system).**
- **Погрижете се сите уреди да користат лиценциран софтвер.**
- **Барајте заштита со лозинка на сите парламентарни уреди, вклучувајќи ги и приватните мобилни уреди кои се користат за комуникации поврзани со парламентот.**
- **Овозможете шифрирање на целиот диск на уредите.**
- **Често потсетувајте ги членовите и вработените да се грижат за физичката безбедност на своите уреди – и управувајте со безбедноста на вашата канцеларија со соодветни брави и начини за заштита на компјутерите.**
- **Не споделувајте датотеки користејќи УСБ-дискови и не приклучувајте УСБ-дискови на вашите компјутери.**
  - Наместо тоа, користете алтернативни безбедни опции за споделување датотеки.

„Фишинг“: Честа закана за уредите и за сметките

„Фишингот“ е најчестиот и најефикасен напад врз организациите, вклучително и парламентите, насекаде низ светот. Оваа техника ја користат најсофистицираните национални и државни армии, како и малите измамници. „Фишинг“, едноставно кажано, е кога противникот се обидува да ве измами за да споделите информации кои би можеле да се искористат против вас или вашата организација. „Фишинг“ може да се случи преку е-пошта, текстуални пораки/СМС (често се нарекува СМС-фишинг или „смишинг“), апликации за пораки, како Вацап (WhatsApp), пораки или објави на социјалните медиуми или телефонски повици (често се нарекува гласовен фишинг или „вишинг“). „Фишинг- пораките“ може да се обидат да ве натераат да внесете чувствителни информации (како лозинки) на лажна веб-страница за да добијат пристап до некоја сметка, да побараат од вас да споделите приватни информации (како број на кредитна картичка) преку глас или текст или да ве убедат да преземете злонамерен софтвер кој може да го зарази вашиот уред. Како нетехнички пример, секој ден милиони луѓе добиваат лажни автоматизирани телефонски повици кои им кажуваат дека нивната банкарска сметка е компромитирана или дека нивниот идентитет е украден – а сето тоа е смислено за да ги измами луѓето несвесно да споделат чувствителни информации.



КАКО МОЖЕМЕ ДА ГО ИДЕНТИФИКУВАМЕ „ФИШИНГОТ“?

„Фишингот“ може да звучи страшно и невозможно да се фати, но има неколку едноставни чекори кои секој во парламентот може да ги преземе за да се заштити од повеќето напади. Следниве совети за одбрана од „фишинг“ се изменети и проширени од детелниот водич за „фишинг“ изготвен од [Фондацијата Слобода на печатот] и треба да се споделат со сите во парламентот и околу него, како и да се интегрираат во вашиот план за безбедност:

Понекогаш полето „од“ ве лаже

Внимавајте затоа што полето „од“ во вашата е-пошта може да биде лажно или фалсификувано за да ве измами. Вообичаено е испраќачите на „фишинг“ да креираат адреса за е-пошта која многу наликува на некоја легитимна адреса што ви е позната, но само малку погрешно напишана за да ве измамат. На пример, може да добиете е-пошта од некого со адреса „john@goooogle.com“ наместо „john@google.com“. Забележете ја вишокот буква во „google“. Можеби познавате некој со адреса на е-пошта „john@gmail.com“, но добивате „фишинг“ од имитатор кој креирал адреса „johm@gmail.com“ - единствената разлика е суптилната промена на буквата на крајот. Секогаш проверете двапати дали ја знаете адресата од каде е испратена е-поштата пред да продолжите. Сличен е концептот на „фишинг“ преку текстуални пораки, повици или апликации за пораки. Ако добиете порака од непознат број, размислете двапати пред да одговорите или да почнете интеракција со пораката.

„Фишингот“ и парламентите


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]

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: [redacted] | [redacted] | [redacted] | [redacted] | ocs.gov.af
Mail: [redacted] | [redacted]

Парламентите и другите владини актери насекаде низ светот редовно се цел на софистицирани, персонализирани „фишинг-напади“.

Федералните и локалните парламентарни функционери во Германија беа цел на „фишинг“ преку е-пошта во пресрет на изборите во 2021 година. Само неколку месеци претходно во Авганистан, **хакерска група користеше техники на фишинг за успешно да се инфилтрира** во поранешниот Совет за национална безбедност со преземање на идентитетот на портпаролот на поранешниот авганистански претседател Ашраф Гани. Хакерите испратија е-пошта (прикажана погоре) во која бараа од жртвите да отворат приложена датотека за која „портпаролот“ тврдел дека содржи грешка. Кога жртвите ја презеле и ја отвориле датотеката за да ја „потврдат грешката“, злонамерниот прилог внел злонамерен софтвер кој им овозможил на хакерите постојан пристап до компјутерите. Таквиот пристап им овозможил на хакерите да поставуваат и преземаат датотеки, да извршуваат команди на уредите по желба и да крадат високо чувствителни владини податоци.

Внимавајте на прилози

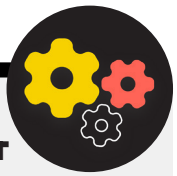
Прилозите може да имаат злонамерен софтвер и вируси, и најчесто ја придружуваат е-поштата што е „фишинг“. **Најдобар начин да избегнете злонамерен софтвер од прилозите е никогаш да не ги преземате**. По правило, не отворајте ги прилозите веднаш, особено ако се од лица што не ги познавате. Ако е можно, замолете го лицето што ви го испратило документот да го копира и залепи текстот во е-пошта или да го сподели документот преку услуга како Google Drive или Microsoft OneDrive, кои имаат вградено скенирање за вируси на повеќето документи поставени на нивните платформи. Изградете организациска култура во која не се користат прилози.

Доколку мора да го отворите прилогот, тој треба да се отвори само во безбедна средина (видете го делот Напредно ниво подолу), каде што потенцијалниот злонамерен софтвер не може да се пренесе на вашиот уред.

Ако користите Џимеил и примите прилог во е-пошта, наместо да го преземете и отворите на вашиот компјутер, едноставно кликнете на приложената датотека и прочитајте ја во преглед („preview“) во рамките на вашиот веб-пребарувач. Овој чекор ви овозможува да ги погледнете текстот и содржината на датотеката без да ја преземете или да ѝ дозволите да вчита можен злонамерен софтвер на вашиот компјутер. Ова функционира добро за документи во Ворд, ПДФ, па дури и за пауерпоинт-презентации. Ако треба да го уредите документот, отворете ја датотеката во програма во облак како Google Drive и конвертирајте ја датотеката во Google Doc или Google Slides.

Ако користите Аутлук (Outlook), можете на сличен начин да ги прегледате прилозите без да ги преземате од веб-клиентот. Ако треба да го уредите прилогот, отворете го во OneDrive, ако ви е достапен. Ако користите Јаху (Yahoo Mail), се применува истиот концепт. Не преземајте ги прилозите, туку прегледајте ги во рамките на веб-пребарувачот.

Без оглед на тоа какви алатки имате на располагање, најдобриот пристап е едноставно **никогаш да не преземате прилози што не ги знаете или на кои не им верувате**, и без оглед колку може да изгледа важен прилогот, никогаш не отворајте нешто во вид на датотека што не го препознавате или немате намера да го користите.



Напредно ниво: Одбрана од „фишинг“ за вашиот парламент

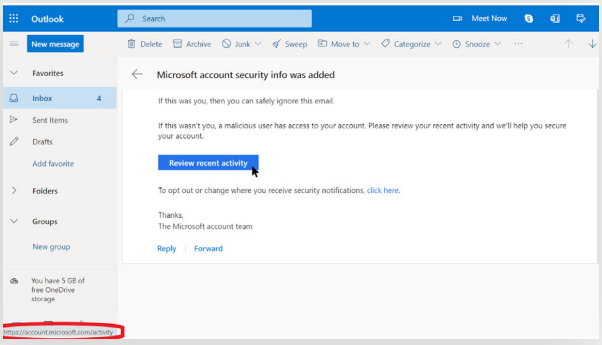
Ако вашиот парламент користи Мајкрософт 365 за е-пошта и други апликации, администраторот на вашиот домен треба да ја конфигурира политиката за Безбедни прилози за заштита од опасни прилози. Ако користите Гугл воркспејс (порано познат како GSuite), постои слична ефективна опција што треба да ја конфигурира вашиот администратор, наречена Google Security Sandbox. Понапредните индивидуални корисници може да размислат за поставување софистицирани sandbox програми, како што е Dangerzone или, за оние со Pro или Enterprise верзија на Windows 10, Windows Sandbox.

Друга напредна опција што може да се спроведе во рамките на парламентот е безбедна услуга за филтрирање на системот за имиња на домени (DNS). Парламентите може да ја користат оваа технологија за да ги блокираат вработените од случајно пристапување или интеракција со злонамерна содржина, обезбедувајќи дополнителен слој на заштита од фишинг. Новите услуги, како, на пример, Cloudflare's Gateway, им обезбедуваат такви можности на организациите без да бараат големи суми пари. Дополнителните бесплатни алатки, вклучувајќи ја и Quad9 од Комплетот со алатки на Глобалната сајбер алијанса, ќе ви помогнат да го блокирате пристапот до познати веб-страници кои имаат вируси или друг злонамерен софтвер и може да се постават за помалку од пет минути.

Кликнувајте со претпазливост

Бидете скептични кога се работи за врски во е-пошта или други текстуални пораки. Врските може да бидат маскирани за да преземете злонамерни датотеки или да ве одведат на лажни веб-страници кои може да ви побараат лозинки или други чувствителни информации. Кога сте на компјутер, постои едноставен трик за да бидете сигурни дека врската во е-пошта или порака ќе ве испрати таму каде што треба: Користете го глувчето за да поминете врз која било врска пред да кликнете на неа и погледнете во долниот дел од прозорецот на вашиот веб-пребарувач за да видите која е вистинската УРЛ-адреса (видете ја сликата подолу).

Потешко е да се проверат врските во е-пошта на мобилен уред без случајно да кликнете на нив – затоа бидете внимателни. Можете да ја проверите дестинацијата на врската на повеќето паметни телефони со долго притискање (држење) на врската додека не се појави целосната УРЛ-адреса. При „фишинг“ преку СМС и апликации за пораки, скратените врски се многу вообичаена практика што се користи за прикривање на дестинацијата на некоја УРЛ-адреса. Ако видите кратка врска (на пр., bit.ly или tinyurl.com) наместо целосна УРЛ-адреса, не кликнувајте на неа. Ако врската е важна, копирајте ја во проширувач на УРЛ-адреси, каков што е https://www.expandurl.net/, за да ја видите вистинската дестинација на скратената УРЛ-адреса. Исто така, не кликнувајте на врски до веб-страници што не ви се познати. Ако се сомневате, направете пребарување за веб-страницата, со нејзиното име во наводници (на пр. „www.badwebsite.com“) за да видите дали е легитимна веб-страница. Можете и да пуштите некои сомнителни врски низ скенерот за УРЛ-адреси на VirusTotal. Ова не е 100 проценти точно, но е добра мерка на претпазливост.



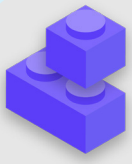
На крајот, ако кликнете на некоја врска од пораката и од вас се бара да се најавите на нешто, не правете го тоа освен ако не сте 100 проценти сигурни дека е-поштата е легитимна и дека ве испраќа на соодветната страница. Многу „фишинг-напади“ ќе содржат врски што ве испраќаат до лажни веб-страници за најавување на Џимеил, Фејсбук или други популарни страници. Не паѓајте на нив. Секогаш можете да отворите нов веб-пребарувач и сами да отидете директно на некоја позната страница како Џимеил, Фејсбук, итн. доколку сакате или треба да се најавите. На тој начин безбедно ќе дојдете до содржината – ако била воопшто легитимна.

Што треба да направиме кога ќе добиеме „фишинг-порака“?

Ако некој во парламентот добие непобаран прилог, врска, слика или поинаква сомнителна порака или повик, важно е веднаш да го пријави тоа до тимот задолжен за ИТ безбедност. Ако немате такво лице или тим, треба да го идентификувате како дел од изработката на вашиот план за безбедност. Вработените или членовите може да ја пријават е-поштата како спам или „фишинг“ и директно во Џимеил или во Аутлук.

Од клучна важност е да имате план за тоа што треба да направат вработените, членовите или волонтерите ако/кога ќе добијат можна „фишинг-порака“. Освен тоа, препорачуваме да ги искористите овие најдобри практики за „фишинг“ – да не кликнувате на сомнителни врски, да избегнувате прилози и да ја проверите адресата „од“ – и да не ги споделувате со другите колеги со кои работите, по можност преку широко користен канал за комуникација. Тоа покажува дека се грижите за луѓето со кои комуницирате и дека во рамките на вашите мрежи се поттикнува култура на внимателност и свесност за опасностите од „фишинг“. Вашата безбедност зависи од организациите на кои им верувате, и обратно. Подобрите практики ги штитат сите.

Покрај споделувањето на советите дадени погоре со сите, можете и да вежбате идентификување „фишинг“ со квизот за „фишинг“ Google Phishing Quiz. Исто така, силно препорачуваме да воспоставите редовна обука за „фишинг“ за вработените за да ја тестирате свесноста и за луѓето да бидат внимателни. Таквата обука може да се формализира како дел од редовните тимски и парламентарни состаноци или да се одржува понеформално. Она што е важно е сите што се вклучени во работењето на парламентот да се чувствуваат слободно да поставуваат прашања за „фишинг“ и да пријавуваат „фишинг“ (дури и ако сметаат дека можеби направиле грешка така што, на пример, кликнале на некоја врска), како и тоа дека секој може да помогне во одбраната на парламентот од оваа закана, која е со високо влијание и голема веројатност.



Основни елементи на планот за безбедност: „Фишинг“

- **Редовно обучувајте ги членовите и вработените за тоа што е „фишинг“ и како да го забележат и да се одбранат од него, вклучително и за „фишинг“ на текстуални пораки, апликации за пораки и телефонски повици, а не само преку е-пошта.**
- **Често потсетувајте ги членовите и вработените на најдобрите практики, како што се:**
- не преземајте непознати или потенцијално сомнителни прилози;
- проверете ја УРЛ-адресата на врската пред да кликнете, не кликнувајте на непознати или потенцијално сомнителни врски;
- не давајте чувствителни или приватни информации преку е-пошта, текстуална порака или телефонски повик на непознати или непотврдени адреси или лица.
- **Поттикнете пријавување на „фишингот“.**
  - Воспоставете механизам за известување и лице задолжено за „фишинг“ во парламентот.
  - Наградете го пријавувањето, но не казнувајте го непријавувањето
  - Reward reporting, and do not punish failure.

Безбедно комуницирање и складирање податоци

Комуницирање и споделување податоци

За да ги донесете најдобрите одлуки за вашиот парламент за тоа како да комуницирате, од суштинска важност е да ги разберете различните видови заштита којашто можете да ја имате и зошто таквата заштита е важна. Еден од најважните елементи на безбедноста на комуникацијата се однесува на одржувањето на приватноста на приватното комуницирање – за што, во модерната ера, во голема мера се грижи шифрирањето. Без соодветно шифрирање, внатрешната комуникација во рамките на парламентот може да ја видат голем број противници. Небезбедната комуникација може да разоткрие чувствителни или засрамувачки информации и пораки, да открие лозинки или други приватни податоци и можеби да ги изложи на ризик вашите членови или вработени во зависност од природата на информациите и содржината што ја споделувате.

Како парламент, исто така е важно да се осигурите дека официјалната владина комуникација меѓу членовите и вработените е во согласност со сите релевантни обврски на отворена влада (како што се барањата за слобода на информации) и обврските за безбедност на податоците. Затоа, кога дизајнирате и поставувате безбедни комуникациски системи и политики во рамките на парламентот, не заборавајте да ги имате предвид овие фактори за да можат релевантните пораки да бидат соодветно заштитени и зачувани (кога тоа е потребно според законот).

Безбедна комуникација и парламенти

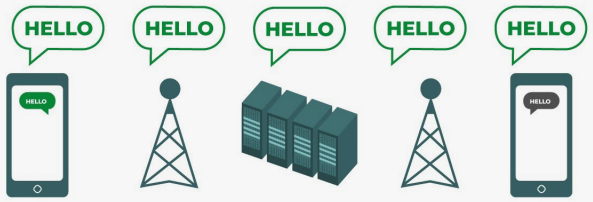
Во последниве години имаше многу инциденти во кои беа компромитирани комуникациските системи на парламентите и сметките на пратениците и нивниот кадар, што доведе до прекин во работењето на парламентите, а во некои случаи и кражба на чувствителни информации. Во јули 2021 година, на пример, полските власти објавија дека сметките на е-пошта на речиси десетина локални **пратеници биле хакирани**, вклучително и личната сметка на главниот помошник на премиерот и сметките на членови од речиси секоја парламентарна опозициска група. Овој извештај дојде само неколку месеци откако се појавија слични вести за кибернетски напад врз информациските и комуникациските системи на **финскиот парламент**. Властите во Финска **го опишаа тој напад** како „тешка шпионажа и пресретнување пораки“ насочени кон нејзиниот парламент.

ШТО Е ШИФРИРАЊЕ И ЗОШТО Е ВАЖНО?

Шифрирањето е математички процес кој се користи за менување порака или датотека, така што само лице или субјект со клуч може да ја „дешифрира“ и прочита. Без никакво шифрирање, нашите пораки се отворени и можат да бидат прочитани од потенцијални противници, вклучително и непријателски странски влади или хакери на интернет. Таквото шифрирање е важно не само за внатрешната комуникација во рамките на парламентот, туку и за надворешната комуникација во која треба да се заштитат приватноста и интегритетот. **Водичот за самоодбрана од надзор** на фондацијата Електронски граници дава практично објаснување, со графикони, за тоа што значи шифрирањето:

Нешифрирано пренесување пораки

Without any encryption in place, our messages are left open to being read by potential adversaries, including unfriendly foreign governments, or hackers on the web. Such encryption is important not just for internal parliamentary communications but also for external communications in which privacy and integrity need to be protected.

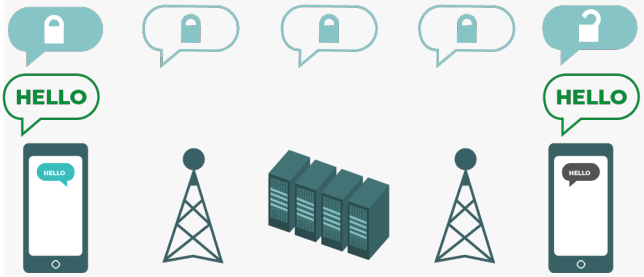


Како што можете да видите на сликата погоре, паметен телефон испраќа зелена, нешифрирана текстуална порака („здраво“) на друг паметен телефон. При тој процес, базната станица (или во случај кога нешто се испраќа преку интернет, вашиот давател на интернет-услуги, познат како ISP) ја пренесува пораката до серверите на компанијата. Оттаму таа поминува низ мрежата до друга базна станица, која може да ја види нешифрираната порака „здраво“ и потоа се насочува кон дестинацијата. Важно е да се спомне дека без никакво шифрирање, секој што е вклучен во пренесувањето на пораката и секој што може да ја сирне додека таа поминува, може да ја прочита нејзината содржина. Ова можеби не е многу важно ако кажувате само „здраво“, но може да биде голема работа ако комуницирате за нешто поприватно или чувствително што не сакате вашиот давател на телекомуникациски услуги, давател на интернет-услуги, непријателска влада или кој било друг противник да го види. Поради тоа, од суштинска важност е да се избегнува користење нешифрирани алатки за испраќање чувствителни пораки (и најдобро за никакви пораки). Имајте предвид дека некои од најпопуларните начини на комуникација – како што се СМС и телефонски повици – практично функционираат без никакво шифрирање (како на сликата погоре).

