NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Довідник із кібербезпеки

для

парламентів

Посібник для парламентів, які хочуть розпочати роботу над планом кібербезпеки

IRI
INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP
UNITED STATES HOUSE OF REPRESENTATIVES

Довідник із кібербезпеки

для

парламентів

Посібник для парламентів, які хочуть розпочати роботу над планом кібербезпеки

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

Зміст

Візуальна легенда

У довіднику на додаток до основного тексту ви знайдете кілька різних повторюваних виділених елементів. Ось коротка «легенда», яка допоможе зрозуміти основні елементи:

Вивчення проблеми

Вказує на тематичні дослідження, які висвітлюють реальний вплив певної теми на парламенти в усьому світі чи в конкретній країні.

Додаткові поради

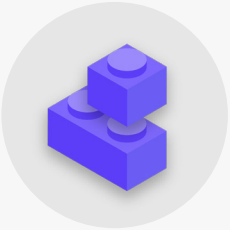
Виділяє деякі додаткові поради та інформацію, на які варто звернути увагу під час читання Посібника.

Реальність

Викликає поширені приклади інструментів тактики кібербезпеки, які використовуються в «реальному світі» як на користь, так і на зло.

Вищий рівень

Вказує на складну тему — інформацію, яку важливий для розгляду вашим парламентом, але яка може бути дещо більш технічної чи складнішою.



Будівельні блоки плану безпеки

Вказує на «Блоки плану безпеки», які є ключовими висновками з кожного розділу Посібника.

Перша десятка

Ці 10 елементів мають вирішальне значення для плану безпеки вашого парламенту. Якщо ви не знаєте, з чого почати, спочатку погляньте сюди.

1. **Проводьте регулярні тренінги з безпеки у вашому парламенті.**
2. **Будьте уважні до фішингу та створіть систему звітності.**
3. **Використовуйте шифрування для всього зв'язку — наскрізного, якщо це можливо.**
4. **Вимагайте надійних паролів і запровадьте менеджер паролів у своєму парламенті.**
5. **По можливості вимагайте двофакторну автентифікацію.**
6. **Переконайтеся, що всі пристрої та програмне забезпечення співробітників оновлюються.**
7. **Використовуйте безпечне хмарне сховище.**
8. **Використовуйте HTTPS і, якщо необхідно, VPN для доступу до Інтернету.**
9. **Захистіть фізичні активи вашого парламенту.**
10. **Розробіть організаційний план реагування на інцидент.**

1

Формування культури безпеки

2

Міцна основа: захист облікових записів і пристроїв

3

Безпечна комунікація і Безпечне зберігання даних

4

Безпека в інтернеті

5

Фізична Безпека

6

Що робити, коли все йде не так?

Автори та подяка

Цей посібник підготували Національний демократичний інститут (NDI) і Партнерство з питань демократії в Палаті представників (HDP).

Провідний автор: **Evan Summers (NDI)**
Співавтори: **Sarah Moulton (NDI); Chris Doten (NDI)**

Під час розробки цього Довідника ми хотіли б особливо подякувати нашим експертам і зовнішнім рецензентам, які надавали нам цінні відгуки, зміни та пропозиції під час підготовки вмісту, зокрема:

Фіона Кракенбургер, Фонд відкритих технологій; Білл Будінгтон і Ширін Морі, Electronic Frontier Foundation; Джоселін Вулбрайт, Cloudflare; Мартін Шелтон, Фонд свободи преси; Дейв Лейхтман, Microsoft; Стівен Бойс, Міжнародна фундація виборчих систем; Емі Стаддарт, Міжнародний республіканський інститут; Емма Холлінгсворт, Global Cyber Alliance; Керолайн Сіндерс, Convocation Design + Research; Дхіта Катурані; Сандра Пепера, НДІ; Аарон Азельтон, НДІ; Фріда Аренос, НДІ; Ентоні Де Анджело, NDI; Вітні Пфайфер, NDI; і Дерек Люйтен, Партнерство з питань демократії в Палаті представників. Ми також хотіли б подякувати Полу Коллі в Службі законодавчої інформації в Ліберії, Ніхаду Бахраму та Фуаду Ахмеду в парламенті Курдистану в Іраку, Діані Платі в Сенаті Колумбії; Аяду Аббасу та Маджиду Худхуру в Раді представників Іраку, а також Тані Данаїловській в Асамблеї Північної Македонії за цінні ідеї та внесок.

Ми також хочемо відзначити чудові посібники, довідники, робочі зошити, навчальні модулі та інші матеріали, які розробила та веде Спільнота організаційної безпеки (OrgSec). Цей Посібник створено, щоб доповнити ці більш поглиблені матеріали, об'єднавши ключові уроки в єдиний, легкий для читання ресурс для парламентів, які хочуть розпочати роботу над планом кібербезпеки.

Окрім натхнення з багатьох чудових ресурсів, зібраних спільнотою, ми напряму запозичили корисні тексти з кількох існуючих ресурсів і включили їх до цього Довідника, зокрема, Посібник із самозахисту шляхом спостереження від Electronic Frontier Foundation, Комплексний посібник із безпеки від Tactical Tech, а також ряд пояснень від Center for Democracy and Technology і Freedom of the Press Foundation. Конкретні посилання на ці ресурси знаходяться в розділах нижче, а повні посилання, інформація про автора та ліцензію наведено в Додатку А.

Хто ми?

Національний Демократичний Інститут Міжнародних Відносин (НДІ) (National Democratic Institute for International Affairs (NDI) — це некомерційна, позапартійна організація зі штаб-квартирою у м. Вашингтон, округ Колумбія (США), яка працює в усьому світі для зміцнення та захисту демократичних інститутів, процесів, норм і цінностей із метою забезпечення кращої якості життя для всіх.

НДІ вважає, що всі люди мають право жити у світі, в якому поважається їхня гідність, безпека та політичні права, і що цифровий світ не є винятком.

В рамках НДІ Відділ із питань демократії та технологій прагне сприяти створенню глобальної цифрової екосистеми, у якій демократичні цінності захищаються, пропагуються та можуть процвітати; уряди є більш прозорими та інклюзивними; і всі громадяни мають право вимагати від свого уряду звітування про свою роботу. Ми працюємо над підтримкою глобальної мережі активістів, які присвятили себе втіленню гнучкої стратегії кібербезпеки, і співпрацюємо з партнерами над інструментами та ресурсами, такими як цей Довідник. Детальніше про нашу роботу ви можете дізнатися на нашому веб-сайті, із нашого аккаунту у Twitter або звернувшись до нас безпосередньо на адресу електронної пошти cyberhandbook@ndi.org. Ми завжди раді чути ваші відгуки та відповісти на запитання про нашу команду й нашу роботу щодо кібербезпеки, технології та демократії.

Партнерство з питань демократії Палати представників (HDP) співпрацює з законодавчими органами в усьому світі, щоб сприяти чуйному, ефективному уряду та зміцнювати демократичні інститути. Центральне місце в нашій роботі займає рівноправна співпраця для створення технічної експертизи в партнерських законодавчих органах, що сприятиме підвищенню підзвітності, прозорості, законодавчої незалежності, доступу до інформації та державного нагляду. Зараз HDP має партнерські відносини з більш ніж 20 національними законодавчими органами світу. Сфери співпраці з парламентами-партнерами HDP включають вирішення бюджетних питань, забезпечення більш ефективної роботи комітетів, покращення послуг установчих органів, надання інструментів для посилення нагляду, посилення законодавчої етики та вдосконалення IT, бібліотеки та досліджень, а також законодавчих процесів і процедур. Програми HDP реалізуються Національним демократичним інститутом (NDI) і Міжнародним республіканським інститутом (IRI) через угоду про співробітництво з Агентством США міжнародного розвитку (USAID).

Хто керує кібербезпекою у парламенті?

Ефективний і безпечний парламент потребує співробітників з навичками та належними повноваженнями для виконання рекомендацій, включених у цей Посібник. З огляду на це, особи, відповідальні за кібербезпеку в парламентах, можуть дуже відрізнятися, і не існує єдиної «правильної» моделі того, хто повинен займатися кібербезпекою. У деяких випадках це може бути спеціальна команда з кібербезпеки у вашому IT-підрозділі, а в інших — група різних адміністративних працівників і депутатів. Незважаючи на це, майте на увазі, що хоча важливо мати хорошу команду, яка відповідає за кібербезпеку вашого парламенту, це також відповідальність кожного в парламенті та навколо нього за дотримання політики та процедур, необхідних для забезпечення безпеки парламенту. Нижче наведено кілька прикладів різних моделей кадрового забезпечення для управління парламентською кібербезпекою:

Палата представників Сполучених Штатів Америки
У **Палаті представників Сполучених Штатів Америки** деякі окремі депутатські офіси наймають **системного адміністратора**, який відповідає за керування всіма комп'ютерними апаратними та програмними системами, що використовуються в офісі, включно з питаннями кібербезпеки, і навчає співробітників передовим практикам. На інституційному рівні головний адміністративний офіцер Палати представників містить групу інформаційних ресурсів, яка включає **відділ, присвячений інформаційній безпеці**.

Національна асамблея Замбії
Національна асамблея Замбії покладається на свій Департамент інформаційно-комунікаційних технологій (ІКТ) для виконання різноманітних функцій, включаючи управління програмним забезпеченням, апаратним забезпеченням та інформаційною інфраструктурою парламенту, навчання депутатів та/або співробітників парламенту технологічним системам, а також забезпечення безпеки інформаційної інфраструктури парламенту. від внутрішніх і зовнішніх загроз кібербезпеці.

Парламент Малайзії
У **парламенті Малайзії** є відділ інформаційних технологій під керівництвом головного адміністратора парламенту, що дозволяє йому обслуговувати обидві палати парламенту. Цей підрозділ включає спеціальну посаду з мережевої безпеки, яка дозволяє йому гарантувати, що мережеві системи, центри обробки даних та інфраструктура ІКТ є актуальними та максимально безпечними.

Для кого призначений цей Довідник?

Цей Довідник було написано з простою метою: допомогти вашій громадській організації розробити зрозумілий план кібербезпеки, який можна реалізувати.

Оскільки світ все більше переходить в Інтернет, кібербезпека є не просто модним словом, а критично важливою концепцією для успіху парламентів, а безпека інформації (як онлайн, так і поза ним) є викликом, який вимагає зосередженості, інвестицій і пильності.

Ваш парламент, швидше за все, опиниться — якщо він ще не став — мішенню кібератаки. Ми не хочемо марно бити на сполох: це реальність навіть для тих організацій, які не вважають себе конкретними цілями.

У середньому за рік Center for Strategic and International Studies, який веде **поточний список** випадків, які називаються «значними кіберінцидентами», реєструє сотні серйозних кібератак, багато з яких націлені на десятки, якщо не сотні організацій одночасно. Окрім таких зареєстрованих атак, ймовірно, щороку відбуваються сотні інших менших атак, які залишаються непоміченими або про які не повідомляється.

Багато з них спрямовані на урядові установи, законодавчі органи та політичні організації.

Такі кібератаки мають серйозні наслідки. Незалежно від того, що у них на меті — зірвати роботу парламенту, завдати шкоди вашій репутації чи навіть викрасти інформацію, яка може призвести до психологічної чи фізичної шкоди депутатам чи співробітникам, такі погрози потрібно сприймати серйозно.

Хороша новина: вам не потрібно ставати програмістом або технічним спеціалістом, щоб захистити себе та свою організацію від поширених загроз. Однак слід бути готовими докладати зусилля, енергію та час у розробку та впровадження надійного організаційного плану безпеки парламенту.

Якщо ви ніколи не думали про кібербезпеку свого парламенту, не мали часу зосередитися на цьому або знаєте деякі основи цієї теми, але вважаєте, що ваш парламент міг би посилити свою кібербезпеку, цей посібник для вас. **Незалежно від того, звідки ви, цей Посібник має на меті надати вашому парламенту важливу інформацію, необхідну для впровадження надійного плану безпеки — плану, який виходить за рамки простого викладення слів на папері та дає вам змогу застосувати найкращі практики в життя.**

Що таке план безпеки і навіщо він потрібен моєму парламенту?

План безпеки — це набір письмових політик, процедур і вказівок, узгоджених вашою організацією для досягнення рівня безпеки, який ви та ваша команда вважаєте доцільним для захисту ваших співробітників, партнерів і даних.

Добре складений план організаційної безпеки, що регулярно оновлюється, може захистити вас і підвищити продуктивність, забезпечуючи душевний спокій, необхідний для зосередження на важливій повсякденній роботі організації. Без продуманого комплексного плану дуже легко не помітити деяких типів загроз, надто зосередитись на одному ризику або ігнорувати кібербезпеку, доки не настане криза. Коли ви починаєте розробляти план безпеки, необхідно поставити собі кілька важливих питань у ході процесу, що називається **оцінкою ризику**. Відповіді на ці запитання допоможуть зрозуміти унікальні загрози, з якими ви стикаєтеся, і дозволять вам відсторонено і всебічно подумати про те, що саме вам потрібно захищати та від кого це слід захищати. Навчені оцінювачі за допомогою таких систем, як **SAFETAG** від для перевірки концепції можуть допомогти пройти такий процес. Якщо ви можете отримати доступ до такого рівня професійних знань, це того варте, але навіть якщо ви не можете пройти повну оцінку, вам слід зустрітися зі своїми зацікавленими сторонами в парламенті, щоб ретельно розглянути ці ключові питання:

1 Які активи має ваш парламент і які ви хочете захистити?

Ви можете почати відповідати на ці запитання, **створивши каталог усіх активів вашого парламенту**. Така інформація, як повідомлення, електронні листи, контакти, документи, календарі та місця зберігання, є можливими активами. Активами можуть бути телефони, комп'ютери й інші пристрої. Люди, зв'язки та стосунки також можуть бути активами. Зробіть **перелік ваших активів** і спробуйте каталогізувати їх за їхньою важливістю для організації, де ви їх зберігаєте (можливо, у кількох цифрових чи фізичних місцях), і що заважає іншим отримати до них доступ, пошкодити чи порушити їх роботу. Майте на увазі, що не всі активи є однаково важливими. Якщо деякі дані організації є загальнодоступними або ви вже опублікували певну інформацію, вони не є секретами, які потрібно захищати.

2 Хто ваші зловмисники, які їхні можливості та мотивація?

«Зловмисник» — це термін, що зазвичай використовується в організаційній безпеці. Простою мовою, зловмисники — це суб'єкти (індивідууми чи групи), які зацікавлені в завданні цільової шкоди парламенту, перешкоджанні вашій роботі та отриманні доступу або знищенні вашої інформації. Це ваші вороги. Приклади потенційних зловмисників можуть включати фінансових шахраїв, ворожі уряди або ідеологічно чи політично мотивованих хакерів. Важливо скласти список своїх зловмисників і критично подумати про те, хто може захотіти негативно вплинути на парламент та співробітників. Хоча зовнішніх діячів (наприклад, іноземний уряд чи конкретну політичну групу) легко уявити зловмисниками, пам'ятайте, що зловмисниками можуть бути також люди, яких ви знаєте, наприклад незадоволені співробітники, колишні колеги, члени сім'ї чи партнери, які не підтримують вашу організацію. Різні противники створюють різні загрози та мають різні ресурси й можливості, щоб порушити вашу діяльність, отримати доступ або знищити вашу інформацію.

Наприклад, уряди часто мають багато грошей і потужні можливості, зокрема відключення інтернету та використання дорогих технологій стеження; мобільні мережі та інтернет-провайдери часто мають доступ до записів дзвінків та історії перегляду вебсторінок; кваліфіковані хакери в публічних мережах Wi-Fi мають можливість перехоплювати погано захищені комунікації або фінансові операції. Ви навіть можете стати самі собі зловмисником, наприклад, якщо випадково видалите важливі файли або надішлете приватні повідомлення не тій людині.

Мотиви зловмисників, ймовірно, відрізнятимуться, як і їхні можливості, інтереси та стратегії. Вони зацікавлені в дискредитації вашого парламенту? Можливо, вони мають намір замовчувати ваше послання чи зірвати роботу парламенту? Важливо розуміти мотивацію зловмисника, оскільки це може допомогти парламенту краще оцінити загрози, які він може становити.

3 З якими загрозами стикається ваш парламент? Наскільки вони вірогідні та який вплив вони можуть мати?

Коли ви визначите можливі загрози, у вас, швидше за все, з'явиться довгий перелік, який може видатися надмірним. У вас може виникнути відчуття, що будь-які зусилля будуть марними, або ви не будете знати, з чого почати. Щоб ваш парламент міг зробити наступні продуктивні кроки, слід проаналізувати кожну загрозу на основі двох факторів: ймовірність того, що загроза виникне; і наслідок такого виникнення.

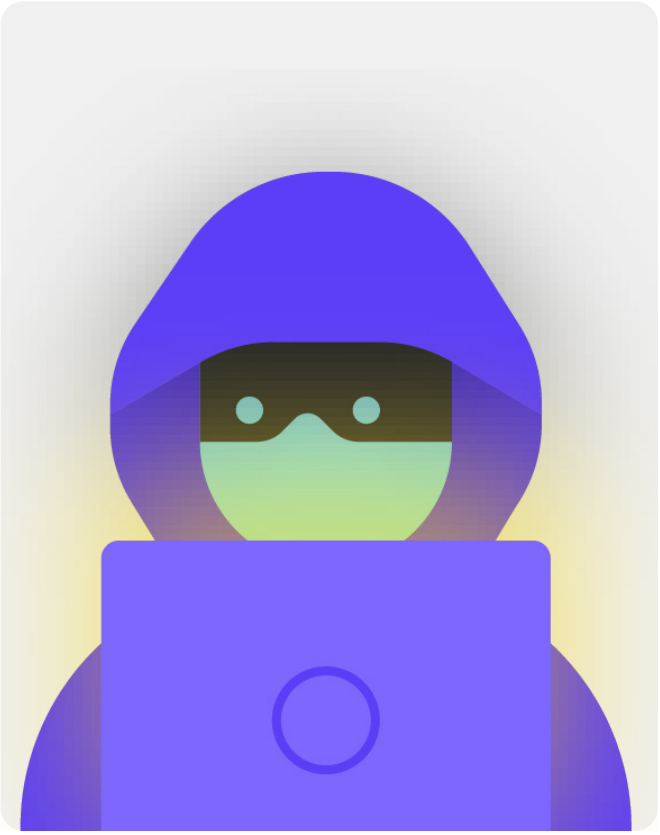
Щоб оцінити ймовірність загрози (як, наприклад, «низьку, середню або високу», залежно від того, чи певна подія відбудеться малоймовірно, може відбутися або трапляється часто), можна використати інформацію, відому вам, про потенціал і мотивацію ваших зловмисників, аналіз минулих інцидентів безпеки, досвід інших подібних організацій і, звісно, наявність існуючих стратегій зменшення ризику, запроваджених вашою організацією.

Щоб оцінити наслідки загрози, подумайте, що трапиться з організацією, якщо загроза справді виникне. Поставте такі запитання: «Якої шкоди, фізичної та психічної, завдасть загроза нам як організації та її співробітникам як людям?», «Наскільки тривалим буде ефект?», «Чи створить це інші шкідливі ситуації?» та «Як вона завадить здатності досягати цілей зараз і в майбутньому?» Відповідаючи на ці запитання, подумайте, чи дія загрози буле слабкою, помірною або сильною.

Після того, як ви зробили перелік загроз і класифікували їх за ймовірністю та впливом, можна переходити до складання більш ґрунтовного плану дій. Якщо ви зосередитесь на тих загрозах, які найімовірніше виникнуть ТА які матимуть значні негативні наслідки, ви спрямуєте свої обмежені ресурси для найбільш ефективного досягнення мети.

Мета полягає в тому, щоб мінімізувати ризики, наскільки це можливо. Але насправді ніхто — навіть уряд і компанії з величезними ресурсами — не може повністю усунути ризик. І це нормально: ви можете зробити багато, щоб захистити себе, своїх колег і свій парламент, подбавши про найбільші загрози.

У якості допоміжного засобу під час оцінки ризику можна використати робочий аркуш, наприклад **ось цей**, розроблений Electronic Frontier Foundation. Майте на увазі, що інформація, яку ви створюєте в рамках цього процесу (наприклад, список ваших зловмисників і загрози, які вони представляють), сама по собі може бути конфіденційною, тому важливо зберігати її захищеною.



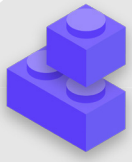
Створення плану кібербезпеки парламенту

Хоча план безпеки виглядатиме дещо по-різному, залежно від оцінки ризиків і організаційної динаміки, деякі основні концепції є майже універсальними.

У цьому Довіднику розглядаються ці важливі поняття для того, щоб ваша організація могла створити конкретний план безпеки на основі практичних рішень і реальних програм.

У цьому Довіднику зібрані варіанти та пропозиції, що є безкоштовними або дуже дешевими. Майте на увазі, що найбільшою вартістю, пов'язаною з впровадженням ефективного плану безпеки, буде час, який вам і співробітникам, депутатам і відділам у парламенті знадобиться для обговорення, вивчення та реалізації вашого нового плану. Однак, враховуючи ризики, з якими може зіткнутися ваш парламент, ці інвестиції будуть більш ніж варті того.

У кожному розділі знаходиться пояснення ключової теми, про яку ваша організація та її співробітники повинні знати, про що йдеться і чому це важливо. Кожна тема поєднується з основними стратегіями, методами та рекомендованими інструментами для обмеження ризику, а також порадами та посиланнями на додаткові ресурси, що допоможуть реалізувати ці рекомендації на місцях.



Стартовий комплект плану безпеки

Щоб опрацювати уроки Довідника та перетворити їх на реальний план для вашої організації, скористайтеся цим стартовим комплектом. Ви можете або роздрукувати комплект, або заповнити його в цифровому вигляді, читаючи Довідник онлайн. Коли ви робите нотатки та починаєте оновлювати чи створювати план безпеки, обов'язково зверніться до «Елементів побудови плану безпеки», детально описаних у кожному розділі. Жоден план безпеки не є повним без впровадження щонайменше цих основних елементів.

Скористайтеся перевагами інших ресурсів, які також допоможуть створити та реалізувати ваш план. Скористайтеся безкоштовними навчальними ресурсами, такими як **Планувальник безпеки** від Consumer Reports, застосунок **Umbrella від Security First**, **Проєкт Totem** від Free Press Unlimited і Greenhost, а також **Інструментарій кібербезпеки для соціально відповідальних організацій** від Global Cyber Alliance, які містять найкращі методи, згадані в цьому Довіднику, і посилання на численні навчальні інструменти, що допоможуть вам реалізувати велику кількість основних заходів безпеки.

Формування культури безпеки

Безпека залежить від людей, і щоб захистити ваш парламент, ви повинні переконатися, що всі залучені особи, включно з депутатами парламенту (депутатами), допоміжним персоналом законодавчих органів і дослідницькими службами, адміністративним персоналом у відділі фінансів, кадрів та IT, серед багатьох інших, — серйозно ставиться до кібербезпеки. Змінити культуру безпеки важко, але кілька простих кроків і серйозних розмов допоможуть створити атмосферу, що зміцнить стійкість співробітників й організації перед обличчям загроз безпеці. Один із найпростіших, але найважливіших кроків для створення такої парламентської культури безпеки, — це інформувати про неї всередині парламенту, а також забезпечити, щоб лідери завжди сприяли формуванню гарної поведінки.

Формування культури безпеки в парламенті

У лютому 2019 року Австралія зазнала кібератаки, яка скомпрометувала мережі австралійського національного парламенту та трьох провідних політичних партій. Зловмисники змогли отримати доступ до програмних документів і приватного листування електронною поштою між депутатами, їхніми співробітниками та виборцями. Атака сталася лише за три місяці до виборів, що підкреслило вразливість незахищених мереж під час виборів.

У відповідь на цю значну та успішну атаку парламент доклав зусиль для підвищення рівню забезпечення кібербезпеки. Такі інвестиції включали розслідування Спільним комітетом державних рахунків і аудиту кіберстійкості Співдружності. Розслідування **ґрунтувалося на результатах перевірок,** які проводилися протягом кількох років і показали відсутність зменшення ризиків для кібербезпеки в парламенті та інших державних установах. Наприклад, Національне контрольно-ревізійне управління Австралії підкреслило неспроможність парламенту зосередитися на довгострокових стратегічних цілях і розробити підхід, що ґрунтується на оцінці ризику, коли мова зайшла про кібербезпеку. І хоча розслідування та перевірки виявились невтішними, готовність парламенту виявляти проблеми кібербезпеки та сприяти їх вирішенню є прикладом створення культури, яка сприяє ефективній парламентській кібербезпеці. Такій, яка починається з розпізнавання проблем і інвестування в ефективні технічні та людські рішення, де безпека не ігнорується, а ставиться на перше місце. Наприклад, шляхом найму групи з «підвищення кібербезпеки» та бюджетних інвестицій до «**Фонду реагування на кібербезпеку**», якщо такі ресурси належним чином підтримуються, тоді як основна увага приділяється кібербезпеці як регулярному елементу парламентських операцій, парламент (та інші державні органи) буде краще оснащений для пом'якшення майбутніх атак кібербезпеці. Зважаючи на це, звичайно, краще виробити зобов'язання щодо безпеки у вашому парламенті *до того, як* станеться серйозне порушення безпеки.

Інтегрування безпеки до вашої звичайної операційної структури

Як детально описано в Комплексному посібнику з безпеки від Tactical Tech, дуже важливо проводити регулярні зустрічі у безпечних місцях для обговорення різних аспектів безпеки.

На таких зустрічах учасники команд можуть висловлювати свої занепокоєння щодо безпеки та будуть менше хвилюватися через те, що можуть видаватися параноїками або тратити марно час інших людей. **Планування регулярних розмов про безпеку** також нормалізує частоту спілкування та роздумів над питаннями, пов'язаними з безпекою, так що проблеми не забуваються, а учасники команд будуть приділяти більше уваги безпеці у своїй поточній роботі. Не обов'язково проводити такі розмови щотижня, але робіть це періодично із нагадуванням. На таких обговореннях має бути місце не лише для технічних тем безпеки, але й для питань, що стосуються комфорту та безпеки співробітників, як-от конфлікти у спільноті, переслідування в інтернеті (і офлайн), проблеми з використанням і впровадженням цифрових інструментів. Розмови можуть навіть включати такі теми, як звички обміну інформацією офлайн і те, як співробітники захищають або не захищають інформацію поза робочим місцем. Зрештою, важливо пам'ятати, що безпека парламенту настільки сильна, наскільки сильна його найслабша ланка. Ви можете досягти послідовного залучення співробітників, додавши тему безпеки до порядку денного звичайних робочих зустрічей. Ви також можете доручати відповідальність за організацію та проведення обговорення питань безпеки по черзі різним учасникам організації. Це допоможе укріпити ідею про те, що безпека є відповідальністю кожного, а не лише кількох обраних осіб чи «відділу IT». Коли ви почнете офіційне обговорення питань безпеки, співробітники почуватимуться комфортніше, обговорюючи ці важливі питання між собою, у менш формальних умовах.

Також важливо включити елементи безпеки в нормальне функціонування парламенту, наприклад, під час входу депутатів і співробітників — і подумати про припинення доступу до систем під час виходу. Безпека має бути не «ще однією річчю», про яку слід турбуватися, а радше ***невід'ємною частиною стратегії та діяльності організації***.

Пам'ятайте, що всі плани безпеки слід вважати живими документами, і їх слід регулярно переглядати та обговорювати, особливо коли ваш контекст безпеки змінюється.

Плануйте перегляд стратегії та внесення оновлень щорічно або в разі серйозних змін у стратегії, інструментах або загрозах, з якими ви стикаєтеся.

Отримання організаційної підтримки

Частиною успішної культури безпеки також є забезпечення підтримки парламентом вашого плану безпеки.

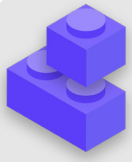
Важливо, щоб це була сильна, озвучена підтримка й управління з боку керівників організацій, які, у багатьох випадках, будуть тими, хто приймає остаточне рішення щодо розподілу часу, ресурсів та енергії для розроблення та реалізації ефективного плану безпеки. Якщо вони не ставитимуться до цього питання серйозно, всі інші також не сприйматимуть його серйозно. Щоб досягти такої підтримки, ретельно продумайте, коли і як представити свій план, зробіть це чітко, переконайтеся, що керівництво підтримує вашу ідею, і доведіть до кожного всі елементи та етапи плану, щоб кінцева мета плану безпеки не була таємницею і не викликала плутанини. Також переконайтеся, що в парламенті передбачено відповідний бюджет на кібербезпеку. Хоча фінанси можуть бути обмеженими, важливо належним чином інвестувати в кібербезпеку, інакше інші інвестиції можуть бути під загрозою. Говорячи про безпеку, уникайте тактики залякування. Іноді загрози, з якими стикається ваш парламент та його співробітники, можуть видаватися страшними. Щоб розвіяти страх, зосередьтеся на обміні фактами та створенні спокійного простору для запитань та обговорення проблем. Якщо ви будете наголошувати на великій небезпеці, що видаватиметься надто загрозливою, люди можуть сприймати вас як любителя сенсацій або просто здадуться, вважаючи, що щоб вони не робили, це не має значення. Однак останнє твердження є дуже далеким від істини.