Постојат два начина на шифрирање на податоците додека се движат: **шифрирање на транспортен слој и целосно, од крај до крај, шифрирање**. Важно е да се знае видот на шифрирање што го поддржува давателот на услугата бидејќи вашиот парламент прави избор со цел да усвои побезбедни комуникациски практики и системи. Ваквите разлики се добро опишани во **Водичот за самоодбрана од надзор**, кој повторно е адаптиран овде:

Шифрирање на транспортниот слој

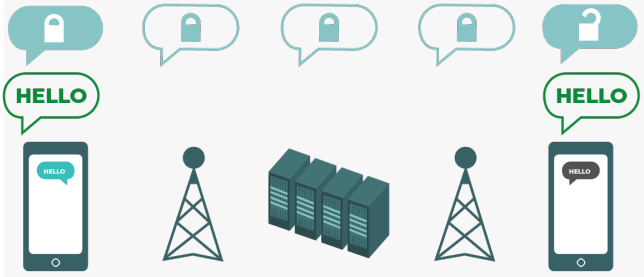
Шифрирањето на транспортниот слој, познато и како безбедност на транспортниот слој (TLS), ги штити пораките додека патуваат од вашиот уред до серверите на апликацијата/услугата за пораки и од таму до уредот на примачот. Тоа ги штити од љубопитните очи на хакерите кои се наоѓаат кај вашите даватели на мрежни, интернетски или телекомуникациски услуги. Меѓутоа, вашиот давател на услуги за пораки/е-пошта, веб-страницата што ја пребарувате или апликацијата што ја користите, кои се наоѓаат во средината, може да гледаат нешифрирани копии од вашите пораки. Бидејќи вашите пораки може да се видат и често се складираат на серверите на компаниите, тие може да бидат ранливи на барањата на органите
за спроведување на законот или на кражба доколку серверите на компанијата се компромитирани.



Сликата погоре покажува пример за шифрирање на транспортниот слој. На левата страна, паметен телефон испраќа зелена, нешифрирана порака „Здраво“. Таа порака е шифрирана и потоа се пренесува до базната страница. Во средината, серверите на компанијата можат да ја дешифрираат пораката, да ја прочитаат содржината, да одлучат каде да ја испратат, повторно да ја шифрираат и да ја испратат до следната базна станица кон нејзината дестинација. На крајот, другиот паметен телефон ја прима шифрираната порака и ја дешифрира за да прочита „Здраво“.

Целосно, од крај до крај, шифрирање

Целосното, од крај до крај, шифрирање ги заштитува пораките во транзит од испраќачот до примачот. Осигурува информациите да се претворат во тајна порака од неговиот оригинален испраќач (првиот „крај“) и да се дешифрираат само од неговиот краен примач (вториот „крај“). Никој, вклучително и апликацијата или услугата што ја користите, не може да „ја слуша“ и да ја прислушува вашата активност.



Сликата погоре покажува пример за целосно, од крај до крај, шифрирање. На левата страна, паметен телефон испраќа зелена, нешифрирана порака „Здраво“. Таа порака е шифрирана, а потоа се пренесува до базната станица и потоа до серверите на апликацијата/услугата, кои не можат да ја прочитаат содржината, но ќе ја пренесат тајната порака до нејзината дестинација. На крајот, другиот паметен телефон ја прима шифрираната порака и ја дешифрира за да прочита „Здраво“. За разлика од шифрирањето на транспортниот слој, вашиот давател на интернет-услуги или хостот за пораки не може да ја дешифрира пораката. Само крајните точки (оригиналните уреди кои испраќаат и примаат шифрирани пораки) ги имаат клучевите за дешифрирање и читање на пораката.

КАКОВ ВИД ШИФРИРАЊЕ НИ Е ПОТРЕБНО?

Кога ќе одлучувате дали на вашиот парламент му треба шифрирање на транспортен слој или целосно, од крај до крај, шифрирање за вашата комуникација (или некоја комбинација од двете за различни системи и активности), важните прашања што треба да ги поставите вклучуваат доверба. На пример, дали Ќ верувате на апликацијата или услугата што ја користите? Дали Ќ верувате на нејзината техничка инфраструктура? Дали сте загрижени за можноста дека една непријателска странска влада би можела да ја принуди компанијата да Ќ ги предаде вашите пораки – и ако е така, дали им верувате на политиките на компанијата за заштита од барања на странски органи за спроведување на законот?

Ако одговорот е „не“ на кое било од овие прашања, тогаш ви треба целосно, од крај до крај, шифрирање. Ако одговорот е „да“ на овие прашања, тогаш услугата што поддржува само шифрирање на транспортен слој може да биде доволна – но, генерално, подобро е да се користат услуги што поддржуваат целосно, од крај до крај, шифрирање, кога е тоа можно.
Друга група прашања што треба да се земат предвид е дали од вас како парламент се бара со закон да одржувате единствен пристап до парламентарната комуникација, дали има какви било барања за локализација на податоците во вашата земја и/или дали одредена комуникација треба да се зачува (на пр., вработените да не ја бришат трајно) со цел да биде во согласност со законите и заложбите за отворена влада. Ако е така, може да размислите за комуникациски систем со овозможено целосно, од крај до крај, шифрирање за компании, во кој вие, како парламент, ќе можете сами да ги контролирате клучевите за шифрирање. Таквите системи (за кои подетално ќе се дискутира во делот „**Безбедно складирање податоци**“) може да бидат моќни, но бараат напредни технички вештини за спроведување.

Исто така, кога разменувате пораки со групи, имајте предвид дека безбедноста на вашите пораки е добра колку што е добра безбедноста на сите што ги примаат пораките. Покрај внимателното избирање безбедни апликации и системи, важно е сите во групата да ги следат другите најдобри практики во врска со безбедноста на сметките и безбедноста на уредите. Доволен е само еден злонамерен актер или еден заразен уред неовластено да ја открие содржината на разговорот или повикот на цела група.

ШТО ТРЕБА ДА НАПРАВИМЕ ВО ВРСКА СО Е-ПОШТАТА?

Општо земено, е-поштата не е најдобрата опција кога станува збор за безбедност. Дури и најдобрите опции за целосно, од крај до крај, шифрирана е-пошта, обично, не се доволно добри од безбедносен аспект, на пример не се шифрира предметот на е-поштата и не се заштитуваат метаподатоците (важен концепт кој ќе биде опишан подолу). Ако треба да пренесете многу чувствителни информации што не треба да се зачуваат за јавна евиденција, имајте предвид дека е најдобро е-поштата (и системот на парламентот и особено нечија лична сметка) да се избегнува и да се замени со безбедни опции за пораки (кои ќе бидат истакнати во следниот дел).

Меѓутоа, како парламент, можеби, ќе сакате или ќе имате потреба членовите и вработените да пренесат чувствителна или приватна содржина преку систем којшто е централно управуван како дел од нивното секојдневно работење. Тука може да биде корисен систем за е-пошта на ниво на цел парламент, со соодветни контроли на сметките, се разбира. Ако, според вашата анализа погоре, шифрирањето на транспортниот слој е доволно, тогаш стандардните деловни понуди од давателите на услуги за е-пошта, како Гугл воркспејс (Џимеил) и Мајкрософт 365 (Аутлук), би можеле да бидат солидни опции за вашиот парламент. Меѓутоа, ако сте загрижени дека од вашиот давател на услуги за е-пошта може законски да биде побарано да обезбеди информации за вашата комуникација на странска влада или на друг противник, или ако можеби сте загрижени за локалните барања за резидентност на податоците, ќе сакате да ја земете предвид опцијата за целосно, од крај до крај, шифрирана е-пошта. Неколку такви опции вклучуваат додавање сопствено управување со клучеви за шифрирање на Гугл воркспејс или Мајкрософт 365 (како што е опишано во делот **„Безбедно складирање податоци“**) или прифаќање услуги за целосно, од крај до крај, шифрирана е-пошта дизајнирани за големи организации, како што се **ProtonMail** Business или **Tutanota** Business.

ШТО СЕ МЕТАПОДАТОЦИ И ДАЛИ ТРЕБА ДА БИДЕМЕ ЗАГРИЖЕНИ ЗА НИВ?

Со кого разговарате вие и вашите вработени, членовите и тимовите, и кога и каде разговарате со тие лица, честопати може да биде подеднакво чувствително како и она за што зборувате. Важно е да се запамети дека целосното, од крај до крај, шифрирање ја заштитува само содржината („што“) на вашата комуникација. Тука стапуваат на сцена метаподатоците. Водичот за самоодбрана од надзор на фондацијата Електронски граници дава преглед на метаподатоците и зошто тие се важни (вклучувајќи и илустрација за тоа како изгледаат метаподатоците):

Метаподатоците често се опишуваат како сè освен содржината на вашата комуникација. Можете да ги замислите метаподатоците како дигитален еквивалент на плик. Исто како што пликот содржи информации за испраќачот, примачот и за дестинацијата на пораката, така и метаподатоците.

Метаподатоците се информации за дигиталните информации што ги испраќате и примате. Некои примери на метаподатоци се:

- со кого комуницирате
- предметот на вашата е-пошта
- должината на вашите разговори
- времето кога се случил разговорот
- вашата локација кога комуницирате

Иако транспарентноста на парламентарното работење е од суштинско значење, ограничувањето на неовластениот пристап до метаподатоците (покрај заштитата на содржината на комуникациите), исто така, е важно. Сепак, метаподатоците може да им откријат чувствителни информации на хакерите, странските влади, компаниите или на други лица кои можеби не сакате да имаат пристап. Неколку примери за тоа колку информации можат да откријат метаподатоците се:

Знаат дека пратеник или вработен повикал новинар и разговарал со него еден час пред тој новинар да објави напис со цитирање анонимен извор. Меѓутоа, не знаат за што зборувале.

Знаат дека сте добиле е-пошта од службата за тестирање за КОВИД, потоа дека сте се јавиле на вашиот лекар, па дека сте ја посетиле веб-страницата на Светската здравствена организација во истиот час. Меѓутоа, не знаат што било напишано во е-поштата или за што сте разговарале на телефон.

Препорачани алатки за целосно, од крај до крај, шифрирана комуникација

ТЕКСТУАЛНИ ПОРАКИ (ЗА ПОЕДИНЦИ ИЛИ ГРУПА)	• **Signal** • **WhatsApp (само со конкретни конфигурации за поставки наведени подолу)**
АУДИО- И ВИДЕОПОВИЦИ	• **Signal (до 40 лица)** • **WhatsApp (до 32 лица на аудио, осум лица на видео)**
СПОДЕЛУВАЊЕ ДАТОТЕКИ	• **Signal** • **Keybase/Keybase Teams** • **Tresorit**

КОИ АЛАТКИ ЗА ЦЕЛОСНО, ОД КРАЈ ДО КРАЈ, ШИФРИРАНИ ПОРАКИ ТРЕБА ДА ГИ КОРИСТИМЕ (ОД 2022 ГОДИНА)?

Ако треба да користите целосно, од крај до крај, шифрирање или ако само сакате да ја усвоите најдобрата практика без оглед на контекстот на заканата за вашиот парламент, еве неколку сигурни примери на услуги кои, од 2022 година, нудат целосно. од крај до крај, шифрирани пораки и повици. Овој дел од прирачникот редовно ќе се ажурира електронски, но имајте предвид дека работите брзо се менуваат во светот на безбедните пораки, така што овие препораки може да не се ажурирани во моментот кога го читате овој дел. Имајте предвид дека вашата комуникација е безбедна колку и самиот уред. Така што, покрај усвојувањето на практиките за безбедни пораки, од суштинска важност е да се спроведат најдобрите практики опишани во делот „Безбедни уреди“.

Метаподатоците не се заштитени со шифрирањето што го обезбедуваат повеќето услуги за пораки. Ако испраќате порака на Вацап (WhatsApp), на пример, имајте предвид дека иако содржината на вашата порака е целосно, од крај до крај, шифрирана, можно е другите да знаат на кого испраќате порака, колку често и, за телефонски повици, колку долго сте зборувале. Како резултат на тоа, треба да имате предвид какви ризици постојат (ако ги има) доколку одредени противници се во можност да откријат со кого разговарате, кога сте разговарале со тие лица и (во случај на е-пошта) општиот предмет на комуникацијата на вашиот парламент.Една од причините поради кои Сигнал **(Signal)** толку многу се препорачува е тоа што обезбедува целосно, од крај до крај, шифрирање, **воведува функции и се обврзува**

да ја намали количината на метаподатоци што ги снима и складира. На пример, функцијата „Запечатен испраќач“ (Sealed Sender) на Сигнал ги шифрира метаподатоците за тоа кој со кого разговара, така што Сигнал го знае само примачот на пораката, но не и испраќачот. Стандардно, оваа функција функционира само кога комуницирате со постојни контакти или профили (лица) со кои веќе сте комуницирале или кои сте ги зачувале во вашиот список со контакти. Меѓутоа, можете да ја овозможите оваа поставка „Запечатен испраќач“ (Sealed Sender) и да ја поставите на „Дозволи од сите“ (Allow from anyone) ако ви е важно да ги елиминирате таквите метаподатоци во сите разговори преку Сигнал, дури и во оние со луѓе што не ги познавате. Ова можеби не е од клучно значење за поголемиот дел од парламентарната комуникација, но важно е да се биде свесен за ризиците што ги носат метаподатоците и според тоа да се изберат соодветни алатки и политики за комуникација.

ДАЛИ, НАВИСТИНА, МОЖЕМЕ ДА Ѝ ВЕРУВАМЕ НА ВАЦАП?

Вацап (WhatsApp) е популарен избор на апликација за безбедна размена на пораки и може да биде добра опција со оглед на нејзината сеприсутност. Некои луѓе се загрижени затоа што е сопственост на Фејсбук и контролирана од Фејсбук, кој работи на нејзино интегрирање со неговите други системи. Луѓето се загрижени и за количината на метаподатоци (т.е. информации за тоа со кого комуницирате и кога) што ги собира Вацап. Ако изберете да користите Вацап како опција за безбедна размена на пораки, не заборавајте да го прочитате горниот дел за метаподатоците. Исто така, има неколку поставки за кои треба да се осигурите дека се правилно конфигурирани. Најважно е да го исклучите креирањето резервни копии во облак или, во најмала рака, да ја овозможите новата функција за креирање целосно, од крај до крај, шифрирани резервни копии на Вацап со користење клуч за шифрирање од 64 цифри или долга, случајна и уникатна лозинка зачувана на безбедно место (како, на пример, во вашата апликација за управување со лозинки). Исто така, погрижете се да го овозможите прикажувањето безбедносни известувања и да ги потврдите безбедносните кодови. Можете да најдете едноставни упатства за конфигурирање на овие поставки за телефони со Андроид **овде** и за ајфон **овде**. **Ако вашите вработени* и оние со кои сите комуницирате* не ги конфигурираат правилно овие опции, тогаш не треба да ја сметате Вацап за добра опција за чувствителни комуникации за кои е потребно целосно, од крај до крај, шифрирање**. Сигнал сè уште е најдобрата опција за потребите за целосно, од крај до крај, шифрирани пораки со оглед на неговите безбедни стандардни поставки и заштитата на метаподатоците.

ШТО СЕ СЛУЧУВА СО РАЗМЕНАТА НА ТЕКСТУАЛНИ ПОРАКИ?

Основните текстуални пораки се многу несигурни (стандардната СМС, всушност, е нешифрирана) и треба да се избегнуваат за сè што не е наменето за јавноста. Иако пораките на „Епл“ од ајфон до ајфон (познати како iMessages) се целосно, од крај до крај, шифрирани, ако во разговорот има некој што не користи ајфон, пораките не се безбедни. Најдобро е да бидете безбедни и да **избегнувате текстуални пораки за сè што е барем малку чувствително, приватно или доверливо**.

ЗОШТО ТЕЛЕГРАМ, ФЕЈСБУК МЕСИНЏЕР ИЛИ ВАЈБЕР НЕ СЕ ПРЕПОРАЧУВААТ ЗА БЕЗБЕДНИ РАЗГОВОРИ?

Некои услуги, како што се Фејсбук месинџер и Телеграм, нудат целосно, од крај до крај, шифрирање само ако намерно го вклучите (и само за разговори еден на еден), така што тие не се добри опции за чувствителни или приватни пораки, особено за тимови. Не потпирајте се на овие алатки ако треба да користите целосно, од крај до крај, шифрирање бидејќи многу лесно може да заборавите да ги смените стандардните поставки кои се помалку безбедни. Вајбер тврди дека нуди целосно, од крај до крај, шифрирање, но не го направил својот код достапен за ревизија на надворешни безбедносни истражувачи. Кодот на Телеграм, исто така, не е достапен за јавна ревизија. Како резултат на тоа, многу експерти стравуваат дека шифрирањето на Вајбер (или „тајните разговори“ на Телеграм) можеби е под стандардите и затоа не е соодветно за комуникација за која е потребно вистинско целосно, од крај до крај, шифрирање.

НАШИТЕ ПАРЛАМЕНТАРНИ КОЛЕГИ И ИЗБИРАЧИ КОРИСТАТ ДРУГИ АПЛИКАЦИИ И СИСТЕМИ ЗА ПОРАКИ ЗА КОМУНИКАЦИЈА – КАКО МОЖЕМЕ ДА ГИ УБЕДИМЕ ДА ПРЕЗЕМАТ НОВА АПЛИКАЦИЈА ЗА ДА КОМУНИЦИРААТ СО НАС?

Понекогаш доаѓа до компромис меѓу безбедноста и удобноста, но вреди да се вложи малку дополнителен напор за чувствителната комуникација. Поставете добар пример за вашите контакти – без разлика дали се во други владини агенции, институции, во рамките на парламентот или надворешни избирачи. Ако треба да користите други помалку безбедни системи, бидете многу внимателни што зборувате. Избегнувајте дискусии на чувствителни теми. Некои парламенти може да имаат различни протоколи за општи разговори или комуникации со јавноста во споредба со доверливите дискусии со раководството, на пример. Класифицирајте ги вашите парламентарни комуникации (внатрешни и надворешни) врз основа на чувствителноста и, соодветно на тоа, погрижете се членовите и вработените да користат соодветни механизми за комуникација! Се разбира, наједноставно е ако сè е постојано автоматски шифрирано – нема што да се запамети или на што да се мисли.

За среќа, целосно, од крај до крај, шифрираните апликации, каква што е Сигнал, стануваат сè попопуларни и лесни за користење – а освен тоа се локализирани на десетици јазици за глобална употреба. Ако на вашите партнери или на други контакти им е потребна помош за да ја префрлат комуникацијата на целосно, од крај до крај, шифрирана опција, каква што е Сигнал, одвојте малку време за да им објасните зошто е толку важно правилно да ја заштитите вашата комуникација. Кога сите ќе ја разберат важноста, неколкуте минути што се потребни за преземање нова апликација и неколкуте дена што можеби ќе бидат потребни за да се навикнат да ја користат нема да изгледаат како голема работа.

ДАЛИ ИМА ДРУГИ ПОСТАВКИ ЗА ЦЕЛОСНО, ОД КРАЈ ДО КРАЈ, ШИФРИРАНИ АПЛИКАЦИИ ШТО ТРЕБА ДА ГИ ЗНАЕМЕ?