Створення навчального плану

Після того, як ви розробите план і візьмете на себе зобов'язання його виконувати, подумайте про те, як ви навчите всіх співробітників (і волонтерів) цим новим кращим практикам.

Вимоги до регулярних тренінгів і обов'язковість відвідування тренінгів можуть бути корисною тактикою. Не карайте суворо співробітників, яким складно дається розуміння концепцій безпеки. Майте на увазі, що деяким співробітником може бути складніше адаптуватися до технологій та опановувати їх, ніж іншим, залежно від різного рівня ознайомлення з цифровими інструментами й інтернетом. Страх перед невдачею ще більше позбавляє персонал мотивації повідомляти про проблеми чи просити про допомогу. Однак створення системи заохочення за повідомлення та винагородою за успішне навчання, а також прийняття відповідної політики, може стимулювати вдосконалення всієї організації. Отримайте цінну підтримку через місцеві або міжнародні навчальні мережі цифрової безпеки та безкоштовні навчальні ресурси, такі як застосунок Umbrella від Security First, Проєкт Totem від Free Press Unlimited і Greenhost, а також Навчальний портал від Global Cyber Alliance.

Подумайте, як ваш навчальний план може охопити депутатів, співробітників і адміністрацію парламенту. Майте на увазі, що відомі депутати часто вимагають ще більше навчання та уваги, коли йдеться про безпеку через їх високий авторитет. Переконайтеся, що ваш план навчання та план безпеки стосуються всіх цих різних типів осіб і будь-яких активів, які вони можуть мати як всередині, так і за межами парламенту.



Формування культури безпеки

- **Заплануйте регулярні бесіди та тренінги про безпеку та план безпеки.**
- **Залучіть усіх — розподіліть відповідальність за впровадження плану безпеки між всіма співробітниками організації.**
- **Переконайтеся, що керівництво демонструє належне дотримання безпеки та виконання плану безпеки.**
- **Уникайте тактики залякування або покарань — винагороджуйте за покращення та створіть зручне місце для співробітників, щоб повідомляти про проблеми та просити про допомогу.**
- **Оновлюйте свій план безпеки щороку або після серйозних змін у штаті, структурі чи робочому середовищі парламенту.**

Міцна основа: захист облікових записів і пристроїв

Чому важливо зосередитися на захисті облікових записів і пристроїв? Оскільки вони складають основу всього, що парламент робить цифровим способом.

Ви майже напевно отримуєте доступ до конфіденційної інформації, спілкуєтеся всередині та ззовні та зберігаєте в них особисту інформацію. Просто враховуйте участь депутатів у пленарних засіданнях, голосуванні (включаючи віртуальне), процесах розробки законопроектів та спілкуванні з співробітниками та громадськістю. Без захищених облікових записів і пристроїв ці найважливіші парламентські операції та інші можуть бути під загрозою.
Наприклад, якщо хакери відстежують ваші натискання клавіш або прослуховують ваш мікрофон, приватні розмови з колегами будуть зафіксовані незалежно від того, наскільки безпечні ваші програми обміну повідомленнями. Або, якщо зловмисник отримає доступ до облікових записів парламенту в соціальних мережах, він може легко завдати шкоди вашій репутації та довірі, підриваючи довіру громадськості. Тому вам, як організації, важливо переконатися, що всі співробітники вживають простих, але ефективних заходів для захисту своїх пристроїв і облікових записів. Важливо зазначити, що ці рекомендації також стосуються особистих облікових записів і пристроїв, оскільки вони часто є легкою мішенню для зловмисників. Хакери охоче виберуть найлегшу ціль і зламають особисті облікові записи чи домашні комп'ютери, якщо співробітники використовують їх для спілкування та доступу до важливої інформації.

Безпечні облікові записи та парламент

Широко розголошений злом SolarWinds, виявлений наприкінці 2020 року, від якого постраждали 250 організацій, у тому числі більшість міністерств Сполучених Штатів, постачальники технологій, як-от Microsoft і Cisco, а також неурядові організації, стався в результаті того, що **хакери вгадали слабкі паролі**, що використовувалися для важливих облікових записів адміністраторів. Загалом близько 80 відсотків усіх хакерських зломів відбуваються через слабкі або повторно використані паролі.

У зв'язку зі зростаючою поширеністю подібних зломів паролів і легшим доступом для всіх типів зловмисників до складних інструментів злому паролів, найкращі методи захисту паролів і двофакторна автентифікація є обов'язковими елементами безпеки для громадських організацій. Жоден інцидент не ілюструє це більш чітко, ніж **атака 2017 року** на систему електронної пошти британського парламенту. У цьому інциденті неправильне використання пароля невеликою, але значною кількістю депутатів призвело до розкриття облікових записів електронної пошти та розмов, витоку тисяч облікових даних і величезних збоїв у роботі парламенту. За **даними прес-служби британського парламенту**, зламані облікові записи були «скомпрометовані через слабкі паролі, які не відповідали вказівкам, виданим Парламентською цифровою службою».

Захищені облікові записи: паролі та двофакторна автентифікація

У сучасних умовах організація та її співробітники мають десятки, якщо не сотні облікових записів, які в разі зламу можуть розкрити конфіденційну інформацію або навіть піддати ризику їх власників.

Подумайте про різні облікові записи, які мають як окремі співробітники, так і організація в цілому: електронна пошта, програми для чату, соціальні мережі, онлайн-банкінг, хмарне сховище даних, а також магазини одягу, місцеві ресторани, газети та багато інших веб-сайтів або додатків, у яких ви реєструєтеся. Надійна безпека в сучасному світі вимагає ретельного підходу до захисту всіх цих облікових записів від атак. Це починається із забезпечення надійної гігієни пароля та використання двофакторної автентифікації всіма.

ЩО ТАКЕ НАДІЙНИЙ ПАРОЛЬ?

Сильний, надійній пароль має три характеристики: довжина, випадковість і унікальність.

ДОВЖИНА

Чим довший пароль, тим важче зловмиснику його вгадати. У більшості випадків злом паролів сьогодні виконується комп'ютерними програмами, і цим зловмисним програмам не потрібно багато часу, щоб зламати короткий пароль. Тому дуже важливо, щоб ваші паролі мали щонайменше 16 символів або принаймні п'ять слів, а краще — ще більше.

ВИПАДКОВІСТЬ

Навіть якщо пароль довгий, не дуже добре, якщо він містить дані, які зловмисник може легко вгадати про вас. Не вказуйте таку інформацію, як ваш день народження, рідне місто, улюблені заняття чи інші факти, які хтось може дізнатися про вас під час швидкого пошуку в інтернеті.

УНІКАЛЬНІСТЬ

Можливо, найбільш поширеною «найгіршою практикою» є використання одного пароля для кількох веб-сайтів. Повторення паролів є великою проблемою, оскільки це означає, що коли лише один із цих облікових записів зламано, всі інші облікові записи, в яких використовується той самий пароль, також стають уразливими. Якщо ви використовуєте одну і ту саму парольну фразу на кількох веб-сайтах, це може значно посилити наслідки однієї помилки або витоку даних. Хоча вас не турбує доля паролю для входу до місцевої бібліотеки, якщо його буде зламано, а ви використовуєте той самий пароль для більш конфіденційного облікового запису, важливу інформацію можуть викрасти.

Один із простих способів досягти бажаної довжини, випадковості та унікальності — це вибрати три-чотири звичайних, але випадкових слів. Наприклад, ваш пароль може бути «квіткова лампа зелений ведмідь», який легко запам'ятати, але важко вгадати. Ви можете зайти на **цей веб-сайт** від Better Buys, щоб дізнатися, наскільки швидко можна зламати слабкі паролі.

ВИКОРИСТОВУЙТЕ МЕНЕДЖЕР ПАРОЛІВ

Отже, ви знаєте, що кожному в парламенті важливо використовувати довгий, випадковий і різний пароль для кожного зі своїх особистих і парламентських облікових записів, але як це зробити? Запам'ятати надійні паролі для десятків (якщо не сотень) облікових записів неможливо, тому всім доводиться хитрувати. Неправильний спосіб робити це — повторно використовувати паролі. На щастя, ми можемо звернутися до менеджерів цифрових паролів, щоб зробити наше життя набагато простішим (а наші методи зберігання паролів набагато безпечнішими). Ці програми, доступні на комп'ютері або мобільному пристрої, можуть створювати, зберігати та керувати паролями для вас і всієї вашої організації. Застосування безпечного менеджера паролів означає, що вам доведеться запам'ятовувати лише один дуже надійний, довгий пароль, який називається основним паролем (або «головним паролем»). Завдяки цьому менеджеру ви скористаєтеся перевагами безпеки від використання надійних унікальних паролів для всіх ваших облікових записів. Ви використовуватимете цей основний пароль (і в ідеалі другий фактор автентифікації (2FA), що буде розглядатися в наступному розділі), щоб відкрити менеджер паролів і розблокувати доступ до всіх ваших інших паролів. Менеджери паролів також можна спільно використовувати для кількох облікових записів, щоб полегшити безпечний обмін паролями в усій організації.

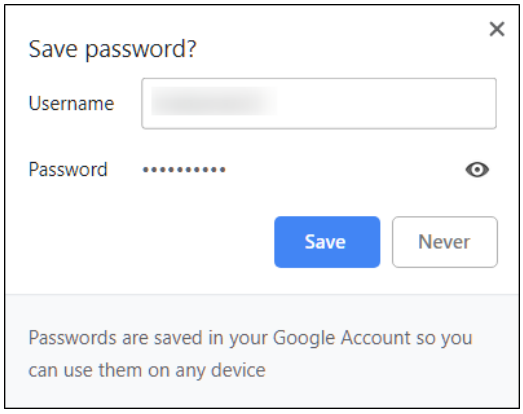
Чому нам потрібно використовувати щось нове? Чи можна просто записати їх на папері або в електронній таблиці на комп'ютері?

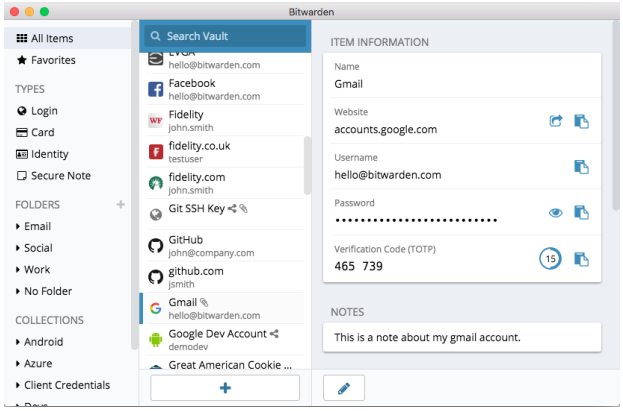
На жаль, існує багато поширених методів управління паролями, які не є безпечними. Зберігання паролів на аркушах паперу (якщо ви не зберігаєте їх під замком у сейфі) означає ризик фізичного викрадення, потрапляння на сторонні очі, легкої втрати чи пошкодження. Якщо ви зберігаєте паролі в документі на комп'ютері, хакерам буде набагато легше отримати доступ до них. А ті, хто викраде ваш комп'ютер, отримають не лише ваш пристрій, але й доступ до всіх ваших облікових записів. Користуватися хорошим менеджером паролів так само легко, як і цим документом, але набагато безпечніше.

Чому слід довіряти менеджеру паролів?

Якісні менеджери паролів докладають надзвичайних зусиль (і залучають чудові команди фахівців із питання безпеки) для забезпечення безпеки своїх систем. Надійні додатки для керування паролями (декілька з яких рекомендовані нижче) також налаштовані так, що вони не мають можливості «розблокувати» ваші облікові записи. Це означає, що в більшості випадків, навіть якщо їх зламали або законно примусили передати інформацію, вони не зможуть втратити або видати ваші паролі. Пам'ятайте, що набагато більш імовірним є те, що зловмисник вгадає один із ваших слабких або повторюваних паролів, або знайде його у **публічному витоку даних**, ніж те, що системи безпеки надійного менеджеру паролів буде зламано. Здоровий скепсис є важливим: не слід сліпо довіряти всьому програмному забезпеченню та всім програмам, але визнані менеджери паролів мають усе необхідне для ефективної роботи.

Замість використання вебоглядача (як-от, Chrome, показаний ліворуч) для збереження паролів, використовуйте спеціальний менеджер паролів (як-от, Bitwarden, показаний праворуч). Менеджери паролів мають функції, що роблять діяльність вашої організації безпечнішим і зручнішим.





Як щодо збереження паролів у вебоглядачі?

Зберігання паролів у вебоглядачі — це не те саме, що використання безпечного менеджера паролів. Простіше кажучи, не слід використовувати Chrome, Firefox, Safari чи будь-який інший вебоглядачі як менеджер паролів. Незважаючи на те, що це, безумовно, краще, ніж записувати їх на папері чи зберігати в електронній таблиці, основні функції збереження паролів вашого вебоглядачі недосконалі з точки зору безпеки. Ці недоліки також позбавляють вас зручності, яку надає надійний менеджер паролів. Втрата цієї зручності збільшує ймовірність того, що люди в парламенті продовжуватимуть погано створювати паролі та обмінюватися ними.

Наприклад, на відміну від спеціалізованих менеджерів паролів, вбудовані в браузери функції «зберегти цей пароль» або «запам'ятати цей пароль» не забезпечують простої сумісності з мобільними пристроями, використання в інших вебоглядачах та не надають інструментів для створення і перевірки надійних паролів. Ці функції є у значній мірі тим, що робить спеціалізований менеджер паролів таким корисним і вигідним для безпеки організації. Менеджери паролів також включають специфічні для парламенту функції (наприклад, спільний доступ до паролів), які забезпечують не лише індивідуальну безпеку, але й приносять користь для організації в цілому. Якщо ви зберігали паролі у своєму вебоглядачі (навмисно чи ненавмисно), видаліть їх.

Який менеджер паролів слід використовувати?

Існує багато надійних інструментів керування паролями, які можна налаштувати менш ніж за 30 хвилин. Якщо ви шукаєте надійний онлайн-варіант для своєї організації, до якого люди можуть отримати доступ із кількох пристроїв у будь-який час, 1Password (від 2,99 дол. США за користувача на місяць) або безкоштовний із відкритим кодом Bitwarden мають належну технічну підтримку та хороші відгуки. Варіант онлайн, як-от Bitwarden, може бути чудовим вибором з огляду як на безпеку, так і на зручність. Bitwarden, наприклад, допоможе вам створити надійні унікальні паролі й отримати доступ до паролів із кількох пристроїв за допомогою розширень браузера та мобільного додатку.

У платній версії (10 дол. США на рік) Bitwarden також надає звіти про повторно використані, слабкі та, можливо, зламані паролі, щоб тримати вас у курсі. Після встановлення основного пароля (який називають головним паролем) також слід увімкнути двофакторну автентифікацію, щоб зробити сховище менеджера паролів якомога безпечнішим.

Важливо дотримуватися надійних методів безпеки під час використання менеджера паролів. Наприклад, якщо ви використовуєте розширення вебоглядача менеджера паролів або заходите до Bitwarden (або будь-якого іншого менеджеру паролів) на пристрої, не забудьте вийти з системи після закінчення роботи, якщо користуєтеся цим пристроєм спільно з кимось або вважаєте, що може бути підвищений ризик фізичного викрадення пристрою. Не забудьте також вийти з менеджера паролів, якщо залишаєте комп'ютер або мобільний пристрій без нагляду. Якщо ви ділитеся паролями між відділами чи в парламенті загалом, не забудьте відкликати доступ до паролів (і змінити самі паролі), коли люди залишають. Наприклад, ви не хочете, щоб колишній співробітник мав доступ до пароля вашого парламенту у Facebook.

Що робити, якщо хтось забув основний пароль?

Важливо пам'ятати основний пароль. Надійні системи керування паролями, подібні до рекомендованих вище, не зберігають основний пароль і не дозволяють скинути його безпосередньо електронною поштою, як це можливо для веб-сайтів. Це надійна функція безпеки, але важливо запам'ятати основний пароль під час першого налаштування менеджера паролів. Щоб допомогти з цим, налаштуйте щоденне нагадування основного пароля під час першого створення облікового запису менеджера паролів.

Використання менеджера паролів в парламенті

Ви можете покращити використання паролів у всій організації та забезпечити всім співробітникам доступ до менеджера паролів і його використання, запровадивши його для всієї організації. Замість того, щоб кожен окремий співробітник створював власний план, розгляньте доцільність інвестування в «командний» або «бізнес-план». Наприклад, план «команд організації» від Bitwarden коштує 3 дол. США на користувача на місяць. З ним (або іншими командними планами від менеджерів паролів, таких як «1Password»), ви маєте можливість керувати всіма спільно використовуваними паролями в організації. Функції парламентського або загальнокомандного менеджера паролів не тільки забезпечують більший захист, але й зручність для співробітників. Ви можете безпечно ділитися обліковими даними в самому менеджері паролів з різними обліковими записами користувачів. Bitwarden, наприклад, також надає зручну функцію наскрізного шифрування обміну текстовими повідомленнями та файлами під назвою «Bitwarden Send» у своєму командному плані. Обидві ці функції надають організації контроль над тим, хто може переглядати паролі та ділитися ними, а також забезпечують більш безпечний варіант для спільного використання облікових даних для облікових записів усієї команди чи групи. Якщо ви налаштували менеджер паролів для всієї організації, призначте особу, яка буде відповідати за видалення облікових записів співробітників і зміну паролів, що спільно використовуються, після звільнення співробітників.

ЩО ТАКЕ ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ?

Яким би надійним не був захист паролів, хакери надто часто обходять паролі. Щоб захистити ваші облікові записи від деяких типових існуючих загроз, потрібен інший рівень захисту. Ось тут і вступає в гру багатофакторна або двофакторна автентифікація, що називається MFA або 2FA.

Існує багато чудових посібників і ресурсів, в яких пояснюється двофакторна автентифікація, зокрема стаття Martin Shelton **Двофакторна автентифікація для початківців** і **Польовий посібник із виборчої кібербезпеки 101** від Center for Democracy &Technology. У цьому розділі наведено багато інформації з цих обох ресурсів, щоб пояснити, чому так важливо запровадити 2FA у парламенті.

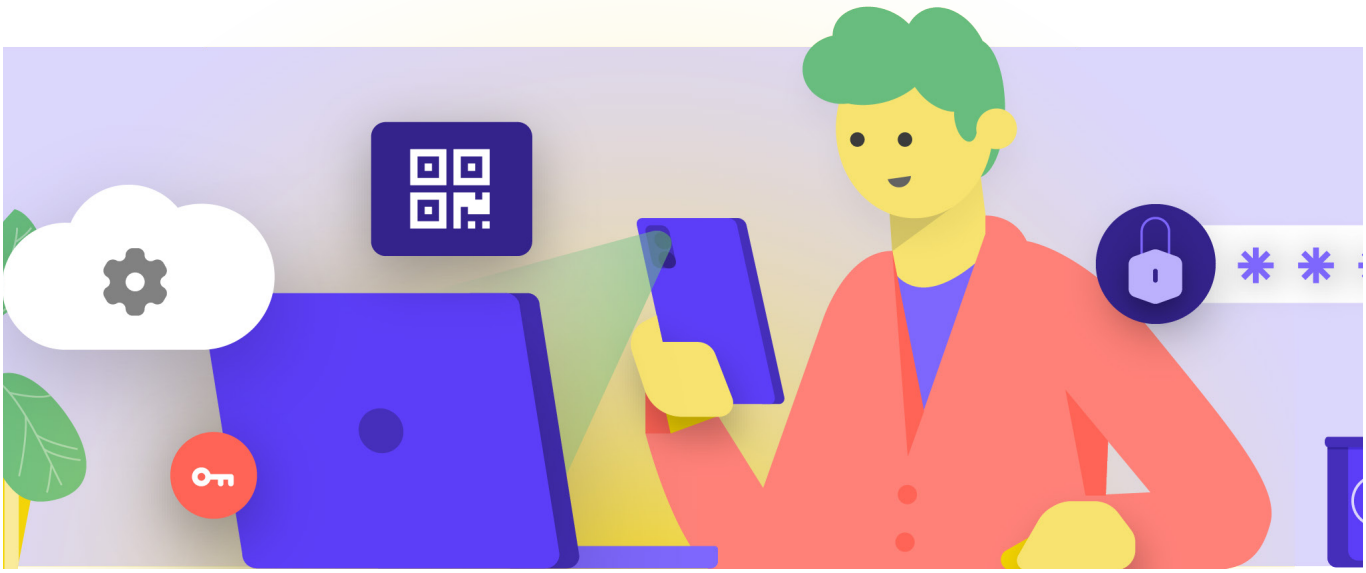
Коротко кажучи, 2FA зміцнює безпеку облікового запису, вимагаючи другу частину інформації — щось більше, ніж просто пароль, — для отримання доступу. Друга частина інформації — це зазвичай щось, що у вас є, як-от код із програми на вашому телефоні, фізичний токен або ключ. Ця друга частина інформації діє як другий рівень захисту. Якщо хакер викраде пароль або отримає доступ до нього через перелік паролів у результаті великого витоку даних, ефективний метод 2FA може запобігти його доступу до вашого облікового запису (і таким чином, захистить приватну та конфіденційну інформацію). Забезпечення того, щоб кожен у парламенті впровадив 2FA у своїх облікових записах, є надзвичайно важливим.

ЯК МИ МОЖЕМО НАЛАШТУВАТИ 2FA?

Є три поширені методи 2FA: ключі безпеки, програми автентифікації та одноразові SMS-коди.

Ключі безпеки

Ключі безпеки — найкращий варіант, частково тому, що вони майже повністю захищені від фішингу. Ці «ключі» є апаратними токенами (наприклад, міні-USB-накопичувачі), які можна приєднати до брелоку (або залишити у вашому комп'ютері) для легкого доступу та безпечного зберігання. Коли прийде час використати ключ для розблокування даного облікового запису, ви просто вставите його у пристрій і торкнетеся його, коли з'явиться запит під час входу. Існує широкий асортимент моделей, які можна придбати в інтернеті (20–50 дол. США), у тому числі вельми рекомендовані **YubiKeys**. Wirecutter від The New York Times має **корисний посібник** із деякими рекомендаціями, які ключі слід купувати. Майте на увазі, що один і той самий ключ безпеки можна використовувати для будь-якої кількості облікових записів.



Програми автентифікації

Другим найкращим варіантом 2FA є програми автентифікації. Ці служби дозволяють отримати тимчасовий двофакторний код входу через мобільний додаток або push-повідомлення на смартфоні. Деякі популярні та надійні варіанти включають Google Authenticator, Authy та Duo Mobile. Додатки Authenticator також чудові, тому що вони працюють, коли у вас немає доступу до стільникової мережі, і безкоштовні для використання фізичними особами. Однак програми автентифікації більш уразливі для фішингу, ніж ключі безпеки, оскільки користувачів можна обманом змусити ввести коди безпеки з програми автентифікації на підробленому веб-сайті. Вводіть коди входу лише на дійсних веб-сайтах. Не «приймайте» push-сповіщення про вхід, якщо не впевнені, що це ви зробили запит про вхід. У разі використання програми автентифікації також важливо підготувати резервні коди (розглянуті нижче) на випадок втрати або викрадення телефону.

Коди через SMS

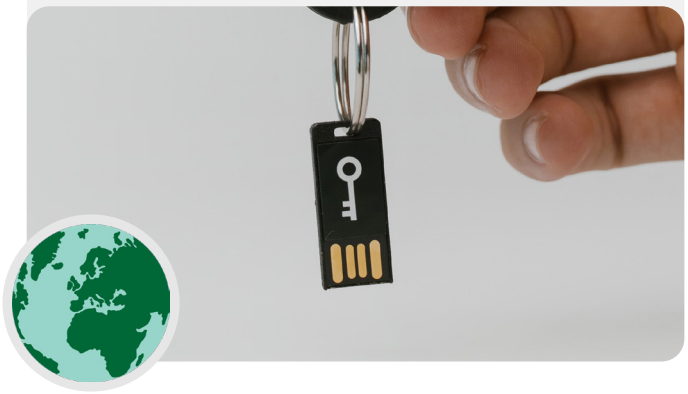
Найменш безпечною, але, на жаль, все ще найпоширенішою формою 2FA є коди, надіслані через SMS. Оскільки SMS можна перехопити, а номери телефонів можна підробити або зламати через оператора мобільного зв'язку, SMS є ненадійним методом запиту кодів 2FA. Це краще, ніж використовувати лише пароль, але за можливості, рекомендується використовувати програми автентифікації або фізичний ключ безпеки. Рішуче налаштований зловмисник може отримати доступ до SMS-кодів 2FA, зазвичай просто **зателефонувавши в телефонну компанію** і замінивши вашу SIM-картку. Коли ви будете готові почати вмикати 2FA для облікових записів вашої організації, скористайтеся цим веб-сайтом (**https://2fa.directory/**), щоб швидко знайти інформацію та інструкції для певних служб (наприклад, Gmail, Office 365, Facebook, Twitter тощо), а також побачити, які служби підтримують які типи 2FA.

2FA та парламент

Згідно з повідомленнями, у 2020 році **хакери проникли в систему електронної пошти парламенту Норвегії,** скомпрометувавши облікові записи електронної пошти, що належать кільком посадовим особам парламенту, і навіть завантаживши деяку інформацію з парламентських систем. Хоча повні подробиці злому не були оприлюднені, Норвегія приписала вторгнення APT28, хакерській групі, пов'язаній з російськими службами безпеки. Незважаючи на те, що APT28 та інші хакери дуже складні, вони часто використовують менш складні тактики, такі як «атаки грубою силою» (де зловмисник використовує інструменти, щоб спробувати багато паролів з надією врешті-решт вгадати правильний), щоб отримати доступ до облікового запису. Ця тактика дозволяє хакерам вгадувати навіть надійні паролі, як вважалося в Норвегії. Хороші новини? Ці типи атак мають набагато меншу ймовірність успіху з належним ключем або двофакторною автентифікацією на основі програми!

Ключі безпеки в реальному світі

Надавши фізичні ключі безпеки для двофакторної автентифікації всім своїм 85 000 співробітникам, Google (організація з високим ризиком) **ефективно усунула можливість фішингової атаки** на організацію. Цей випадок показує, наскільки ефективними можуть бути ключі безпеки навіть для організацій із найбільшим ризиком.



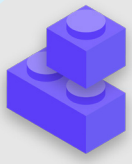
ЩО РОБИТИ В РАЗІ ВТРАТИ ПРИСТРОЮ 2FA?

Якщо ви використовуєте ключ безпеки, поводьтеся з ним так само, як і з ключем від будинку чи квартири, якщо він у вас є. Одним словом, не губіть його. Так само, як і для ключа від будинку, завжди варто мати резервний ключ, зареєстрований у вашому обліковому записі, що зберігається у надійному місці під замком (наприклад, у домашньому сейфі) на випадок втрати чи крадіжки. Крім того, ви повинні створити резервні коди для облікових записів, які це дозволяють. Зберігайте ці коди в надійному місці, наприклад у менеджері паролів або фізичному сейфі. Такі резервні коди можна згенерувати в налаштуваннях 2FA більшості веб-сайтів (там, де ви спочатку вмикаєте 2FA), і вони можуть діяти як резервний ключ у разі надзвичайної ситуації. Найпоширеніша помилка 2FA виникає, коли люди замінюють або втрачають телефони, які вони використовують для програм автентифікації. Якщо ви використовуєте Google Authenticator, вам не пощастить у разі крадіжки телефону, якщо тільки ви не збережете резервні коди, що генеруються під час підключення облікового запису до Google Authenticator. Тому, якщо ви використовуєте Google Authenticator як програму 2FA, обов'язково зберігайте резервні коди для всіх облікових записів, які ви підключаєте, у безпечному місці. Якщо ви використовуєте Authy або Duo, обидві програми мають вбудовані функції резервного копіювання з надійними налаштуваннями безпеки, які ви можете ввімкнути. Якщо ви виберете одну з цих програм, ви зможете налаштувати параметри резервного копіювання на випадок поломки, втрати або крадіжки пристрою. Перегляньте інструкції Authy **тут** і Duo **тут**. Переконайтеся, що всі знають про ці кроки, коли вони починають вмикати 2FA для всіх своїх облікових записів.

Застосування 2FA у всьому парламенті

Якщо ваша організація надає облікові записи електронної пошти всім співробітникам через Google Workspace (раніше відомий як GSuite) або Microsoft 365, використовуючи власний домен (наприклад, @ndi.org), ви можете застосувати 2FA та надійні налаштування безпеки для всіх облікових записів. Такий контроль не тільки допомагає захистити ці облікові записи, але також діє як спосіб представити та призвичаїти депутатів і співробітників до 2FA, щоб їм було зручніше застосовувати її для особистих облікових записів. Як адміністратор Google Workspace ви можете слідувати **цим інструкціям**, щоб застосувати 2FA для вашого домену. Ви можете зробити **ці кроки** в Microsoft 365 як адміністратор домену.