Во апликацијата Сигнал е важно и потврдувањето на безбедносните кодови (кои тие ги нарекуваат Безбедносни броеви). За да го видите безбедносниот број и да го потврдите во Сигнал, можете да го отворите разговорот со контактот, да го допрете неговото име на горниот дел од екранот и да одите надолу за да го допрете „Прикажи безбедносен број“ (View Safety Number). Ако вашиот безбедносен број се совпаѓа со вашиот контакт, можете да го означите како „потврден“ од истиот екран. Особено е важно да обрнете внимание на овие безбедносни броеви и да ги потврдите вашите контакти ако добиете известување во разговор дека безбедносниот број за одреден контакт е променет. Ако вам или на другите вработени ви треба помош при конфигурирање на овие поставки, Сигнал **обезбедува корисни упатства**. Ако ја користите апликацијата Сигнал, која нашироко се смета за најдобра и лесна за користење опција за безбедни пораки и повици еден на еден, погрижете се да **поставите силна шифра**. Користете најмалку шест цифри, а не нешто што може да се погоди лесно, како, на пример, вашиот датум на раѓање.
За повеќе совети за тоа како правилно да ги конфигурирате **Signal** и **WhatsApp,** можете да ги погледнете **упатствата со алатки** за двете апликации, креирани од фондацијата Електронски граници во нивниот **Водич за самоодбрана од надзор**.

ШТО СО ПОГОЛЕМИТЕ ГРУПНИ ВИДЕОПОВИЦИ? ДАЛИ ИМА ОПЦИИ ЗА ЦЕЛОСНО, ОД КРАЈ ДО КРАЈ, ШИФРИРАЊЕ?

Со зголемувањето на работењето од далечина, важно е да имате безбедна опција за големи групни видеоповици од вашата канцеларија или виртуелни сали за пратениците. За жал, во моментов не постојат одлични опции што ги исполнуваат сите критериуми: лесни за користење,

поддржуваат голем број учесници и функции за соработка и стандардно овозможуваат целосно, од крај до крај, шифрирање. Специфичните потреби на пленарните сесии и состаноците на комисиите ќе бидат дискутирани подоцна во овој прирачник, но за другите ваши поопшти состаноци за кои не се потребни напредни функции за соработка, како што се посебни соби за состаноци, се препорачува Сигнал. На групните видеоповици на Сигнал може да се придружат најмногу 40 учесници, или од паметен телефон или од десктоп апликацијата на Сигнал на компјутер, што овозможува споделување на екранот. Сепак, имајте предвид дека само вашите контакти што веќе користат Сигнал, може да се додадат во групата на Сигнал.

Ако барате други опции, една платформа која неодамна додаде опција за целосно, од крај до крај, шифрирање е Џитси мит (**Jitsi Meet**). Џитси мит е решение за аудио- и за видеоконференции засновано на веб што може да се користи за големи групи (до 100 луѓе) и не бара преземање апликација или посебен софтвер. Имајте предвид дека ако ја користите оваа функција со големи групи (повеќе од 15-20 луѓе), квалитетот на повикот може да се намали. За да закажете состанок на Џитси мит, можете да отидете на **meet.jit.si**, да го внесете кодот за состанокот и да ја споделите врската (преку безбеден канал, каков што е Сигнал) со вашите учесници. За да користите целосно, од крај до крај, шифрирање, погледнете ги овие **упатства** изработени од Џитси. Имајте предвид дека сите поединечни корисници ќе треба сами да овозможат целосно, од крај до крај, шифрирање за да може тоа да функционира. Кога користите Џитси мит, погрижете се да креирате случајни имиња на посебните соби за состаноци и да користите силни лозинки за да ги заштитите вашите повици.

Ако оваа опција не функционира за вашите тимови, можете да користите некоја популарна комерцијална опција, како Вебекс (Webex) или Зум (Zoom), која овозможува целосно, од крај до крај, шифрирање. Вебекс долго време овозможува целосно, од крај до крај, шифрирање; сепак, оваа опција не е стандардно вклучена и учесниците треба да го преземат Вебекс за да се приклучат на вашиот состанок. За да ја добиете целосно, од крај до крај, шифрираната опција за вашата сметка на Вебекс, мора да отворите случај за поддршка на Вебекс (Webex support case) и да ги следите **овие упатства** за да се осигурите дека целосното, од крај до крај, шифрирање е конфигурирано. Само домаќинот на состанокот треба да овозможи целосно, од крај до крај, шифрирање. Ако тој го стори тоа, целиот состанок ќе биде целосно, од крај до крај, шифриран. Ако користите Вебекс за безбедни групни состаноци и работилници, поставете и силни лозинки за вашите повици.

По неколку месеци негативни критики во медиумите, Зум креираше **опција за целосно од-крај-до-крај шифрирање** за своите повици. Сепак, таа опција не е стандардно вклучена, туку домаќинот на повикот треба да ја поврзе својата сметка со телефонски број и функционира само ако сите учесници се приклучат преку десктоп или преку мобилната апликација на Зум наместо да се приклучуваат преку повик. Бидејќи лесно може случајно погрешно да се конфигурираат овие поставки, не е најдобра опција да се потпрете на Зум како целосно, од крај до крај, шифрирана опција. Меѓутоа, ако е потребно целосно, од крај до крај, шифрирање, а Зум е вашата единствена опција, можете да ги следите **упатствата** на Зум за да го конфигурирате. Само не заборавајте да го проверите повикот пред тој да почне за да се осигурите дека е навистина целосно, од крај до крај, шифриран со кликнување на зеленият катанец во горниот лев агол на екранот на Зум, каде што ќе можете да видите „од крај до крај“ наведено до поставката за шифрирање. Треба да поставите и силна лозинка за секој состанок на Зум.

Меѓутоа, треба да се спомне дека одредени популарни функции на наведените алатки работат само со шифрирање на транспортниот слој. На пример, со вклучување на целосното, од крај до крај, шифрирање во Зум се оневозможуваат посебните соби за состаноци, можностите за правење анкети и снимањето во облак. Во Џитси мит посебните соби за состаноци може да ја оневозможат функцијата за целосно, од крај до крај, шифрирање, што доведува до несвесно намалување на безбедноста.

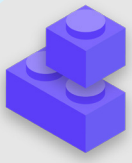
БЕЛЕШКА ЗА СПОДЕЛУВАЊЕ ДАТОТЕКИ

Покрај безбедното споделување пораки, безбедното споделување датотеки, веројатно, е важен дел од планот за безбедност на вашиот парламент. Повеќето опции за споделување датотеки се вградени во апликациите или услугите за пораки кои можеби веќе ги користите. На пример, споделувањето датотеки преку Сигнал е одлична опција доколку е потребно целосно, од крај до крај, шифрирање. Ако шифрирањето на транспортниот слој е доволно, користењето на Google Drive или Microsoft SharePoint може да биде добра опција за вашиот парламент. Само погрижете се правилно да ги конфигурирате поставките за споделување, така што само соодветните луѓе да имаат пристап до даден документ или папка и осигурете се дека овие услуги се поврзани со организациските (не личните) сметки за е-пошта на вработените. Ако можете, забранете споделување чувствителни датотеки преку прилози на е-пошта или физички со УСБ-меморија. Користењето уреди како УСБ-меморија во вашиот парламент значително ја зголемува веројатноста од злонамерен софтвер или кражба, а потпирањето на е-пошта или други форми на прилози ја ослабува одбраната на вашиот парламент од „фишинг-напади“.

ШТО АКО НАВИСТИНА НЕ НИ ТРЕБА ЦЕЛОСНО, ОД КРАЈ ДО КРАЈ, ШИФРИРАЊЕ ЗА ЦЕЛАТА НАША КОМУНИКАЦИЈА?

Ако не е потребно целосно, од крај до крај, шифрирање за целата комуникација на вашиот парламент врз основа на вашата процена на ризикот, можете да користите апликации заштитени со шифрирање на транспортниот слој. Запомнете, за овој тип шифрирање е потребно да му верувате на давателот на услугата, како што се Гугл за Џимеил, Мајкрософт за Аутлук/Ексчејнџ или Фејсбук за Месинџер, бидејќи тие (и секој со кој тие би биле принудени да споделуваат информации) можат да ги видат/слушаат споделените информации. Уште еднаш, најдобрите опции ќе зависат од вашиот модел на закани (на пример, ако не му верувате на Гугл или ако Владата на САД е ваш противник, тогаш Џимеил не е добра опција), но некои популарни и генерално сигурни опции се:

Е-ПОШТА	• **Gmail (преку Google Workspace)** • **Outlook (преку Office 365)** • Не хостирајте го вашиот Microsoft Exchange сервер за е-поштата на вашиот парламент. Ако моментално го правите тоа, треба да **мигрирате** на Office 365.
ТЕКСТУАЛНИ ПОРАКИ (ЗА ПОЕДИНЦИ ИЛИ ЗА ГРУПА)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
ГРУПНИ КОНФЕРЕНЦИСКИ, АУДИО- И ВИДЕОПОВИЦИ	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
СПОДЕЛУВАЊЕ ДАТОТЕКИ	• **Google Drive** • **Microsoft SharePoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Основни елементи на планот за безбедност: Безбедно комуницирање и споделување податоци

- **Класифицирајте ја комуникацијата врз основа на нејзината чувствителност.**
  - Одредете ги соодветните системи и алатки за комуникација соодветно.
  - Воспоставете политика за тоа колку долго ќе ги чувате пораките, имајќи ги предвид безбедноста и заложбите за транспарентност на парламентот.
- **Барајте да се користат сигурни услуги за целосно, од крај до крај, шифрирана размена на пораки за чувствителната комуникација на вашиот парламент.**
  - Одвојте време да им објасните на вработените и на надворешните партнери зошто безбедната комуникација е толку важна; тоа ќе го подобри успехот на вашиот план.
- **Осигурете се дека се поставени соодветните поставки за апликациите за безбедна комуникација, односно:**
  - Осигурете се дека сите вработени посветуваат внимание на безбедносните известувања и, доколку користат Вацап, не прават резервни копии од разговорите.
  - Ако користите апликација во која целосното, од крај до крај, шифрирање не е стандардно овозможено (на пр., Зум или Вебекс), осигурете дека потребните корисници ги вклучиле соодветните поставки на почетокот на кој било повик или состанок.
- **Не обидувајте се да го хостирате вашиот сопствен сервер за е-пошта – користете ги како алтернативи услугите за е-пошта засновани на облак, како што се Офис 365 или Гугл воркспејс.**
  - Не дозволувајте им на вработените да користи лични сметки за е-пошта за работа.
- **Често потсетувајте ги вработените и членовите за најдобрите безбедносни практики поврзани со групните пораки и метаподатоци.**
  - Водете сметка за тоа кој е вклучен во групните пораки, разговори и нишки со последователни пораки преку е-пошта (email threads).

Дигитални парламенти (е-парламент)

Како парламент, важно е да посветите особено внимание на комуникациските и на оперативните безбедносни политики на вашите најважни функции, вклучително и оние на интернет и во дигиталниот простор. Без оглед на тоа дали вашиот парламент размислува за целосен „е-парламент“, кој може да дигитализира сè, од изготвување нацрт-закони до дебати и електронско гласање (како што се **Nextsense**, **Propylon** или **Granicus** кои се само неколку примери), или дали користите поедноставни, помалку скапи алатки за олеснување на вашето парламентарно работење, од суштинско значење е да разгледате како секоја алатка (или алатки) и процес (или процеси) ги земаат предвид безбедноста, интегритетот и достапноста на информациите.

Безбедноста и дигиталните парламенти

Како што беше потврдено од **серијата инциденти** во Јужна Африка, транзицијата на парламентарното работење кон дигиталниот свет бара внимавање на кибернетската безбедноста за да се избегне не само губење или кражба на чувствителни податоци, туку и потенцијална засраменост, навреда и штета на членовите и на вработените. Во мај 2020 година се појавија порнографски слики неколку минути пред почетокот на виртуелниот состанок на Националното собрание на земјата. По прикажувањето на навредливите слики, „хакерот“ или „натрапникот на Зум“ потоа упати сексистички и расни навреди кон спикерот на Собранието, кој беше домаќин на седницата, принудувајќи го да го прекине состанокот. Сличен инцидент се случи еден месец претходно кога состанокот со кој претседаваше министерката за жени, млади и лица со попреченост беше прекинат со порнографски слики.

ПЛЕНАРНИ СЕДНИЦИ И СОСТАНОЦИ НА КОМИСИИТЕ ОД ДАЛЕЧИНА

Главни меѓу тие процеси се пленарните седници и состаноците на комисиите. Овие седници, дискусиите, одлуките и гласањата што се случуваат на нив се клучни за поголемиот дел од работата на вашиот парламент и како такви можат да бидат особена цел за противниците. Во модерниот свет погоден од пандемијата, ваквите сесии и состаноци се одржуваат на сè поразновиден начин, во зависност од контекстот на вашата земја - лично, целосно преку интернет и на „хибриден“ начин.

Како што е наведено во неодамнешниот водич за **Одговор на парламентите на пандемијата** на Комисијата за демократско партнерство на Претставничкиот дом, типичната структура на парламентарна расправа се разликува од една вообичаена конференциска дискусија или стандарден организациски состанок. Потребите за гласање од далечина, поднесување официјални предлози и амандмани, структурирана расправа, па дури и симултано толкување за да се обезбеди вклучување на сите изборни единици честопати изискуваат дополнителни функции кои не се наоѓаат во повеќето стандардни технолошки решенија. Како резултат на тоа, при хостирање виртуелна или хибридна сесија, веројатно е дека вашиот парламент, можеби, ќе треба да развие (или веќе има развиено) прилагоден софтвер или да купи скапи, деловни решенија (како што е **Cisco's Webex Legislate**) дизајнирани специјално за управување со парламентарни седници од далечина. Без оглед на опцијата што ќе ја избере вашиот парламент, важно е да размислите, како што е наведено во водичот за **Одговор на парламентите на пандемијата**, за тоа како сите членови и вработени ќе можат да пристапат до таков систем. Исто така, од клучно значење е да се осигури дека таквиот систем има соодветна заштита.

Кога се изготвуваат и спроведуваат технички решенија за парламентарните седници, важно е да се обезбеди дека се воспоставени основните безбедносни принципи. Тие вклучуваат чекори за осигурување дека податоците се безбедни „во мирување“ во рамките на самиот систем, соодветно шифрирани додека се во транзит и дека само овластени корисници можат да пристапат до системот. Постојат многу пристапи кои можат да се преземат за да се воспостави таквата безбедност, вклучувајќи и многу од основните принципи наведени во остатокот од овој прирачник. Корисни чекори се целосно, од крај до крај, шифрирање на сите системи за споделување податоци и комуницирање, барања за силна лозинка и автентикација со два фактора и/или ограничување на ИП-адресата за пристап на корисниците до таквите системи (освен ако тие се наменети да бидат отворени за јавноста), барање за виртуелни приватни мрежи (за што ќе се дискутира подоцна во прирачникот) и ограничување на пристапот само на сигурни, чисти уреди.

ГЛАСАЊЕ ОД ДАЛЕЧИНА

Потребата за силна безбедност, можеби, е најважна кога се работи за гласање од далечина. Како што е нагласено во споменатиот водич за **Одговор на парламентите на пандемијата**, пратениците се избираат во парламентот со конкретна цел да гласаат во име на нивните избирачи. Можноста да им верувате и да ги потврдите овие гласови е од клучно значење не само за функционирањето на вашиот парламент, туку и за демократскиот систем како целина. Ваквите гласови релативно лесно се проверуваат кога пратеникот гласа лично, но кога се учествува виртуелно, техничката автентикација станува поголем предизвик што изискува значителна грижа и фокус. Како што е наведено во експертското **сведочење** пред Постојаниот комитет за процедурални и внатрешни прашања на канадскиот Долен Дом, парламентите обично избираат една од четирите опции за гласање од далечина:

- Гласање преку е-пошта: каде што членовите добиваат формулар за гласање по електронски пат и го доставуваат својот глас преку е-пошта. Оваа опција, генерално, се смета за небезбедна, делумно поради недостигот на целосно, од крај до крај, шифрирање, и треба да се избегнува.
- Гласање засновано на веб: каде што членовите пристапуваат и гласаат преку веб-страница или на компјутер или на мобилен телефон. За овој пристап е потребна инвестиција во безбедна инфраструктура, вклучително и безбедни уреди со силни контроли за автентикација како што е споменато погоре.
- Гласање засновано на апликација: каде што членовите преземаат апликација за да пристапат и да гласаат. Слично на гласањето засновано на веб, но се користи специфична апликација, која може да се преземе на телефон или на таблет, за разлика од пристапот преку веб-пребарувач.
- Видеогласање: каде што членовите гласаат на екранот со кревање рака или на глас. За неанонимно гласање, ова може да биде најмалку технички компликувано и најмалку технички софистицирано за поставување и заштита. Сепак, потребни се силни системи за шифрирање и автентикација за да се избегне имитирање или прекин за време на сесиите за гласање.

Без оглед на опцијата што ќе ја избере вашиот парламент за да спроведе гласање од далечина – ако воопшто користи гласање од далечина – важно е да се земат предвид основите на кибернетската безбедност и во текот на процесот на гласање. Ваквите основи вклучуваат осигурување дека уредите што ги користат пратениците за да гласаат се соодветно физички заштитени и немаат злонамерен софтвер, дека пристапот до интернет е соодветно заштитен при гласањето (и при спроведување други парламентарни активности) и дека пратениците имаат стабилни интернет-врски и можат да гласаат кога ќе бидат повикани. Како што е наведено во водичот за **Одговор на парламентите на пандемијата**, кога се усвојува гласање од далечина, постои

потреба од опширно тестирање на системот пред да почне да се применува и потреба да се обезбеди поддршка и обука на пратениците за да се осигури дека тие можат да го користат системот ефективно. Важно е да се запамети дека дел од безбедноста е достапноста. Исто така, постои потреба особено да се осигури дека пратеничките и вработените можат безбедно да ги користат електронските системи, вклучително и гласањето од далечина, и да имаат пристап до технологијата за таа цел. Кога жените, особено жените избрани на одредена функција, одат на интернет, тие се соочуваат со поголемо ниво на заплашување и вознемирување, а овој фактор треба да се земе предвид при развивањето и користењето технологија како што е гласањето од далечина за да се осигури дека сите пратеници можат да ги исполнуваат своите функции ефикасно. Понатаму, од клучно значење е да се обезбеди соодветен далечински повеќејазичен пристап во земјите каде што членовите и вработените зборуваат повеќе формални јазици.

НАБАВУВАЧ НА Е-ПАРЛАМЕНТ И БЕЗБЕДНОСТ НА СОФТВЕРОТ

Секој софтвер што ќе го набавите – без разлика дали се користи за гласање од далечина или за поширок опсег на парламентарни потреби – **треба да потекнува од безбеден и акредитиран извор, да помине ревизија за безбедност од независни тимови и да добие соодветни сертификати**. Важно е да се запамети дека развивачите на софтвер, оние кои ги ангажирате за да направат апликација или алатка, не се секогаш експерти за безбедност. Затоа, вклучувањето безбедносни експерти за тестирање на апликацијата во однос на потенцијални безбедносни недостатоци преку ревизија е од клучно значење за намалување на ризикот вашата платформа, алатка или апликација да биде хакирана или компромитирана. Дури и најдобрите развивачи на софтвер прават грешки ако втор (или трет) експерт не ја провери нивната работа!

Гласање од далечина во реалниот свет

Различни парламенти имаат спроведено системи за гласање од далечина и притоа имаат преземено значителни чекори за да ги осигураат безбедноста и интегритетот на гласовите на членовите. Еден елемент во овој процес, меѓу другите споменати погоре, е да се обезбеди соодветна автентикација. Неколку примери се Долниот Дом на Обединетото Кралство каде што членовите користат процес на еднократна најава за да се најават на нивните парламентарни сметки пред да гласаат, за што е потребно да се користи лозинка на одреден, доделен уред. Во Шпанија, на пратениците им се доделуваат лични кодови кои мора да се внесат преку апликација за паметен телефон пред да се евидентира гласањето од далечина. Во Чиле, сенаторите што гласаат од далечина преку внимателно дизајнираната апликација за гласање од далечина на Домот на пратеници мора да се гледаат на екранот за да можат да гласаат.

Безбедно складирање податоци

За повеќето парламенти, една од најважните одлуки што треба да ги донесат е каде да ги складираат нивните податоци. Дали е „побезбедно“ да се складираат податоци на службените компјутери, на локален сервер, на надворешни уреди за складирање или во облак? Во 99 проценти од ситуациите, најлесната и најбезбедна опција е податоците да се складираат кај доверливи даватели на услуги за складирање во облак. Можеби највообичаени примери се Мајкрософт 365 и Гугл драјв. Без сеопфатен план за складирање во облак, веројатно податоците на вашиот парламент ќе бидат складирани на различни места – вклучувајќи ги компјутерите на вработените и пратениците, надворешните тврди дискови, па дури и на неколку локални сервери. Иако е можно да се направат безбедни податоците на сите овие уреди, многу е тешко тоа да се направи успешно без да се потрошат многу пари и да се ангажира значаен ИТ кадар.

Складирање на податоците и парламентите

Појавата на достапно (понекогаш бесплатно) складирање податоци засновано на облак го направи работењето на многу парламенти и други организации полесно и побезбедно. За жал, многумина сè уште се обидуваат да хостираат свои сервери со релативно ограничен ИТ буџет, кадар и поддршка. Во март 2021 година, заканата од таквата организациска инфраструктура стана реална за десетици илјади организации, вклучително и парламенти, насекаде низ светот кога еден предизвикувач на закана поврзан со кинеската влада, наречен Хафниум, предизвика глобална катастрофа за кибернетската безбедност со софистициран напад врз самохостираните сервери на Мајкрософт ексчејнџ. Нападот ги компромитираше локалните сервери, вклучително и оној на норвешкиот парламент, овозможувајќи им на хакерите да добијат пристап до парламентарните сметки за е-пошта, да инсталираат дополнителен злонамерен софтвер на серверите на жртвата и на поврзаните системи и на крајот да извлечат чувствителни податоци.

Иако Мајкрософт брзо објави ажурирање и упатства за идентификување и отстранување на потенцијалните натрапници откако хакирањата беа објавени во јавноста, на многу организации им недостигаше ИТ капацитет за брзо да ги применат таквите ажурирања поради што беа незаштитени подолг временски период. Обемот и влијанието на ова глобално хакирање ја покажува опасноста за парламентите и другите организации кои избираат сами да хостираат сервери за е-пошта и други видови чувствителни податоци, особено без значителни инвестиции во кадар посветен на кибернетската безбедност.

ПРИДОБИВКИ ОД СКЛАДИРАЊЕТО ВО ОБЛАК

Дури и ако ги преземете сите вистински чекори за да ги заштитите вашите компјутери од злонамерен софтвер и физичка кражба, сепак е можно некој решителен противник да го хакира вашиот компјутер или локалниот сервер на парламентот. Ним им е многу потешко да ја совладаат безбедносната одбрана на Гугл или на Мајкрософт, на пример. Добрите компании за складирање во облак имаат неспоредливи безбедносни ресурси и имаат силна деловна мотивација да обезбедат максимална безбедност за своите корисници. Накратко: една сигурна стратегија за складирање во облак ќе биде многу полесно да се спроведе и да се одржува безбедноста со текот на времето. Затоа, наместо да се обидувате да го идентификувате (и задржите) посветениот и висококвалификуван кадар за кибернетска безбедност потребен за заштита на локалните сервери во вашиот парламент, фокусирајте ја својата енергија на неколку поедноставни задачи. Тие вклучуваат избор на вистинската опција за складирање во облак за вашите потреби за приватност и локализација на податоците, спроведување добра безбедност на сметките, обука на вработените за правилно споделување (и несподелување) папки и документи (генерално, треба да поставите папки во вашиот диск за складирање во облак кои го ограничуваат пристапот само на кадарот на кој му е потребен пристап до одредени датотеки) и рутинска ревизија на вашиот систем за да се осигурите дека вработените и членовите не „споделуваат премногу“ датотеки (на пример, со вклучување на универзални врски за споделување датотеки кои треба да бидат ограничени само на неколку лица). Складирањето на најголемиот дел од вашите информации во облак помага при низа вообичаени ризици. Дали нечиј компјутер бил оставен во ресторан или нечиј телефон во автобус? Дали вашето дете истурило чаша сок врз вашата тастатура поради што вашиот уред е нефункционален? Дали треба да ги одделите посебно податоците што ѝ припаѓаат на пратеничката од информациите што таа ги креира за парламентот? Дали вработен има злонамерен софтвер и треба да го избрише својот компјутер и да почне одново да работи на него? Ако повеќето документи и податоци се во облак, лесно е повторно да се направи синхронизација и да се почне одново да се работи на исчистен или на целосно нов компјутер. Исто така, ако злонамерен софтвер влезе во некој компјутер или ако некој крадец скенира тврд диск, нема што да украде ако на повеќето документи се пристапува преку веб-пребарувач.

МОЖЕМЕ ЛИ, НАВИСТИНА, ДА МУ ВЕРУВАМЕ НА СКЛАДИРАЊЕТО ВО ОБЛАК?

Накратко, нема никаква суштинска причина зошто не би му верувале на складирањето во облак. Како што веќе беше спомнато, повеќето големи даватели на услуги за складирање во облак имаат тимови од најдобрите светски инженери за безбедност кои секојдневно работат на заштита на нивните производи и нудат безбедносна поддршка за своите клиенти во поголем обем од она што повеќето мали ИТ сектори би можеле да го обезбедат. Меѓутоа, имајте предвид дека традиционалните услуги за складирање во облак обично изискуваат доделување пристап до чувствителни податоци на компанија-трета страна која ја обезбедува услугата. **Имајќи го предвид тоа, секој поединечен парламент ќе има свои политички согледувања и законски барања (како што се барањата за локализација на податоците) кои треба да ги земе предвид кога ќе избира дали може да му верува и да користи одреден давател на услуги за складирање во облак.**

КОЈ ДАВАТЕЛ НА УСЛУГИ ЗА СКЛАДИРАЊЕ ВО ОБЛАК ТРЕБА ДА ГО ИЗБЕРЕМЕ?

Ако вашиот парламент не мора да зема предвид никакви барања за локализација на податоците и нема проблем со тоа да сподели пристап до податоците со доверлива компанија-трета страна, двете најпопуларни опции за складирање во облак се Гугл воркспејс (порано познат како GSuite) и Мајкрософт 365. Ако вашиот парламент веќе користи Џимеил, би имало многу смисла да го регистрирате на Гугл воркспејс и да складирате податоци во Гугл драјв со неговите вградени апликации Гугл докс, шитс и слајдс за обработка на текст, табели и презентации. Слично на тоа, ако вашиот парламент се потпира на Ексел и Ворд, лесната опција е да се регистрирате на Мајкрософт 365, кој овозможува пристап до Аутлук за е-пошта и лиценцирани верзии на Ворд, Ексел, Пауерпоинт и Тимс.

ШТО АКО ТРЕБА ДА ГИ КОНТРОЛИРАМЕ СОПСТВЕНИТЕ ПОДАТОЦИ ИЛИ ДА ГИ ПОЧИТУВАМЕ ЗАКОНИТЕ ЗА ЛОКАЛИЗАЦИЈА НА ПОДАТОЦИ?

За многу парламенти, таквата едноставна опција, можеби, не е изводлива со оглед на барањата за локализација на податоците или специфичните очекувања кои изискуваат ексклузивна контрола на парламентот врз сопствените податоци. Добрата вест е дека неодамна давателите на услуги за безбедно складирање во облак креираа опции кои им овозможуваат на клиентите од претпријатијата или да ја изберат локацијата на нивните податоци (имајте предвид дека засега ова е главно ограничено на европските клиенти) или да ги контролираат нивните клучеви за шифрирање. **Во практика тоа значи дека вашиот парламент има опции да ги контролира сопствените податоци, а, сепак, да има корист од инфраструктурата и безбедноста на складирањето во облак.**

Ако вашиот парламент моментално користи или е заинтересиран за Гугл воркспејс за складирање и споделување податоци во облак, Гугл воведе функција која овозможува **шифрирање на страната на клиентот** за организации во Ентерпрајз плус (Enterprise Plus). Иако моментално е во фаза на тестирање и е достапна само за најскапите планови на Гугл воркспејс, оваа функција обезбедува опција за искористување на целосниот пакет функции за складирање и споделување податоци на Гугл драјв – и безбедносните функции вградени во нив – истовремено ограничувајќи ја способноста на Гугл за пристап до чувствителните или приватните информации на вашиот парламент. Со шифрирање на страната на клиентот, можете да изберете да интегрирате дополнителна услуга за управување со клучеви, како што е Virtru, и да им дозволите на корисниците да управуваат со сопствените клучеви за шифрирање без да му дадат пристап на Гугл. Таквата услуга бара од сите да внимаваат за да ги заштитат тие клучеви со цел правилно да го заштитат пристапот до кој било систем за управување со клучеви што ќе изберат да го интегрираат во Гугл воркспејс. Администраторите на сметките можат да дознаат повеќе за тоа како да овозможат шифрирање на страната на клиентот на **страницата за поддршка** на Гугл воркспејс.

Ако вашиот парламент моментално користи или е заинтересиран за Мајкрософт 365 за складирање и споделување податоци во облак, тој нуди малку посложена, но добро воспоставена опција за управување со вашите клучеви за шифрирање, позната како **шифрирање со два клуча на Microsoft 365**. Оваа безбедносна опција бара од **Microsoft 365 E5,** но ви овозможува и вам да ги контролирате сите чувствителни или приватни парламентарни податоци и да го ограничите пристапот дури и на самиот Мајкрософт.

Tresorit е уште една опција која е поедноставна за спроведување ако вашиот парламент е загрижен во однос на дозволувањето на трета страна да пристапи до вашите внатрешни информации. Tresorit обезбедува целосно, од крај до крај, шифрирање за складирање во облак и споделување датотеки и нуди низа **опции за резидентност на податоците**.

ШТО АКО НЕ МОЖЕМЕ ДА ВЕРУВАМЕ НА НИТУ ЕДНО РЕШЕНИЕ ЗА СКЛАДИРАЊЕ ВО ОБЛАК?

Ако одлучите сами да го сторите тоа и да се потпрете на локални сервери за складирање на податоците на вашиот парламент, од клучно значење е да вложите значително време и ресурси во зајакнувањето на дигиталната одбрана на уредите на вашиот парламент и да се осигурите дека таквите сервери се соодветно конфигурирани, шифрирани и физички безбедни. Како што веќе е наведено, таквиот пристап бара идентификување, ангажирање и задржување на одреден посветен и висококвалификуван кадар за кибернетска безбедност за да ја одржува безбедноста на вашата локална серверска инфраструктура.

Напредно ниво: Зголемување на безбедноста на парламентарните сметки во облак

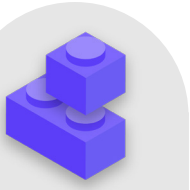
Ако вашиот парламент одлучи да постави домен на Гугл воркспејс или на Мајкрософт 365, имајте предвид дека и двете компании нудат повисоки нивоа на безбедност за ризични сметки. **Програмата за напредна заштита на Google** и **AccountGuard на Microsoft** обезбедуваат уште посилна безбедност на сметките во облак за подобните организации и ви помагаат значително да ја намалите веројатноста за „фишинг“ и компромитирање на сметката. Ако сметате дека вашиот парламент се квалификува и сте заинтересирани да ги вклучите вашите членови и вработени во кој било план, посетете ги веб-страниците дадени во врските погоре или контактирајте со **cyberhandbook@ndi.org** за понатамошна помош.

КРЕИРАЊЕ РЕЗЕРВНА КОПИЈА НА ПОДАТОЦИТЕ

Без разлика дали вашиот парламент складира податоци на физички уреди и сервери или во облак, важно е да имате резервна копија. Имајте предвид дека ако се потпирате на складирање на физички уреди, многу е лесно да го изгубите пристапот до вашите податоци. Може да истурите кафе на вашиот компјутер и да го уништите тврдиот диск. Компјутерите на вработените може да бидат хакирани и сите локални датотеки да бидат заклучени со уценувачки софтвер. Некој може да го изгуби уредот во воз или да му го украдат заедно со актовката. Како што веќе беше спомнато, ова е уште една причина зошто складирањето во облак може да биде корисно, бидејќи не е поврзано со одреден уред кој може да се зарази, изгуби или украде. Компјутерите со оперативен систем Мек имаат вграден софтвер за креирање резервна копија наречен **Time Machine**, кој се користи заедно со надворешен уред за складирање; за уредите со Виндоус, **File History** нуди слична функционалност. Ајфон и

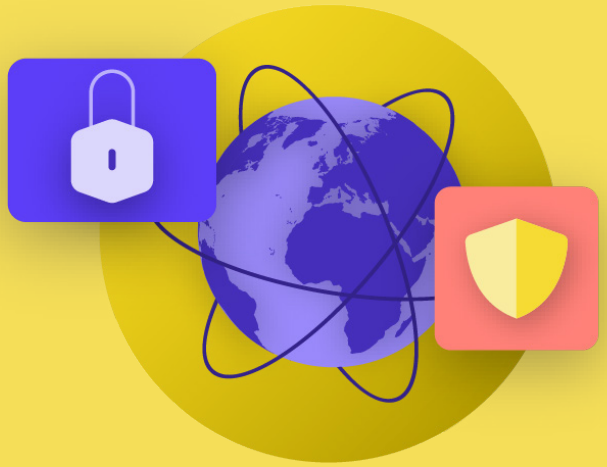
Андроид можат автоматски да креираат резервна копија на нивните најважни содржини во облак доколку тоа е овозможено во поставките на вашиот телефон.
Ако вашиот парламент користи складирање во облак (како Гугл драјв), ризикот Гугл да падне или вашите податоци да бидат уништени во катастрофа е прилично мал, но човечка грешка (како случајно бришење важни датотеки), сепак, е можна. Може да биде корисно да се испитаат решенија за креирање резервна копија во облак, како што се **Backupify** или **SpinOne Backup**.

Ако податоците се зачувани на локален сервер и/или на локални уреди, безбедните резервни копии се уште поважни. Можете да креирате резервна копија од податоците на вашиот парламент на надворешен тврд диск или на повеќе дискови, но не заборавајте да ги шифрирате таквите дискови со силна лозинка. Time Machine може да ви ги шифрира тврдите дискови или можете да користите сигурни алатки за шифрирање на целиот тврд диск, како VeraCrypt или BitLocker. Чувајте ги сите уреди со резервни копии на податоци на посебна локација од другите ваши уреди и датотеки. Запомнете, ако пожар ви ги уништи и вашите компјутери и нивните резервни копии, тоа значи дека воопшто немате резервни копии. Размислете да чувате копија на многу безбедна локација, како, на пример, сеф.



Основни елементи на планот за безбедност: Безбедно складирање податоци

- **Чувајте ги чувствителните податоци исклучиво кај сигурна услуга за складирање во облак.**
  - Погрижете се сите поврзани сметки што се користат за пристап до таква услуга да имаат силни лозинки и 2FA.
- **Воспоставете и спроведете политика за ограничување на поставките за споделување во рамките на облакот.**
  - Обучете ги сите членови и вработени за тоа како правилно да споделуваат (и да не споделуваат премногу) документи.
- **Ако вашиот парламент одлучи да складира податоци локално, инвестирајте во квалификуван кадар за ИТ.**
- **Погрижете се за безбедноста на резервните копии на вашите податоците – шифрирајте ги тврдите дискови или другите уреди со резервни копии на податоци.**



Безбедност на интернет

Кога користите интернет на вашиот телефон или компјутер, вашата активност зборува многу за вас. Важно е да ги чувате чувствителните информации – како што се корисничките имиња и лозинките што ги внесувате на веб-страница, вашите објави на социјалните медиуми или во одредени контексти дури и имињата на веб-страниците што ги посетувате – подалеку од љубопитните очи. Ако вашиот пристап до одредени веб-страници или апликации е блокиран или ограничен, тоа е причина за загриженост. Овие два проблема – надзорот на интернет и цензурата на интернет – одат рака под рака, а стратегиите за намалување на нивното влијание се слични.

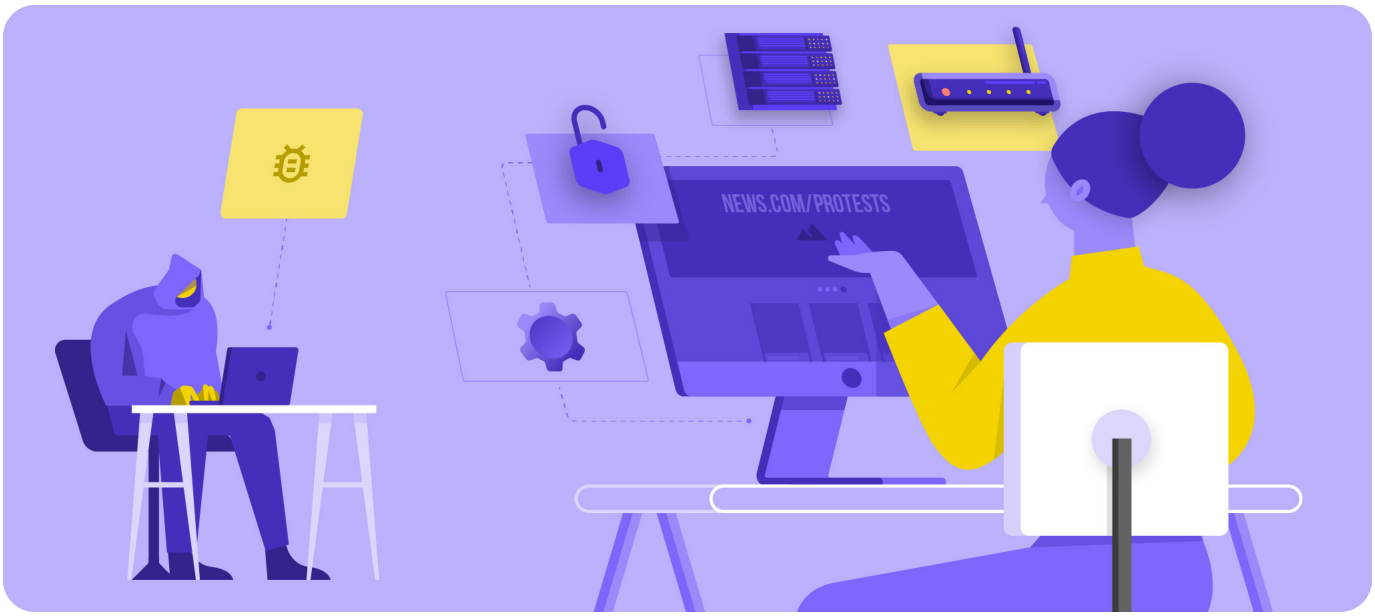
Безбедно пребарување на интернет

КОРИСТЕЊЕ ХТТПС (HTTPS)

Најважниот чекор за ограничување на способноста на противникот да го надгледува вашиот парламент на интернет е да се сведе на минимум количината на достапни информации за вашата активност на интернет, како и на вашите колеги. Секогаш погрижете се безбедно да се поврзувате на веб-страници: осигурете се дека УРЛ-адресата (локацијата) започнува со „https“ и дека се појавува мала икона со катанец во лентата за адреси на вашиот веб-пребарувач.