Також подумайте про реєстрацію облікових записів вашої організації в **Програмі додаткового захисту** (Google) або **AccountGuard** (Microsoft), щоб застосувати додаткові заходи безпеки та ввести фізичні ключі безпеки для двофакторної автентифікації.



Захищені облікові записи:

- **Вимагати надійних паролів для всіх парламентських облікових записів; заохочуйте те саме для особистих облікових записів депутатів, співробітників і волонтерів.**
- **Впровадити довірений менеджер паролів для парламенту (а також заохочувати використання в особистому житті співробітників).**
  - Вимагайте надійний основний пароль і 2FA для всіх облікових записів менеджера паролів.
  - Нагадайте всім вийти з менеджера паролів на спільних пристроях або в разі підвищеного ризику викрадення чи конфіскації пристроїв.
- **Змінюйте спільні паролі, коли співробітники та депутати залишають парламент.**
- **Надсилайте паролі лише безпечно, наприклад, через менеджер паролів вашого парламенту або програми з наскрізним шифруванням.**
- **Вимагайте 2FA для всіх облікових записів парламенту та заохочуйте співробітників також налаштувати 2FA для всіх особистих облікових записів.**
  - Якщо можливо, надайте фізичні ключі безпеки всім депутатам і співробітникам.
  - Якщо бюджет не покриває ключі безпеки, заохочуйте використовувати програми автентифікації замість SMS або телефонних дзвінків для 2FA.
- **Проводьте регулярні тренінги, щоб переконатися, що співробітники ознайомлені з найкращими методами роботи з паролями та 2FA, зокрема про важливість надійних паролів і важливість ніколи не використовувати паролі повторно, приймати лише справжні запити 2FA та генерувати резервні коди 2FA.**

Захищені пристрої

Окрім облікових записів, важливо надійно захищати всі пристрої — комп'ютери, телефони, USB, зовнішні жорсткі диски тощо.

Такий захист починається з обережності щодо того, які типи пристроїв купує та використовує парламент і співробітники. Постачальники або виробники, яких ви виберете, повинні мати докази дотримання світових стандартів щодо безпечного розроблення апаратних пристроїв (наприклад, телефонів і комп'ютерів). Пристрої, які ви купуєте, мають бути виготовлені надійними компаніями, які не мають стимулів передавати дані та інформацію потенційному зловмиснику. Важливо зазначити, що уряд Китаю вимагає від китайських компаній надавати дані центральному уряду. Тому, незважаючи на широкопоширені та недорогі смартфони, такі як Huawei або ZTE, їх слід уникати. Незважаючи на те, що вартість дешевого апаратного забезпечення може бути дуже привабливою, потенційні ризики для безпеки для парламентів мають спрямувати вас до інших варіантів пристроїв і обладнання.

Зловмисники можуть поставити під загрозу безпеку ваших пристроїв — і все, що ви робите на цих пристроях — шляхом отримання фізичного або «віддаленого» доступу до пристроїв.

Безпека пристрою та парламент

Деякі з найдосконаліших у світі зловмисних програм були розроблені та розгорнуті по всьому світу для **націлювання** на депутатів, інших урядовців та їхніх співробітників. В Індії, наприклад, консорціум журналістів **виявив**, що кілька депутатів парламенту та міністрів уряду були мішенню шпигунського програмного забезпечення Pegasus, типу шкідливого програмного забезпечення, яке потрапило в заголовки газет у 2020 році. Pegasus сумно відомий своєю здатністю заражати мобільні пристрої та давати зловмиснику можливість записувати аудіо, перехоплювати натискання клавіш і повідомлення, і фактично поставити жертву під повне спостереження. не вимагаючи взаємодії жертви. Однак переважній більшості шпигунських програм вдається скомпрометувати своїх жертв.

ФІЗИЧНИЙ ДОСТУП ДО ПРИСТРОЮ ЧЕРЕЗ ВТРАТУ АБО КРАДІЖКУ

Щоб запобігти фізичному доступу, важливо забезпечити фізичну безпеку своїх пристроїв. Не дозволяйте зловмисникам вкрасти чи навіть тимчасово відібрати у вас ваш пристрій. Тримайте пристрої під замком, якщо залишаєте їх удома чи в офісі. Або, якщо ви вважаєте, що це безпечніше, тримайте їх при собі. Звісно, це означає, що частиною безпеки пристрою є фізична безпека ваших робочих місць (в офісі чи вдома). Вам потрібно буде встановити надійні замки, камери спостереження або інші системи моніторингу. Нагадайте співробітникам поводитися з пристроями так само, як вони поводилися б із великою пачкою готівки — не залишайте їх лежати без нагляду чи без захисту.

Що робити, якщо пристрій вкрадуть?

Щоб зменшити шкоду, якщо комусь таки вдасться вкрасти пристрій, — або навіть якщо зловмисник отримає до нього доступ на короткий проміжок часу, — **зобов'яжіть співробітників використовувати надійні паролі або коди доступу на всіх комп'ютерах і телефонах**. Поради щодо паролів із розділу «Паролі» цього Довідника стосуються надійних паролів для комп'ютера чи ноутбука. Коли справа доходить до блокування телефону, використовуйте коди, що містять принаймні шість-вісім цифр. Уникайте використання «шаблонів» при розблокуванні телефону. Додаткові поради щодо блокування екрана містяться у Data Detox Kit від Tactical Tech. Використання надійних паролів на пристрої значно ускладнює зловмисникам можливість отримати швидкий доступ до інформації на ньому в разі крадіжки чи конфіскації. Переконайтеся, що всі пристрої, видані парламентом, також зареєстровані в **системі керування мобільними пристроями чи кінцевими точками**. Незважаючи на те, що ці системи недешеві, вони дозволяють вашому парламенту застосовувати політику безпеки на всіх пристроях, знаходити один із них і видаляти його вміст у разі його викрадення, втрати чи конфіскації. Хоча існує багато різних рішень для керування мобільними пристроями, кілька надійних варіантів, які працюють на різних платформах (iPhone, Android, Mac і Windows), включають Hexnode, Meraki Systems Manager від Cisco, MDM від IBM і вбудовану функцію керування мобільними пристроями Google Workspace. Якщо вартість є стримуючим фактором, принаймні заохочуйте депутатів і співробітників використовувати вбудовані функції «Знайти мій пристрій» на їхніх парламентських і особистих смартфонах, таких як «Знайти мій iPhone» для iPhone і «Знайти мій пристрій» для Android.

Як щодо шифрування пристрою?

Важливо використовувати шифрування або засекречування даних, щоб вони були нечитабельними та непридатними для використання на всіх пристроях, особливо на комп'ютерах і смартфонах. Якщо це можливо, вам слід налаштувати на всіх пристроях у парламенті щось, що називається **повним дисковим шифруванням**. Повнодискове шифрування означає, що весь пристрій буде зашифровано таким чином, що зловмисник, якщо він його фізично вкраде, не зможе отримати вміст пристрою, не знаючи пароля чи ключа, який ви використали для шифрування. Багато сучасних смартфонів і комп'ютерів пропонують функцію повнодискового шифрування. На пристроях Apple, як-от iPhone та iPad, досить зручно вмикати повнодискове шифрування, коли ви встановлюєте звичайний пароль пристрою. Комп'ютери Apple із macOS мають функцію FileVault, яку можна ввімкнути для повнодискового шифрування. На комп'ютерах із ОС Windows із ліцензіями Pro, Enterprise або Education пропонується функція BitLocker, яку можна ввімкнути для повнодискового шифрування. Ви можете ввімкнути BitLocker, виконавши ці інструкції від корпорації Microsoft, дозвіл на що, можливо, має спочатку надати адміністратор вашої організації. Якщо персонал має лише домашню ліцензію для своїх комп'ютерів на Windows, BitLocker буде недоступний. Однак співробітники все одно можуть увімкнути повнодискове шифрування, перейшовши на вкладку «Оновлення та безпека > Шифрування пристрою» в налаштуваннях ОС Windows.

Пристрої Android, починаючи з версії 9.0, постачаються з шифруванням на основі файлів, увімкненим за замовчуванням. Шифрування Android на основі файлів працює інакше, ніж повнодискове шифрування, але все одно забезпечує надійний захист. Якщо ви користуєтеся відносно новим телефоном Android і встановили пароль, слід увімкнути шифрування на основі файлів. Однак радимо перевірити налаштування, особливо якщо вашому телефону вже кілька років. Щоб перевірити, перейдіть до вкладки Налаштування > Безпека на вашому пристрої Android. У налаштуваннях безпеки ви побачите підрозділ «шифрування» або «шифрування та облікові дані», у якому вказується, чи зашифровано ваш телефон, і, якщо ні, ви зможете ввімкнути шифрування.

Для комп'ютерів (на Windows або Mac) особливо важливо зберігати будь-які ключі шифрування (так звані ключі відновлення) у безпечному місці. Ці «ключі відновлення» в більшості випадків являють собою довгі паролі або парольні фрази. Якщо ви забудете звичайний пароль пристрою або трапиться щось несподіване (наприклад, збій пристрою), ключі відновлення є єдиним способом відновити зашифровані дані та, якщо необхідно, перемістити їх на новий пристрій. Тому, вмикаючи повнодискове шифрування, обов'язково збережіть ці ключі або паролі в безпечному місці, наприклад у захищеному хмарному обліковому записі або в менеджері паролів вашої організації.

ВІДДАЛЕНИЙ ДОСТУП ДО ПРИСТРОЮ — ТАКОЖ ВІДОМИЙ ЯК ЗЛОМ

Окрім фізичної безпеки пристроїв, важливо захистити їх від шкідливих програм. У довіднику Security-in-a-Box від Tactical Tech наведено корисний опис того, що таке шкідливі програми та чому важливо їх уникати.Цей опис наведено в адаптованій формі далі в цьому розділі.

Розуміння та уникнення шкідливих програм

Існує багато способів класифікації шкідливих програм (цей термін означає «шкідливе програмне забезпечення»). Віруси, шпигунські програми, хробаки, трояни, руткіти, програми-вимагачі та криптоджекери — це все типи шкідливих програм. Деякі види шкідливих програм поширюються в інтернеті через електронну пошту, текстові повідомлення, шкідливі веб-сторінки та іншими способами. Деякі поширюються через такі пристрої, як USB-накопичувачі, що використовуються для обміну даними та крадіжки даних. Тоді як для деяких шкідливих програм треба, щоб людина, яка не підозрює нічого поганого, зробила помилку, інші можуть мовчки заражати вразливі системи без відома жертви.

Окрім загальних шкідливих програм, які широко розповсюджуються та націленеіна широку громадськість, цільові шкідливі програми зазвичай використовується для втручання у справи або шпигування за певною особою, організацією чи мережею. Ці методи використовують як звичайні злочинці, так і військові та розвідувальні служби, терористи, онлайн-переслідувачі, жорстокі партнери та тіньові політичні діячі.

Як би вони не називалися, як би вони не поширювалися, зловмисне програмне забезпечення може псувати комп'ютери, викрадати та знищувати дані, порушувати роботу парламенту, порушувати конфіденційність і наражати користувачів на небезпеку. Одним словом, шкідливі програми дійсно небезпечні. Однак є кілька простих кроків, які ваш парламент може зробити, щоб захистити себе від цієї загальної загрози.

Чи захистить нас інструмент захисту від шкідливих програм?

Інструменти захисту від шкідливих програм, на жаль, не є комплексним рішенням. Однак дуже хорошою ідеєю є використання деяких базових безкоштовних інструментів як основи. Шкідливі програми змінюються настільки швидко, а нові ризики в реальному світі виникають так часто, що покладатися на будь-який такий інструмент не має бути єдиним захистом.

Якщо ви використовуєте Windows, розгляньте можливість використання вбудованої програми Windows Defender.

Комп'ютери Mac і Linux не мають вбудованого програмного забезпечення для захисту від шкідливих програм, як і пристрої на Android і iOS. Ви можете встановити надійний безкоштовний інструмент, наприклад Bitdefender або Malwarebytes для цих пристроїв (а також для комп'ютерів на Windows). **Але не покладайтеся на цей інструмент як на єдину лінію захисту**, оскільки він точно пропустить деякі з найбільш цілеспрямованих, небезпечних нових атак.

Крім того, будьте дуже обережні, завантажуйте лише надійні засоби захисту від шкідливих програм та антивірусні засоби із законних джерел (наприклад, веб-сайтів, наведених вище). На жаль, існує багато підроблених або дефектних версій інструментів захисту від шкідливих програм, що приносять набагато більше шкоди, ніж користі.

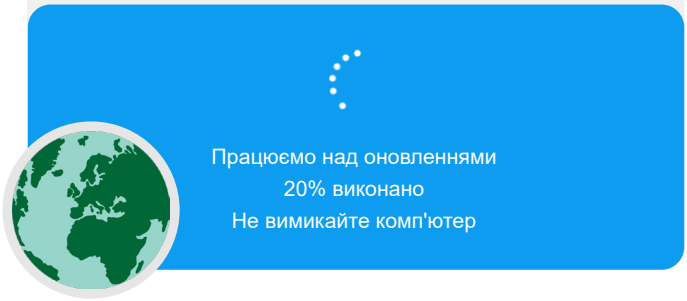
Якщо ви використовуєте Bitdefender або інший інструмент захисту від шкідливих програм у вашій організації, переконайтеся, що не запускаєте два інструменти одночасно. Багато з них визнають поведінку іншого підозрілою та зупинять його роботу, через що обидва працюють неправильно. Bitdefender або інші визнані засоби захисту від шкідливих програм можна оновлювати безкоштовно, а вбудований Windows Defender оновлюється разом із вашим комп'ютером. Переконайтеся, що ваше програмне забезпечення для захисту від шкідливих програм регулярно оновлюється (деякі пробні версії комерційного програмного забезпечення, що постачається з комп'ютером, буде вимкнено після закінчення пробного періоду, що робить їх швидше небезпечними, ніж корисними). Нові шкідливі програми створюється та розповсюджується щодня, і ваш комп'ютер швидко стане ще вразливішим, якщо ви не будете встигати за новими версіями шкідливих програм та методами захисту від них. За можливості налаштуйте програмне забезпечення на автоматичне встановлення оновлень. Якщо ваш інструмент захисту від шкідливих програм має додаткову функцію «завжди ввімкнено», увімкніть її та час від часу скануйте всі файли на вашому комп'ютері.

Тримайте пристрої в актуальному стані

Оновлення вкрай необхідні Використовуйте останню версію будь-якої операційної системи, що працює на пристрої (Windows, Mac, Android, iOS тощо), й оновлюйте цю операційну систему регулярно. Також оновлюйте інше програмне забезпечення, вебоглядач і його плагіни. Встановлюйте оновлення, як тільки вони стануть доступними, в ідеалі шляхом увімкнення автоматичного оновлення. Чим новіша операційна система пристрою, тим менше у вас уразливостей. Уявіть собі, що оновлення — це накладення пластиру на відкритий поріз: він закриває вразливість і значно зменшує ймовірність того, що ви заразитеся. Також видаліть програмне забезпечення, яким ви більше не користуєтеся. Застаріле програмне забезпечення часто має проблеми з безпекою, і, можливо, ви встановили інструмент, який більше не оновлюється розробником, що робить його вразливим для хакерів.

Шкідливі програми в реальному світі: Оновлення вкрай необхідні

У 2017 році атаки програми-вимагача WannaCry заразили мільйони пристроїв по всьому світу, що призвело до закриття лікарень, державних установ, великих і малих організацій і підприємств в десятках країн. Чому атаки була настільки ефективними? Через застарілі, несправні операційні системи Windows, багато з яких були піратськими. Значної частини шкоди — для людей і фінансів — можна було б уникнути за допомогою кращих методів автоматизованого оновлення та використання законних операційних систем.



Будьте обережні з USB-накопичувачами

Будьте обережні, відкриваючи файли, надіслані вам як вкладення, через посилання для завантаження чи будь-яким іншим способом. Також **подумайте двічі, перш ніж вставляти знімні носії, наприклад USB-накопичувачі**, карти флеш-пам'яті, DVD-диски та компакт-диски у комп'ютер, оскільки вони можуть бути переносниками шкідливих програм. Дуже ймовірно, що на USB-накопичувачах, які використовувалися протягом деякого часу, є віруси. Щоб дізнатися про альтернативні варіанти безпечного обміну файлами у вашій організації, ознайомтеся з розділом «Обмін файлами» Довідника.

Також будьте обережні щодо інших пристроїв, до яких ви підключаєтеся через Bluetooth. Можна синхронізувати телефон або комп'ютер із відомим і надійним Bluetooth-динаміком, щоб відтворювати улюблену музику, але будьте обережні, якщо підключаєтесь до будь-яких пристроїв, яких ви не впізнаєте, або приймайте запити від них. Дозволяйте підключення лише до надійних пристроїв і не забудьте вимкнути Bluetooth, коли він не використовується.

Будьте обережні під час перегляду сторінок в інтернеті

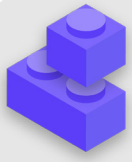
Ніколи не приймайте та не запускайте програми, що надходять із веб-сайтів, яких ви не знаєте та яким не довіряєте. Замість того, щоб приймати «оновлення», яке пропонується, наприклад, у спливаючому вікні вебоглядача, перевірте наявність оновлень на офіційному веб-сайті відповідної програми. Як обговорювалося в розділі «Фішинг» Довідника, важливо бути уважним під час перегляду веб-сайтів. Перевірте, куди веде посилання (навівши на нього курсор), перш ніж клацнути, подивіться на адресу веб-сайту після переходу за посиланням і переконайтеся, що він виглядає належним чином, перш ніж вводити конфіденційну інформацію, як-от свій пароль. Не клацайте повідомлення про помилки чи попередження, стежте за вікнами вебоглядача, що з'являються автоматично, й уважно їх читайте, а не просто клацайте «Так» або «ОК».

Шкідливі програми в реальному світі: Шкідливі мобільні додатки

Хакери в багатьох країнах роками використовують підроблені додатки в магазині Google Play для розповсюдження шкідливих програм. Про один конкретний випадок, націлений на користувачів у В'єтнамі, стало відомо у квітні 2020 року. У цій шпигунській кампанії використовувалися підроблені додатки, які нібито допомагали користувачам знаходити сусідні паби або шукати інформацію про місцеві церкви. Після встановлення користувачами Android, які нічого про це не підозрювали, шкідливі програми збирали журнали викликів, дані про місцезнаходження й інформацію про контакти та текстові повідомлення. Це лише одна з багатьох причин бути обережними щодо додатків, які ви завантажуєте на свої пристрої.

А як щодо смартфонів?

Як і у випадку з комп'ютерами, оновлюйте операційну систему й додатки телефону та ввімкніть автоматичне оновлення. Встановлюйте додатки лише з офіційних чи надійних джерел, як-от Google Play Store і Apple App Store (або F-droid, безкоштовний магазин додатків із відкритим кодом для Android). Додатки можуть мати вбудовані шкідливі програми і разом із тим працювати на вигляд нормально, тому ви не завжди дізнаєтеся, чи є додаток шкідливим. Також переконайтеся, що ви завантажуєте законну версію додатку. Особливо на Android існують «фальшиві» версії популярних додатків. Тому переконайтеся, що програма створена відповідною компанією чи розробником, має хороші відгуки й очікувану кількість завантажень (наприклад, підроблена версія WhatsApp може мати лише кілька тисяч завантажень, але справжня версія має понад п'ять мільярдів). Зверніть увагу на дозволи, які запитують додатки. Якщо вони здаються надмірними (наприклад, калькулятору потрібен доступ до вашої камери або Angry Birds запитує доступ до вашого місцезнаходження), відхиліть запит або видаліть додаток. Видалення додатків, якими ви більше не користуєтеся, також може допомогти захистити ваш смартфон або планшет. Розробники іноді продають право власності на свої додатки іншим людям. Ці нові власники можуть спробувати заробити гроші, додавши шкідливий код.



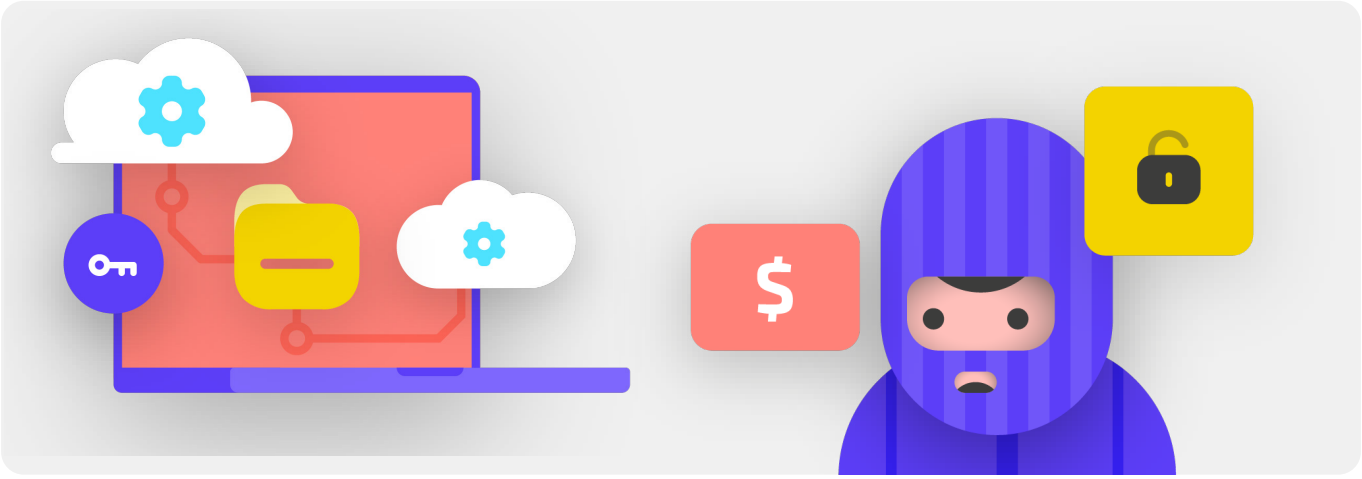
Захист пристроїв

- **Навчіть депутатів і співробітників ризикам зловмисного програмного забезпечення та найкращим методам їх уникнення.**
  - Запровадьте політику безпеки щодо підключення зовнішніх пристроїв, натискання посилань, завантаження файлів і додатків, а також перевірки програмного забезпечення та дозволів для додатків.
- **Зобов'яжіть співробітників регулярно оновлювати пристрої, програмне забезпечення та програми.**
  - Увімкніть автоматичне оновлення, за можливості.
- **Зареєструйте всі парламентські пристрої в системі керування мобільними пристроями або кінцевими точками.**
- **Переконайтеся, що всі пристрої використовують ліцензійне програмне забезпечення.**
- **Вимагати захисту паролем усіх парламентських пристроїв, у тому числі персональних мобільних пристроїв, які використовуються для зв'язку, пов'язаного з парламентом.**
- **Увімкніть шифрування всього диску на пристроях.**
- **Часто нагадуйте співробітникам, щоб їхні пристрої були фізично захищені, — і забезпечте захист офісу за допомогою відповідних замків і способів захисту комп'ютерів.**
- **Не передавайте файли за допомогою USB-накопичувачів і не підключайте USB-накопичувачі до своїх комп'ютерів.**
  - Натомість використовуйте альтернативні безпечні варіанти обміну файлами.

Фішинг: поширена загроза для пристроїв та облікових записів

Фішинг — найпоширеніша та найефективніша атака на організації, включно з парламентами, у всьому світі. Цей метод використовується як дрібними шахраями, так і найбільш просунутими військовими спеціалістами на державному рівні.

Простими словами фішинг трапляється, коли зловмисник намагається обманом змусити вас надати інформацію, що може бути використана проти вас або вашої організації. Фішинг може відбуватися через електронні листи, текстові повідомлення/SMS (SMS-фішинг або «смішинг»), програми для обміну повідомленнями, як-от WhatsApp, повідомлення чи публікації в соціальних мережах або телефонні дзвінки (голосовий фішинг або «вішинг»). Фішингові повідомлення спонукають вас ввести конфіденційну інформацію (наприклад, паролі) на підробленому веб-сайті, щоб отримати доступ до облікового запису, просять надати особисту інформацію (наприклад, номер кредитної картки) голосовим або текстовим повідомленням, або переконують вас завантажити шкідливу програму (шкідливе програмне забезпечення), яке може заразити ваш пристрій. В якості нетехнічного прикладу: щодня мільйони людей отримують фальшиві автоматичні телефонні дзвінки, у яких їм повідомляється, що їхній банківський рахунок зламано або що їхню особисту інформацію викрадено, — для того, щоб обманом змусити необізнаних людей поділитися конфіденційною інформацією.



ЯК ВИЯВИТИ ФІШИНГ?

Метод фішингу може здатися зловісним і таким, що неможливо виявити, але є кілька простих кроків, які кожен у організації може вжити, щоб захиститися від більшості атак. Наведені нижче поради щодо захисту від фішингу змінено та розширено на основі детального посібника з фішингу, розробленого Фундацією свободи преси, і їх слід поділитися з усіма в парламенті та навколо нього та включити до вашого плану безпеки:

Іноді поле «від» містить фальшиві дані

Майте на увазі, що поле «від» у ваших електронних листах може бути підробленим або зміненим, щоб обдурити вас. Зазвичай фішери використовують адресу електронної пошти, що дуже схожа на звичайну, яка знайома вам, лише з невеликою орфографічною помилкою, щоб обдурити вас. Наприклад, ви можете отримати електронний лист від особи з адресою «john@goooogle.com», а не «john@google.com». Зверніть увагу на кілька додаткових «О» у слові «google». Ви також можете знати особу з електронною адресою «john@gmail.com», але отримати фішинговий електронний лист від імітатора, який зареєстрував адресу «johm@gmail.com» — єдиною відмінністю є ледь помітна зміна літери в кінці слова. Перш ніж відкривати листа, завжди перевіряйте, чи знаєте ви адресу відправлення електронної пошти. Такий самий підхід використовується для викриття фішингу за допомогою текстових повідомлень, дзвінків або програм для обміну повідомленнями. Якщо ви отримали повідомлення з невідомого номера, подумайте двічі, перш ніж відповідати на повідомлення або натискати на вкладення в ньому.

Фішинг і парламенти


Thu 4/8/2021 8:48 AM

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

Kindlty mention this email Most Urgent.

To [redacted]@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

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

Regards | [redacted]

[redacted]

Press office | Spokesman

Presidential Palace (ARG) | Islamic Republic of Afghanistan

Mobile: [redacted] | [redacted] | [redacted] | ocs.gov.af

Mail: [redacted] | [redacted]

Складні, персоналізовані фішингові атаки регулярно атакують парламенти та інші урядові установи по всьому світу.

Напередодні виборів восени 2021 року посадові особи федерального та місцевого парламенту Німеччини стали жертвами фішингових листів. Лише кілька місяців тому в Афганістані хакерська група **використала методи фішингу, щоб успішно проникнути в** колишню Раду національної безпеки, прийнявши особу прес-секретаря колишнього президента Афганістану Ашрафа Гані. Хакери надіслали фішингові електронні листи (показані вище), у яких жертвам було запропоновано відкрити вкладений файл, який, як стверджував «представник», містить помилку. Коли жертви завантажили та відкрили файл, щоб «підтвердити помилку», шкідливе вкладення розгорнуло зловмисне програмне забезпечення, яке надало хакерам постійний доступ до комп'ютерів. Такий доступ дозволив хакерам завантажувати файли, запускати команди на пристроях і викрадати конфіденційні урядові дані.

Остерігайтеся вкладень

Вкладення можуть містити шкідливі програми та віруси, та зазвичай супроводжують фішингові електронні листи. **Найкращий спосіб уникнути шкідливих програм із вкладених файлів — ніколи їх не завантажувати.** Візьміть собі за правило не відкривати одразу будь-які вкладення, особливо якщо вони надходять від людей, яких ви не знаєте. За можливості, попросіть особу, яка надіслала вам документ, скопіювати та вставити текст в електронний лист або поділитися документом через такі служби, як Google Drive або Microsoft OneDrive, які мають вбудовану антивірусну перевірку більшості документів, завантажених на їхні платформи. Створіть організаційну культуру, у якій вкладення до електронних листів не заохочуються.

Якщо вам обов'язково потрібно відкрити вкладення, його слід відкривати лише в безпечному середовищі (див. розділ «Вищий рівень» далі), у якому потенційна шкідлива програма не зможе бути запущена на вашому пристрої.