Кога пребарувате на интернет **без шифрирање**, информациите што ги внесувате на страницата (како лозинки, броеви на сметки или пораки) и деталите за локацијата и страниците што ги посетувате се незаштитени. Тоа значи дека (1) сите хакери на вашата мрежа, (2) вашиот мрежен администратор, (3) вашиот давател на интернетски услуги и кој било субјект со кој тие можеби споделуваат податоци (како владини органи), (4) давателот на интернетски услуги на страницата што ја посетувате и кој било субјект со кој тие можеби споделуваат податоци, и се разбира, (5) самата страница што ја посетувате имаат пристап до голем број потенцијално чувствителни информации.

Ајде да погледнеме пример од реалниот свет за тоа како изгледа пребарувањето на интернет без шифрирање:

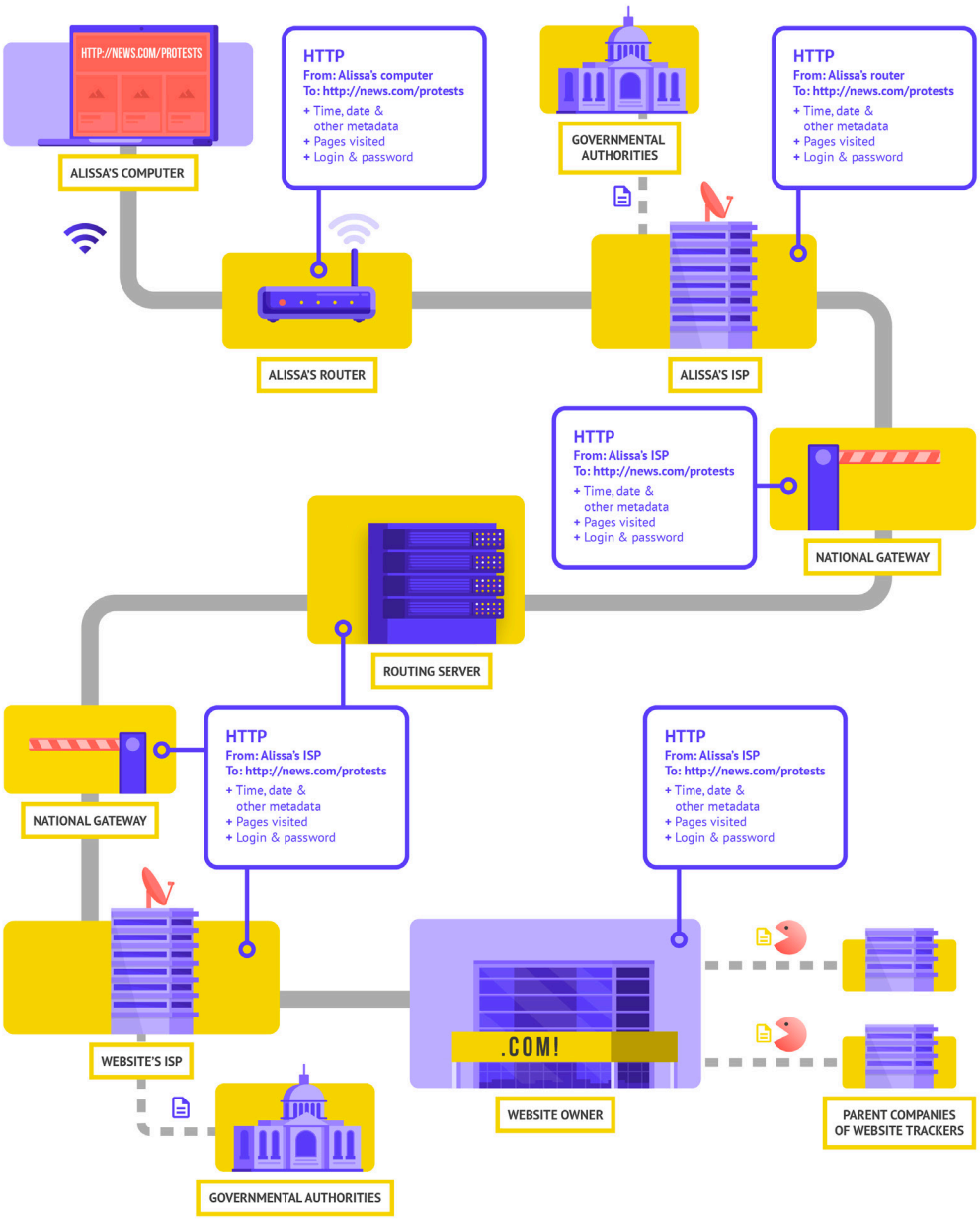


Надзор, цензура и парламентите

Непријателските влади и другите предизвикувачи на закани насекаде низ светот користат сè попристапна технологија за надзор, а во некои случаи користат едноставно хакирање на безжичната мрежа за да ја следат активноста на интернет на пратениците и на другите лица што работат во парламентот. На пример, во 2013 година хакери украле податоци од вработените и посетителите на Европскиот парламент преку **фалсификување на јавната Wi-Fi мрежа на Парламентот**. Тоа било предвесник на многу пософистицирани напади во наредните години.

Покрај киднапирањето на интернет-сообраќајот и крадењето податоци, противниците, исто така, го попречуваат клучното парламентарно работење со блокирање на пристапот на интернет и на системите. Во Брисел, во мај 2021 година, Парламентот на Белгија беше исклучен од интернет поради **голем напад со оневозможување на услуги.** Нападот предизвикал одложување на некои расправи и состаноци на комисиите бидејќи корисниците не можеле да пристапат до виртуелните услуги потребни за учество на седниците. Зголемената зачестеност на таквите напади врз пристапот и слободата на информациите на интернет нагласува колку е важно парламентите да ги разберат ризиците од работењето на интернет и да изработат планови за тоа како да се поврзат кога поврзувањето е засегнато.

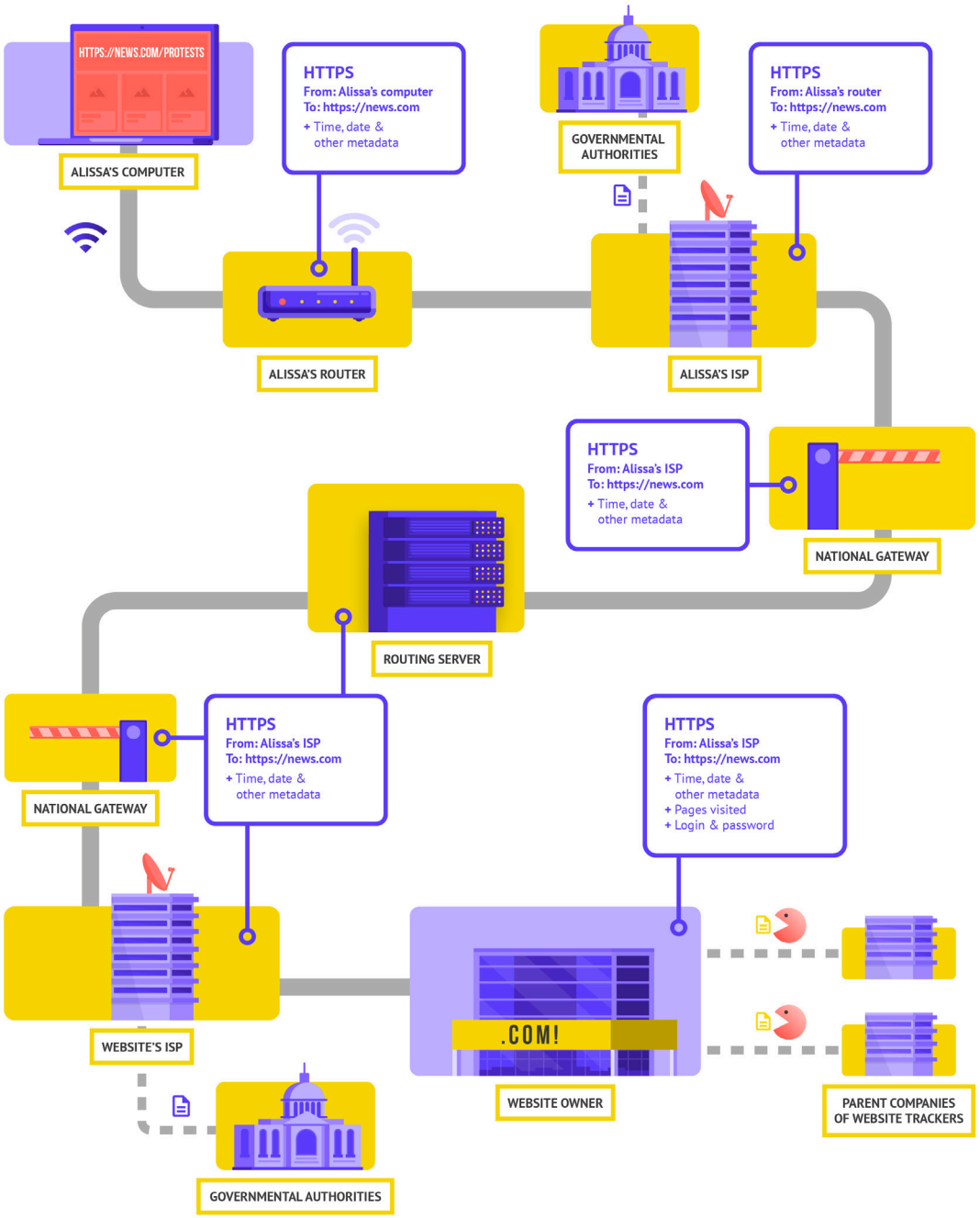
Le të marrim një shembull të botës reale se si duket shfletimi pa kriptim:



Адаптирано од Totem проектот [Како функционира интернетот](#) (CC–BY–NC–SA)

Кога пребарувате на интернет без шифрирање, сите ваши податоци се незаштитени. Како што е прикажано погоре, противникот може да види каде сте, дека одите на news.com, дека ја гледате конкретно страницата за протести во вашата земја и, можеби најважно како пратеник или вработен во парламентот, да ја види вашата лозинка која ја споделувате за да се најавите на самата страница. Ваквите информации во погрешни раце не само што ја прават вашата сметка незаштитена, туку, исто така, им даваат на потенцијалните противници, каде и да се наоѓаат во светот, добра претстава за тоа што можеби правите или за што размислувате.

Користењето ХТТПС (**во HTTPS, „s“ значи безбедно) значи дека се врши шифрирање**. Тоа ви нуди многу повеќе заштита. Ајде да погледнеме како изгледа пребарувањето со ХТТПС (познато како со шифрирање):



Адаптирано од Totem проектот [Како функционира Интернетот](#) (CC–BY–NC–SA)

Кога има ХТТПС, потенцијалниот противник не може да ја види вашата лозинка или други чувствителни информации што може да ги споделите на веб-страницата. Но, сепак, може да види кои домени (на пример, news.com) ги посетувате. Иако ХТТПС, исто така, шифрира информации за поединечните страници во рамките на веб-локацијата (на пример, website.com/protests) што ја посетувате, софистицираните противници можат да ги видат овие информации со проверка на вашиот интернет-сообраќај. Кога има ХТТПС, противникот може да знае дека одите на news.com, но нема да може да ја види вашата лозинка и ќе му биде потешко (но не и невозможно) да види дека барате информации за протести (ако го користиме овој пример). Тоа е важна разлика. Секогаш проверувајте дали има ХТТПС пред да се движите низ веб-страницата или да внесете чувствителни информации. Може да ја користите и **наставката на веб-пребарувачот HTTPS Everywhere** за да се осигурите дека постојано користите ХТТПС или ако користите Фајрфокс, вклучете го **режимот само HTTPS** во веб-пребарувачот.

Ако добиете предупредување од вашиот веб-пребарувач дека веб-страницата може да не е безбедна, не игнорирајте го. Нешто не е во ред. Тоа може да биде безопасно – на пример страницата има истечен безбедносен сертификат – или страницата може да е злонамерно фалсификувана или лажна. Во секој случај, важно е да го почитувате предупредувањето и да не одите на страницата.

Напредно ниво: Користење шифриран ДНС (DNS)

Ако сакате на давателот на интернетски услуги да му биде потешко (но не и невозможно) да ги дознае деталите за веб-страниците што ги посетувате, можете да користите шифриран ДНС (DNS).

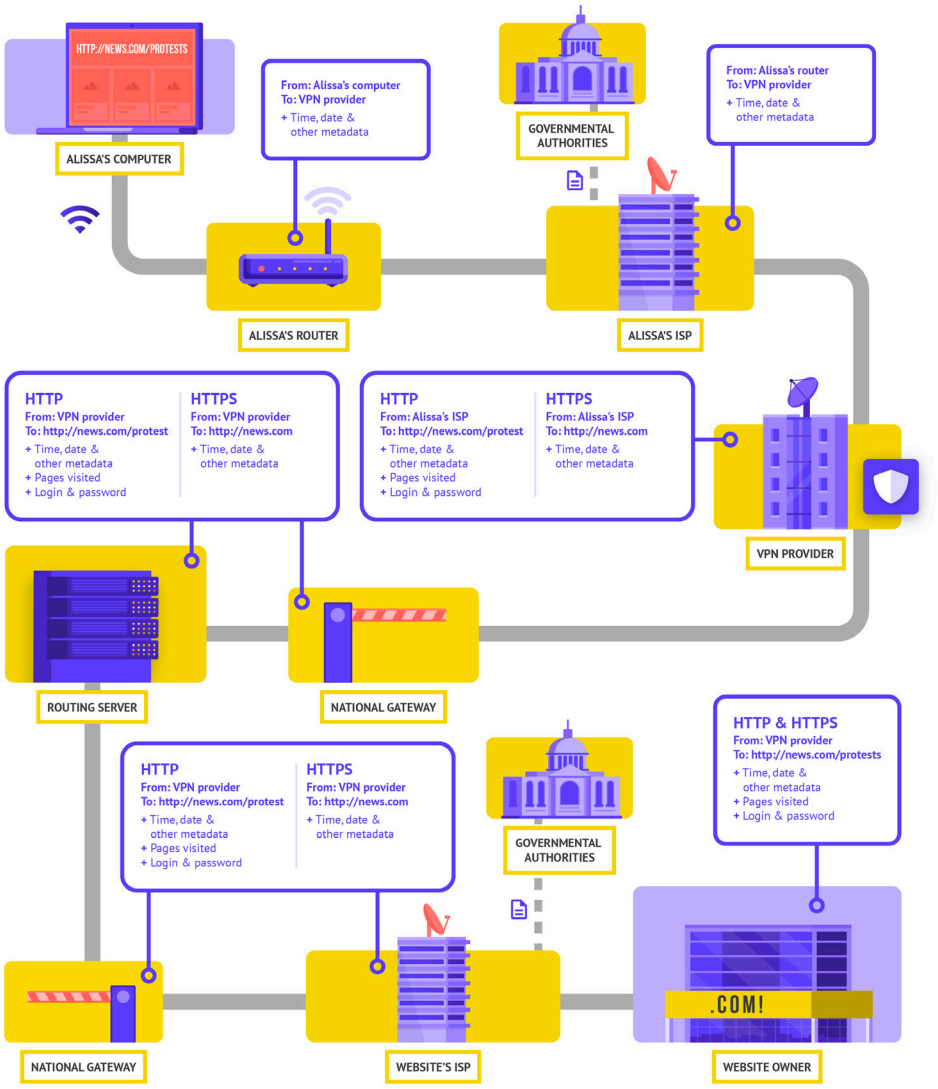
Ако се **прашувате**, ДНС значи Систем на имиња на домени. Во суштина, тоа е телефонскиот именик на интернет, кој ги преведува имињата на домени кои се разбирливи за луѓето (како ndi.org) во адреси на интернет протокол (ИП) кои се разбирливи за веб. Тоа им овозможува на луѓето да користат веб-пребарувачи за лесно да бараат и вчитуваат ресурси на интернет и да посетуваат веб-страници. Сепак, стандардно, ДНС (DNS) не е шифриран.

За да користите шифриран ДНС и истовремено да додадете малку заштита на вашиот интернет сообраќај, една лесна опција е да ја преземете и вклучите **апликацијата Cloudflare's 1.1.1.1** на вашиот компјутер и мобилен уред. Достапни се и други шифрирани опции за ДНС, вклучително и 8.8.8.8 на Гугл, но за нив се потребни **повеќе технички чекори** за конфигурирање. Ако го користите веб-пребарувачот Фајрфокс, шифрираниот ДНС е стандардно вклучен. Корисниците на веб-пребарувачите Хром или Еџ можат **да вклучат шифриран DNS** преку напредните безбедносни поставки на веб-пребарувачот со вклучување на „користи безбеден ДНС“ (use secure DNS) и избирање „Со: Cloudflare (1.1.1.1)“ (With: Cloudflare (1.1.1.1)) или давател на таа услуга по нивен избор.

1.1.1.1 на Cloudflare со WARP го шифрира вашиот ДНС и ги шифрира податоците за вашето пребарување, обезбедувајќи услуга слична на традиционалната ВПН (VPN). Иако WARP не ја заштитува целосно вашата локација од сите веб-страници што ги посетувате, тоа е функција која е лесна за користење и може да им помогне на вработените во вашиот парламент да ги искористат предностите од шифрираниот ДНС и дополнителната заштита од вашиот давател на интернет услуги во ситуации кога целосната ВПН или е нефункционална или е потребна со оглед на контекстот на заканата. Во 1.1.1.1 со WARP напредните поставки за DNS, вработените можат да го вклучат и 1.1.1.1 за семејства (1.1.1.1 for Families) за да добијат дополнителна заштита од злонамерен софтвер додека пристапуваат на интернет.

ШТО Е ВПН (VPN)?

Виртуелна приватна мрежа – ВПН (VPN), во суштина, е тунел што штити од надзор и блокирање на вашиот интернет сообраќај од страна на хакери на вашата мрежа, вашиот мрежен администратор, вашиот давател на интернетски услуги и сите со кои тие би можеле да споделуваат податоци. Во голема организација – како парламент –„ деловните“ или „корпоративните“ ВПН мрежи често се користат и за да се заштити интегритетот на пристапот до внатрешните системи и апликации (како што се оние што се користат за гласање од далечина). Без разлика дали користите лична ВПН или мрежа дизајнирана за деловни цели, концептот за заштита на вашиот интернет сообраќај од прислушување функционира генерално на ист начин и е од суштинска важност да продолжите да користите ХТТПС (дури и кога имате ВПН мрежа). Исто така, од клучно значење е да се осигурите дека ѝ верувате на ВПН што ја користи вашиот парламент. Еве пример за тоа како изгледа пребарувањето со ВПН:



Адаптирано од Totem проектот [Како функционира Интернетот](#) (CC–BY–NC–SA)

За подетален опис на ВПН, во овој дел има упатување на Водичот за самоодбрана од надзор на фондацијата Електронски граници.