Якщо ви використовуєте Gmail і отримуєте вкладення в електронному листі, замість того, щоб завантажувати його та відкривати на своєму комп'ютері, просто клацніть вкладений файл і прочитайте його в режимі «попереднього перегляду» у вебоглядачі. Цей крок дозволяє переглядати текст і вміст файлу без завантаження й можливості запуску шкідливої програми на вашому комп'ютері. Такий метод добре діє для документів Word, PDF-файлів і навіть презентацій із показом слайдів. Якщо вам потрібно відредагувати документ, ви можете відкрити файл у хмарній програмі, як-от Google Drive, і перетворити файл на Google Doc або Google Slides.

Якщо ви використовуєте Outlook, ви також можете попередньо переглядати вкладення, не завантажуючи їх із вебклієнта Outlook. Якщо вам потрібно відредагувати вкладення, спробуйте відкрити його в OneDrive, якщо він встановлений у вас. Якщо ви використовуєте Yahoo Mail, застосовуйте той самий метод. Не завантажуйте вкладення, а перегляньте їх у вебоглядачі.

Незалежно від того, які інструменти є у вашому розпорядженні, найкращим підходом є просто ніколи не завантажувати вкладення від осіб, яких ви не знаєте або яким не довіряєте. Незалежно від того, наскільки важливим здається вкладення, ніколи не відкривайте щось із типом файлу, який ви не впізнаєте або не маєте наміру використовувати.

Захист від фішингу для вашого парламенту

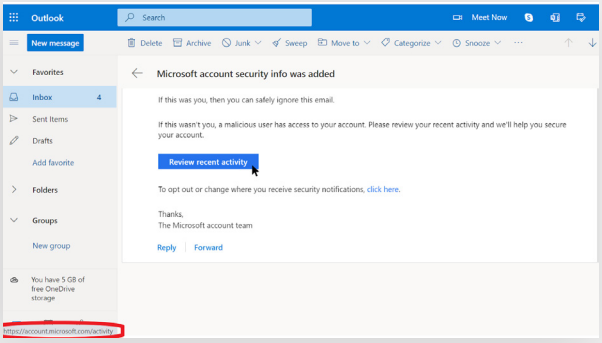
Якщо ваша організація використовує корпоративну версію Microsoft 365 для електронної пошти та інших програм, адміністратор домену повинен налаштувати Політику безпечних вкладень для захисту від небезпечних вкладень. Якщо ви використовуєте корпоративну версію Google Workspace (раніше відому як GSuite), у ньому є так само ефективна функція, яку ваш адміністратор повинен налаштувати, під назвою Google Security Sandbox. Більш досвідчені користувачі можуть розглянути можливість налаштування ізольованого програмного середовища просунутого рівня, як-от Dangerzone або, для версії Windows 10 Pro чи Enterprise, Windows Sandbox. Іншим розширеним варіантом, який варто розглянути щодо впровадження в парламенті, є служба фільтрації безпечної системи доменних імен (DNS).

Організації можуть використовувати цю технологію для блокування дій співробітників для попередження випадкового доступу або взаємодії із шкідливим вмістом, що забезпечує додатковий рівень захисту від фішингу. Нові сервіси, такі як Cloudflare Gateway, надають такі можливості організаціям, не вимагаючи великих сум грошей. Додаткові безкоштовні інструменти, в тому числі Quad9 від Global Cyber Alliance Toolkit, допоможе вам заблокувати доступ до відомих сайтів, які містять віруси чи інші шкідливі програми, і можуть бути встановлені менше ніж за п'ять хвилин.

Натискайте обережно

Скептично ставтеся до посилань в електронних листах чи інших текстових повідомленнях. Посилання можуть бути замасковані для завантаження шкідливих файлів або переходу на підроблені сайти, що можуть вимагати від вас надати паролі чи іншу конфіденційну інформацію. Коли ви користуєтеся комп'ютером, існує простий спосіб, щоб переконатися, що посилання в електронному листі чи повідомленні спрямує вас туди, куди потрібно: наведіть вказівник миші на посилання, перш ніж натиснути на нього, і подивіться внизу вікна вебоглядача, щоб побачити фактичну URL-адресу (див. зображення нижче).

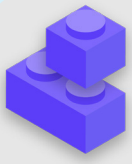
Перевірити посилання в електронному листі на мобільному пристрої, не натиснувши випадково, складніше, тому будьте обережні. Ви можете перевірити, куди веде посилання, на більшості смартфонів, довгим натисненням (утриманням) посилання, доки не з'явиться повна URL-адреса.
У разі фішингу через SMS і програми обміну повідомленнями скорочені посилання є дуже поширеною практикою, що використовується для маскування цільової URL-адреси. Якщо ви бачите коротке посилання (наприклад, bit.ly або tinyurl.com) замість повної URL-адреси, не натискайте на нього. Якщо посилання важливе, скопіюйте його в розширювач URL-адрес, наприклад https://www.expandurl.net/, щоб побачити, куди фактично веде скорочена URL-адреса. Крім того, не натискайте посилання на веб-сайти, незнайомі вам. Якщо ви сумніваєтеся, виконайте пошук сайту, взявши назву сайту в лапки (наприклад: «www.badwebsite.com»), щоб перевірити, чи це справжній веб-сайт. Також можна запускати потенційно підозрілі посилання у сканері URL-адрес VirusTotal. Сканер не забезпечує 100-відсоткової точності, але є хорошим запобіжним заходом.



Нарешті, якщо ви клацнете на посилання в повідомленні й вас попросять увести облікові дані на якомусь веб-сайті, не робіть цього, якщо ви не впевнені на 100 відсотків, що електронний лист є непідробленим і спрямовує вас на відповідний веб-сайт. Багато фішингових атак надають посилання, що спрямовують на підроблені сторінки входу в Gmail, Facebook або на інші популярні веб-сайти. Не ведіться на це. Ви завжди можете відкрити новий вебоглядач і самостійно перейти безпосередньо на відомий сайт, як-от Gmail.com, Facebook.com тощо, якщо хочете чи вам потрібно ввійти на них. Це також безпечно спрямує вас до вмісту, — якщо він був непідробленим від початку.

Що робити в разі отримання фішингового повідомлення?

Якщо будь-хто в парламенті отримує небажане вкладення, посилання, зображення чи інше підозріле повідомлення чи дзвінок, важливо негайно повідомити про це особі або групі служби безпеки IT. Якщо у вас немає такої особи, слід призначити її під час розроблення плану безпеки. Співробітники та учасники також можуть повідомити про електронний лист як про спам або фішинг безпосередньо в Gmail або Outlook.
Дуже важливо мати план того, що повинні робити співробітники або волонтери, якщо/коли вони отримають можливе фішингове повідомлення. Крім того, ми рекомендуємо скористатися найкращими методами запобігання фішингу — не натискати на підозрілі посилання, уникати вкладень і перевіряти адресу, «від» кого було отримано повідомлення. Поділіться цими порадами з іншими людьми, з якими ви працюєте, бажано через широко використовуваний канал зв'язку. Це покаже, що ви дбаєте про людей, з якими спілкуєтеся, і заохочуєте впровадження культури у своїх мережах для усвідомлення небезпеки фішингу. Ваша безпека залежить від організацій, яким ви довіряєте, і навпаки. Кращі методи захищають усіх.
Крім того, щоб поділитися наведеними вище порадами з усіма, ви також можете потренуватися розпізнавати фішинг за допомогою вікторини Google Phishing Quiz. Ми також наполегливо рекомендуємо організовувати регулярні тренінги з фішингу з персоналом, щоб перевірити обізнаність і заохотити людей бути пильними. Таке навчання може бути формалізовано як частину регулярних командних і парламентських зустрічей або проводитися більш неформально. Важливо, щоб кожен, хто бере участь у роботі парламенту, почувався комфортно, ставлячи запитання про фішинг, повідомляючи про фішинг (навіть якщо вони відчувають, що могли зробити помилку, наприклад, натиснувши посилання), і що кожен має право допомогти захистити парламент від цього вплив і висока ймовірність загрози.



Фішинг

- **Регулярно навчайте співробітників тому, що таке фішинг, як його виявити та захиститися від нього, зокрема фішинг у текстових повідомленнях, програмах для обміну повідомленнями та телефонних дзвінках, а не лише в електронній пошті.**
- **Часто нагадуйте депатам і співробітникам про найкращі практики, такі як:**
  - Не завантажувати невідомі або потенційно підозрілі вкладення.
  - Перевіряти URL-адресу посилання, перш ніж клацнути її. Не натискати на невідомі або потенційно підозрілі посилання.
  - Не надавати секретну чи конфіденційну інформацію в електронних листах, текстових повідомленнях або телефонних дзвінках невідомим чи непідтвердженим адресам або людям.
- **Заохочувати повідомляти про фішинг.**
  - Створити механізм звітності та вказати особу для фішингу в парламенті.
  - Винагороджувати за повідомлення, а не карати за невдачу.

Communicating and Storing Data Securely

Комунікація й обмін даними

Щоб прийняти найкраще рішення про спосіб комунікації, важливо розуміти різні типи захисту комунікації, і чому такий захист є важливим.

Одним із найважливіших елементів безпеки комунікації є збереження конфіденційності приватних повідомлень, що в сучасну епоху значною мірою забезпечується шифруванням. Без належного шифрування внутрішню парламентську комунікацію можуть бачити зловмисники. Внаслідок незахищеної комунікації може бути розкрита конфіденційна або делікатна інформація й повідомлення, паролі чи інші особисті дані та, можуть бути поставлені під загрозу ваші співробітники залежно від характеру повідомлень і вмісту, яким ви ділитеся. Парламенту також важливо забезпечити, щоб комунікація депутатів і співробітників відповідала чинним відповідним нормам та зобов'язанням (таким як норми щодо запитів на доступ до публічної інформації) і зобов'язанням щодо безпеки даних. Тому, розробляючи та впроваджуючи захищені комунікаційні системи та політику в парламенті, обов'язково враховуйте ці фактори, щоб відповідні повідомлення могли бути як належним чином захищені, так і, якщо це необхідно згідно із законом, збережені.

Безпечні комунікації і парламент

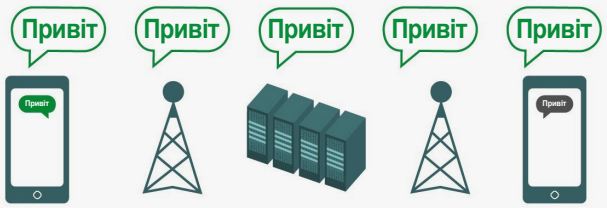
За останні роки було багато інцидентів, під час яких комунікаційні системи парламентів та облікові записи депутатів та їхніх співробітників були скомпрометовані, що призвело до збоїв у роботі парламенту та в деяких випадках до крадіжки конфіденційних даних. У липні 2021 року, наприклад, польська влада оголосила, що облікові записи електронної пошти майже десятка місцевих **депутатів були зламані**, включно з особистим обліковим записом головного помічника прем'єр-міністра та обліковими записами депутатів майже кожної парламентської опозиційної групи. Цей звіт надійшов лише через кілька місяців після того, як з'явилася подібна новина про кібератаку на інформаційні та комунікаційні системи **фінського парламенту**. Влада Фінляндії **описала цей напад** як «шпигунство при обтяжуючих обставинах і перехоплення повідомлень», спрямоване проти парламенту.

ЩО ТАКЕ ШИФРУВАННЯ І ЧОМУ ВОНО ВАЖЛИВО?

Шифрування — це математичний процес, який використовується для шифрування повідомлення або файлу, щоб лише особа чи організація, яка має ключ, могла «розшифрувати» його та прочитати. У Посібнику із самозахисту від спостереження від Electronic Frontier Foundation надається практичне пояснення (з ілюстраціями) того, що означає шифрування:

Незашифровані повідомлення

Без жодного шифрування наші повідомлення залишаються відкритими для читання потенційними ворогами, зокрема недружніми іноземними урядами, або хакерами в Інтернеті. Таке шифрування є важливим не лише для внутрішніх комунікацій парламенту, а й для зовнішніх комунікацій, у яких необхідно захищати конфіденційність і цілісність.



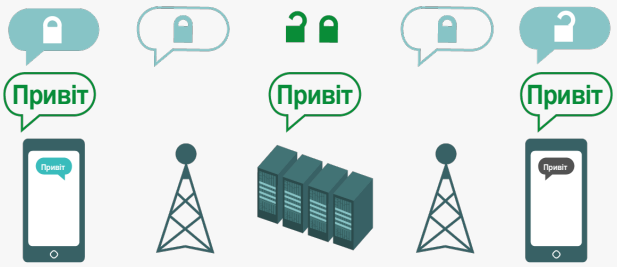
Як видно на зображенні вище, смартфон надсилає зелене незашифроване текстове повідомлення («привіт») на інший смартфон праворуч. Вежа мобільного зв'язку (або, якщо дані надсилаються через інтернет, ваш постачальник послуг інтернету, або інтернет-провайдер) передає повідомлення на сервери компанії. Звідти воно переходить через мережу на іншу вежу мобільного зв'язку, що може бачити незашифроване повідомлення «привіт», і, нарешті, направляється до місця призначення. Важливо зазначити, що за відсутності шифрування всі, хто бере участь у передачі повідомлення, і будь-хто, хто може крадькома зазирнути у нього під час проходження, може прочитати його вміст.

Це може не мати великого значення, якщо ви говорите лише «привіт»; проблема виникає, коли ви повідомляєте щось приватне чи конфіденційне і не хочете, щоб оператор телекомунікацій, інтернет-провайдер, недружній уряд чи будь-який інший зловмисник побачили це повідомлення. Через це важливо уникати використання інструментів, що не мають функції шифрування, для надсилання конфіденційних повідомлень (а в ідеалі взагалі будь-яких повідомлень). Зауважте, що деякі з найпопулярніших методів зв'язку, як-от SMS і телефонні дзвінки, фактично функціонують без жодного шифрування (як на зображенні вище).

Є два способи зашифрувати дані під час передачі: ***шифрування транспортного рівня*** і ***наскрізне шифрування***. Важливо знати тип шифрування, що підтримується постачальником послуг зв'язку, оскільки ваша організація має прийняти рішення про застосування більш безпечних методів і систем зв'язку. Такі відмінності добре описані Посібнику із самозахисту проти спостереження, дані з якого наведено далі в адаптованій формі:

Шифрування транспортного рівня;

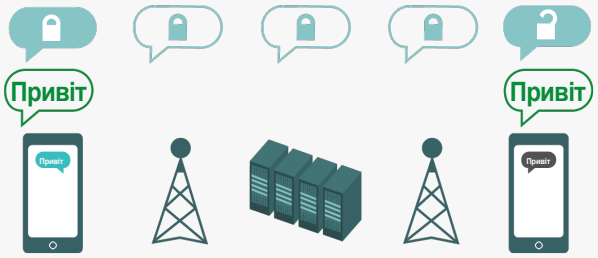
Шифрування транспортного рівня, також відоме як захист транспортного рівня (TLS), захищає повідомлення під час їх переміщення з вашого пристрою на сервери програми/служби обміну повідомленнями, а звідти — на пристрій одержувача. Це захищає їх від очей хакерів, які сидять у вашій мережі або у мережі інтернет-провайдера чи постачальника телекомунікаційних послуг. Однак під час передачі постачальник послуг обміну повідомленнями/електронної пошти, веб-сайт, який ви переглядаєте, або програма, яку ви використовуєте, можуть бачити незашифровані копії ваших повідомлень. Оскільки ваші повідомлення можуть переглядатися (і часто зберігаються на) серверах компанії, їм загрожує ризик запитів правоохоронних органів або крадіжки, якщо сервери компанії зламано.



На зображенні вище показано приклад шифрування транспортного рівня. Смартфон ліворуч надсилає зелене незашифроване повідомлення: «Привіт!». Це повідомлення шифрується, а потім передається на вежу мобільного зв'язку. Під час передачі сервери компанії можуть розшифрувати повідомлення, прочитати вміст, вирішити, куди його надіслати, повторно зашифрувати та відправити на наступну вежу мобільного зв'язку до місця призначення. Наприкінці інший смартфон отримує зашифроване повідомлення та розшифровує його, щоб користувач міг прочитати: «Привіт!».

Наскрізне шифрування

Наскрізне шифрування захищає повідомлення під час передачі на всьому шляху від відправника до одержувача. Воно гарантує, що інформація перетворюється на секретне повідомлення її початковим відправником (на першому «кінці») і декодується лише кінцевим одержувачем (на другому «кінці»). Ніхто, включно з програмою чи службою зв'язку, якою ви користуєтеся, не може «прослуховувати» та дізнатися вміст ваших повідомлень.



На зображенні вище показано приклад наскрізного шифрування. Смартфон ліворуч надсилає зелене незашифроване повідомлення: «Привіт!». Це повідомлення шифрується, передається на вежу мобільного зв'язку, а потім на сервери програми/сервісу, які не можуть прочитати вміст, але передадуть секретне повідомлення до місця призначення. Наприкінці інший смартфон отримує зашифроване повідомлення та розшифровує його, щоб користувач міг прочитати: «Привіт!». На відміну від шифрування транспортного рівня, ваш інтернет-провайдер і служба обміну повідомленнями не можуть розшифрувати повідомлення. Лише кінцеві точки (оригінальні пристрої, що надсилають і отримують зашифровані повідомлення) мають ключі для розшифровки та читання повідомлення.

ЯКИЙ ТИП ШИФРУВАННЯ НАМ ПОТРІБЕН?

Коли ви вирішуєте, потрібне вашій організації шифрування транспортного рівня чи наскрізне шифрування для ваших комунікацій (чи якась комбінація обох для різних систем і видів діяльності), головне питання, яке ви повинні поставити, стосується довіри. Чи довіряєте ви додатку або службі, якими користуєтеся? Чи довіряєте ви їхній технічній інфраструктурі? Чи непокоїть вас можливість того, що недружній уряд може змусити компанію передати ваші повідомлення, — і, якщо так, чи довіряєте ви політиці компанії щодо захисту від запитів правоохоронних органів?

Якщо ви відповіли «ні» на будь-яке з цих запитань, то вам потрібне наскрізне шифрування. Якщо ви відповісте на них «так», тоді служби, яка підтримує лише шифрування транспортного рівня, може бути достатньо, але, як правило, краще використовувати служби, які підтримують наскрізне шифрування, за можливості.

Інший набір запитань, які слід розглянути, полягає в тому, чи зобов'язані ви як парламент за законом мати одноосібний доступ до будь-якої парламентської комунікації, чи існують якісь вимоги щодо локалізації даних у вашій країні та/або чи потрібно зберігати певні комунікації (наприклад, не видалені співробітниками остаточно) для дотримання законів і зобов'язань відкритого уряду. Якщо так, ви можете розглянути систему зв'язку корпоративного рівня з підтримкою наскрізного шифрування, у якій ви, як парламент, можете самостійно контролювати ключі шифрування. Такі системи (про які буде розказано більш детально в розділі «**Безпечне зберігання даних**» Посібника) можуть бути потужними, але вимагають передових технічних навичок для впровадження.

Під час обміну повідомленнями з групами пам'ятайте, що безпека ваших повідомлень знаходиться на тому ж рівні, що і безпека всіх, хто отримує повідомлення. Крім ретельного вибору безпечних програм і систем, важливо, щоб усі у групі дотримувався інших найкращих методів захисту облікових записів і пристроїв. Для витоку змісту цілого групового чату чи дзвінка достатньо лише однієї особи, яка не дотримується правил безпеки, або одного зараженого пристрою.

ЩО РОБИТИ З ЕЛЕКТРОННОЮ ПОШТОЮ?

Загалом, електронна пошта — не найкращий варіант, коли йдеться про безпеку. Навіть найкращі варіанти електронної пошти з наскрізним шифруванням зазвичай не э ыдеальними з точки зору безпеки, наприклад, не шифрувати рядки теми електронних листів і не захищати метадані (важлива концепція, яку буде описано нижче). Якщо вам потрібно повідомити конфіденційну інформацію, яку не потрібно зберігати для загального доступу, майте на увазі, що електронної пошти (як системи парламенту, так і особливо чийсь особистий обліковий запис) краще уникати на користь безпечних варіантів обміну повідомленнями (які будуть виділені) у наступному розділі).

Однак, як парламент, ви все одно можете захотіти або потребувати, щоб депутати та співробітники повідомляли конфіденційний або приватний вміст через систему, якою керують централізовано в рамках їх повсякденної роботи. Загальнопарламентська система електронної пошти, звичайно, з належним контролем облікових записів, може бути тут корисною. Якщо, згідно з вашим аналізом вище, шифрування на транспортному рівні буде достатнім, тоді стандартні бізнес-пропозиції від постачальників електронної пошти, таких як Google Workspace (Gmail) і Microsoft 365 (Outlook), можуть бути хорошими варіантами для вашого парламенту. Однак якщо ви хвилюєтеся, що ваш постачальник послуг електронної пошти може бути зобов'язаний надавати інформацію про ваші повідомлення іноземному уряду чи іншому опоненту, або якщо місцеві вимоги щодо постійності даних можуть викликати занепокоєння, ви захочете розглянути можливість використання наскрізного зв'язку варіант зашифрованої електронної пошти. Кілька таких варіантів включають додавання власного керування ключами шифрування до Google Workspace або Microsoft 365 (як описано в розділі **«Безпечне зберігання даних»** цього посібника) або застосування наскрізних зашифрованих служб електронної пошти, розроблених для великих організацій, таких як **ProtonMail**. Бізнес або **Тутанота** Бізнес.

ЩО ТАКЕ МЕТАДАНІ І ЧИ ВАРТО ЗА НИХ ХВИЛЮВАТИСЯ?

З ким розмовляєте ви, ваші співробітники, депутати парламенту та їх команда, а також коли й де ви з ними розмовляєте, часто може бути настільки ж делікатним, як і те, про що ви говорите. Важливо пам'ятати, що наскрізне шифрування захищає лише вміст («що») ваших повідомлень. І тут у гру вступають метадані. У Посібнику із самозахисту від спостереження від EFF надається огляд метаданих і пояснюється, чому вони важливі для організацій (включно з ілюстрацією того, як виглядають метадані):

Метадані часто описуються як усе, крім змісту ваших повідомлень. Метадані можна розглядати як цифровий еквівалент конверта. Подібно до того, як конверт містить інформацію про відправника, одержувача та адресата повідомлення, метадані також містять таку інформацію. Метадані — це інформація про цифрові повідомлення, які ви надсилаєте й отримуєте.

Метадані включають таку інформацію:
- з ким ви спілкуєтеся;
- рядок теми ваших електронних листів;
- тривалість ваших розмов;
- час, коли відбулася розмова;
- ваше місцезнаходження під час спілкування.

Хоча прозорість відповідних парламентських операцій є важливою, обмеження несанкціонованого доступу до метаданих (на додаток до захисту змісту повідомлень) також є важливим. Зрештою, метадані можуть розкрити конфіденційну інформацію хакерам, іноземним урядам, компаніям чи іншим особам, яким ми, можливо, не хочете надавати доступ. Кілька прикладів того, як метадані можуть бути відкритими, включають:

Вони знатимуть, що ви зателефонували журналісту і розмовляли з ним протягом години, перш ніж той журналіст опублікував розповідь із анонімною цитатою. Однак вони не знатимуть, про що ви говорили.

Вони знатимуть, що ви отримали електронний лист від лабораторії тестування на COVID, потім зателефонували своєму лікарю, а потім відвідали веб-сайт Всесвітньої організації охорони здоров'я протягом тієї ж години. Однак вони не знатимуть, що було в електронному листі або про що ви говорили по телефону.

Рекомендовані інструменти зв'язку з наскрізним шифруванням

ТЕКСТОВІ ПОВІДОМЛЕННЯ (ІНДИВІДУАЛЬНІ АБО ГРУПОВІ)	• **Signal** • **WhatsApp (тільки зі спеціальними конфігураціями налаштувань, описаними нижче)**
АУДІО ТА ВІДЕОДЗВІНКИ:	• **Signal (до 40 осіб)** • **WhatsApp (до 32 осіб на аудіо, вісім на відео)**
ФАЙЛООБМІННИК:	• **Signal** • **Keybase / Keybase Teams** • **Tresorit**

ЯКІ ІНСТРУМЕНТИ ОБМІНУ ПОВІДОМЛЕННЯМИ З НАСКРІЗНИМ ШИФРУВАННЯМ МИ ПОВИННІ ВИКОРИСТОВУВАТИ (СТАНОМ НА 2022 РІК)?

Якщо вам потрібно використовувати наскрізне шифрування або ви просто хочете застосувати найкращі методи незалежно від контексту загроз вашої організації, ось кілька прикладів надійних служб, які, **станом на 2022 рік**, пропонують обмін повідомленнями та дзвінки з наскрізним шифруванням. Цей розділ Довідника регулярно оновлюватиметься в інтернеті, але зауважте, що технології безпечного обміну повідомленнями швидко змінюються, тому ці рекомендації можуть бути неактуальними на момент, коли ви читаєте цей розділ. Майте на увазі, що ваші комунікації безпечні лише в тій мірі, у якій безпечний сам пристрій. Тому, окрім впровадження безпечних методів обміну повідомленнями, важливо застосовувати найкращі методі, описані в розділі «**Захищені пристрої**» цього Довідника.

Метадані не захищені шифруванням, яке надає більшість служб обміну повідомленнями. Наприклад, якщо ви надсилаєте повідомлення через WhatsApp, майте на увазі, що, незважаючи на те, що вміст вашого повідомлення зашифровано наскрізно, інші можуть знати, кому ви надсилаєте повідомлення, як часто й, у разі телефонних дзвінків, як довго. Як наслідок, ви повинні пам'ятати, які ризики існують (якщо такі є), якщо певні противники зможуть дізнатися, з ким ви розмовляєте, коли ви з ними розмовляли, і (у випадку електронної пошти) загальні теми вашого парламенту. комунікацій.

Однією з причин того, чому **Signal** настільки настійно рекомендується, це те, що крім забезпечення наскрізного шифрування, у ньому компанія **запровадила функції та взяла на себе зобов'язання зменшити кількість метаданих, що записуються та зберігаються в ньому.** Наприклад, функція Sealed Sender у Signal шифрує метадані про те, хто з ким розмовляє, так що Signal знає лише одержувача повідомлення, але не відправника. За замовчуванням ця функція працює лише під час спілкування з наявними контактами чи профілями (людьми), з якими ви вже спілкувалися або яких ви зберегли у своєму списку контактів. Однак ви можете ввімкнути для параметра «Sealed Sender» значення «Дозволити від будь-кого», якщо для вас важливо видалити такі метадані з усіх розмов у Signal, навіть із тих, що були з невідомими вам людьми.

Це може не бути критичним для більшості парламентських комунікацій, але важливо усвідомлювати ризики, пов'язані з метаданими, і відповідно обирати відповідні інструменти та політику комунікації.

ЧИ МОЖНА СПРАВДІ ДОВІРЯТИ WHATSAPP?

WhatsApp є популярним додатком для безпечного обміну повідомленнями, і може бути хорошим варіантом, враховуючи його розповсюдженість. Деякі люди стурбовані тим, що він належить і контролюється Facebook, що працює над інтеграцією його з іншими своїми системами. Також непокоїть кількість метаданих (тобто інформації про те, з ким і коли ви спілкуєтеся), які збирає WhatsApp. Якщо ви вирішите використовувати WhatsApp як безпечний варіант обміну повідомленнями, обов'язково прочитайте наведений вище розділ про метадані. Є також кілька параметрів, щодо яких слід переконатися, що вони правильно налаштовані. Найважливіше: обов'язково вимкніть хмарне резервне копіювання або, принаймні, увімкніть нову функцію резервного копіювання з наскрізним шифруванням WhatsApp, із використанням 64-значного ключа шифрування або довгого, випадкового й унікального пароля, збереженого у безпечному місці (наприклад, у вашому менеджері паролів). Також обов'язково ввімкніть показ сповіщень безпеки та перевірте коди безпеки. Прості вказівки щодо налаштування цих параметрів для телефонів Android знаходяться тут, а для iPhone — тут. **Якщо ваші співробітники (і ті, з ким ви всі спілкуєтеся), неправильно налаштують ці параметри, не слід вважати WhatsApp хорошим варіантом для конфіденційних комунікацій, які потребують наскрізного шифрування.** Signal все ще залишається найкращим варіантом для таких потреб із наскрізним шифруванням повідомлень, враховуючи його налаштування безпеки за замовчуванням і захист метаданих.

А ЯК ЩОДО ТЕКСТОВИХ ПОВІДОМЛЕНЬ?

Звичайні текстові повідомлення зовсім незахищені (стандартні SMS фактично незашифровані), і їх слід уникати для всього, що не призначено для загального відома. Хоча повідомлення iPhone-to-iPhone від Apple (відомі як iMessages) мають наскрізне шифрування, якщо в розмові бере участь не iPhone, повідомлення не будуть захищені. Найкраще перестрахуватися й **уникати текстових повідомлень щодо будь-чого секретного, приватного чи конфіденційного**.

ЧОМУ TELEGRAM, FACEBOOK MESSENGER АБО VIBER НЕ РЕКОМЕНДУЮТЬСЯ ДЛЯ БЕЗПЕЧНИХ ЧАТІВ?

Деякі служби, як-от Facebook Messenger і Telegram, пропонують наскрізне шифрування, лише якщо ви спеціально його ввімкнули (і лише для чатів один на один), тому вони не є хорошими варіантами для конфіденційних або приватних повідомлень, особливо для організації. Не покладайтеся на ці інструменти, якщо вам потрібно використовувати наскрізне шифрування, тому що досить легко забути змінити стандартні, менш безпечні налаштування. Viber стверджує, що пропонує наскрізне шифрування, але не надав свій код для перевірки сторонніми дослідниками безпеки. Код Telegram також не був наданий для публічного аудиту. В результаті багато експертів побоюються, що шифрування Viber (або «секретні чати» Telegram) може не відповідати стандартам і, отже, бути непридатним для спілкування, що вимагає справжнього наскрізного шифрування.

НАШІ КОЛЕГИ В ПАРЛАМЕНТІ ТА ВИБОРЦІ ВИКОРИСТОВУЮТЬ ІНШІ ПРОГРАМИ ТА СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ ДЛЯ СПІЛКУВАННЯ — ЯК МИ МОЖЕМО ПЕРЕКОНАТИ ЇХ ЗАВАНТАЖИТИ НОВУ ПРОГРАМУ ДЛЯ СПІЛКУВАННЯ З НАМИ?

Іноді існує компроміс між безпекою та зручністю, але варто докласти трохи додаткових зусиль для конфіденційності комунікацій. Подавайте гарний приклад своїм контактам — будь то в інших урядових установах, установах, у парламенті чи зовнішніх складових. Якщо вам доводиться використовувати інші, менш безпечні системи, будьте уважні до того, що ви говорите. Уникайте обговорення секретних тем. Деякі парламенти можуть мати інші протоколи для загального спілкування в чаті або спілкування з громадськістю порівняно з конфіденційними обговореннями з керівництвом, наприклад. Класифікуйте ваші парламентські комунікації (внутрішні та зовнішні) на основі конфіденційності та переконайтеся, що депутати та співробітники відповідно використовують відповідні механізми комунікації! Звичайно, найпростіше, якщо все постійно автоматично шифрується - нема про що пам'ятати чи думати.

На щастя, програми з наскрізним шифруванням, такі як Signal, стають дедалі популярнішими та зручнішими, не кажучи вже про те, що їх локалізовано десятками мов для глобального використання. Якщо вашим партнерам або іншим контактним особам потрібна допомога з переходом на комунікацію з наскрізним шифруванням, як-от Signal, знайдіть час, щоб пояснити їм, чому так важливо належним чином захищати ваші комунікації. Коли всі розуміють важливість, кілька хвилин, необхідних для завантаження нової програми, і кілька днів, які можуть знадобитися, щоб звикнути до неї, не будуть здаватися великою проблемою.

ЧИ ІСНУЮТЬ ІНШІ НАЛАШТУВАННЯ ДОДАТКІВ ІЗ НАСКРІЗНИМ ШИФРУВАННЯМ, ПРО ЯКІ НАМ СЛІД ЗНАТИ?

У додатку Signal перевірка з підтвердженням кодів безпеки (які вони називаються номерами безпеки) також важлива. Щоб переглянути номер безпеки та підтвердити його в Signal, ви можете відкрити свій чат із контактом, торкнутися імені у верхній частині екрана та прокрутити вниз, щоб натиснути «Переглянути номер безпеки». Якщо ваш номер безпеки збігається з вашим контактом, ви можете позначити його як «підтвердженого» на тому самому екрані. Особливо важливо звернути увагу на ці номери безпеки та перевірити свої контакти, якщо ви отримаєте сповіщення в чаті про те, що ваш номер безпеки з даним контактом змінився. Якщо вам або іншому співробітнику потрібна допомога в конфугірації цих налаштувань, Signal сам **надає корисні інструкції**. Якщо ви використовуєте Signal, що вважається найкращим зручним варіантом для безпечного обміну повідомленнями та дзвінків один на один, переконайтеся, що **встановили сильний пін-код.** Використовуйте принаймні шість цифр, які нелегко вгадати, наприклад, дату народження. Для отримання додаткових порад щодо правильного налаштування **Signal** і **WhatsApp** зверніться до **довідників із використання інструментів** для обох додатків, розроблених компанією EFF у **Посібнику із самозахисту проти спостереження.**

А ЯК ЩОДО ГРУПОВИХ ВІДЕОДЗВІНКІВ? ЧИ Є ВАРІАНТИ НАСКРІЗНОГО ШИФРУВАННЯ?

Зі збільшенням віддаленої роботи важливо мати безпечний варіант для великих групових відеодзвінків у вашому офісі або віртуальних ратуш для депутатів. На жаль, наразі немає універсальних варіантів, які покривають всі потреби: зручні сть користування, підтримка великої кількості учасників і доступність функції співпраці, а також наявність увімкненого наскрізного шифрування за замовчуванням.

Конкретні потреби пленарних засідань і засідань комітетів обговорюватимуться пізніше в цьому довіднику, але для інших більш загальних зборів, які не вимагають таких функцій співпраці, як спільне використання екрана або кімнати для сеансів, є кілька варіантів. Для груп до восьми осіб настійно рекомендується Signal. До групових відеодзвінків у Signal можна приєднатися зі смартфона або настільного додатка Signal на комп'ютері. Однак майте на увазі, що лише ваші контакти, які вже використовують Signal, можуть бути додані до групи у Signal.

Якщо ви шукаєте інші варіанти, існує платформа, що нещодавно додала налаштування наскрізного шифрування **Jitsi Meet**. Jitsi Meet — це вебрішення для аудіо- та відеоконференцій, що може використовуватися для великої аудиторії (до 100 осіб) і не потребує завантаження програми чи спеціального програмного забезпечення. Зауважте, що якщо ви використовуєте цю функцію у великих групах (більше 15-20 осіб), якість зв'язку може погіршитися. Щоб організувати зустріч на Jitsi Meet, ви можете перейти на **meet.jit.si**, ввести код зустрічі та поділитися цим посиланням (через безпечний канал, наприклад Signal) із запрошеними учасниками. Щоб використовувати наскрізне шифрування, перегляньте **інструкції** від Jitsi. Зауважте, що всі окремі користувачі повинні самі ввімкнути наскрізне шифрування, щоб воно працювало. Використовуючи Jitsi, обов'язково створюйте випадкові назви кімнат для нарад і надійні паролі, щоб захистити свої дзвінки.

Якщо ця опція не підходить для вашої організації, ви можете скористатися популярним комерційним варіантом, таким як Webex або Zoom, із увімкненим наскрізним шифруванням. Webex давно допускає наскрізне шифрування; однак цей параметр не ввімкнено за замовчуванням. Учасники повинні завантажити Webex, щоб приєднатися до вашої зустрічі. Щоб отримати опцію наскрізного шифрування для свого облікового запису Webex, ви повинні відкрити запит у служби підтримки Webex і слідувати **цим інструкціям** для налаштування наскрізного шифрування. Лише організатор зустрічі повинен увімкнути наскрізне шифрування. Після цього вся зустріч буде наскрізь зашифрована. Якщо ви використовуєте Webex для безпечних групових зустрічей і семінарів, обов'язково застосовуйте надійні паролі для дзвінків.

Після кількох місяців негативних відгуків компанія Zoom розробила **опцію наскрізного шифрування** для своїх дзвінків. Однак цей параметр не ввімкнено за замовчуванням, обліковий запис організатора виклику має бути пов'язаний із номером телефону, і шифрування можливе лише тоді, коли всі учасники приєднуються через програму Zoom для комп'ютера чи мобільного пристрою, а не набирають номер через телефон. Оскільки легко випадково неправильно налаштувати цю конфігурацію, не слід покладатися на наскрізне шифрування у Zoom. Однак, якщо потрібне наскрізне шифрування і Zoom є вашим єдиним вибором, ви можете дотримуватися **інструкцій** Zoom, щоб налаштувати його.
Не забудьте перевірити виклик перед його початком, щоб переконатися, що він справді наскрізь зашифрований. Для цього клацніть зелений замок у верхньому лівому куті екрана Zoom і побачите «наскрізне шифрування» у списку поруч із налаштуванням шифрування. Ви також повинні встановити надійний пароль для будь-якої зустрічі Zoom.
Однак варто зазначити, що деякі популярні функції вищезазначених інструментів працюють лише з шифруванням транспортного рівня. Наприклад, увімкнення наскрізного шифрування в Zoom вимикає кімнати підгруп, можливості опитування та запис у хмарі. У Jitsi Meet кімнати підгруп можуть вимкнути функцію наскрізного шифрування, що призведе до небажаного зниження рівню безпеки.

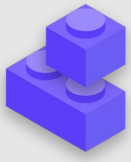
ПРИМІТКА ЩОДО ОБМІНУ ФАЙЛАМИ

Окрім безпечного обміну повідомленнями, безпечний обмін файлами, ймовірно, є важливою частиною плану безпеки вашої організації. Більшість параметрів обміну файлами вбудовані в програми або до служб обміну повідомленнями, якими ви, можливо, вже користуєтеся. Наприклад, обмін файлами через Signal є чудовим варіантом, якщо потрібне наскрізне шифрування. Якщо шифрування транспортного рівня (TLS) є достатнім, використання Google Диску або Microsoft SharePoint може бути хорошим варіантом для вашої організації. Не забудьте правильно налаштувати параметри спільного доступу, щоб лише авторизовані співробітники мали доступ до певного документа чи папки, і переконайтеся, що ці служби підключено до організаційних (не особистих) облікових записів електронної пошти співробітників. За можливості забороніть ділитися конфіденційними файлами через вкладення електронної пошти або фізично через USB-накопичувачі. Використання таких пристроїв, як USB, у вашому парламенті значно підвищує ймовірність зловмисного програмного забезпечення або крадіжки, а використання електронної пошти чи інших форм вкладень послаблює захист вашого парламенту від фішингових атак.

ЩО, ЯКЩО НАМ НАСПРАВДІ НЕ ПОТРІБНЕ НАСКРІЗНЕ ШИФРУВАННЯ ДЛЯ ВСІХ НАШИХ КОМУНІКАЦІЙ?

Якщо наскрізне шифрування не потрібне для всіх комунікацій вашої організації на основі вашої оцінки ризику, ви можете розглянути можливість використання програм, захищених шифруванням транспортного рівня. Для використання цього виду шифрування потрібно, щоб ви довіряли постачальнику послуг, наприклад Google для Gmail, Microsoft для Outlook/ Exchange або Facebook для Messenger, оскільки вони (і всі, з ким вони можуть бути змушені поділитися інформацією) можуть бачити/чути ваші комунікації. Знову ж таки, найкращі варіанти залежатимуть від вашої моделі загрози (наприклад, якщо ви не довіряєте Google або якщо уряд США є вашим зловмисником, Gmail не підходить), але ось кілька популярних і загалом надійних варіантів:

ЕЛЕКТРОННА ПОШТА	• **Gmail (через Google Workspace)** • **Outlook (через Office 365)** • Не розміщуйте свій власний сервер Microsoft Exchange для електронної пошти вашого парламенту. Якщо ви зараз це робите, слід **перейти** на Office 365.
ТЕКСТОВІ ПОВІДОМЛЕННЯ (ІНДИВІДУАЛЬНІ АБО ГРУПОВІ)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
ГРУПОВІ КОНФЕРЕНЦІЇ, АУДІО- ТА ВІДЕОДЗВІНКИ	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
ФАЙЛООБМІННИК:	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Безпечна передача даних

- **Класифікуйте повідомлення на основі їх чутливості.**
  - Відповідно визначте відповідні системи та інструменти для спілкування.
  - Відповідно встановіть політику щодо того, як довго ви зберігатимете повідомлення, пам'ятаючи як про безпеку, так і про зобов'язання щодо прозорості парламенту.
- **Вимагайте використання надійних служб обміну повідомленнями з наскрізним шифруванням для конфіденційних комунікацій вашого парламенту.**
  - Знайдіть час, щоб пояснити співробітникам та зовнішнім партнерам, чому безпечний зв'язок такий важливий; це сприятиме успішному втіленню вашого плану.
- **Переконайтеся, що встановлено належні налаштування для програм захищеного зв'язку, зокрема:**
  - Переконайтеся, що всі співробітники звертають увагу на сповіщення безпеки та, якщо ви використовуєте WhatsApp, не створюють резервні копії чатів.
  - Якщо ви використовуєте програму, де наскрізне шифрування не ввімкнено за замовчуванням (як-от Zoom або Webex), переконайтеся, що відповідні користувачі ввімкнули належні налаштування на початку будь-якого дзвінка чи зустрічі.
- **Не намагайтеся розмістити власний сервер електронної пошти — використовуйте хмарні служби електронної пошти, такі як Office 365 або Google Workspace, як альтернативу.**
  - Не дозволяйте співробітникам використовувати особисті облікові записи електронної пошти для робочих цілей.
- **Часто нагадуйте співробітникам і депутатам про найкращі інструменти безпеки, пов'язані з груповими повідомленнями та метаданими.**
  - Слідкуйте за тим, хто входить до групи повідомлень, чатів і ланцюжків електронних листів.

Цифрові парламенти (електронний парламент)

Як парламенту, важливо приділяти особливу увагу політиці комунікацій та оперативної безпеки ваших найважливіших функцій, у тому числі тих, які виконуються онлайн і в цифровому просторі.

Незалежно від того, чи розглядає ваш парламент повну систему «електронного парламенту», яка може оцифрувати все, від розробки законопроектів до дебатів і електронного голосування (наприклад, Nextsense, Propylon або Granicus, щоб назвати кілька прикладів), чи ви використовуєте простішу, меншу — дорогі інструменти для полегшення ваших парламентських операцій, важливо розглянути, як будь-який інструмент (або інструменти) і процес (або процеси) враховують безпеку, цілісність і доступність інформації.

Безпека та цифрові парламенти

Як свідчить низка інцидентів у Південній Африці, перехід роботи парламенту в цифровий світ потребує уваги до кібербезпеки, щоб уникнути не лише втрати чи крадіжки конфіденційних даних, але й потенційного приниження, образи та шкоди репутації депутатів і співробітників парламенту. У травні 2020 року порнографічні зображення з'явилися за кілька хвилин до початку віртуального засідання Національних зборів країни. Після показу образливих зображень «хакер» або «зум-бомбардувальник» кинув сексистські та расові образи на адресу спікера асамблеї, яка вела сесію, змусивши перервати засідання. Подібний інцидент стався місяць тому, коли зустріч під головуванням міністра у справах жінок, молоді та людей з інвалідністю була зірвана порнографічними зображеннями.

ДИСТАНЦІЙНІ ПЛЕНАРНІ ЗАСІДАННЯ ТА ЗАСІДАННЯ КОМІТЕТІВ

Головними серед цих процесів є пленарні засідання та засідання комітетів. Ці сесії та дискусії, рішення та голосування, які відбуваються під час них, є основою більшої частини роботи вашого парламенту і тому можуть стати особливою мішенню для зловмисників. У сучасному світі такі зустрічі та зустрічі та засідання відбуваються в різних форматах залежно від контексту вашої країни, як особисто, повністю онлайн, так і «гібридним» способом.

Як зазначено в нещодавньому посібнику «**Реагування парламентів на пандемію**» Партнерства з питань демократії Палати представників, типова структура парламентських дебатів відрізняється від звичайної дискусії на конференції чи стандартної організаційної зустрічі. Потреби у дистанційному голосуванні, поданні офіційних пропозицій і поправок, структурованих дебатах і навіть синхронному перекладі для забезпечення включення всіх виборців часто вимагають додаткових функцій, яких немає в більшості стандартних технологічних рішень. У результаті під час розміщення віртуальної чи гібридної сесії парламенту, ймовірно, знадобиться розробити індивідуальне програмне забезпечення або придбати дорогі корпоративні рішення (наприклад, **Webex Legislate** від Cisco), розроблені спеціально для керування парламентськими сесіями. віддалено. Який би варіант не вибрав ваш парламент, важливо подумати, як зазначено в посібнику «**Реагування парламентів на пандемію**», про те, як усі депутати та співробітники зможуть отримати доступ до такої системи. Також важливо забезпечити належну безпеку такої системи.

Розробляючи та впроваджуючи технічні рішення для парламентських сесій, важливо забезпечити наявність основ безпеки. Вони включають кроки для забезпечення безпеки даних у стані спокою в самій системі, правильного шифрування під час передачі та того, що лише авторизовані користувачі можуть отримати доступ до системи. Існує багато підходів, які можна використати для забезпечення такої безпеки, включаючи багато основних принципів, викладених у решті цього Підручника. Наскрізне шифрування в будь-яких використовуваних системах обміну даними та зв'язку, вимоги до надійного пароля та двофакторної автентифікації та/або обмеження доступу користувачів до таких систем за IP-адресами (якщо вони не призначені для загального доступу), вимога віртуальних приватних мереж (про які йтиметься далі в посібнику), а також обмеження доступу лише довіреним чистим пристроям — усе це корисні кроки.

ДИСТАНЦІЙНЕ ГОЛОСУВАННЯ

Потреба в надійній безпеці є, мабуть, найважливішою при роботі з дистанційним голосуванням. Як підкреслюється у вищезазначеному посібнику «**Реагування парламентів на пандемію**», депутати обираються до парламенту з конкретною метою голосування від імені своїх виборців. Здатність довіряти цим голосам і перевіряти їх є вирішальною не лише для функціонування вашого парламенту, а й для демократичної системи в цілому. Такі голоси відносно легко перевірити, коли депутат голосує особисто, але під час віртуальної участі технічна автентифікація стає більш складним завданням, яке вимагає значної уваги та зосередженості. Як зазначено в **свідченнях** експертів, наданих Постійному комітету Палати громад Канади з процедур і справ Палати громад, парламенти зазвичай обирають один із чотирьох варіантів дистанційного голосування:

- Голосування електронною поштою: учасники отримують електронний бюлетень для голосування та подають свій голос електронною поштою. Цей варіант зазвичай вважається небезпечним, частково через відсутність наскрізного шифрування, тому його слід уникати.
- Веб-голосування: учасники отримують доступ і голосують через веб-сайт на комп'ютері чи мобільному телефоні. Цей підхід потребує інвестицій у захищену інфраструктуру, включаючи захищені пристрої з надійними засобами контролю автентифікації, як зазначено вище.
- Голосування за допомогою програми: учасники завантажують програму для доступу та голосування. Подібно до веб-голосування, але використовує спеціальну програму, яку можна завантажити на телефон або планшет, а не через браузер.
- Відеоголосування: учасники голосують на екрані підняттям рук або голосом. Для неанонімного голосування це може бути найменш технічно складним і найменш технічно складним для налаштування та захисту. Однак для цього все ще потрібні надійні системи шифрування та автентифікації, щоб уникнути уособлення або переривання під час сеансів голосування.

Незалежно від того, який варіант дистанційного голосування ваш парламент вибере — якщо він взагалі використовує дистанційне голосування — важливо також розглянути основи кібербезпеки протягом усього процесу голосування. Такі основи включають гарантію, що пристрої, які депутати використовують для голосування, належним чином фізично захищені та вільні від зловмисного програмного забезпечення, що доступ депутатів до Інтернету є належним чином захищеним під час голосування (а також під час ведення інших парламентських справ), і що депутати мають

стабільне підключення до Інтернету та можуть голосувати, коли їх покличуть. Як зазначено в посібнику «Реагування парламентів на пандемію», при прийнятті дистанційного голосування існує потреба в ретельному тестуванні системи, перш ніж вона буде запущена, а також необхідно забезпечити підтримку та навчання депутатів, щоб вони могли ефективно використовувати систему. Важливо пам'ятати, що частиною безпеки є *доступність*. Зокрема, необхідно забезпечити, щоб жінки-депутатки та співробітниці могли безпечно використовувати онлайн-системи, включаючи дистанційне голосування, і мати доступ до технологій для цього. Коли жінки, особливо обрані жінки, виходять в Інтернет, вони стикаються з більшим рівнем залякування та переслідувань, і цей фактор слід враховувати під час розробки та використання таких технологій, як дистанційне голосування, щоб гарантувати, що всі депутати зможуть ефективно виконувати свої функції. Крім того, надзвичайно важливо забезпечити адекватний віддалений багатомовний доступ у країнах, де депутати та співробітники розмовляють кількома офіційними мовами.

ПОСТАЧАЛЬНИК ПОСЛУГ ЕЛЕКТРОННОГО ПАРЛАМЕНТУ ТА БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Будь-яке програмне забезпечення, яке ви купуєте, незалежно від того, чи воно використовується для дистанційного голосування чи для більш широкого спектру парламентських потреб**, має надходити з надійного та акредитованого джерела, пройти перевірку безпеки незалежними групами та отримати відповідні сертифікати.** Важливо пам'ятати, що розробники програмного забезпечення, ті, кого ви найняли для створення програми чи інструменту, самі не завжди є експертами з безпеки. Тому залучення експертів із безпеки для перевірки програми на наявність потенційних прогалин у безпеці за допомогою аудиту має вирішальне значення для зменшення ризику того, що вашу платформу, інструмент або програму можуть зламати чи зламати. Навіть найкращі розробники програмного забезпечення роблять помилки без другого (або третього) експертного огляду, який перевіряє їхню роботу!

Дистанційне голосування в світі

Різні парламенти запровадили системи дистанційного голосування і, роблячи це, вжили значних заходів для забезпечення безпеки та цілісності голосів депутатів. Одним із елементів цього процесу, серед інших, згаданих вище, є забезпечення належної автентифікації. Кілька прикладів стосуються палати громад Великої Британії, де депутати використовують процес єдиного входу для входу в свої парламентські облікові записи перед голосуванням, що вимагає використання пароля на певному призначеному пристрої. В Іспанії депутатам призначаються персональні коди, які необхідно ввести через додаток для смартфона, перш ніж голосування можна записати дистанційно. У Чилі сенатори, які голосують дистанційно за допомогою ретельно розробленої програми дистанційного голосування палати має бути видно на екрані, щоб проголосувати.

Безпечне зберігання даних

Для більшості парламентів одним із найважливіших рішень є те, де зберігати свої дані.

Де «безпечніше» зберігати дані: на комп'ютерах співробітників, на локальному сервері, на зовнішніх пристроях зберігання чи в хмарному сховищі? У 99 % ситуацій найпростішим і найбезпечнішим варіантом є зберігання даних у надійних хмарних службах зберігання. Можливо, найпоширенішими прикладами є Microsoft 365 і Google Drive. Без комплексного плану хмарного сховища дані вашої організації, ймовірно, зберігаються в різних місцях, зокрема на комп'ютерах співробітників, на зовнішніх жорстких дисках і навіть на локальних серверах. Хоча можна захистити дані на всіх цих пристроях, дуже важко зробити це успішно, не витрачаючи багато грошей і не наймаючи значної кількості IT-персоналу.

Зберігання даних і парламенти

Поява доступного (іноді безкоштовного) хмарного сховища даних спростила (і захищала) життя багатьох парламентів та інших організацій. На жаль, багато хто все ще намагається розмістити власні сервери з відносно обмеженим IT-бюджетом, кадрами та підтримкою. У березні 2021 року загроза такій організаційній інфраструктурі стала реальністю для десятки тисяч організацій у всьому світі, коли пов'язаний із китайським урядом хакер на ім'я Гафніум ініціював глобальну кібербезпекову катастрофу за допомогою цілеспрямованої атаки на резидентні сервери Microsoft Exchange. Атака скомпрометувала локальні сервери, включно з сервером парламенту Норвегії, дозволивши хакерам отримати доступ до облікових записів електронної пошти парламенту, встановити додаткове шкідливе програмне забезпечення на серверах жертви та підключених системах і, зрештою, **отримати конфіденційні дані**. Хоча корпорація Microsoft швидко опублікувала оновлення та інструкції щодо виявлення та видалення потенційних зловмисних програм після оприлюднення інформації про злом, багатьом організаціям не вистачило IT-потенціалу для швидкого застосування таких оновлень, через що вони залишалися незахищеними протягом тривалого часу. Масштаби та вплив цього глобального злому свідчать про те, наскільки небезпечним для громадських організацій є вибір резидентних серверів для розміщення електронної пошти та інших типів конфіденційних даних, особливо без значних інвестицій у спеціалізований персонал із кібербезпеки.

ПЕРЕВАГИ ХМАРНОГО СХОВИЩА

Навіть якщо ви вживаєте всіх належних заходів для захисту своїх комп'ютерів від шкідливих програм і фізичної крадіжки, рішучий зловмисник все одно може зламати ваш комп'ютер або локальний сервер. Набагато важче зламати захист безпеки від таких фірм, як Google або Microsoft. Компанії, що надають надійні хмарні сховища, мають неперевершені ресурси безпеки та сильну комерційну мотивацію надавати максимальну безпеку своїм користувачам. Отже, стратегію надійного хмарного зберігання буде набагато легше реалізувати та підтримувати з часом. Тож замість того, щоб намагатися визначити (і зберегти) кількість спеціального та висококваліфікованого персоналу з кібербезпеки, необхідного для захисту локальних серверів у вашому парламенті, зосередьте свою енергію на кількох простіших завданнях. До них належать вибір правильного варіанта хмарного сховища для ваших потреб у конфіденційності та локалізації даних, впровадження надійної безпеки облікового запису, навчання співробітників належному спільному (і не спільному) папкам і документам (загалом, ви повинні налаштувати папки на своєму хмарному накопичувачі, які обмежують доступ лише до тих співробітників, яким це потрібно для певних файлів), а також регулярний аудит вашої системи, щоб переконатися, що співробітники та учасники не надають надмірного доступу до будь-яких файлів (наприклад, увімкнувши універсальний спільний доступ за посиланнями для файлів, який замість цього слід обмежити лише кілька людей). Зберігання основної частини вашої інформації в хмарному середовищі допоможе подолати низку поширених ризиків. Хтось залишив комп'ютер у ресторані чи телефон в автобусі? Дитина перекинула склянку соку на вашу клавіатуру, через що пристрій не працює? Чи потрібно вам відокремлювати дані, які належать самому депутату, від інформації, яку вона створює для самого парламенту? У співробітника виявилася шкідлива програма і йому потрібно стерти дані з комп'ютера та почати все заново? Якщо більшість документів і даних зберігаються в хмарі, їх легко повторно синхронізувати та почати заново на очищеному чи новому комп'ютері. Крім того, якщо шкідлива програма потрапляє на комп'ютер або якщо злодій сканує жорсткий диск, нема чого красти, якщо доступ до більшості документів здійснюється через вебоглядач.

ЧИ СПРАВДІ МИ МОЖЕМО ДОВІРЯТИ ХМАРНОМУ СХОВИЩУ?

Загалом, у хмарному сховищі немає нічого ненадійного. Як згадувалося вище, більшість великих постачальників хмарних сховищ мають команди найкращих у світі інженерів безпеки, які щодня працюють над захистом їхніх продуктів і пропонують своїм клієнтам підтримку безпеки, що перевищує те, що більшість малих IT-відділів можуть надати самостійно. Однак майте на увазі, що традиційні хмарні служби зберігання зазвичай вимагають надання доступу до конфіденційних даних сторонній компанії, яка надає послуги. **Зважаючи на це, кожен окремий парламент матиме свої власні політичні міркування та юридичні вимоги (наприклад, повноваження щодо локалізації даних), які необхідно враховувати, коли вирішуватиме, чи можна йому довіряти певному постачальнику хмарних сховищ і використовувати його.**

ЯКОГО ПОСТАЧАЛЬНИКА ХМАРНОГО СХОВИЩА ВИБРАТИ?

Якщо вашому парламенту не потрібно розглядати вимоги щодо локалізації даних і немає проблем із наданням доступу до даних надійною сторонньою компанією, двома найпопулярнішими варіантами хмарного сховища є Google Workspace (раніше відомий як GSuite) і Microsoft 365. Якщо ваш парламент уже використовує Gmail, зареєструватися в Google Workspace і зберігати дані на Google Drive за допомогою вбудованих програм Google Docs, Sheets і Slides для обробки текстів, електронних таблиць і презентацій має великий сенс. Так само, якщо ваш парламент покладається на Excel і Word, простим вибором буде зареєструватися в Microsoft 365, який надає доступ до Outlook для електронної пошти та ліцензованих версій Microsoft Word, Excel, PowerPoint і Teams.

ЩО РОБИТИ, ЯКЩО НАМ ПОТРІБНО КОНТРОЛЮВАТИ ВЛАСНІ ДАНІ АБО ДОТРИМУВАТИСЯ ЗАКОНІВ ПРО ЛОКАЛІЗАЦІЮ ДАНИХ?