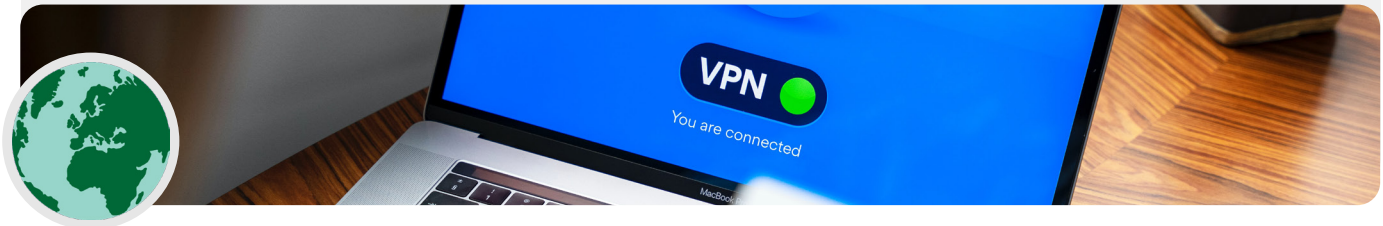
Традиционалните ВПН се дизајнирани за да ја прикријат вашата вистинска мрежна ИП-адреса и да создадат шифриран тунел за интернет сообраќајот помеѓу вашиот компјутер (или телефонот или кој било вмрежен „паметен" уред) и серверот на виртуелната приватна мрежа. Бидејќи сообраќајот во тунелот е шифриран и испратен до вашата ВПН мрежа, на трети страни, како давателите на интернетски услуги или хакерите на јавна безжична мрежа, им е многу потешко да го следат, менуваат или блокираат вашиот сообраќај. Откако ќе помине низ тунелот од вас до ВПН мрежата, вашиот сообраќај потоа ја напушта ВПН мрежата и продолжува до својата крајна дестинација, прикривајќи ја вашата оригинална ИП-адреса. Тоа помага да се прикрие вашата физичка локација за секој што го гледа сообраќајот откако ќе ја напушти ВПН мрежата. Ова ви нуди поголема приватност и безбедност, но користењето на ВПН не ве прави целосно анонимни на интернет: вашиот сообраќај сè уште е видлив за операторот на ВПН. Вашиот давател на интернетски услуги, исто така, ќе знае дека користите ВПН, што може да го зголеми вашиот профил на ризик.

Тоа значи дека **изборот на доверлив давател на ВПН мрежа е од суштинско значење**. На некои места, како, на пример, Иран, непријателските влади, всушност, имаат поставено свои сопствени ВПН мрежи за да можат да следат што прават граѓаните. За да ја пронајдете ВПН мрежата што е соодветна за вашиот парламент и неговите вработени, можете да ги оцените ВПН мрежите врз основа на нивниот деловен модел и реноме, какви податоци собираат или не собираат и, секако, безбедноста на самата алатка.

Зошто не треба да користите бесплатна виртуелна приватна мрежа?
Краткиот одговор е дека повеќето бесплатни ВПН, вклучително и оние што се претходно инсталирани на некои паметни телефони, доаѓаат со голема замка. Како и сите бизниси и даватели на услуги, ВПН мора да се одржуваат некако. Ако ВПН не ја продаде својата услуга, како ќе го одржува својот бизнис? Дали бара донации? Дали наплаќа за премиум услуги? Дали е поддржана од добротворни организации или финансиери? За жал, многу бесплатни ВПН заработуваат пари со собирање и потоа продавање на вашите податоци.
Давателот на ВПН што не собира податоци е најдобриот избор. Доколку податоците не се собираат, тие не можат да се продадат или да се предадат на странска влада доколку бидат побарани. Кога ја разгледувате политиката за приватност на давателот на ВПН мрежа, видете дали ВПН мрежата собира кориснички податоци. Ако експлицитно не е наведено дека податоците за конекцијата на корисниците не се евидентираат, големи се шансите дека се евидентираат. Дури и ако компанијата тврди дека не ги евидентира податоците за конекцијата, тоа не секогаш може да биде гаранција за добро однесување.
Корисно е да се направи истражување на компанијата што ја обезбедува ВПН мрежата. Дали е одобрена од независни професионалци за безбедност? Дали има статии со вести за таа ВПН? Дали некогаш била фатена како ги доведува во заблуда или ги лаже своите клиенти? Ако виртуелната приватна мрежа била основана од луѓе што се познати во заедницата за безбедност на информации, поголема е веројатноста дека е доверлива. Бидете скептични во врска со ВПН што нуди услуга за која никој не сака да ја загрози својата репутација или со која раководи компанија за која никој не знае.

Лажни ВПН во реалниот свет

Кон крајот на 2017 година, по напливот на протести во земјата, Иранците почнаа да откриваат „бесплатна" (но лажна) верзија на популарна ВПН која се споделуваше преку текстуални пораки. Бесплатната ВПН, која всушност не функционираше, ветуваше дека ќе овозможи пристап до Телеграм, кој во тоа време беше блокиран локално. За жал, лажната апликација беше само злонамерен софтвер кој им овозможи на властите да го следат движењето и да ги следат комуникациите на оние што ја преземале.



Па, каква ВПН треба да користиме?

Ако, покрај осигурувањето на безбедноста на парламентарниот интернет сообраќај, ви треба и решение за безбедно ограничување на пристапот само на лицата во вашата парламентарна мрежа (дури и додека работите од далечина) до внатрешните парламентарни системи и апликации, можеби ќе сакате да имплементирате „ бизнис“ или „корпоративна“ ВПН. Постојат низа опции коишто користат различни технологии што може да ги земете предвид, вклучувајќи ги AnyConnect на Cisco, Global Protect на PaloAlto или Access на „Клаудфлер“ (Cloudflare) (технички, систем за пристап со нула доверба, а не ВПН), кои се само неколку примери. Во секој случај, таквите системи бараат квалификуван ИТ кадар за имплементација и ефикасно управување.
Ако напредниот „корпоративен“ ВПН систем не влегува во вашиот буџет или е непотребно компликуван за вашиот парламент, можете да размислите да користите лични ВПН опции, како ProtonVPN или TunnelBear (кој, исто така, нуди план за тимови за поедноставно управување со сметките) за сите пратеници и вработени во парламентот. Друга доверлива опција е да го конфигурирате вашиот сопствен сервер користејќи Outline на Jigsaw, каде што компанија не управува со вашата сметка, но треба да поставите свој сопствен сервер. Иако повеќето модерни ВПН мрежи се подобрени во однос на работењето и брзината, треба да се има предвид дека користењето ВПН може да ја забави брзината на пребарување ако сте на мрежа со многу низок опсег, ако имате проблем со голема латентност или доцнење на мрежата или ако се соочувате со повремени прекини на интернетот. Ако сте на побрза мрежа, стандардно треба да користите ВПН цело време. Ако им препорачате на вработените да користат ВПН, исто така е важно да се погрижите тие да ја одржуваат вклучена. Можеби звучи очигледно, но ВПН која е инсталирана, но не се користи, не обезбедува никаква заштита.

Напредно ниво: Анонимност преку Тор (Tor)

Покрај ВПН, можеби сте слушнале за Тор (Tor) како уште една алатка за побезбедно користење на интернет. Важно е да разберете што се двете и зошто можете да ја користите едната или другата.

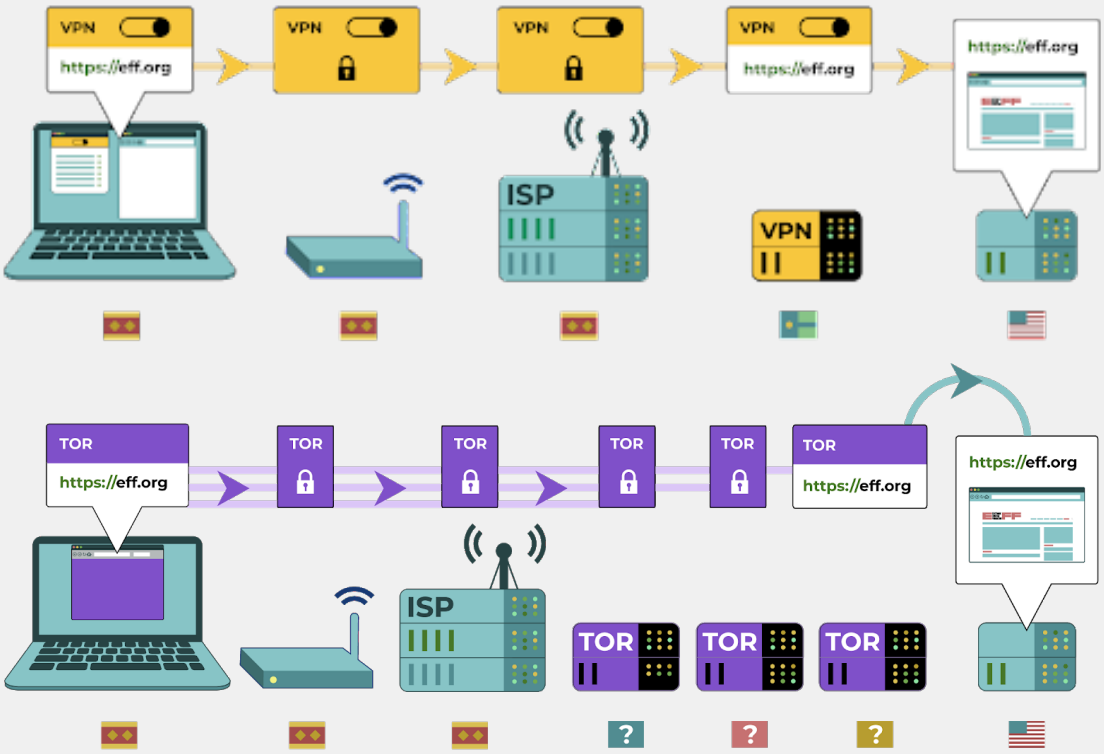
Тор е протокол за анонимно пренесување податоци преку интернет со насочување на пораките или податоците преку децентрализирана мрежа. Можете да дознаете повеќе за тоа како работи Тор овде, но, накратко, тој го насочува вашиот сообраќај низ повеќе точки на патот до неговата дестинација, така што ниту една точка нема доволно информации за да открие одеднаш кои сте и што правите на интернет.

Тор се разликува од ВПН на повеќе начини. Најосновно, тој се разликува затоа што не се потпира на довербата во која било конкретна точка (како давателот на ВПН).

Оваа графикон, креиран од фондацијата Електронски граници, ја покажува разликата помеѓу традиционалната ВПН и Тор.

Најлесен начин да се користи Тор е преку веб-пребарувачот Tor. Тој работи како и секој друг веб-пребарувач, само што го насочува вашиот сообраќај преку мрежата Тор. Можете да го преземете веб-пребарувачот Тор на уредите со Виндоус, Мек, Линукс или Андроид. Имајте предвид дека кога го користите веб-пребарувачот Тор, ги заштитувате само информациите до кои пристапувате додека сте на веб-пребарувачот. Тој не обезбедува никаква заштита на други апликации или преземени датотеки кои може да ги отворите посебно на вашиот уред. Исто така, имајте предвид дека Тор не го шифрира вашиот сообраќај, така што – слично како кога користите ВПН – сè уште е од суштинска важност да ги користите најдобрите практики, како ХТТПС, кога пребарувате на интернет.

Ако сакате да ја проширите заштитата на анонимноста од Тор на целиот ваш компјутер, корисниците што имаат поголемо техничко знаење можат да го инсталираат Тор како системска интернет-конекција или можат да го користат оперативниот систем Тејлс (Tails), кој стандардно го насочува целиот сообраќај низ Тор. Корисниците на Андроид, исто така, можат да ја користат апликацијата Orbot за Тор да функционира за целиот интернет-сообраќај и апликациите на нивниот уред. Без оглед на тоа како го користите Тор, важно е да знаете дека кога го користите, вашиот давател на интернет-услуги не може да види кои веб-страници ги посетувате, но *може* да види дека го користите Тор. Слично како кога користите ВПН, ова може значително да



го зголеми вашиот профил на ризик бидејќи Tor не е многу вообичаена алатка и затоа се истакнува кај противниците кои можеби го следат вашиот интернет-сообраќај.

Затоа, иако веројатно има многу малку примери кога било неопходно да се користи Tor во парламентарен контекст, или ако не можете да си дозволите доверлива ВПН или вашиот парламент да работи во средина каде што ВПН рутински се блокира, Tor може да биде добра опција, ако е легален, за ограничување на влијанието на надзорот и избегнување цензура на интернет.

Дали има некои причини поради кои не треба да користиме ВПН или Tor?

Освен загриженоста околу ВПН услугите без добра репутација, најголемата работа што треба да се земе предвид е дали користењето ВПН или Tor може да привлече несакано внимание или, локално, да биде спротивно на законот.
Иако вашиот давател на интернет- услуги нема да знае кои страници ги посетувате додека ги користите овие услуги, тој може да види дека сте поврзани на Tor или на ВПН. Ако тие се незаконски таму каде што работи вашиот парламент или неговите вработени или можат да предизвикаат поголемо внимание или ризик од едноставната навигација на интернет со стандарден HTTPS и шифриран ДНС, можеби ВПН или, особено, Tor (кој многу поретко се користи и затоа има поголемо „црвено знаменце“) не е вистинскиот избор.

КАКОВ ВЕБ-ПРЕБАРУВАЧ ТРЕБА ДА КОРИСТИМЕ?

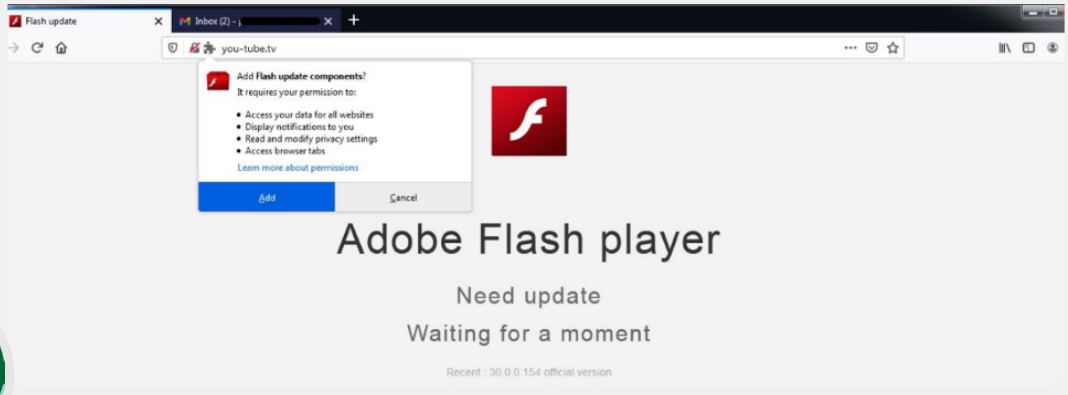
Користете реномиран веб-пребарувач, како Хром, Фајрфокс, Брејв, Сафари, Еџ или Тор. И Хром и многу се користат и се одлични во однос на безбедноста. Некои луѓе претпочитаат Фајрфокс поради неговиот фокус на приватноста. Во секој случај, важно е релативно често да ги рестартирате веб-пребарувачите и вашиот компјутер за да го ажурирате вашиот веб-пребарувач. Ако сте заинтересирани да ги споредите карактеристиките на веб-пребарувачите, погледнете го овој ресурс од фондацијата Слобода на печатот.

Без оглед на тоа кој веб-пребарувач го користите, исто така е добра идеја да користите наставка или додаток како **Privacy Badger**, **uBlock Origin** или **DuckDuckGo's Privacy Essentials** кој ги спречува огласувачите и другите следачи трети страни (third-party trackers) да следат каде одите и кои страници ги посетувате. И кога пребарувате на интернет, размислете да ги префрлите вашите стандардни веб-пребарувања од Гугл на **DuckDuckGo**, **Startpage** или на друг пребарувач за заштита на приватноста. Ваквата промена ќе ви помогне и во ограничувањето на огласувачите и следачите трети страни.

Безбедност на веб-пребарувачот во реалниот свет

Нападите преку наставките или додатоците на веб-пребарувачот може да бидат исто толку штетни колку и злонамерниот софтвер споделен директно преку преземања од „фишинг" или друг софтвер. На пример, на почетокот на 2021 година **паметно дизајнираниот злонамерен додаток** наречен „Flash update components" беше насочен против тибетските политички организации. Додатокот им се појавуваше на корисниците што посетуваа веб-страници поврзани со „фишинг" е-пошта, а кога ќе беше инсталиран, им овозможуваше на хакерите да крадат е-пошта и податоци од пребарување на интернет.

Додатоците на веб-пребарувачите, исто така, можат да бидат вектор за заразување на парламентарните ресурси, како што се веб-страниците, кои пак можат да шират злонамерен софтвер на голем број посетители на страницата (вклучувајќи ја поширокатa јавност, парламентарната служба и самите членови). Земете го, на пример, користењето од страна на хакерите на популарниот додаток за веб-пребарувач Browsealoud (сега познат како ReachDeck), програма која го конвертира текстот на веб-страницата во аудио за корисниците со оштетен вид. Во 2018 година хакерите вметнаа злонамерен код во додатокот на веб-пребарувачот кој се употребуваше на веб-страниците на различни владини субјекти, вклучително и на **парламентот на државата Викторија во Австралија**. Со заразениот додаток на веб-пребарувачот, кој беше поставен и неправилно конфигуриран, уредите на посетителите на веб-страницата беа заразени со злонамерен софтвер откако ќе ја посетеа страницата. Во овој случај, злонамерниот софтвер беше искористен за употреба на уредите за рударење на криптовалути, но таквата тактика може да се користи од страна на хакерите и за ширење злонамерен софтвер за кражба на податоци или за шпионажа.



Безбедност на социјалните медиуми

Вработените во службата на парламентот и пратениците можат да обелоденат многу работи – а понекогаш и повеќе отколку што имаат намера – со објавување и коментирање на социјалните медиуми. Без разлика дали се работи за Фејсбук, Твитер, Инстаграм, Јутјуб или социјални медиуми карактеристични за некој регион, како што се VKontakte и Odnoklassniki, секогаш треба внимателно да размислите за тоа што објавувате и соодветно да ги конфигурирате сите достапни поставки за приватност. Ова важи не само за официјалните страници на парламентот, туку во некои случаи и за личните сметки на вработените, како и за оние на нивните семејства и пријатели.

Безбедност на социјалните медиуми и парламентите

Дури и организациите со низок ризик можат да бидат цел и да бидат вознемирувани на социјалните медиуми ако немаат воспоставено соодветни безбедносни политики. Во **овој пример** од 2018 година, непрофитно засолниште за животни изгуби илјадници долари и ги изгуби поддржувачите откако неовластен администратор на сметки постави лажна акција за собирање средства, а на платформата се појавија лажни сметки на вработените. Ако хакерите се подготвени да одат дотаму за да заработат неколку илјади долари од засолниште за животни, можете да замислите каква штета би можеле да нанесат софистицираните противници ако добијат пристап до сметките на вашиот парламент или успеат лажно да се претстават на интернет како истакнат пратеник или вработен.

Покрај хакирањето на сметките на социјалните медиуми, веб-страниците на парламентот, исто така, се вообичаена цел со оглед на нивната јавна видливост и значење за угледот. Во еден пример од 2017 година, веб-страницата на парламентот на Австрија беше **срушена од хакерска група** која наводно била лута поради влошените односи на земјата со Турција во тоа време.

КРЕИРАЊЕ ПАРЛАМЕНТАРНА ПОЛИТИКА ЗА СОЦИЈАЛНИ МЕДИУМИ

Претпоставете дека сè што е објавено на социјалните медиуми може да стане јавно достапно и затоа соодветно креирајте парламентарна политика за социјалните медиуми. Со оглед на јавната природа на поголемиот дел од работата на парламентот, веројатно ќе сакате да ги споделите повеќето објави и пораки јавно, но, сепак, од клучно значење е да поставувате и да одговарате на прашања како на пример: Кој има пристап до вашите сметки на социјалните медиуми? Кој смее да објавува и кој треба да одобрува објави? Што е со коментарите и одговорите? Кои информации треба/не треба да се споделуваат на социјалните медиуми? Ако објавувате фотографии, информации за локација или други идентификациски информации за вашите вработени, членови или партнери, дали сте побарале дозвола од нив и дали сте размислувале за можни ризици? Ваквите прашања се особено важни ако вашиот парламент јавно комуницира со граѓаните преку социјалните медиуми или слични интернет-портали за јавен ангажман.