Для багатьох парламентів такий простий варіант може бути неможливим з огляду на вимоги локалізації даних або конкретні очікування, які вимагають виключного парламентського контролю над власними даними. Хороша новина полягає в тому, що нещодавно постачальники безпечних хмарних сховищ розробили варіанти, які дозволяють корпоративним клієнтам або вибирати розташування своїх даних (зауважте, що наразі це здебільшого обмежено європейськими клієнтами), або контролювати власні ключі шифрування. **На практиці це означає, що ваш парламент має можливість контролювати власні дані, водночас користуючись перевагами інфраструктури та безпеки хмарного сховища.**

Якщо ваш парламент наразі використовує або зацікавлений у Google Workspace для хмарного зберігання та обміну даними, Google представив функцію, яка вмикає **шифрування на стороні клієнта** для організацій Enterprise Plus. Хоча ця функція наразі перебуває на стадії тестування та доступна лише для найдорожчих тарифних планів Google Workspace, вона дає змогу скористатися всіма перевагами повного набору функцій зберігання та обміну даними Google Диска, а також вбудованих у них функцій безпеки, обмежуючи при цьому можливість Google отримати доступ до конфіденційної або приватної інформації вашого парламенту. За допомогою шифрування на стороні клієнта ви можете вибрати інтеграцію додаткової служби керування ключами, як-от Virtru, і дозволити користувачам керувати своїми власними ключами шифрування, не дозволяючи доступу до самої Google. Така послуга вимагає від усіх ретельного захисту цих ключів, щоб належним чином захистити доступ до будь-якої системи керування ключами, яку ви вирішите інтегрувати в Google Workspace. Адміністратори облікових записів можуть дізнатися більше про те, як увімкнути шифрування на стороні клієнта на **сторінці підтримки** в Google Workspace.

Якщо ваш парламент наразі використовує або зацікавлений у Microsoft 365 для хмарного зберігання та обміну даними, він пропонує трохи складніший, але добре відомий варіант керування вашими власними ключами шифрування, відомий як **Microsoft 365 Double Key Encryption**. Для цього параметра безпеки потрібен **Microsoft 365 E5**, але він дозволяє контролювати будь-які конфіденційні чи приватні парламентські дані та обмежити доступ навіть до самої Microsoft.

Tresorit — це ще один варіант, який простіше реалізувати, якщо ваш парламент стурбований тим, щоб сторонні особи мали доступ до вашої внутрішньої інформації. Tresorit забезпечує наскрізне шифрування для хмарного зберігання та обміну файлами, а також пропонує ряд **параметри резидентності даних**.

ЩО РОБИТИ, ЯКЩО МИ НЕ МОЖЕМО ДОВІРЯТИ ЖОДНОМУ ХМАРНОМУ СХОВИЩУ?

Якщо ви все-таки вирішите діяти самостійно та покладатися на локальні сервери для зберігання даних вашого парламенту, надзвичайно важливо, щоб ви інвестували значний час і ресурси в посилення цифрового захисту пристроїв вашого парламенту та переконалися, що такі сервери належним чином налаштовані, зашифровані та і зберігався у фізичній безпеці. Як зазначалося вище, такий підхід вимагає визначення, найму та утримання певної кількості спеціального та висококваліфікованого персоналу з кібербезпеки для підтримки безпеки вашої локальної серверної інфраструктури.

Підвищення безпеки облікових записів у хмарі парламенту

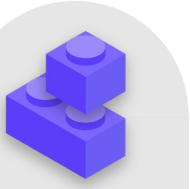
Якщо ваш парламент вирішить налаштувати домен у Google Workspace або Microsoft 365, майте на увазі, що обидві компанії пропонують вищий рівень безпеки для облікових записів, які знаходяться під загрозою. **Програма розширеного захисту від Google** і **AccountGuard від Microsoft** забезпечують ще більш надійний захист хмарних облікових записів відповідних організацій і допомагають значно зменшити ймовірність ефективного фішингу та зламу облікового запису. Якщо ви вважаєте, що ваш парламент відповідає вимогам, і зацікавлені в тому, щоб залучити депутатів і співробітників до будь-якого плану, відвідайте веб-сайти, посилання на які наведені вище, або зв'яжіться з **cyberhandbook@ndi.org** для отримання додаткової допомоги.

РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ

Незалежно від того, чи ваш парламент зберігає дані на фізичних пристроях і серверах чи в хмарі, важливо мати резервну копію. Майте на увазі, особливо якщо ви використовуєте фізичне сховище на пристрої, дуже легко втратити доступ до даних. Ви можете пролити каву на свій комп'ютер і знищити жорсткий диск. Комп'ютери співробітників можуть бути зламані, а локальні файли заблоковані за допомогою програми-вимагача. Співробітник може забути пристрій у поїзді або його можуть викрасти разом із портфелем. Як згадувалося вище, це ще одна перевага використання хмарного сховища: воно не прив'язане до певного пристрою, який можна заразити, втратити чи вкрасти. Комп'ютери Mac оснащені вбудованим програмним забезпеченням резервного копіювання під назвою **Time Machine**, який використовується разом із зовнішнім накопичувачем; у пристроях із Windows **File History** виконує аналогічні функції.Пристрої iPhone та Android можуть

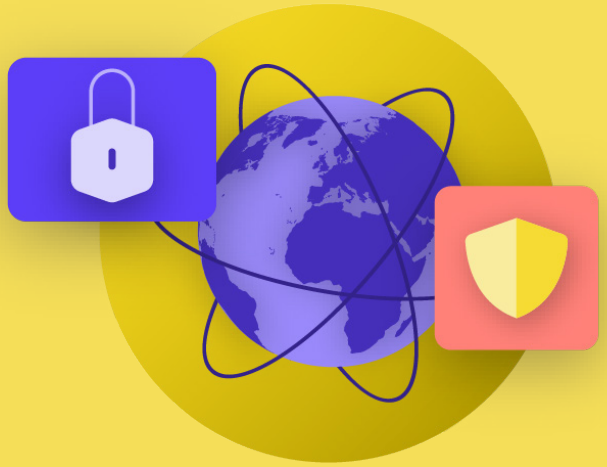
автоматично створювати резервні копії найважливішого вмісту в хмарі, якщо це ввімкнено в налаштуваннях телефону. Якщо ваша організація використовує хмарне сховище (наприклад, Google Диск), ризик того, що Google буде виведено з ладу або ваші дані знищено в результаті аварії, досить низький, але залишається можливість помилки з боку людини (наприклад, випадкове видалення важливих файлів). Може бути корисним розглянути варіанти хмарного рішення для резервного копіювання даних, як-от Backupify або SpinOne Backup.

Якщо дані зберігаються на локальному сервері та/або локальних пристроях, безпечне резервне копіювання стає ще важливішим. Ви можете створити резервну копію даних свого парламенту на зовнішній жорсткий диск або серію дисків, але обов'язково зашифруйте такі диски надійним паролем. Time Machine може зашифрувати жорсткі диски для вас, або ви можете використовувати надійні засоби шифрування всього жорсткого диска, як-от VeraCrypt або BitLocker. Зберігайте пристрої для резервного копіювання окремо від інших пристроїв і файлів. Пам'ятайте, що пожежа, що знищить ваші комп'ютери та їхні резервні копії, означатиме, що у вас взагалі не залишиться резервних копій. Зберігайте копію в надійному місці, наприклад, у сейфі.



Безпечне зберігання даних

- **Зберігайте конфіденційні дані виключно в надійній службі хмарного зберігання.**
  - Переконайтеся, що всі підключені облікові записи, що використовуються для доступу до такої служби, мають надійні паролі та 2FA.
- **Установіть і застосуйте політику обмеження спільного доступу до файлів у хмарному сховищі.**
  - Навчіть усіх депутатів і співробітників тому, як правильно надавати спільний доступ (а не надсилати) документи.
- **Якщо ваш парламент вирішує зберігати дані локально, інвестуйте в кваліфікованого IT-персоналу.**
- **Зберігайте резервні копії даних у безпеці — зашифруйте резервні копії жорстких дисків або інших резервних пристроїв.**



Безпека в інтернеті

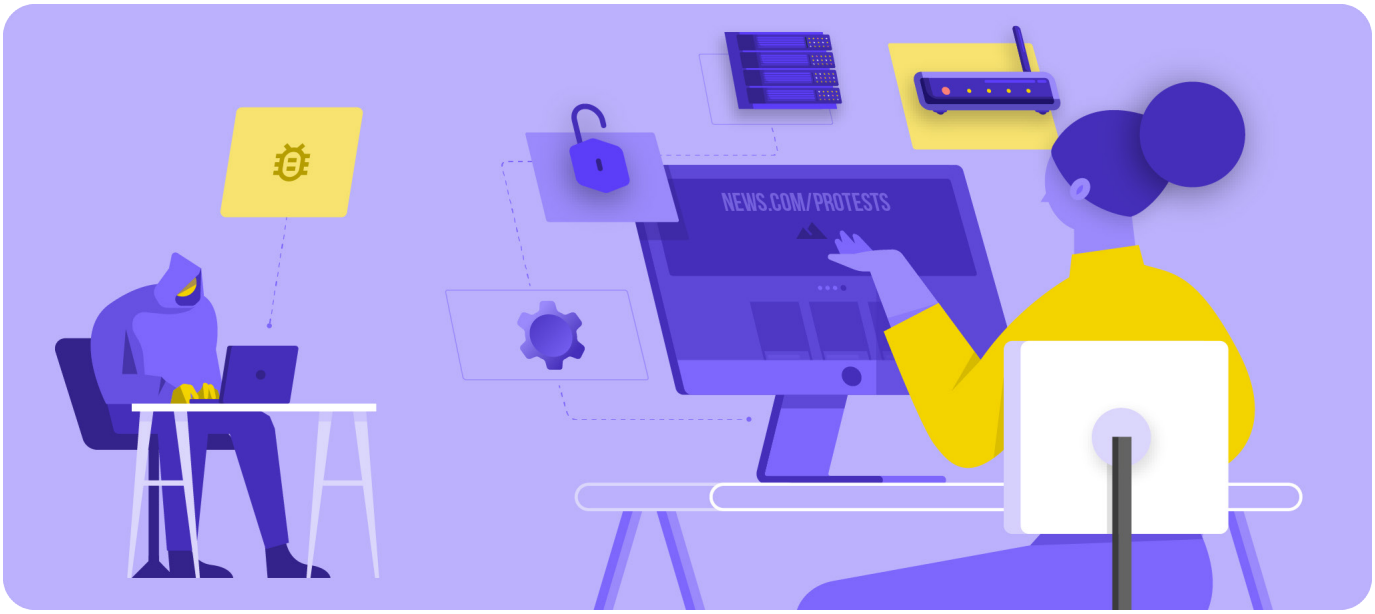
Під час користування Інтернетом на телефоні чи комп'ютері ваша діяльність може багато сказати про вас і вашу організацію.

Важливо тримати конфіденційну інформацію, як-от імена користувачів і паролі, які ви вводите на весайті, ваші публікації в соціальних мережах або, за певних обставин, навіть назви веб-сайтів, які ви відвідуєте, подалі від сторонніх очей. Блокування або обмеження доступу до певних веб-сайтів або програм також є поширеною проблемою. Ці дві проблеми — інтернет-стеження та інтернет-цензура — йдуть пліч-о-пліч, а стратегії їх подолання є схожими.

Безпечний перегляд вебсторінок

ВИКОРИСТАННЯ HTTPS

Найважливішим кроком до обмеження можливостей зловмисника стежити за вашою організацією в інтернеті є мінімізація обсягу доступної інформації про вас і вашу діяльність онлайн. Завжди перевіряйте, чи надійне підключення до веб-сайтів: переконайтеся, що URL-адреса (розташування) починається з «https», а маленький значок замка відображається в адресному рядку вебоглядача. Коли ви переглядаєте сторінки в інтернеті **без шифрування**, інформація, яку ви вводите на веб-сайті (наприклад, паролі, номери облікових записів або повідомлення), а також деталі сайту та сторінок, які ви відвідуєте, будуть відкритими. Це означає, що (1) хакери у вашій мережі, (2) ваш адміністратор мережі, (3) ваш інтернет-провайдер і будь-яка організація, з якою він обмінюється даними (наприклад, державні органи), (4) інтернет-провайдер веб-сайту, який ви відвідуєте, і будь-яка організація, з якою він обмінюється даними, і, звичайно, (5) сам веб-сайт, який ви відвідуєте, має доступ до великої кількості потенційно конфіденційної інформації.



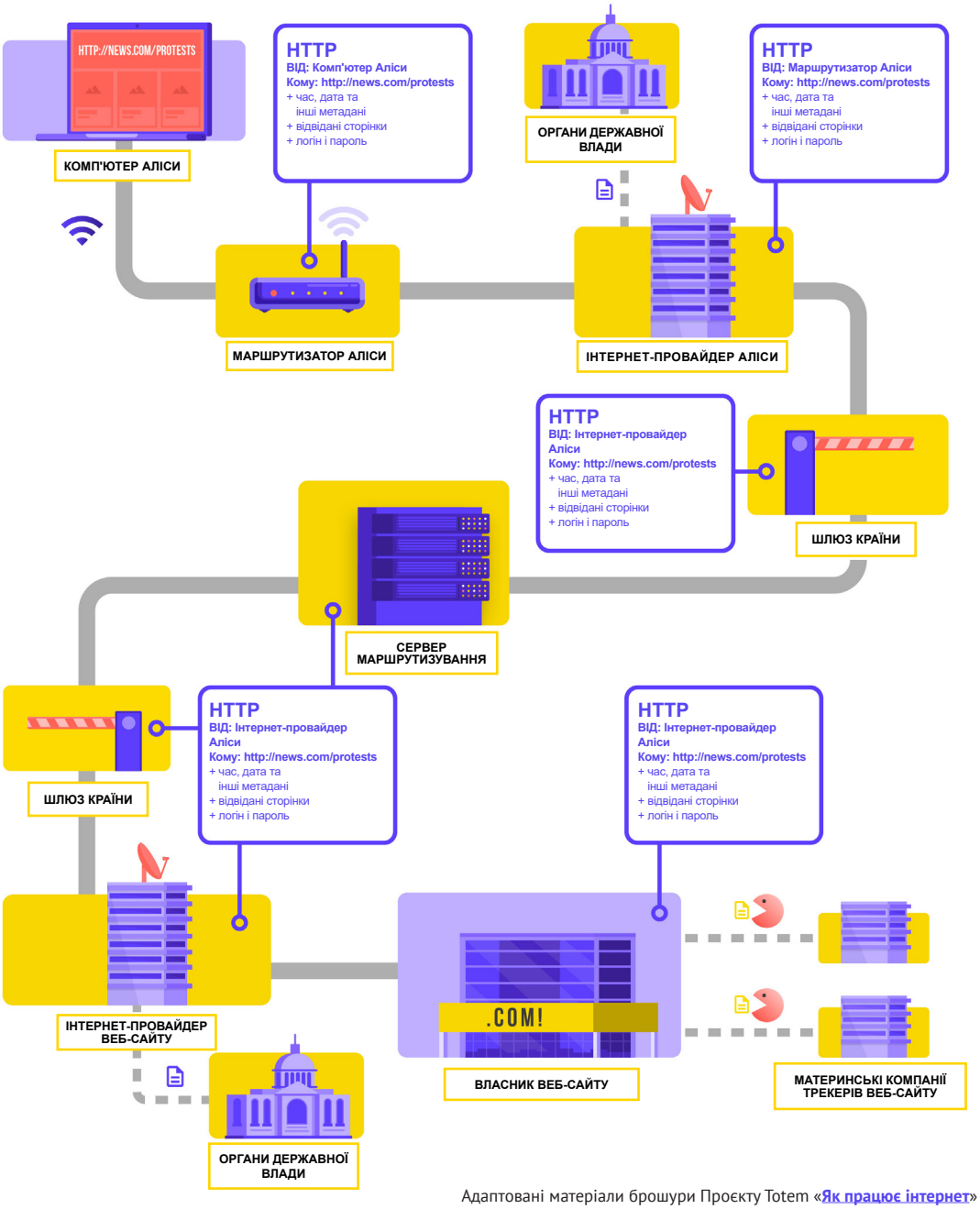
Нагляд, цензура та парламент

Недружні уряди та інші зловмисники використовують все більш доступні технології спостереження, а в деяких випадках і простий злом Wi-Fi, щоб контролювати онлайн-активність депутатів та інших працівників парламенту. Наприклад, хакери вкрали дані співробітників європейського парламенту та відвідувачів шляхом **підробки публічної мережі Wi-Fi парламенту** в 2013 році. Огляд набагато складніших атак за наступні роки буде наведений нижче.

Окрім викрадення інтернет-трафіку та крадіжки даних, зловмисники також порушують важливі парламентські процедури, блокуючи доступ до Інтернету та системи. У Брюсселі парламент Бельгії був виведений з ладу в результаті **масової атаки на відмову в обслуговуванні** в травні 2021 року. Атака змусила відкласти деякі дебати та засідання комітетів, оскільки користувачі не мали доступу до віртуальних сервісів, необхідних для участі в сесії.

Зростаюча частота таких атак на доступ до інформації та свободу інформації в інтернеті свідчить про те, наскільки важливо розуміти ризики роботи онлайн і розробляти плани щодо зв'язку, коли підключення до інтернету відсутнє.

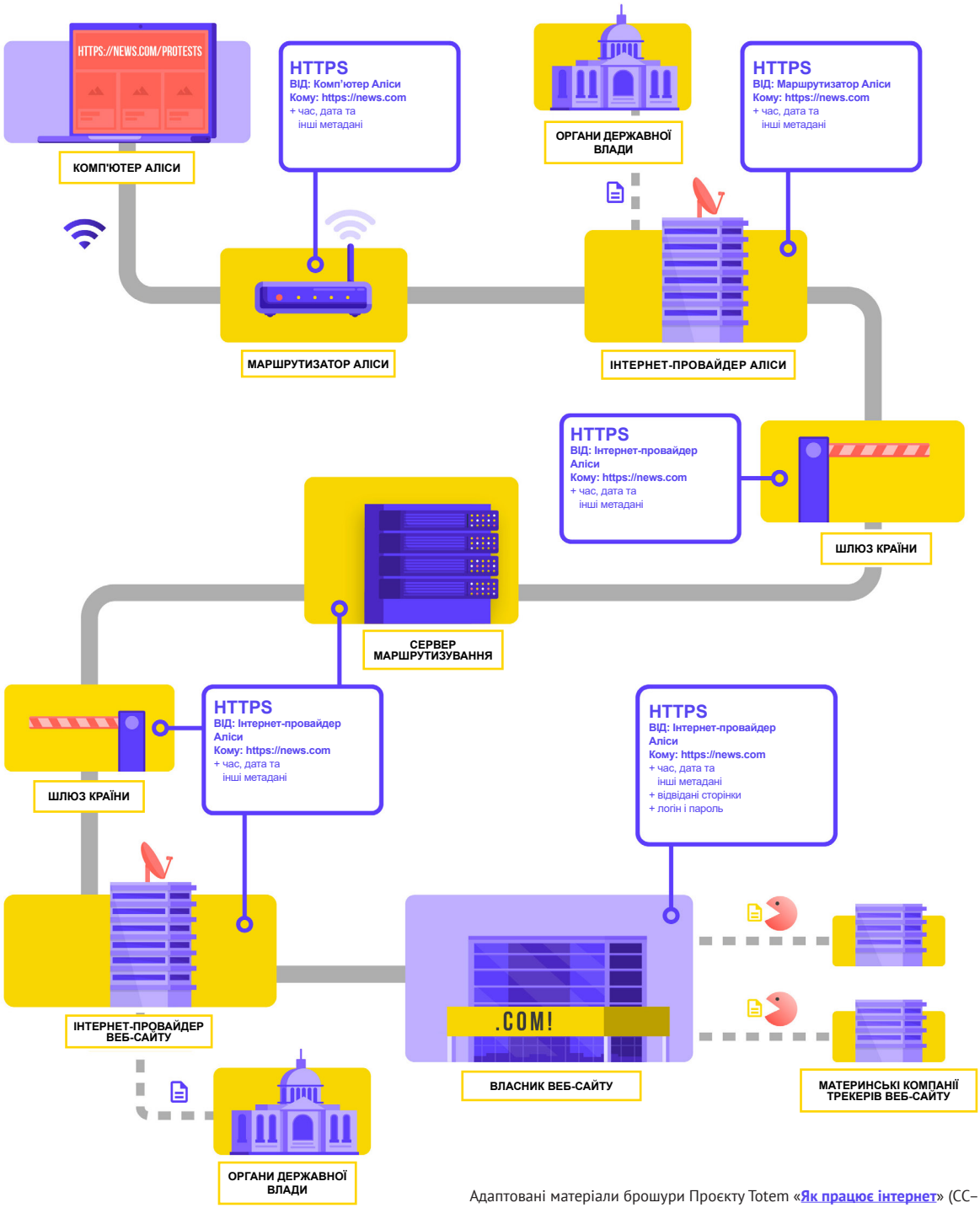
Розглянемо реальний приклад того, як виглядає перегляд вебсторінок без шифрування.



Адаптовані матеріали брошури Проєкту Totem «Як працює інтернет» (CC–BY–NC–SA)

Під час перегляду вебсторінок без шифрування всі ваші дані є відкритими. Як показано вище, зловмисник може бачити, де ви перебуваєте, що ви йдете на news.com, дивлячись конкретно на сторінку протестів у вашій країні, і, можливо, найголовніше, як депутат чи співробітник парламенту, він може бачити ваш пароль, який ви поділитися, щоб увійти на сам сайт. Така інформація в чужих руках не тільки розкриває ваш обліковий запис, але й дає потенційним зловмисникам, де б вони не були в світі, гарне уявлення про те, що ви робите або про що думаєте.

Використання **HTTPS («s» означає «безпечний») означає, що використовується шифрування.** Це надає вам набагато більший захист. Подивимося, як виглядає перегляд вебсторінок через HTTPS (тобто із шифруванням):



Завдяки HTTPS потенційний зловмисник більше не зможе побачити ваш пароль чи іншу конфіденційну інформацію, яку ви можете надавати веб-сайту. Однак він зможе бачити, які домени (наприклад, news.com) ви відвідуєте. І хоча HTTPS також шифрує інформацію про окремі сторінки сайту (наприклад, website.com/protests), які ви відвідуєте, досвідчені зловмисники можуть бачити цю інформацію, перевіряючи ваш інтернет-трафік. За умови використання HTTPS зловмисник може знати, що ви переходите на news.com, але він не зможе побачити ваш пароль, і йому буде важче (але не неможливо) побачити, що ви шукаєте інформацію про протести (до прикладу). Це важлива відмінність. Завжди перевіряйте наявність протоколу HTTPS, перш ніж переходити на веб-сайт або вводити конфіденційну інформацію. Ви також можете використовувати **розширення для вебоглядача HTTPS Everywhere**, щоб переконатися, що ви завжди використовуєте HTTPS, або, якщо ви користуєтеся Firefox, увімкніть **режим лише HTTPS** у вебоглядачі.

Якщо у вебоглядачі з'являється попередження про те, що веб-сайт може бути небезпечним, не ігноруйте його. Це означає, що щось не так. Це може бути нешкідливим, наприклад, у веб-сайта прострочений сертифікат безпеки, або сайт може бути зловмисно фальсифікований або підроблений. У будь-якому випадку важливо дослухатися попередження та не переходити на такий веб-сайт. HTTPS має важливе значення, а зашифрована DNS забезпечує додатковий захист від стеження та блокування сайтів, але якщо ваша організація стурбована цільовим стеженням за вашою діяльністю в інтернеті та стикається із цілеспрямованою онлайн-цензурою (наприклад, блокування веб-сайтів і програм), ви можете скористатися віртуальною приватною мережею (VPN), якій довіряєте.

Використання зашифрованої DNS

Якщо ви хочете ускладнити (але не унеможливити) для провайдера отримання інформації про веб-сайти, які ви відвідуєте, ви можете використовувати зашифровану DNS.

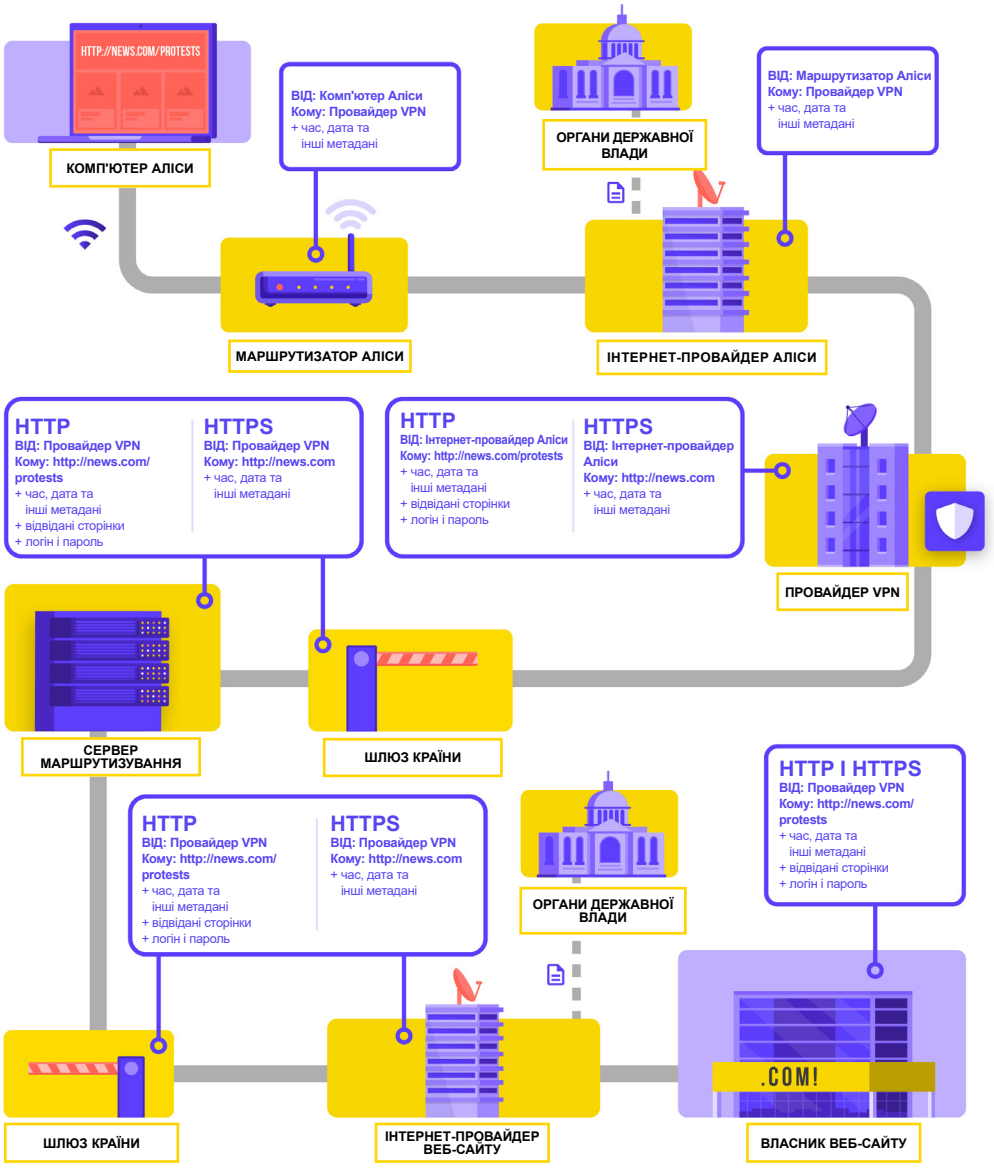
Якщо вам **цікаво знати**, DNS означає «Система доменних імен» (Domain Name System). По суті, це телефонна книга інтернету, яка перетворює зручні для людини доменні імена (наприклад, ndi.org) на адреси зручних для всесвітньої мережі інтернет-протоколів (IP). Завдяки цій системі люди використовують вебоглядачі для легкого пошуку та завантаження інтернет-ресурсів і відвідування веб-сайтів. Однак за замовчуванням DNS не зашифрована.

Щоб використовувати зашифровану DNS і ще більше захистити свій інтернет-трафік, скористайтеся простим варіантом: завантажте та ввімкніть додаток **Cloudflare 1.1.1.1** на вашому комп'ютері та мобільному пристрої. Інші параметри зашифрованої DNS, зокрема Google 8.8.8.8, доступні, але потребують **більше технічних кроків** для налаштування. Якщо ви використовуєте браузер Firefox, зашифрована DNS увімкнена в ньому за замовчуванням. Користувачі браузерів Chrome і Edge можуть **увімкнути зашифровану DNS** за допомогою розширених налаштувань безпеки вебоглядача, увімкнувши «використовувати безпечну DNS» і вибравши «3: Cloudflare (1.1.1.1)» або постачальника на вибір.

Cloudflare 1.1.1.1 із WARP шифрує вашу DNS і дані перегляду вебсторінок за допомогою послуги, подібної до традиційної VPN. Хоча WARP не повністю приховує ваше місцезнаходження від усіх веб-сайтів, які ви відвідуєте, ця проста у використанні функція може допомогти співробітникам вашої організації скористатися перевагами зашифрованої DNS і додаткового захисту від вашого інтернет-провайдера в ситуаціях, коли повна VPN не функціонує або у ній немає потреби з огляду на контекст загроз. У версії 1.1.1.1 із розширеними налаштуваннями DNS WARP співробітники також можуть увімкнути 1.1.1.1 для Сімей, щоб забезпечити додатковий захист від шкідливих програм під час доступу до інтернету.

ЩО ТАКЕ VPN?

VPN — це, по суті, тунель, який захищає ваш інтернет-трафік від стеження та блокування з боку хакерів у вашій мережі, адміністратора мережі, інтернет-провайдера та будь-кого, з ким вони можуть обмінюватися даними. У великих організаціях, таких як парламент, «ділові» або «корпоративні» мережі VPN також часто використовуються, щоб допомогти захистити цілісність доступу до внутрішніх систем і програм (таких як ті, що використовуються для віддаленого голосування). Незалежно від того, чи використовується персональна мережа VPN чи призначена для комерційних цілей, концепція захисту вашого інтернет-трафіку від стеження загалом працює однаково, і важливо продовжувати використовувати HTTPS (навіть за наявності VPN). Також важливо переконатися, що ви довіряєте VPN, який використовує ваш парламент. Ось приклад того, як виглядає перегляд вебсторінок за допомогою VPN:



Детальний опис VPN міститься у Посібнику із самозахисту від спостереження від EFF, матеріали з якого використані в цьому розділі.

Традиційні VPN створені для маскування вашої фактичної мережевої IP-адреси та створення зашифрованого тунелю для інтернет-трафіку між вашим комп'ютером (чи телефоном або будь-яким «розумним» пристроєм, що має доступ до мережі) і сервером VPN. Оскільки трафік у тунелі шифрується та надсилається до вашої VPN, третім сторонам, як-от провайдерам чи хакерам у загальнодоступній мережі Wi-Fi, набагато важче відстежувати, змінювати чи блокувати ваш трафік. Пройшовши через тунель від вас до VPN, ваш трафік потім залишає VPN і переходить до свого кінцевого пункту призначення, маскуючи вашу початкову IP-адресу. Це допомагає приховати ваше фізичне місцезнаходження для тих, хто спостерігає трафік після того, як він покине мережу VPN. Це забезпечує більшу конфіденційність і безпеку, але використання VPN не робить вас повністю анонімними в інтернеті: ваш трафік усе одно буде видно оператору VPN. Ваш інтернет-провайдер також знатиме, що ви використовуєте VPN, що може підвищити ваш профіль ризику.

Це означає, що **важливо вибрати надійного постачальника VPN**. У деяких місцях, наприклад в Ірані, вороже налаштовані уряди фактично створили власні VPN, щоб мати можливість відстежувати, що роблять громадяни. Щоб знайти VPN, який підходить для вашої організації та її співробітників, ви можете оцінити VPN на основі її бізнес-моделі та репутації, які дані вона збирає, а які ні, і, звичайно, безпеку самого інструменту.

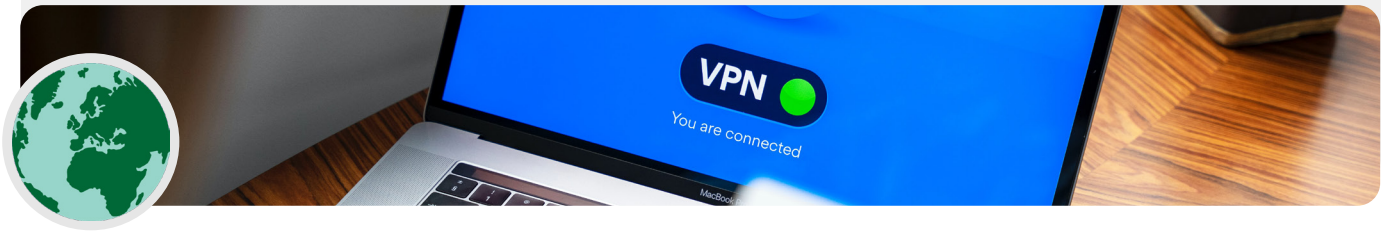
Чому би просто не скористатися безкоштовною VPN? Коротка відповідь полягає в тому, що більшість безкоштовних VPN, включно з тими, які попередньо встановлені на деяких смартфонах, мають значний прихований недолік. Як і всі компанії та постачальники послуг, мережі VPN повинні якимось чином фінансуватися. Якщо послуги VPN безкоштовні, за рахунок чого фінансується цей бізнес? За пожертви? Чи стягується плата за послуги преміум-класу? Її підтримують благодійні організації чи спонсори? На жаль, багато безкоштовних VPN заробляють гроші, збираючи та продаючи ваші дані.

Найкращий вибір — це провайдер VPN, який не збирає дані. Якщо дані не збираються, їх не можна продати або передати уряду на його запит. Переглядаючи політику конфіденційності постачальника VPN, перевірте, чи VPN збирає дані користувачів. Якщо явно не вказано, що дані підключення користувача не реєструються, швидше за все, що дані збираються. Навіть якщо компанія стверджує, що не веде журналів із даними підключення, це не завжди може бути гарантією сумлінної поведінки.

Варто дізнатися про компанію, яка стоїть за VPN. Чи схвалюють цю мережу незалежні фахівці з безпеки? Чи є про цю VPN статті? Чи було коли-небудь цю мережу спіймано на тому, що вона вводила в оману або брехала своїм клієнтам? Якщо мережа VPN була створена людьми, відомими у колах інформаційної безпеки, вона, швидше за все, заслуговує довіри. Ставтеся обережно до VPN, що пропонує послугу, на яку немає професійних відгуків, або до такої, якою керує компанія, про яку ніхто не знає.

Підробки VPN у реальному світі

Наприкінці 2017 року, після сплеску протестів у країні, іранці відкрили для себе «безкоштовну» (але підроблену) версію популярної VPN, якою ділилися через текстові повідомлення. Безкоштовна VPN, яка насправді не діяла, обіцяла надати доступ до Telegram, який на той момент був заблокований на місцевому рівні. На жаль, підроблений додаток був не чим іншим, як шкідливою програмою, що дозволяла владі відстежувати переміщення та стежити за спілкуванням тих, хто його завантажив.



Отже, який VPN слід використовувати?

Якщо окрім забезпечення безпеки парламентського інтернет-трафіку вам також потрібне рішення для безпечного обмеження доступу лише для тих, хто у вашій парламентській мережі (навіть під час віддаленої роботи), до внутрішніх парламентських систем і програм, ви можете запровадити «ділову» або «корпоративну» VPN. Існує низка варіантів із використанням різних технологій, які ви можете розглянути, зокрема **AnyConnect** від Cisco, **Global Protect** від PaloAlto або **Access** від Cloudflare (технічно система доступу з нульовою довірою, а не VPN), і це лише деякі з них. У будь-якому випадку такі системи потребують кваліфікованого IT-персоналу для впровадження та ефективного керування.

Якщо просунута «корпоративна» система VPN надто дорога або надто складна для вашого парламенту, ви також можете розглянути можливість використання особистих варіантів VPN, як-от **ProtonVPN** або **TunnelBear** (який також пропонує план Teams для спрощення керування обліковими записами) для всіх депутатів парламенту та співробітників. Ще один варіант — налаштувати власний сервер за допомогою **Outline** від Jigsaw. У цьому випадку немає компанії, що керуватиме вашим обліковим записом, але натомість ви повинні налаштувати власний сервер.

Хоча більшість сучасних VPN покращили продуктивність і швидкість, варто пам'ятати, що використання VPN може сповільнити швидкість перегляду вебсторінок, якщо ви перебуваєте в мережі з дуже низькою пропускною здатністю, у вашій мережі бувають значні затримки або трапляються періодичні збої доступу до інтернету. Якщо ви користуєтеся швидкою мережею, слід постійно використовувати VPN за замовчуванням.

Якщо ви рекомендуєте співробітникам використовувати VPN, важливо також переконатися, що співробітники залишають VPN увімкненим. Це може здатися очевидним, але VPN, що встановлений, але не працює, не надає жодного захисту.

Анонімність через Tor

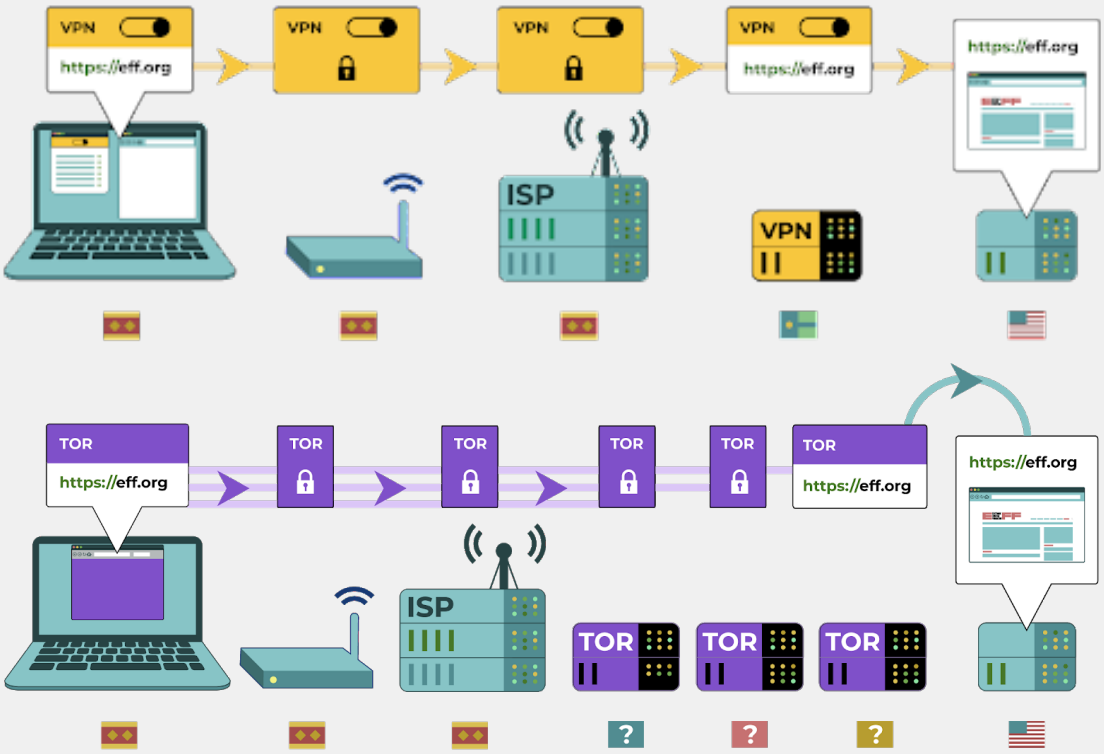
На додачу до VPN, ви, можливо, чули про Tor як ще один інструмент для безпечного користування інтернетом. Важливо розуміти, що таке обидва, і чому ви можете використовувати те чи інше.

Tor — це протокол для анонімної передачі даних через інтернет шляхом маршрутизації повідомлень або даних через децентралізовану мережу. Ви можете дізнатися більше про те, як працює Tor, **тут**, але коротко кажучи, він направляє ваш трафік через кілька точок на шляху до місця призначення таким чином, щоб жодна точка не мала достатньо інформації, що вказує, хто ви є та що ви робите в інтернеті.

Tor відрізняється від VPN у кількох аспектах. Основна відмінність полягає в тому, що він не покладається сліпо на будь-яку конкретну точку (наприклад, провайдера VPN). На ілюстрації, розробленій EFF, показана різниця між традиційною VPN і Tor.

Найпростіший спосіб використовувати Tor — **через вебоглядач Tor**. Він працює як будь-який звичайний вебоглядач, за винятком того, що спрямовує ваш трафік через мережу Tor. Ви можете завантажити вебоглядач Tor на пристрої Windows, Mac, Linux або Android. Майте на увазі, що використовуючи вебоглядач Tor, ви захищаєте лише ту інформацію, до якої отримуєте доступ, **коли знаходитеся у браузері**. Він не забезпечує жодного захисту інших програм або завантажених файлів, які ви можете відкривати окремо на своєму пристрої. Також майте на увазі, що Tor не шифрує ваш трафік, тому, як і під час використання VPN, під час перегляду вебсторінок все одно важливо використовувати найкращі методи, такі як HTTPS.

Якщо ви бажаєте поширити захист анонімності Tor на весь комп'ютер, технічно обізнані користувачі можуть встановити Tor як загальносистемне підключення до інтернету або розглянути можливість використання операційної системи **Tails**, яка за замовчуванням



направляє весь трафік через Tor. Користувачі Android також можуть використовувати додаток Orbot для застосування Tor для всього інтернет-трафіку та програм на своєму пристрої. Незалежно від того, як ви використовуєте Tor, важливо знати, що під час його використання ваш постачальник інтернету не може бачити, які веб-сайти ви відвідуєте, але він «може» бачити, що ви використовуєте сам Tor. Подібно до використання VPN, це може значно підвищити профіль ризику вашої організації. Оскільки Tor не є дуже поширеним інструментом, він може зацікавити зловмисників, які можуть стежити за вашим інтернет-трафіком.

Отже, хоча існує дуже мало випадків, коли Tor буде необхідно використовувати в парламентському контексті, якщо ви або не можете дозволити собі надійну VPN, або ваш парламент працює в середовищі, де VPN регулярно блокуються, Tor може бути хорошим варіантом, якщо це законно, для обмеження впливу стеження та уникнення цензури в Інтернеті.

Чи є якісь причини, чому не слід використовувати VPN або Tor?

Окрім занепокоєння з приводу послуг VPN із поганою репутацією, треба розглянути, чи може використання VPN або Tor привернути небажану увагу або, у деяких регіонах, суперечити закону. Хоча ваш інтернет-провайдер не знатиме, які сайти ви відвідуєте під час використання цих служб, він може побачити, що ви підключені до Tor або VPN. Якщо це незаконно там, де ви працюєте, це може викликати підвищену увагу чи збільшити рівень ризику, ніж проста навігація в інтернеті за допомогою стандартного HTTPS і зашифрованого DNS, використання VPN і особливо Tor (що використовується набагато рідше, а тому може стати тривожним «дзвіночком») не буде правильним варіантом для вашої організації.

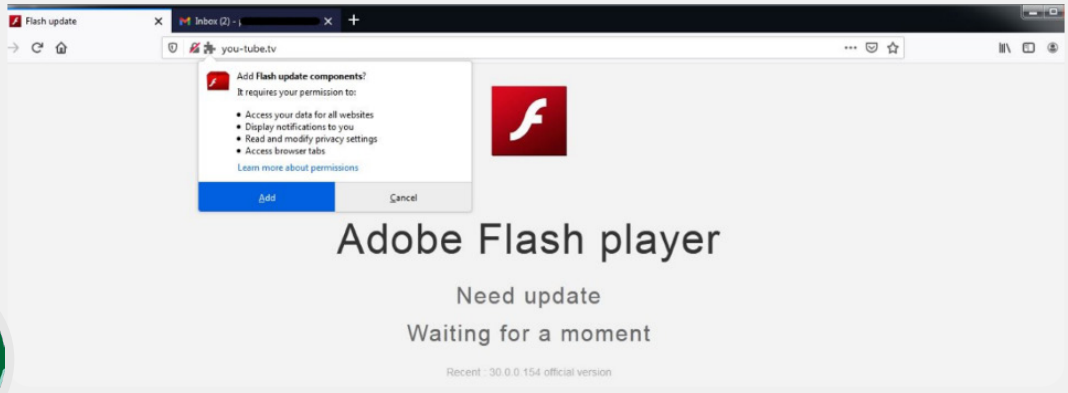
ЯКИЙ ВЕБОГЛЯДАЧ СЛІД ВИКОРИСТОВУВАТИ?

Використовуйте перевірений вебоглядач, наприклад Chrome, Firefox, Brave, Safari, Edge або Tor. І Chrome, і Firefox дуже широко використовуються та чудово забезпечують захист. Деякі люди віддають перевагу Firefox, зважаючи на його конфіденційність. У будь-якому випадку важливо перезавантажувати їх і комп'ютер відносно часто, щоб ваш вебоглядач регулярно оновлювався. Якщо вам цікаво порівняти функції вебоглядачів, перегляньте цей ресурс від Фонду свободи преси. Незалежно від вебоглядача також доцільно використовувати розширення чи додатки, як-от Privacy Badger, uBlock Origin або Privacy Essentials від DuckDuckGo що не дозволяє рекламодавцям та іншим стороннім трекерам відстежувати, які веб-сайти відвідуєте. Для перегляду вебсторінок розгляньте можливість переходу вебпошуку за умовчанням із Google на DuckDuckGo, Startpage або іншу пошукову систему із захистом конфіденційності. Такий перехід також допоможе обмежити рекламу та відстежувачі сторонніх розробників.

Безпека вебоглядача в реальному світі

Такі атаки з боку розширень або додатків для вебоглядачів можуть завдавати такої самої шкоди, що і шкідливі програми, які поширюються безпосередньо через фішингові завантаження чи інше програмне забезпечення. Наприклад, на початку 2021 року хитро розроблене шкідливе доповнення під назвою «Компоненти флеш-оновлення» було націлено на тибетські політичні організації. Доповнення було представлено користувачам, які відвідували веб-сайти, пов'язані з фішинговими електронними листами, і після встановлення дозволило хакерам викрасти електронну пошту та дані веб-перегляду.

Додатки для браузера також можуть бути вектором для зараження парламентських ресурсів, таких як веб-сайти, які, у свою чергу, можуть поширювати зловмисне програмне забезпечення для широкого кола відвідувачів сайту (включаючи широку громадськість, працівників парламенту та самих депутатів). Візьмемо, наприклад, використання хакерами популярного доповнення для браузера Browsealoud (тепер відомого як ReachDeck), програми, яка перетворює текст веб-сайту на аудіо для користувачів із вадами зору. У 2018 році хакери вставили шкідливий код у надбудову браузера, який використовувався на веб-сайтах різних державних установ, у тому числі парламенту штату Вікторія в Австралії. З інфікованим доповненням до веб-переглядача та неправильно налаштованим, пристрої відвідувачів веб-сайту були заражені шкідливим програмним забезпеченням під час відвідування сайту. У цьому випадку зловмисне програмне забезпечення використовувалося для використання пристроїв для видобутку криптовалюти, але така тактика може бути використана хакерами для поширення шкідливого програмного забезпечення з метою крадіжки даних або шпигунства.



Безпека соціальних мереж

Співробітники парламенту та депутати можуть розкрити багато — а іноді й більше, ніж вони мають намір — шляхом публікацій і коментарів у соціальних мережах.

Незалежно від того, чи це Facebook, Twitter, Instagram, YouTube, соціальні мережі для певних регіонів, як-от «ВКонтакте» та «Одноклассники», слід завжди ретельно обмірковувати те, що ви публікуєте, і належним чином налаштувати доступні параметри конфіденційності. Це стосується не лише офіційних сторінок парламентів, а й у деяких випадках особистих облікових записів співробітників, а також їхніх родин і друзів.

Безпека соціальних мереж і парламент

Навіть організації з низьким рівнем ризику можуть бути об'єктами нападів і переслідувань у соціальних мережах, якщо вони не мають належної політики безпеки. У цьому прикладі з 2018 року некомерційний притулок для тварин втратив тисячі доларів і відштовхнув прихильників після того, як неавторизований адміністратор облікового запису організував фальшивий збір коштів, і на платформі з'явилися фальшиві облікові записи осіб, які видавали себе за співробітників.
Якщо хакери підуть на все, щоб заробити кілька тисяч доларів на притулку для тварин, ви можете собі уявити, якої шкоди можуть завдати досвідчені вороги, якщо вони отримають доступ до облікових записів вашого парламенту або успішно видадуть себе за видатного депутата чи співробітника онлайн.
Окрім злому облікових записів у соціальних мережах, веб-сайти парламенту також є поширеними цілями, враховуючи їх публічну видимість та репутаційну значимість. Одним із прикладів 2017 року є веб-сайт парламенту Австрії було знято хакерською групою, яка нібито була розлючена через погіршення відносин країни з Туреччиною в той час.

РОЗРОБИТИ ПАРЛАМЕНТСЬКУ ПОЛІТИКУ ЩОДО СОЦІАЛЬНИХ МЕРЕЖ

З огляду на те, що будь-що, опубліковане в соціальних мережах, може стати загальнодоступним, необхідно розробити відповідну парламентську політику щодо соціальних мереж. Враховуючи публічний характер більшості парламентської роботи, цілком імовірно, що ви захочете публічно поділитися більшістю публікацій і повідомлень, але все одно вкрай важливо ставити такі запитання та відповідати на них: Хто має доступ до ваших облікових записів у соціальних мережах? Кому дозволено публікувати дописи та хто має затверджувати дописи? А як щодо коментарів і відповідей? Якою інформацією слід/не слід ділитися в соціальних мережах? Якщо ви публікуєте фотографії, інформацію про місцезнаходження чи іншу ідентифікаційну інформацію про співробітників, депутатів або партнерів, чи запитували ви їхнього дозволу, і чи враховували вони можливі ризики? Такі запитання особливо важливі, якщо ваш парламент публічно спілкується з громадянами через соціальні медіа чи подібні онлайн-портали для залучення громадськості.
Окрім розробки політики та пояснення її персоналу, обов'язково правильно налаштуйте параметри конфіденційності та захисту (часто їх називають «безпекою»). Деякі ключові запитання, які варто поставити собі, коли ви вирішуєте, які параметри конфіденційності та безпеки є найбільш доцільними для парламентських і особистих облікових записів, включають:

- Чи бажаєте ви поділитися своїми публікаціями з громадськістю чи лише з певною групою людей у рамках або за межами організації?
- Чи повинен хтось мати можливість коментувати, відповідати чи взаємодіяти з вашими повідомленнями чи публікаціями?
- Чи мають люди знаходити вас за адресою електронної пошти або (особистим чи службовим) номером телефону?
- Чи хочете ви, щоб ваше місцезнаходження повідомлялося автоматично під час публікації?
- Чи хочете ви заблокувати або вимкнути недружні облікові записи?
- Чи хочете ви заблокувати певні слова або хештеги?

Кожна соціальна мережа має різні параметри конфіденційності та безпеки, але ці загальні поняття застосовуються універсально. Розглядаючи ці запитання, скористайтеся корисними посібниками з конфіденційності на основних платформах: **Facebook**, **Twitter**, **Instagram** та **YouTube**. Особливо на Facebook будьте обережні щодо налаштувань конфіденційності для Груп. Групи у Facebook є популярним місцем для взаємодії, поширення ідей та обміну інформацією, але до груп, для яких не встановлені обмеження, може приєднатися кожен. Нерідкі випадки, коли «підроблені» облікові записи видають себе за реальних людей, намагаючись проникнути до приватних груп або сторінок у соціальних мережах. Тому уважно приймайте запити «дружби» та «підписки». Пам'ятайте, що облікові записи вашого парламенту в соціальних мережах настільки безпечні, наскільки безпечні облікові записи, «пов'язані» з ним. Це особливо важливо пам'ятати для Facebook, де вашими сторінками може керувати чийсь пов'язаний особистий обліковий запис.

ПЕРЕСЛІДУВАННЯ В ІНТЕРНЕТІ

На жаль, багато парламентів і афілійованих груп стикаються із значними переслідуваннями в Інтернеті, особливо в соціальних мережах. Таке переслідування **часто спрямоване ще більш інтенсивно проти жінок і маргінальних груп населення**. Насильство щодо жінок в інтернеті, зокрема, може створити вороже середовище, що призводить до самоцензури або відходу від політичного чи громадянського дискурсу. Як визначила група NDI з питань гендеру, жінок і демократії у звіті «**Загрозливі твіти**» (Tweets that Chill), коли напади на політично активних жінок здійснюються в інтернеті, широке охоплення у соціальних мережах може посилити ефект від переслідувань і психологічного насильства, підриваючи почуття особистої безпеки жінок у способи, яких не зазнають чоловіки.

Коли ваш парламент розробляє свою політику щодо соціальних медіа, важливо знати про цю динаміку. Передбачте у своєму плані безпеки структуровану підтримку співробітників, які стикаються з негативними повідомленнями, дошкульними образами та погрозами в соціальних мережах як на роботі, так і в особистому житті. Розробіть у своїй організації інфраструктуру протидії переслідуванням, включно з опитуванням своїх співробітників, щоб зрозуміти, як на них впливають переслідування в інтернеті, і створіть групу швидкого реагування, щоб допомогти співробітникам долати складні ситуації. **Практичний посібник щодо переслідування в інтернеті** від PEN America також містить детальні рекомендації щодо того, як ви можете підтримати співробітників, які стикаються з такими переслідуваннями. Ви можете розглянути доцільність, якщо ваших співробітників влаштовує це, **повідомлення про інциденти** переслідування та/або проблемні облікові записи також безпосередньо на платформах.

Спілкуючись зі співробітниками, які стали жертвами переслідувань в інтернеті (а також у реальному світі), важливо бути чуйними. Як зазначено в Програмі прав жінок Асоціації прогресивних комунікацій **Take Back the Tech**, слід зрозуміти, що постраждала може зазнати травми, і визнати, що насильство (як онлайн, так і офлайн) ніколи не є провиною жертви. Переконайтеся, що такі питання можна порушувати й обговорювати (якщо персонал не проти) у конфіденційній та безпечній обстановці, як варіант, анонімно. Додайте до плану безпеки вашої організації список місцевих спеціалістів, організацій і правоохоронних органів, з якими ви можете сконтактувати своїх співробітників для надання юридичної, медичної, психічної та технічної допомоги, за необхідності. Додаткові ідеї можна отримати з **Інструкції з безпеки в інтернеті** від Feminist Frequency.

Робота веб-сайтів онлайн

Окрім захисту можливості безпечного доступу до інтернету, також важливо робити все можливе, щоб інші могли отримати доступ до веб-сайтів або ресурсів вашої організації в інтернеті.

Для сторінок у соціальних мережах це означає захист облікових записів надійними унікальними паролями та двофакторною автентифікацією. Для вашого веб-сайту це означає захист від злому й атак типу «відмова в обслуговуванні». Атака з розподіленим доступом і відмовою в обслуговуванні (DDoS) — це випадки, коли велика група комп'ютерів одночасно направляє на ваш сервер зловмисний трафік, із яким той не може впоратися. Кілька варіантів захисту від DDoS, які значно ускладнюють зловмисникам зламати ваш веб-сайт, включають **Cloudflare**, **AWS Shield** від Amazon або службу **Deflect** від eQualitie.

Безпечне розміщення веб-сайту вашого парламенту

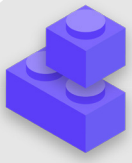
Веб-сайти розміщуються на комп'ютерах, і їм загрожує ризик злому, як і вашим власним пристроям. Якщо можливо, ваш парламент має скористатися перевагами існуючих служб хостингу, таких як WordPress, Wix або інших, які керують безпекою сайту за вас. Якщо потрібен більш складний веб-сайт або якщо вам потрібно самостійно розмістити свій веб-сайт, то обов'язково приділіть увагу підтримці операційної системи та програмного забезпечення для вебхостингу в актуальному стані, як і оновленню свого персонального комп'ютера. Розгляньте доцільність використання відомих постачальників хмарного хостингу, як-от Amazon Web Services (AWS), Microsoft Azure або **eclips.is** від Greenhost, що забезпечують кращі параметри безпеки для розміщених веб-сайтів. Незалежно від того, які інструменти ви використовуєте для розміщення свого веб-сайту, переконайтеся, що всі облікові записи, що використовуються для доступу до редагування вмісту та параметрів конфігурації, захищені надійними паролями та двофакторною автентифікацією.

Якщо ваша організація має технічних спеціалістів для розміщення власного веб-сайту, вам слід розглянути можливість вибору так званого «статичного сайту» або плоского веб-сайту. На відміну від динамічних веб-сайтів, веб-сайти цих типів зменшують площу атаки для хакерів і мають більшу стійкість до атак.

Захист мережі Wi-Fi

Усі ці кроки для захисту веб-трафіку від стеження та цензури є важливими, але вони не замінять базової безпеки мережі в офісі та вдома.

Не забувайте про основи, як-от використання надійного пароля (а не пароля за замовчуванням) на маршрутизаторах WiFi, забезпечення доступу до вашої мережі лише авторизованих користувачів шляхом частої зміни пароля та ввімкнення вбудованого брандмауера бездротових маршрутизаторів. Розгляньте також можливість створення гостьової мережі в парламентських приміщеннях, якщо до вас приходять і виходять відвідувачі, які користуються Інтернетом.