Освен што ќе ја креирате вашата политика и ќе им ја образложите на вработените, погрижете се правилно да ги конфигурирате вашите поставки за приватност и безбедност (често се нарекуваат „безбедносни“). Некои клучни прашања што треба да си ги поставите додека одлучувате кои поставки за приватност и безбедност се најсоодветни за парламентарните и за личните сметки се:

- Дали сакате да ги споделувате вашите објави со јавноста или само со одредена група луѓе внатрешно или надворешно?
- Дали некој треба да може да коментира, да одговара или да има интеракција со вашите пораки или објави?
- Дали луѓето треба да можат да ве најдат користејќи ја вашата адреса за е-пошта или (приватен или службен) телефонски број?
- Дали сакате вашата локација автоматски да се споделува кога објавувате нешто?
- Дали сакате да блокирате или да исклучите непријателски настроени сметки?
- Дали сакате да блокирате одредени зборови или хаштагови?

Секоја страница на социјалните медиуми ќе има различни поставки за приватност и безбедност, но овие општи концепти се применуваат универзално. Додека ги разгледувате овие прашања, искористете ги корисните водичи за приватност од големите платформи: **Фејсбук**, **Твитер**, **Инстаграм** и **Јутјуб**. Особено кога се работи за Фејсбук, бидете внимателни во врска со изборот на приватноста во групите. Групите на Фејсбук се популарно место за ангажирање, застапување и споделување информации, но на неограничените групи може да им се придружи кој било. Не е невообичаено лажни сметки да се претставуваат како вистински луѓе во обид да се инфилтрираат во приватни групи или страници на социјалните медиуми. Затоа, бидете внимателни кога прифаќате барања за „пријател“ и за „следење“. Запомнете дека сметките на социјалните медиуми на вашиот парламент се безбедни исто колку и сметките што се „поврзани“ со него. Ова е особено важно да се запамети за Фејсбук, каде што страниците може да бидат управувани од нечија поврзана лична сметка.

ВОЗНЕМИРУВАЊЕ НА ИНТЕРНЕТ

За жал, многу парламенти и поврзани групи се соочуваат со значително вознемирување на интернет, особено на социјалните медиуми. Ваквото вознемирување често е насочено со уште поголем интензитет кон жените и маргинализираните популации. Особено насилството на интернет врз жените може да создаде непријателска средина што води до самоцензура или повлекување од политичкиот или граѓанскиот дискурс. Како што е идентификувано во извештајот „**Tweets That Chill**“ на тимот за род, жени и демократија на НДИ, кога нападите врз политички активните жени се канализираат на интернет, широкиот опсег на социјалните медиуми може да го зголеми ефектот од вознемирувањето и психолошката злоупотреба, поткопувајќи го чувството на жените за лична безбедност на начини кои мажите не ги почувствувале.

Како вашиот парламент ја подготвува својата политика за социјалните медиуми, важно е да ја знаете оваа динамика. Вградете во вашиот план за безбедност структурирана поддршка за членовите и вработените кои се соочуваат со негативни пораки, навреди и закани на социјалните медиуми, и како дел од нивните работни места и во нивниот приватен живот. Креирајте инфраструктура против вознемирување во рамките на парламентот, вклучително и анкетирање на вашите вработени за да разберете како вознемирувањето на интернет влијае на нив и направете тим за брз одговор кој ќе им помогне на вработените да се соочат со ситуации кои носат предизвици. Практичниот прирачник во случај на вознемирување на интернет (**Online Harassment Field Manual**) на ПЕН Америка (PEN America), исто така, дава детални препораки за тоа како можете да ги поддржите вработените што се соочуваат со такво

вознемирување. Може да размислите, доколку вашите вработени се согласуваат, да пријавувате инциденти со вознемирување и/или проблематични сметки и директно на платформите.

Кога комуницирате со членови или вработени кои биле жртви на вознемирување на интернет (како и во физичкиот свет), важно е да бидете чувствителни. Како што е наведено во Програмата за правата на жените на Здружението за прогресивни комуникации, Take Back the Tech, треба да разберете дека жртвата, можеби, се справува со траума и да прифатите дека насилството, на интернет или надвор од интернет, никогаш не е по вина на жртвата. Погрижете се таквите прашања да можат да се покренат и да се дискутираат (ако вработените немаат проблем со тоа) во доверлива и безбедна средина, со опција за анонимност. И вклучете во планот за безбедност на вашиот парламент список на локални професионалци, организации и агенции за спроведување на законот со кои можете да ги поврзете вработените за правна помош, медицинска помош, помош со менталното здравје и техничка помош доколку е потребно. За дополнителни идеи, погледнете го Водичот за безбедност на интернет на „Феминист фриквенси“ (Feminist Frequency).

Одржување на вашите веб-страници на интернет

Покрај заштитата на вашата способност за безбеден пристап до интернет, исто така е важно да направите сè што можете за да осигурите дека и другите можат да пристапат до веб-страниците и други точки на присуство на интернет на вашиот парламент. За страниците на социјалните медиуми, ова значи заштита на тие сметки со силни, уникатни лозинки и автентикација со два фактора. За вашата веб-страница, ова значи заштита од хакирање и напади со оневозможување на услугата. Напади со дистрибуирано оневозможување на услугата (Distributed Denial of Service - DDoS) се кога голема група компјутери истовремено го преоптоваруваат вашиот сервер со злонамерен сообраќај. Неколку опции за заштита од DDoS – со кои на противникот ќе му биде многу потешко да ја сруши вашата веб-страница – се Cloudflare, AWS Shield на Amazon или услугата Deflect на eQualitie.

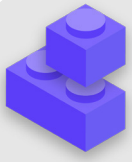
Напредно ниво: Безбедно хостирање на веб-страницата на вашиот парламент

Веб-страниците се хостирани на компјутери – и тие се ранливи на хакирање исто како и вашите сопствени уреди. Ако е можно, вашиот парламент треба да ги искористи постојните хостинг-услуги како Вордпрес (WordPress), Викс (Wix) или други кои за вас управуваат со целокупната безбедност на веб-страницата. Ако потребите на вашата веб-страница се посложени и/или треба сами да ја хостирате вашата веб-страница, тогаш не заборавајте да се фокусирате на ажурирање на вашиот оперативен систем и софтверот за веб-хостирање, исто како што би правеле со вашиот персонален компјутер. Размислете за користење на добро етаблирани даватели на услуги за хостирање во облак, како што се веб-услугите на Амазон (AWS), Мајкрософт азур (Microsoft Azure) или eclips.is на Гринхост, кои обезбедуваат подобрени безбедносни опции за хостирани веб-страници. Без оглед на тоа кои алатки ги користите за да ја хостирате вашата веб-страница, осигурете се дека сите сметки што се користат за пристап до поставките за уредување и конфигурација на содржината се заштитени со силни лозинки и автентикација со два фактора.

Ако вашиот парламент има лице со поголемо техничко знаење за хостирање на вашата веб-страница, треба да размислите за избор на таканаречена статичка веб-страница или едноставна веб-страница. За разлика од динамичните веб-страници, овие видови веб-страници ја намалуваат површината за напад на хакерите и ќе ја направат вашата веб-страница поотпорна на напади.

Заштитете ја вашата безжична мрежа

Сите овие чекори за заштита на веб-сообраќајот од надзор и цензура се важни, но тие не се замена за основната мрежна безбедност во парламентот и во домот. Не заборавајте ги основите, како користење силна лозинка (не стандардната лозинка) на рутер(-ите) на вашата безжична мрежа (Wi-Fi), со што ќе се осигурите дека само овластени корисници имаат пристап до вашата мрежа со често менување на лозинката и овозможување на вграден заштитен ѕид (firewall) на вашите безжични рутери. Размислете и за креирање мрежа за гости во просториите на парламентот доколку имате посетители кои користат интернет и кои влегуваат и излегуваат од зградата.



Основни елементи на планот за безбедност: Безбедност на интернет

- **Спроведувајте редовна обука за членовите и вработените за важноста од следењето на основните мерки за безбедност на веб.**
- **Потсетете ги вработените секогаш да пребаруваат на интернет со ХТТПС и шифриран ДНС.**
- **Барајте од вработените редовно да ги рестартираат своите веб-пребарувачи за да се инсталираат ажурирања.**
- **Поттикнете ја употребата на веб-пребарувачи и наставки за заштита на приватноста.**
- **Ако е соодветно да користите ВПН, изберете таква мрежа од реномиран давател, обучете ги вработените за нејзина употреба и погрижете се доследно да се користи.**
- **Креирајте и дистрибуирајте јасна парламентарна политика за користење на социјалните медиуми.**
- **Овозможете ги поставките за приватност и безбедност на сите сметки на социјалните медиуми.**
- **Разберете го влијанието од вознемирувањето на интернет и бидете подготвени да ги поддржите членовите и вработените што се засегнати.**
- **Направете список на локални професионалци, организации и агенции за спроведување на законот со кои можете да ги поврзете членовите и вработените за правна помош, помош со менталното здравје и техничка помош како одговор на вознемирувањето на интернет.**
- **Регистрирајте се за заштита од оневозможување на услугата (DDoS) на вашите веб-страници.**
- **Користете доверлив, сигурен давател на услуги за веб-хостирање.**
- **Користете силна лозинка и мрежа за гости за безжичната мрежа во вашите простории.**

Заштита на физичката безбедност

Од суштинска важност е да ја одржувате физичката безбедност на вашите уреди. Имајте предвид дека физичката безбедност опфаќа многу повеќе од само уредите и треба да вклучува стратегии за заштита на сè друго во вашиот свет. Таа вклучува документи во печатена форма, канцелариите на вашиот парламент, салите за седници или работните простори, и, се разбира, вие, вашите вработени и членови.

Физичката безбедност и парламентот

За жал, физичките напади врз парламентите и другите законодавни тела не се невообичаени и често имаат значителни импликации и врз физичката и врз безбедноста на информациите. На 6 јануари 2021 година, бунтовници упаднаа во зградата на Капитолот на Соединетите Американски Држави – седиште на двата дома на законодавната власт на САД – во обид да го спречат потврдувањето на резултатите од претседателските избори. Физичкиот напад трагично доведе до пет смртни случаи и предизвика значителна психолошка вознемиреност за членовите и вработените во Конгресот. Меѓутоа, тоа не беше единственото негативно влијание. Напаѓачите, исто така, уништија ИТ опрема, добија пристап до чувствителни материјали во канцелариите на членовите и можеби најштетно беше тоа што украдоа компјутери и други уреди со потенцијално доверливи информации од Капитолот на САД.

Напредно ниво: Простории наменети за чувствителни информации (SCIF)

За водење многу чувствителни разговори, некои парламенти имаат заштитени физички простории наречени СЦИФ (SCIF). Овие простории се направени така што чувствителните информации, како што се прашањата поврзани со националната безбедност или разузнавањето, може да бидат разгледувани и дискутирани меѓу пратениците и нивниот кадар без да се грижат за надворешен надзор или шпионирање. Покрај соодветната физичка конструкција, за соодветна СЦИФ луѓето треба да ги остават уредите (како што се нивните мобилни телефони) надвор од просторијата пред да влезат за да дискутираат.

Заштита на физичките средства

Суштинска компонента на безбедноста на информациите е физичката безбедност на вашите уреди. Покрај ублажувањето на влијанието од украдениот уред со користење на заклучени екрани и лозинки, спроведување на целосно шифрирање на дискот и вклучување на функциите за далечинско бришење, треба да размислите и како да спречите тие уреди да бидат воопшто украдени. За да ја отежнете кражбата, погрижете се да поставите силни брави (и да ги ротирате секогаш кога се менуваат вработените) во просториите на парламентот и/или во домот. Дополнително, размислете да купите сеф за лаптопот или шкаф што може да се заклучува за да ги заштитите уредите навечер. Безбедносните камери или системите со сензори за движење низ просториите може да откријат и, да се надеваме, да спречат физичка кражба. Побарајте опција за **почитување на приватноста** која е достапна во вашата земја и изберете камери и безбедносни системи обезбедени од доверливи компании кои немаат мотивација да ги предадат податоците и информациите на потенцијален противник.

Ако старите уреди сè уште имаат зачувани информации на нив, но веќе не се во употреба, треба да ги избришете – **овој водич** од „Вајркатер“ (Wirecutter) е одличен ресурс како да го направите тоа кај повеќето модерни уреди. Ако не е возможно да се избришат вашите уреди, можете и физички да ги уништите. Најлесен, ако не и најеколошки, начин да го направите тоа е да ги искршите уредите и нивните тврди дискови со чекан. Понекогаш најстарите решенија сè уште функционираат најдобро!

Дури и пред овие технички чекори, одвојте време за да направите попис на целата опрема во рамките на парламентот. Ако немате список на сите ваши уреди, потешко е да следите што може да недостига ако некој ви биде украден.

ШТО ДА ПРАВИМЕ СО ЦЕЛАТА ОВАА ХАРТИЈА?

Веројатно вашиот парламент има многу информации кои се отпечатени на хартија, напишани во тетратки или запишани на самолепливи белешки. Некои од нив може да бидат многу чувствителни – белешки од доверливи сведочења или приватни состаноци, на пример. Неопходно е да се размислува за безбедноста и на овие информации. Ако апсолутно треба да чувате печатени копии од чувствителни информации, погрижете се тие да се чуваат безбедно во заклучен шкаф или на друго безбедно место. Не чувајте никакви приватни или чувствителни информации (вклучувајќи лозинки) оставени на маса или напишани на табла. Чувајте ги многу чувствителните информации на помалку таргетирана, добро заштитена локација. Колку што е можно, настојувајте да ги отстраните непотребните информации во печатена форма. Запомнете: ако ги немате, не можат да бидат украдени. Воспоставете парламентарна политика во врска со сопственоста на хартиените белешки и не заборавајте да ги земете сите хартиени белешки од вработените ако тие одлучат да дадат отказ или ако добијат отказ од организацијата, исто како што би земале компјутер или телефон издаден од парламентот. За да се ослободите од чувствителната хартија, купете квалитетен уништувач на хартија (шредер). Забавна активност на крајот на неделата може да биде 15-минутна пауза со вашите тимови за да ги уништите сите останати, чувствителни отпечатени материјали или белешки од претходната недела.

ПОЛИТИКА ЗА КАНЦЕЛАРИИТЕ НА ПАРЛАМЕНТОТ

Иако за многумина реалноста на „канцеларијата“ значително се промени од почетокот на пандемијата со КОВИД-19, сè уште е важно вашиот парламент да воспостави јасна политика во однос на пристапот до просториите. Таквата политика треба да одговори на клучните прашања, вклучително и кој може да влезе во просториите на парламентот (и кога), кој до кои канцелариски ресурси може да пристапи (како безжичната мрежа) и како да се постапува со гостите.
Едноставно, но важно прашање на кое треба да се одговори е кој ќе добие клуч од канцеларија или картичка за пристап. Само вработените од доверба треба да имаат клучеви или картички, а бравите треба да се менуваат кога некој вработен ќе си замине и/или на полуредовна основа. Во текот на денот, сите врати што се оставени отклучени треба да бидат под постојан надзор на некое лице од доверба и/или чувар. Освен тоа, погрижете се вашиот парламент да има доверлив однос со давателите на услуги, како што се персоналот за чистење и надворешните техничари кои имаат пристап до просториите. Размислете за тоа до кои информации или уреди би можеле да имаат пристап тие луѓе и погрижете се истите да бидат заштитени, особено ако го немате тој доверлив однос. Кој и да има пристап, некое лице од доверба треба секогаш да биде назначено да ги заклучува канцеларииите и зградите и да се погрижи уредите да бидат соодветно заштитени пред да си оди на крајот од денот.

Дали на гласачите им е дозволено да влезат во вашиот парламент? Можеби јавноста има право на пристап до делови од просториите на парламентот? Ако е така, погрижете се јавноста да нема пристап (или барем пристап без надзор) до уреди или чувствителни податоци во печатена форма. Ако постои барање или очекување јавноста или гостите да имаат пристап до интернет кога го посетуваат парламентот,

треба да воспоставите мрежа за гости, така што таквите гости да немаат можност да го следат вашиот редовен сообраќај. Општо земено, само вработените од доверба треба да имаат пристап до мрежата и до мрежните уреди, како што се печатачите. Исто така, обично е добра идеја да се бара регистрација на гостите за да имате евиденција за тоа кој го посетил парламентот.

Додека ја креирате канцелариската политика, целта треба да биде да им дозволите само на луѓе од доверба да имаат пристап до чувствителни уреди, документи, простории и системи.

ПОДДРШКА НА ВРАБОТЕНИТЕ И НА ВОЛОНТЕРИТЕ

Заканите за физичката безбедност на вашиот парламент може да влијаат и на вашите вработени. Слично на вознемирувањето на социјалните медиуми, заканите за физичката безбедност честопати непропорционално влијаат на жените и маргинализираните заедници. Не се работи само за скршени прозорци и украдени лаптопи. Заплашувањето, заканите или случаите на физичко или сексуално насилство, семејно насилство и страв од напади може да имаат сериозно негативно влијание врз животот на членовите и вработените. Алатката за планирање на безбедноста **#Think10** на НДИ е корисен ресурс за политички активните жени кои би можеле да бидат изложени на зголемен личен ризик како резултат на нивното учество во парламентот и генерално во политиката.

Добросостојбата на вработените е очигледно важна за нив како поединци, но, исто така, е клучен елемент за здрав и добро функционален парламент. За таа цел, размислете кои дополнителни ресурси можете да им ги обезбедите на вработените за да ги заштитите и, во случај на физички или дигитален напад, да им помогнете да заздравуваат. Како што беше споменато претходно во прирачникот, тоа значи минимум креирање список со ресурси со кои можете да ги поврзете вработените за правна помош, медицинска помош, помош со менталното здравје и техничка помош доколку е потребно. Уште еднаш, Практичниот прирачник при вознемирување на интернет (**Online Harassment Field Manual**) на ПЕН Америка (PEN America) содржи идеи за тоа како организациите можат да им обезбедат поддршка на вработените за време на кризи и по нив.

БЕЗБЕДНОСТ ПРИ ПАТУВАЊЕ

Патувањето – во друга земја или до близок град – често ги интензивира физичките ризици за безбедноста на информациите. Генерално, може да се претпостави дека вие и вашите уреди немате права на приватност кога одите преку граница. Затоа, добра идеја е да вклучите парламентарна политика за службени патувања во вашиот план за безбедност којашто ќе вклучува потсетници за клучните најдобри безбедносни практики.

Политиката за службени патувања на вашиот парламент треба да содржи многу информации кои се опфатени во другите делови од прирачникот, вклучително и безбедно користење на интернет и одржување на физичката безбедност на уредите и други извори на информации и нивно постојано чување до вас кога патувате. Ако е можно, не носете со вас чувствителни информации и едноставно користете нов, избришан компјутер, пристапете до датотеките што ви се апсолутно потребни од облак и потоа избришете ги кога ќе се вратите дома.

Покрај подготовката за патувањето и сведувањето на податоците што се споделуваат кога патувате на минимум, има неколку основни оперативни совети за кои треба да размислите и да ги вклучите во вашата парламентарна политика за службени патувања.

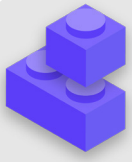
Размислете за користење лаптопи или телефони наменети за патувања кои имаат малку или воопшто немаат чувствителни податоци складирани на нив. Ако поголемиот дел од работата на вашиот парламент се врши во облак, релативно евтиниот Хромбук (Chromebook) може да биде добра опција за таков уред. Вратете ги фабричките поставки или „избришете“ ги овие уреди откако ќе ги вратите пред да се поврзете на заедничките безжични мрежи дома или на работа.