Безпека в інтернеті

- **Проводьте регулярні тренінги для депутатів і співробітників щодо важливості дотримання основних заходів веб-безпеки.**
- **Нагадайте персоналу завжди переглядати сторінки з HTTPS і зашифрованою DNS.**
- **Вимагайте від персоналу регулярного перезавантажувати браузери для встановлення оновлень.**
- **Заохочуйте використання браузерів і розширень із захистом конфіденційності.**
- **Якщо VPN підходить, виберіть надійну, навчіть співробітників її використанню та переконайтеся, що вона постійно використовується.**
- **Розробити та поширити чітку парламентську політику щодо використання соціальних мереж.**
- **Увімкніть налаштування конфіденційності та безпеки в усіх облікових записах соціальних мереж.**
- **Зрозумійте наслідки переслідувань в Інтернеті та будьте готові підтримати депутатів і співробітників, які постраждали.**
- **Розробіть список місцевих спеціалістів, організацій і правоохоронних органів, з якими ви можете зв'язати своїх співробітників для надання юридичної, психічної та технічної допомоги у відповідь на переслідування в інтернеті.**
- **Підпишіться на захист від DDOS для своїх веб-сайтів.**
- **Використовуйте надійного постачальника вебхостингу.**
- **Використовуйте надійний пароль і гостьову мережу для свого локального Wi-Fi.**

Фізична безпека

Дуже важливо забезпечити фізичну безпеку своїх пристроїв. Майте на увазі, що фізична безпека виходить за рамки лише пристроїв і має включати стратегії захисту всіх інших активів вашої організації. Це включає друковані документи; офіси парламенту; камери, або робочі приміщення; і, звичайно, ви, ваші співробітники та учасники.

Фізична охорона і парламент

На жаль, фізичні напади на парламенти та інші законодавчі органи не є рідкістю і часто мають значні наслідки як для фізичної, так і для інформаційної безпеки. 6 січня 2021 року повстанці штурмували будівлю Капітолію Сполучених Штатів, де розташовані обидві палати законодавчих зборів США, намагаючись зупинити затвердження результатів президентських виборів. Фізична атака трагічно призвела до п'ятьох смертей і викликала значний психологічний стрес для депутатів і співробітників Конгресу. Однак це був не єдиний негативний вплив. Зловмисники також знищили IT-обладнання, отримали доступ до конфіденційних матеріалів в офісах депутатів і, що, мабуть, найбільш згубно, викрали комп'ютери та інші пристрої з потенційно конфіденційною інформацією з Капітолію США.

Засоби конфіденційної інформації (SCIF)

Для проведення дуже конфіденційних розмов деякі парламенти забезпечили фізичні кімнати, які називаються SCIF. Ці простори створені для того, щоб депутати та співробітники парламенту могли переглядати та обговорювати конфіденційну інформацію, таку як питання, пов'язані з національною безпекою чи розвідкою, без побоювань зовнішнього спостереження чи шпигунства. На додаток до належної фізичної конструкції, належний SCIF вимагає, щоб люди залишали пристрої (наприклад, свої мобільні телефони) за межами кімнати перед входом для обговорення.

Захист фізичних активів

Важливою складовою інформаційної безпеки є фізична безпека ваших пристроїв.

Окрім пом'якшення наслідків викрадення пристрою за допомогою блокування екрану й паролю, впровадження повного шифрування диска та ввімкнення функцій віддаленого стирання, також слід подумати про те, як уберегти ці пристрої від викрадення. Щоб ускладнити крадіжку, обов'язково встановіть міцні замки (і обертайте їх щоразу, коли змінюється персонал) у парламентських приміщеннях та/або вдома. Крім того, подумайте про придбання сейфа для ноутбука або шафи, що замикається, щоб захистити пристрої протягом ночі. Такі камери або системи датчиків руху в приміщеннях можуть виявляти та, сподіваємося, запобігати фізичним проникненням і крадіжкам. Шукайте варіанти із **захистом конфіденційності приватних даних**, доступні у вашій країні, і обов'язково вибирайте камери, надані перевіреними компаніями, які не мають стимулів передавати дані й інформацію потенційному зловмиснику.

Якщо на старих пристроях все ще зберігається інформація, але вони більше не використовуються, видаліть її. У **цьому посібнику** від Wirecutter детально розповідається про те, як це зробити на більшості сучасних пристроїв. Якщо стерти інформацію з ваших пристроїв неможливо, ви також можете їх фізично знищити. Найпростіший, хоч і не найкорисніший для екології, спосіб зробити це — розбити пристрої та їхні жорсткі диски молотком. Іноді найстаріші рішення все ще є найбільш дієвими!

Ще до виконання цих технічних кроків знайдіть час, щоб створити перелік усього обладнання в парламенті. Якщо у вас немає переліку всіх ваших пристроїв, важче відстежити, що могло бути втрачено, якщо один із них викрадуть.

ЩО НАМ РОБИТИ З УСІМА ЦИМИ ПАПЕРАМИ?

Ймовірно, у вашій організації є багато інформації, надрукованої на папері, записаної в блокнотах або нашкрябаної на листочках. Деякі з них можуть бути дуже конфіденційними — наприклад, нотатки з конфіденційних свідчень або приватних зустрічей. Важливо також подумати про безпеку цієї інформації. Якщо вам конче потрібно зберегти друковані копії конфіденційної інформації, переконайтеся, що вона надійно зберігається в закритій шафі або в іншому безпечному місці. Не зберігайте конфіденційну чи секретну інформацію (зокрема паролі) на столі або записаною на дошці. Зберігайте конфіденційну інформацію в менш цільовому, добре захищеному місці.

Наскільки це можливо, постарайтеся позбутися непотрібної друкованої інформації. Пам'ятайте: якщо у вас чогось немає, це неможливо вкрасти. Встановіть парламентську політику щодо володіння паперовими нотатками та обов'язково збирайте будь-які паперові нотатки від співробітників, якщо вони вирішать піти з організації або їх звільнять, так само, як ви збираєте комп'ютер або телефон, виданий парламентом. Щоб позбутися секретних паперів, придбайте якісний шредер. Наприкінці тижня в якості розваги ви можете зробити 15-хвилинну перерву для співробітників, щоб подрібнити будь-які залишки, конфіденційні роздруківки чи нотатки за попередній тиждень.

ПАРЛАМЕНТСЬКА ПОЛІТИКА

Хоча для багатьох реалії «офісу» суттєво змінилися з початку пандемії COVID-19, для вашого парламенту все ще важливо встановити чітку політику щодо доступу до приміщень. Така політика має відповідати на ключові питання, у тому числі кому дозволено входити в офіс (і коли), хто може отримати доступ і до яких ресурсів офісу (наприклад, мережі Wi-Fi) і що мають право робити гості.

Просте, але важливе запитання, на яке потрібно відповісти, — хто отримує ключ від офісу чи бейдж доступу. Лише довірений персонал повинен мати ключі, а замки слід міняти, коли співробітник звільняється, та/або на більш-менш регулярній основі. Протягом дня будь-які двері, які залишаються незамкненими, повинні постійно перебувати в полі зору довіреної особи та/або охоронця. Крім того, переконайтеся, що ваш парламент має довірчі відносини з постачальниками послуг, такими як прибиральники та сторонні технічні спеціалісти, які мають доступ до приміщень. Подумайте, до якої інформації чи пристроїв такі люди можуть мати доступ, і переконайтеся, що вони захищені, особливо якщо у вас немає таких довірливих стосунків. Незалежно від того, хто має доступ, завжди слід призначати когось, кому можна довіряти, щоб зачинити офіс і переконатися, що пристрої належним чином захищені перед тим, як співробітник покине офіс наприкінці дня.

Чи допускаються виборці до вашого парламенту? Можливо, громадськість має право на доступ до частини парламентського приміщення? Якщо так, переконайтеся, що вони не мають доступу (або принаймні доступу без нагляду) до пристроїв або конфіденційних паперових даних. Якщо під час відвідування гості повинні мати доступ до інтернету, слід налаштувати «гостьову» мережу, щоб такі відвідувачі не мали можливості відстежувати ваш робочий трафік. Загалом доступ до мережі та мережевих пристроїв, наприклад принтерів, повинен мати лише довірений персонал. Також доцільно ввести обов'язкову реєстрацію гостей, щоб у вас був журнал відвідувань.

Коли ви розробляєте політику щодо офісу, метою має бути надання доступу до конфіденційних пристроїв, документів, приміщень і систем лише довіреним людям.

ДОПОМІЖНИЙ ПЕРСОНАЛ І ВОЛОНТЕРИ

Загрози фізичній безпеці вашого парламенту також можуть вплинути на співробітників. Подібно до переслідувань у соціальних мережах, цих загроз фізичній безпеці часто найбільше зазнають жінки та маргіналізовані спільноти. Йдеться не лише про розбиті вікна та вкрадені ноутбуки. Залякування, погрози та випадки фізичного чи сексуального насильства, побутове насильство та страх нападу можуть мати серйозний негативний вплив на життя співробітників. Інструмент планування безпеки NDI **#Think10** є корисним ресурсом для політично активних жінок, які можуть піддаватися підвищеному ризику внаслідок своєї участі в парламенті та політиці загалом.

Очевидно, що благополуччя співробітників є важливим активом для них як окремих осіб, але це також важливий елемент здорової та добре функціонуючої організації. З цією метою подумайте, які додаткові ресурси ви можете надати співробітникам, щоб захистити їх і, у разі фізичної чи цифрової атаки, допомогти їм повернутися до норми. Як згадувалося раніше в Довіднику, це означає, щонайменше, розробити перелік ресурсів, до яких ви можете направити персонал для отримання юридичної, медичної, психічної та технічної допомоги, за необхідності. Знову **Онлайн-посібник щодо агресивних дій** від PEN America містить ідеї щодо того, як організації можуть підтримувати співробітників під час та після криз.

БЕЗПЕКА ПІД ЧАС ПОДОРОЖІ

Подорожі — до іншої країни чи до сусіднього міста — часто посилюють ризики фізичної інформаційної безпеки. Загалом можна з упевненістю припустити, що для вас і ваших пристроїв не має прав на конфіденційність під час перетину кордону. Таким чином, було б гарною ідеєю включити організаційну політику щодо подорожей у ваш план безпеки, що містить нагадування про основні найкращі методи безпеки. Політика вашої організації щодо подорожей має включати багато інформації, описаної в інших розділах Довідника, включно з безпечним використанням інтернету, зберіганням пристроїв та інших джерел інформації у фізичній безпеці та тримання їх при собі під час подорожі. Якщо можливо, залиште конфіденційну інформацію та скористайтеся свіжим, начисто стертим диском комп'ютеру, й отримайте доступ до файлів, які вам дуже потрібні, із хмарного сховища, а потім зітріть їх, повернувшись додому.

На додаток до підготовки до подорожі та мінімізації даних, що передаються під час подорожі, є кілька важливих операційних рекомендацій, які ви повинні продумати та включити до політики щодо подорожей своєї організації.

Подумайте про те, щоб використовувати для подорожей ноутбуки або телефони, на яких майже немає конфіденційних даних. Якщо більшість роботи вашої організації виконується в хмарному середовищі, відносно недорогий Chromebook може стати хорошим варіантом такого пристрою. Після повернення до заводських налаштувань або «стирання даних» ці пристрої готові до підключення до звичайних мереж WiFi вдома чи в офісі. Надайте співробітникам контактну інформацію та план дій щодо того, що вони повинні робити, якщо під час поїздки щось піде не так. Це включає інформацію про місцеві лікарні, клініки й аптеки, якщо їм знадобиться медична допомога під час подорожі.

Співробітники також повинні тримати всі пристрої при собі під час подорожі. Наприклад, тримайте ноутбук біля ніг (а не у відділенні над головою чи в зареєстрованому багажі), коли ви знаходитеся в автобусі, поїзді чи літаку. Не вважайте, що готельний номер або навіть готельний сейф є «безпечним місцем» для зберігання конфіденційних пристроїв і предметів. І не довіряйте загальнодоступним зарядним портам USB. USB-порти для зарядки в аеропортах, на вокзалах і у транспортних засобах стають все більш поширеним явищем і дуже зручним способом живлення пристроїв. Однак вони можуть бути також засобами перенесення шкідливих програм. Тому обов'язково заряджайте пристрої традиційним способом через розетку або купуйте **блокувальник даних USB**, щоб співробітник, який подорожує, міг безпечно заряджати свої пристрої через USB-прилади загального користування.

Безпечне бронювання подорожей для вашого парламенту

Складаючи політику щодо подорожей, зазначте, яка інформація може бути розкрита під час планування або бронювання подорожі. Це може бути особливо важливо, якщо ви організовуєте великі заходи, тренінги чи конференції, для яких ви обробляєте конфіденційну інформацію від різних співробітників, партнерів або відвідувачів. Ретельно подумайте про те, як ви будете безпечно передавати та зберігати (за потреби) особисту інформацію, як-от паспортні дані, маршрути подорожей і медичну документацію.

Захист вашої фізичної безпеки

- **Нагадайте депутатам і співробітникам постійно тримати пристрої під фізичним захистом.**
- **Перевірте та захистіть усі шляхи, якими люди можуть потрапити у ваші приміщення.**
- **Розробіть політику гостьового доступу та доступу.**
- **Використовуйте надійні замки, ідентифікаційні системи/системи бейджів і обертайте/міняйте їх, коли це необхідно.**
- **Розгляньте можливість встановлення камер або інших локальних систем безпеки.**
- **Майте та використовуйте знищувачі паперу.**
  - Виділіть певний час співробітникам для утилізації паперових документів, що містять конфіденційну інформацію.
- **Розробіть список місцевих спеціалістів, організацій і правоохоронних органів, з якими ви можете зв'язати своїх співробітників для надання юридичної, медичної та психічної допомоги після фізичних нападів і погроз.**
- **Розробити парламентську політику подорожей.**
- **Переконайтеся, що співробітник знає, що робити в екстрених випадках під час подорожі.**
- **Пам'ятайте про додаткові дані, які створюються та передаються під час організації подорожей або заходів.**

Що робити, коли все йде не так

Отже, ви знаєте, як і що треба робити. Ви запровадили політику та навчили всіх у парламенті найкращим практикам. Навіть попри всю цю важку роботу дуже ймовірно, що щось піде не так.

Всяке трапляється. Коли відбувається щось не те, важливо мати план реагування на інцидент. Реагування на інциденти є важливою, і часто недооцінюваною, частиною плану безпеки вашого парламенту, оскільки це може бути різницею між нападом, який знищить вашу репутацію, або стане неприємною перешкодою на дорозі. Майте на увазі, що ви можете відреагувати на інцидент, лише якщо знаєте про нього. Дуже важливо мати сильну культуру безпеки та заохочувати депутатів і співробітників повідомляти про проблеми. Ось чому краще винагороджувати за належне втілення заходів із безпеки, а не карати за прогалини або помилки, пов'язані з безпекою. Також важливо висловлювати співчуття та переконатися у доброму самопочутті співробітників, коли вони повідомляють про інцидент. Співробітники мають негайно повідомляти про натиснуте посилання у фішинговому повідомленні, викрадений телефон або зламаний обліковий запис у соціальних мережах, — а не зволікати, боячись покарання чи відсутності підтримки. Зрештою, реагування на інциденти, як і стратегії пом'якшення наслідків, згадані в інших розділах Довідника, запроваджуються у всій організації.

Що саме потрібно включити до плану? Коротко кажучи, все, що може ймовірно статися. Ризики є різними для кожної організації, але типові запитання, на які допоможе відповісти план реагування на інциденти, включають такі:

- Що ми будемо робити, якщо наші облікові записи або веб-сайти буде зламано?
- Що ми будемо робити, якщо хтось натисне посилання у фішинговому електронному листі або якщо пристрій веде себе підозріло?
- Що ми будемо робити, якщо наші електронні листи чи найбільш конфіденційні документи викрадено та стався витік даних?
- Що ми робимо, якщо одному з наших співробітників загрожує фізична небезпека? Або якщо вони потерпають через стрес і тривогу внаслідок таких загроз?
- Що ми будемо робити, якщо наш офіс постраждає від пожежі, повені чи стихійного лиха?
- Що ми робимо, якщо комп'ютер або телефон учасника загублено чи вкрадено?

Відповіді на ці та інші питання залежатимуть від парламенту, але важливо продумати їх разом і чітко сформулювати та поділитися планом, щоб кожен був готовий негайно вжити заходів для обмеження шкоди.
Цитуючи Комплексний посібник із безпеки від Tactical Tech, під час розробки плану реагування на інциденти добре буде почати з **визначення інциденту або надзвичайної ситуації** в контексті вашої організації. Вирішіть, що таке «надзвичайна ситуація», тобто момент, коли ви повинні почати впроваджувати заплановані дії та заходи із реагування на інцидент. Це важливо, оскільки іноді буває незрозуміло: наприклад, у такому сценарії, як втрата контакту з колегою під час виконання операції на місці; як довго треба чекати, перш ніж визнати ситуацію екстреною? Не хочеться панікувати занадто рано, але надто довге очікування за деяких обставин може бути катастрофічним. Також важливо продумати етапи **операції**. Призначте кожній людині чітку роль, яку вона знає і приймає заздалегідь — це зменшить дезорганізацію та паніку в разі інциденту. Для кожної загрози розгляньте різні ролі, які вам, можливо, доведеться взяти на себе, і практичні аспекти реагування на надзвичайну ситуацію. Ця важлива стратегія для надзвичайних ситуацій передбачає активацію мережі підтримки — широкої мережі союзників, яка може включати різні гілки вашого власного уряду, інші дружні уряди, технологічні компанії, постачальників засобів безпеки та багатосторонні установи, щоб назвати лише кілька прикладів. Як ваші союзники можуть підтримати вас? Чи варто зв'язатися з ними заздалегідь, щоб переконатися, що вони готові допомогти вам у надзвичайних ситуаціях, і повідомити їм, чого ви від них очікуєте?

Під час реагування на інцидент **ефективна комунікація** стає дедалі важливішою. Вирішіть, що є найбільш безпечним і ефективним засобом комунікації з кожним учасником у різних сценаріях, і також визначте резервний засіб. Майте на увазі, що в надзвичайних ситуаціях може бути корисним мати чіткі вказівки щодо того, що саме передавати (а що ні), коли спілкуватися, які канали використовувати для спілкування та з ким слід спілкуватися. Також врахуйте репутаційний вплив інциденту на ваш парламент і будьте готові відповідним чином відреагувати. Переконайтеся, що керівник комунікацій парламенту знає про інцидент і може стежити за соціальними мережами чи іншими засобами масової інформації для потенційного впливу. Ця особа також повинна бути готова до можливих запитів громадськості чи ЗМІ щодо інциденту, у відповідних випадках. Це особливо важливо для того, щоб випередити потенційні негативні історії та запобігти репутаційній шкоді. Хоча всі інциденти та контексти різні, чесна та прозора комунікація часто допомагає зміцнити довіру після інциденту.

Створення системи раннього оповіщення та реагування

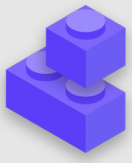
Розгляньте можливість створення системи раннього оповіщення та реагування. Це звучить складно, але, по суті, це просто централізований документ (електронний чи інший), який відкривається в разі надзвичайної ситуації. У документі слід описати всі подробиці про показники безпеки та інциденти, які сталися на часовій шкалі, надати чіткий опис дій і послідовність запланованого реагування, а також вказати, що слід зробити, щоб зменшити ризик повторного виникнення інциденту. Цей документ також має включати дії, яких слід вжити після інциденту, щоб захистити учасників від подальшої шкоди та допомогти їм відновитися фізично й емоційно. Система раннього оповіщення та реагування може надати корисну документацію для передачі правоохоронним органам (за необхідності), проведення подальшого аналізу того, що трапилося, і вказівки щодо вдосконалення вашої тактики запобігання та реагування на загрози в майбутньому.

На додачу до цих важливих концепцій реагування на інциденти ваша організація також має підготуватися до будь-яких конкретних **технічних** заходів реагування. У деяких випадках технічними заходами реагування може керувати IT-персонал або системні адміністратори організації. Наприклад, якщо здається, що обліковий запис електронної пошти було зламано, адміністратор вашого облікового запису має бути готовий і мати можливість закрити або вимкнути ушкоджений обліковий запис. Однак для подолання наслідків деяких технічних інцидентів може знадобитися досвід, якого у вашій організації немає. У подібних ситуаціях важливо визначити надійний список сторонніх технічних експертів, які можуть допомогти вам у реагуванні на інцидент. У деяких випадках ви можете попередньо узгодити умови з постачальниками послуг (наприклад, хостингом вашого веб-сайту чи IT-консультантом), щоб переконатися, що вони доступні (і не стягуватимуть додаткової плати) для такого реагування на технічні інциденти.

І останнє, але не менш важливе: ви повинні розглянути **правові** кроки. Важливо зрозуміти, які можливості правового захисту у вас є, а також юридичні зобов'язання або наслідки, з якими може зіткнутися ваша організація в результаті витоку даних або іншого порушення безпеки. Як парламент, ви маєте особливу владу та значущість, коли справа доходить до розуміння та дотримання місцевих правил безпеки даних і конфіденційності.

Знайдіть час, щоб розглянути можливі інциденти з відповідним юридичним консультантом, за необхідності, і складіть план того, як ви будете реагувати на них. Добра ідея укласти угоду з цим довіреним консультантом, який буде представляти вас і ваші інтереси, якщо це знадобиться після інциденту. У рамках цієї правової підготовки переконайтеся, що ви розумієте юридичні зобов'язання постачальників і партнерів. Чи зобов'язані вони повідомляти вас у разі витоку їхніх даних? Яку підтримку (за наявності) вони повинні надати вам у разі інциденту? Коли ви укладаєте контракти й угоди зі сторонніми постачальниками, пам'ятайте про можливість витоку даних або іншого інциденту.

Хоча не існує універсального методу реагування на інциденти, важливо мати чіткі плани операційних, комунікаційних, технічних і правових заходів. Коли ви складаєте свій план реагування на інциденти, ми наполегливо рекомендуємо вам скористатися деякими відмінними наявними ресурсами, розробленими, щоб допомогти організаціям орієнтуватися в реагуванні на інциденти. Хоча не всі ці ресурси розроблені спеціально для парламентів, їх зміст все одно є дуже актуальним. Ці ресурси включають **Цифрову аптечку першої допомоги**, розроблену RaReNet і CiviCERT, **Практичний посібник щодо переслідування в інтернеті** від PEN America, **Порядок проведення кампанії з кібербезпеки** від Belfer Center, **Шаблон плану повідомлень про кіберінциденти** і **Гарячу лінію цифрової безпеки** від Access Now.



Реагування на інциденти

- **Розробіть парламентський план реагування на інциденти та практикуйте його.**
  - Проведіть мозковий штурм щодо можливих інцидентів і приготуйтеся реагувати до того, як це станеться.
- **Переконайтеся, що всі в парламенті знають про те, як ви будете спілкуватися та які технічні кроки будуть вжиті у випадку інциденту.**
- **Знайдіть час, щоб дізнатися про засоби правового захисту й усвідомити свої зобов'язання.**
- **Будьте готові надати депутатам і співробітникам необхідну емоційну та соціальну підтримку після інциденту.**

Додаток A. Рекомендовані ресурси

- Комплексний посібник із безпеки від Tactical Tech; Міжнародна ліцензія Creative Commons Attribution-ShareAlike 4.0
  - Розділ 2.4 — Розуміння та каталогізація нашої інформації
  - Розділ 1.5 — Сповіщення про загрози команд та організацій
  - Розділ 3.4 — Безпека в групах і організаціях
- The Electronic Frontier Foundation's Security Education Companion; Ліцензія США Creative Commons Attribution 3.0
  - Роздатковий матеріал із моделювання загроз
- Посібник із запобігання фішингу та належного поводження з електронними листами від Freedom of the Press Foundation; Міжнародна ліцензія Creative Commons Attribution 4.0
- Керівництво зі встановлення додатку Signal від Freedom of the Press Foundation; Міжнародна ліцензія Creative Commons Attribution 4.0
- Посібник із самозахисту від спостереження (SSD) від Electronic Frontier Foundation; Ліцензія США Creative Commons Attribution 3.0
  - Що треба знати про шифрування
  - Спілкування з іншими
  - Вибір правильної VPN
- Посібник із інструментів безпечного проведення групових чатів і конференцій від Frontline Defenders
- Data Detox Kit від Tactical Tech
  - Допуск лише для авторизованих осіб: Зробіть паролі сильнішими
  - Зробіть блокування екрана більш надійним
- Керівництво з безпеки виборів щодо паролів від Center for Democracy and Technology; Міжнародна ліцензія Creative Commons Attribution 4.0
- Керівництво з безпеки виборів щодо двофакторної автентифікації від Center for Democracy and Technology; Міжнародна ліцензія Creative Commons Attribution 4.0
- Двофакторна автентифікація для початківців від Martin Shelton; Міжнародна ліцензія Creative Commons Attribution 4.0
- Security in a Box від Tactical Tech і Frontline Defender; Creative Commons Attribution-ShareAlike 3.0 Ліцензія без прив'язки до юрисдикції
  - Захистіть свій пристрій від шкідливих програм і фішингових атак
  - Захист від фізичних загроз
- SANS ОЙ! Бюлетень: Зупиніть цю шкідливу програму
- Доступ до пристроїв і даних, коли особиста безпека під загрозою від Apple
- Набір інструментів кібербезпеки Global Cyber Alliance для місійних організацій
- Інструмент оцінки кібербезпеки Фонду Форда

Додаток B. Стартовий комплект плану безпеки

Використовуйте наведений нижче початковий набір, щоб робити нотатки, коли ви та ваш парламент читаєте Посібник і вивчаєте матеріал, а також обміркуйте супровідні запитання зі своїми колегами, щоб допомогти створити продуктивну дискусію.

Обов'язково посилайтеся на ключові «будівельні блоки» в кожному розділі Посібника, щоб переконатися, що ви охоплюєте важливі теми під час створення плану безпеки. Наприкінці Посібника будівельні блоки, відповіді на ці запитання для обговорення та ваші нотатки повинні стати основою успішного плану безпеки.

Формування культури безпеки

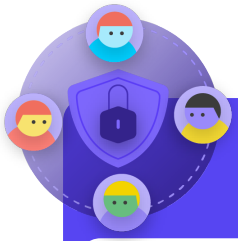
Міцна основа: захист облікових записів і пристроїв

Безпечна передача даних

Безпека в інтернеті

Фізична безпека

Що робити, коли все йде не так



Формування культури безпеки

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Коли ви можете запланувати розмову для перегляду вашого плану безпеки з усім парламентом?
- У які дні чи години парламенту краще запланувати регулярні бесіди та навчання з безпеки?
- Які кроки може вжити керівництво, щоб змоделювати належну поведінку щодо безпеки та відданість плану безпеки? Як інші депутати парламенту можуть відігравати роль у безпеці?

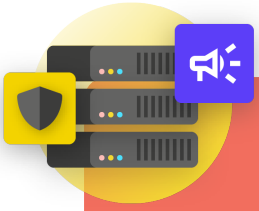
ВАШІ ПРИМІТКИ ТА ІДЕЇ:

Міцна основа: захист облікових записів і пристроїв

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як ви будете впроваджувати заходи безпеки облікових записів, як-от менеджер паролів і 2FA, у парламенті? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваш парламент гарантуватиме безпеку та оновлення пристроїв? Чи знадобиться парламенту в рамках цього план боротьби з неліцензійним програмним забезпеченням чи комп'ютерами?
- Коли краще організувати навчання для всіх співробітників щодо небезпеки фішингу, зловмисного програмного забезпечення та найкращих методів захисту пристроїв?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

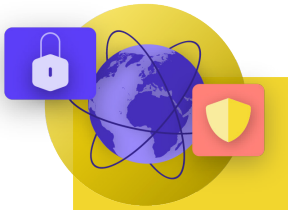


Безпечна передача та зберігання даних

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як ваш парламент запровадить наскрізне шифрування повідомлень для безпечного спілкування? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваш парламент запровадить безпечне рішення для обміну файлами як всередині, так і ззовні? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваш парламент запровадить безпечне рішення для зберігання та резервного копіювання даних? З якими перешкодами ви можете зіткнутися під час впровадження?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:



Безпека в інтернеті

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Яким чином ваш парламент запровадить вимоги безпечного веб-перегляду, такі як HTTPS, надійний браузер і, за необхідності, VPN для співробітників?
- Якими будуть ключові елементи політики вашого парламенту щодо соціальних медіа? Як він буде виконуватися?
- Як ваш парламент захищатиме свої веб-сайти та веб-власність?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

Фізична безпека

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Яким чином парламент розподілятиме та забезпечуватиме дотримання своєї політики відвідувачів і доступу до офісу?
- Хто відповідає за підготовку співробітників до проблем із фізичною та цифровою безпекою, з якими вони можуть зіткнутися під час подорожі на роботу?
- Які кроки може вжити співробітник, щоб захистити свої пристрої в офісі та під час подорожі?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

Що робити, коли все йде не так?

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як парламент поширюватиме та практикуватиме свою політику реагування на інциденти?
- Чи є ресурси для персоналу, який може потребувати емоційної та соціальної підтримки після інциденту? Якщо ні, то як парламент міг би забезпечити ці ресурси у разі інциденту?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

Додаток C. Image Citations

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