Обезбедете им на вработените информации за контакт и план со активности за тоа што треба да направат ако нешто тргне наопаку на нивното патување. Тоа вклучува информации за локални болници, клиники или аптеки доколку имаат потреба од медицинска помош додека патуваат.

Вработените, исто така, треба да ги чуваат сите уреди до нив додека патуваат. На пример, држете го лаптопот до вашите нозе (не во преградата над вас или во багажот) кога сте во автобус, воз или авион. Не претпоставувајте дека хотелската соба – па дури и хотелскиот сеф – е безбедно место за чување чувствителни уреди и предмети. Не им верувајте на јавните УСБ порти за полнење. УСБ портите за полнење на аеродромите, станиците и возилата стануваат сè повообичаена глетка и многу удобен начин за напојување на уредите. Меѓутоа, тие може да бидат лесен вектор за закачување злонамерен софтвер. Затоа, погрижете се или да ги наполните уредите на традиционален начин преку приклучок во ѕид или да купите **УСБ блокатори на податоци** за да им овозможите на вработените кои патуваат безбедно да ги наполнат своите уреди преку УСБ.

Напредно ниво: Безбедно резервирање патувања за вашиот парламент

Кога изготвувате политика за службени патувања, имајте предвид кои информации можат да бидат незаштитени кога организирате или резервирате патување. Тоа може да биде особено важно ако организирате големи настани или конференции за чијашто цел постапувате со чувствителни информации од различни вработени, членови или присутни. Размислете внимателно за тоа како безбедно ќе ги споделите и складирате (доколку е потребно) личните информации, како што се податоците од пасошот, маршрутите за патување и медицинското досие.



Основни елементи на планот за безбедност: Заштита на вашата физичка безбедност

- **Потсетете ги членовите и вработените да ги чуваат уредите физички заштитени во секое време.**
- **Проверете ги и заштитете се од сите начини на кои луѓето можат да влезат во вашите простории.**
- **Креирајте политика за гости и пристап.**
- **Користете силни брави, системи за идентификација/картички и ротирајте/променете ги кога е потребно.**
- **Размислете за поставување камери или други безбедносни системи во просториите.**
- **Имајте и користете уништувачи на хартија.**
  - Одредете време кое вработените ќе го посветат на отстранување документи во печатена форма што содржат чувствителни информации.
- **Направете список на локални професионалци, организации и агенции за спроведување на законот со кои можете да ги поврзете членовите и вработените за правна помош, медицинска помош и помош со менталното здравје како одговор на физички напади или закани.**
- **Креирајте парламентарна политика за службени патувања.**
- **Погрижете се вработените да знаат што да направат при итни случаи во текот на патувањето.**
- **Внимавајте на дополнителните податоци кои се креираат и споделуваат кога организирате патувања или настани.**

Што да направите кога работите ќе тргнат наопаку

Значи, знаете што треба да направите. Ги воспоставивте политиките и ги обучивте сите во парламентот за сите најдобри практики. И покрај сета таа напорна работа, многу е веројатно дека на крајот нешто ќе тргне наопаку. Такви работи се случуваат. Кога ќе се случат, од суштинско значење е да имате план за одговор на инцидентот. Одговорот на инцидентот е клучен, и често потценет, дел од планот за безбедност на вашиот парламент, бидејќи тој може да биде разликата помеѓу напад што ќе ја уништи вашата репутација или непријатна препрека на патот.

Имајте предвид дека можете да одговорите на некој инцидент само ако знаете за него. Многу е важно да постои силна безбедносна култура и да се поттикнуваат членовите и вработените да пријавуваат проблеми. Затоа е подобро да се награди доброто безбедносно однесување отколку да се казнуваат безбедносните пропусти или грешки. Исто така, важно е да се изрази емпатија и да се провери добросостојбата на вработените кога ќе пријават инцидент. Сакате вработените веднаш да пријават кликнување на линк во „фишинг-порака“, украден телефон или хакирана сметка на социјалните медиуми – да не се двоумат од страв од одмазда или недостиг на поддршка. Сепак, одговорот на инцидентот, исто како и стратегиите за ублажување споменати во другите делови од прирачникот, претставува вложување напори во рамките на целиот парламент.

За што треба да планирате? Накратко, за сè што е донекаде веројатно дека ќе се случи. Тоа ќе биде различно за секој парламент, но вообичаените прашања кои планот за одговор на инциденти ќе помогне да се одговорат се:

- Што да правиме ако нашите сметки или веб-страници бидат хакирани?
- Што да правиме ако некој кликне на „фишинг“ е-пошта или ако уредот се однесува сомнително?
- Што да правиме ако нашите е-пошти или најчувствителните документи се украдени и неовластено откриени?
- Што да правиме ако некој од нашите вработени е доведен во физичка опасност? Или ако се бори со стрес и анксиозност поради таквите закани?
- Што да правиме ако нашата канцеларија е оштетена во пожар, поплава или природна катастрофа?
- Што да правиме ако компјутерот или телефонот на некој член е изгубен или украден?

Одговорите на овие и на други прашања ќе се разликуваат за секој парламент, но важно е да размислите за нив заедно и јасно да формулирате и споделите план, така што секој ќе биде подготвен веднаш да преземе акција за да ја ограничи штетата.

Да се послужиме со **Холистичкиот водич за безбедност** на „Тактикал тек“ (Tactical Tech), добар начин да почнете со планот за одговор на инциденти е **да дефинирате инцидент или итен случај** во контекст на вашиот парламент. Одлучете што е „итен случај“ - т.е. моментот во кој треба да почнеме да ги спроведуваме планираните активности и мерки за непредвидени ситуации. Ова е важно бидејќи понекогаш нема да биде јасно – ако замислите сценарио како што е губење контакт со колега на теренска мисија; колку долго би чекале пред да прогласите итен случај? Никој не сака да реагира премногу рано, но предолгото чекање во некои околности може да биде катастрофално.

Исто така, важно е да размислите и за сите чекори од **операцијата**. На секое лице доделете му јасна улога со која тоа ќе биде запознаено и на која однапред се согласило – тоа ќе ги намали неорганизираноста и паниката во случај на инцидент. При секоја закана, разгледајте ги различните улоги што можеби ќе треба да ги преземете и практичните аспекти вклучени во одговорот на итниот случај. Во рамките на оваа важна стратегија за итни случаи е активирањето мрежа за поддршка – широка мрежа на сојузници, која може да вклучува различни гранки на вашата влада, други пријателски влади, технолошки компании, продавачи на услуги за безбедност и мултилатерални институции, се само неколку примери. Како можат да ве поддржат вашите сојузници? Дали треба да контактирате со нив однапред за да проверите дали ќе сакаат да ви помогнат при итен случај и да ги известите што очекувате од нив?

Кога реагирате на инцидент, ефективните **комуникации** се многу важни. Одлучете кое е најбезбедното и најефикасно средство за комуникација со секој актер во различни сценарија и идентификувајте резервни средства за комуникација. Имајте предвид дека за итни случаи, можеби, ќе биде корисно да имате јасни упатства за тоа што да (и што да не) комуницирате, кога да комуницирате, кои канали да ги користите за да комуницирате и со кого треба да комуницирате. Исто така, земете го предвид влијанието на инцидентот врз репутацијата на вашиот парламент и бидете подготвени да одговорите соодветно. Погрижете се одговорното лице за комуникации во парламентот да биде запознаено со инцидентот и да може да ги следи социјалните медиуми или другите медиуми во однос на потенцијалното влијание. Тој/таа, исто така, треба да биде подготвен/а за евентуални прашања од јавноста или медиумите за инцидентот, доколку е релевантно. Ова е особено важно за подобро справување со какви било потенцијално негативни написи или наштетување на репутацијата. Иако секој инцидент и контекст е различен, искрените и транспарентни комуникации често помагаат да се изгради доверба по инцидентот.

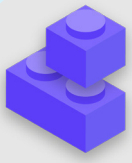
Напредно ниво: Креирање систем за рано предупредување и одговор

Размислете за воспоставување систем за рано предупредување и одговор. Таквиот систем звучи модерно, но, во суштина, тој е само централизиран документ (електронски или поинаков) кој треба да се отвори во случај на итност. Во документот треба да ги наведете сите детали за безбедносните показатели и инциденти кои се случиле по временски редослед, да дадете јасен опис на активностите и редоследот на планираниот одговор и да наведете што треба да се постигне за намалување на ризикот. Тој, исто така, треба да содржи активности што треба да се преземат по инцидентот со цел да се заштитат вклучените лица од понатамошно повредување и да им се помогне да заздравт физички и емоционално. Системот за рано предупредување и одговор може да обезбеди корисна документација за споделување со органите за спроведување на законот (ако е применливо), последователна анализа на она што се случило и насоки за тоа како да ги подобрите вашите тактики за спречување на заканите и одговор на заканите во иднина.

Покрај овие важни концепти за одговор на инциденти, вашиот парламент треба да се подготви и за каков било конкретен **технички** одговор. Во некои случаи, со техничкиот одговор може да управува внатрешниот ИТ кадар или системските администратори. На пример, ако ви изгледа дека сметката за е-пошта е хакирана, администраторот на вашата сметка треба да биде подготвен и да ја исклучи или оневозможи засегнатата сметка. Меѓутоа, за некои технички инциденти може да биде потребна експертиза која ја немате во вашиот парламент. За такви ситуации, важно е да се идентификува список на надворешни технички експерти од доверба кои можат да ви помогнат во одговорот на инцидентот. Во некои случаи, можеби ќе сакате однапред да преговарате за условите со давателите на услуги (како што е хостот на вашата веб-страница или фирмата за ИТ безбедност) за да се осигурите дека тие ќе бидат достапни (и нема да наплаќаат дополнително) за одговор на таков технички инцидент.

Последно, но секако не и најмалку важно, треба да размислите за **правните** чекори. Важно е да се разбере правната заштита која може да ја имате, како и правните обврски или последици со кои може да се соочи вашиот парламент како резултат на нарушување на безбедноста на податоците или друг безбедносен инцидент. Како парламент, вие сте во позиција со особена моќ и важност кога станува збор за разбирање и за почитување на локалните прописи за безбедност и приватност на податоците. Одвојте време за да ги разгледате можните инциденти со релевантен правен советник, доколку е потребно, и да направите план за тоа што би направиле како одговор. Добра идеја е да склучите договор со правен советник од доверба за да ве застапува вас и вашите интереси, доколку е потребно, по инцидентот. Како дел од оваа правна подготовка, осигурете се дека ги разбирате правните обврски на кој било набавувач или партнер. Дали тие треба да ве известат во случај на нарушување на безбедноста на нивните податоци? Каква поддршка (ако ја има) треба да ви обезбедат во случај на инцидент? Додека ги подготвувате договорите и спогодбите со надворешни набавувачи, имајте ја предвид можноста за нарушување на безбедноста на податоците или друг инцидент.

Иако не постои единствен пристап за одговор на сите инциденти, неопходно е да се има јасни оперативни, комуникациски, технички и правни планови. Додека го подготвувате вашиот план за одговор на инциденти, ве поттикнуваме да користите некои одлични постојни ресурси кои се дизајнирани да им помогнат на организациите да управуваат со одговорот на инциденти. Иако сите овие ресурси не се дизајнирани конкретно за парламенти, нивната содржина е многу релевантна. Овие ресурси се Digital First Aid Kit (Комплет за дигитална прва помош), креиран од Реарнет (Rarenet) и СивиСЕРТ (CiviCERT), Online Harassment Field Manual (Практичен прирачник при вознемирување на интернет) на ПЕН Америка (PEN America), Cybersecurity Campaign Playbook (Книга за кибернетска безбедност на кампањи) и Cyber Incident Communications Plan Template (Образец за план за комуникации при кибернетски инциденти) на центарот Белфер (Belfer), како и Digital Security Helpline (Линијата за помош за дигитална безбедност) на Аксес нау (Access Now).



Основни елементи на планот за безбедност: Одговор на инциденти

- **Направете парламентарен план за одговор на инциденти и применувајте го.**
  - Размислете за можните инциденти и подгответе се за вашиот одговор пред да се случат.
- **Осигурете се дека сите во рамките на парламентот се запознаени со тоа како ќе комуницирате и кои технички чекори ќе бидат преземени во случај на инцидент.**
- **Одвојте време за да ги разберете вашата правна заштита и обврски.**
- **Бидете подготвени да им обезбедите на членовите и на вработените емоционална и социјална поддршка која им е потребна по инцидентот**

Додаток А: Препорачани ресурси

- Холистички прирачник за безбедност на Tactical Tech; Creative Commons Attribution-ShareAlike 4.0 меѓународна лиценца
  - Поглавје 2.4 – Разбирање и каталогизирање на нашите информации
  - Поглавје 1.5 – Комуницирање за закани во тимовите и организациите
  - Поглавје 3.4 – Безбедност во групи и организации
- Едукативен прирачник за безбедност на Фондацијата Електронски граници; Creative Commons Attribution 3.0 US лиценца
  - Печатен материјал за активност за моделирање закани
- Водич за спречување фишинг и добра грижа за е-пошта на Фондацијата Слобода на печатот; Creative Commons Attribution 4.0 меѓународна лиценца
- Locking Down Signal водич на Фондацијата Слободна на печатот; Creative Commons Attribution 4.0 меѓународна лиценца
- Водич за самоодбрана од надзор (SSD) на Фондацијата Електронски граници ; Creative Commons Attribution 3.0 US лиценца
  - Што треба да знам за шифрирањето
  - Комуницирање со другите
  - Избирање на соодветната VPN за вас
- Водич за безбедни разговори во група и алатки за конференции на Front Line Defenders
- Data Detox Kit на Tactical Tech
  - Let the Right One In: Направете ги вашите лозинки посилни
  - Зајакнете го заклучувањето на екранот
- Водич за лозинки за безбедност на избори на Центарот за демократија и технологија; Creative Commons Attribution 4.0 меѓународна лиценца
- Водич за автентикација со два фактора за безбедност на избори на Центарот за демократија и технологија; Creative Commons Attribution 4.0 меѓународналиценца
- Автентикација со два фактора за почетници на Мартин Шелтон ; Creative Commons Attribution 4.0 меѓународна лиценца
- Security in a Box на Tactical Tech и Frontline Defender; Creative Commons Attribution-ShareAlike 3.0 непренесена лиценца
  - Заштитете го вашиот уред од напади од злонамерен софтвер и фишинг
  - Заштитете се од физички закани
- SANS' OUCH! Билтен: Запрете го тој злонамерен софтвер
- Пристап до уреди и податоци на Apple кога е загрозена личната безбедност
- Комплет алатки за кибернетска безбедност за организации базирани на мисии на Глобалната сајбер алијанса
- Алатка за проценка на сајбер безбедноста на Фондацијата Форд

Додаток Б: Комплет со почетни упатства за план за безбедност

Користете го следниов комплет со почетни упатства за да направите белешки додека вие и вашата организација го читате прирачникот и го совладувате материјалот, и разгледајте ги придружните прашања со вашите колеги за да помогнете во создавањето продуктивна дискусија. Не заборавајте да се повикате на клучните „основни елементи“ во секој дел од прирачникот за да се осигурите дека сте ги опфатиле важните теми додека го подготвувате вашиот план за безбедност. На крајот на прирачникот, основните елементи, одговорите на овие прашања за дискусија и вашите белешки треба да ја формираат основата на еден успешен план за безбедност.

Градење култура на безбедност

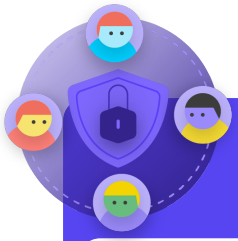
Силна основа: Обезбедување на сметките и на уредите

Силна основа: Обезбедување на сметките и на уредите

Безбедно комуницирање и складирање податоци

Безбедност на интернет

Заштита на физичката безбедност



Градење култура на безбедност

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Кога можете да закажете дискусија за да го прегледате вашиот план за безбедност со целата организација?
- Кои денови или термини ѝ одговараат на организацијата за да се закажат редовни дискусии и обуки за безбедност?
- Кои чекори може да ги преземе раководството за моделирање на добро безбедносно однесување и посветеност на планот за безбедност? Како можат другите лица во организацијата да придонесат за безбедноста?

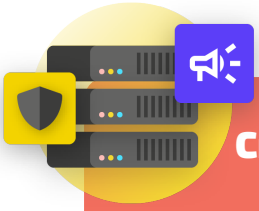
ВАШИ БЕЛЕШКИ И ИДЕИ

Силна основа: Обезбедување на сметките и на уредите

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Како ќе ги спроведете мерките за безбедност на сметките – како што се апликација за управување со лозинки и 2FA – во рамките на целата организација? Со какви пречки може да се соочите при спроведувањето?
- Како вашата организација ќе се погрижи уредите да бидат безбедни и ажурирани? Како дел од ова, дали на организацијата ѝ треба план за справување со нелиценциран софтвер или компјутери?
- Кога е добар момент да се организира обука за сите вработени за опасностите од „фишинг“, злонамерен софтвер и најдобрите практики за безбедност на уредите?

ВАШИ БЕЛЕШКИ И ИДЕИ

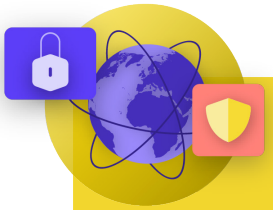


Силна основа: Обезбедување на сметките и на уредите

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Како вашата организација ќе спроведе целосно, од крај до крај, шифрирање на пораките за безбедна комуникација? Со какви пречки може да се соочите при спроведувањето?
- Како вашата организација ќе спроведе решение за безбедно споделување датотеки, како внатрешно така и надворешно? Со какви пречки може да се соочите при спроведувањето?
- Како вашата организација ќе спроведе решение за безбедно складирање и креирање резервна копија на податоците? Со какви пречки може да се соочите при спроведувањето?

ВАШИ БЕЛЕШКИ И ИДЕИ



Безбедно комуницирање и складирање податоци

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Како вашата организација ќе ги спроведе барањата за безбедно пребарување на интернет, како што се ХТТПС, доверлив веб-пребарувач и, доколку е соодветно, ВПН за вработените?
- Кои ќе бидат клучните елементи на политиката за социјални медиуми на вашата организација? Како ќе се спроведе таа?
- Како вашата организација ќе ги заштити своите веб-страници и други точки на присуство на интернет?

ВАШИ БЕЛЕШКИ И ИДЕИ

Безбедност на интернет

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Како организацијата ќе ја дистрибуира и ќе ја спроведе својата политика за пристап и гости во просториите?
- Кој е одговорен за подготовка на вработените за физичките и дигиталните безбедносни предизвици со кои можат да се соочат додека се на службен пат?
- Кои чекори можат да ги преземат вработените за да ги чуваат своите уреди сигурни и безбедни, и во канцеларија и додека се на службен пат?

ВАШИ БЕЛЕШКИ И ИДЕИ

Заштита на физичката безбедност

ПРАШАЊА ШТО ТРЕБА ДА СЕ РАЗГЛЕДААТ:

- Како организацијата ќе ја дистрибуира и применува својата политика за одговор на инциденти?
- Дали има достапни ресурси за вработените на кои можеби ќе им треба емоционална и социјална поддршка по инцидент? Доколку нема, како организацијата може да ги обезбеди тие ресурси во случај на инцидент?

ВАШИ БЕЛЕШКИ И ИДЕИ

Додаток C: Image Citations

Страница 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.
Страница 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.
Страница 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.
Страница 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.
Страница 27: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Страница 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.
Страница 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/.
Страница 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/
Страница 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Страница 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.
Страница 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.
Страница 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Страница 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
Страница 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Страница 52: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Страница 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/.
Страница 63: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Страница 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
Страница 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Страница 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