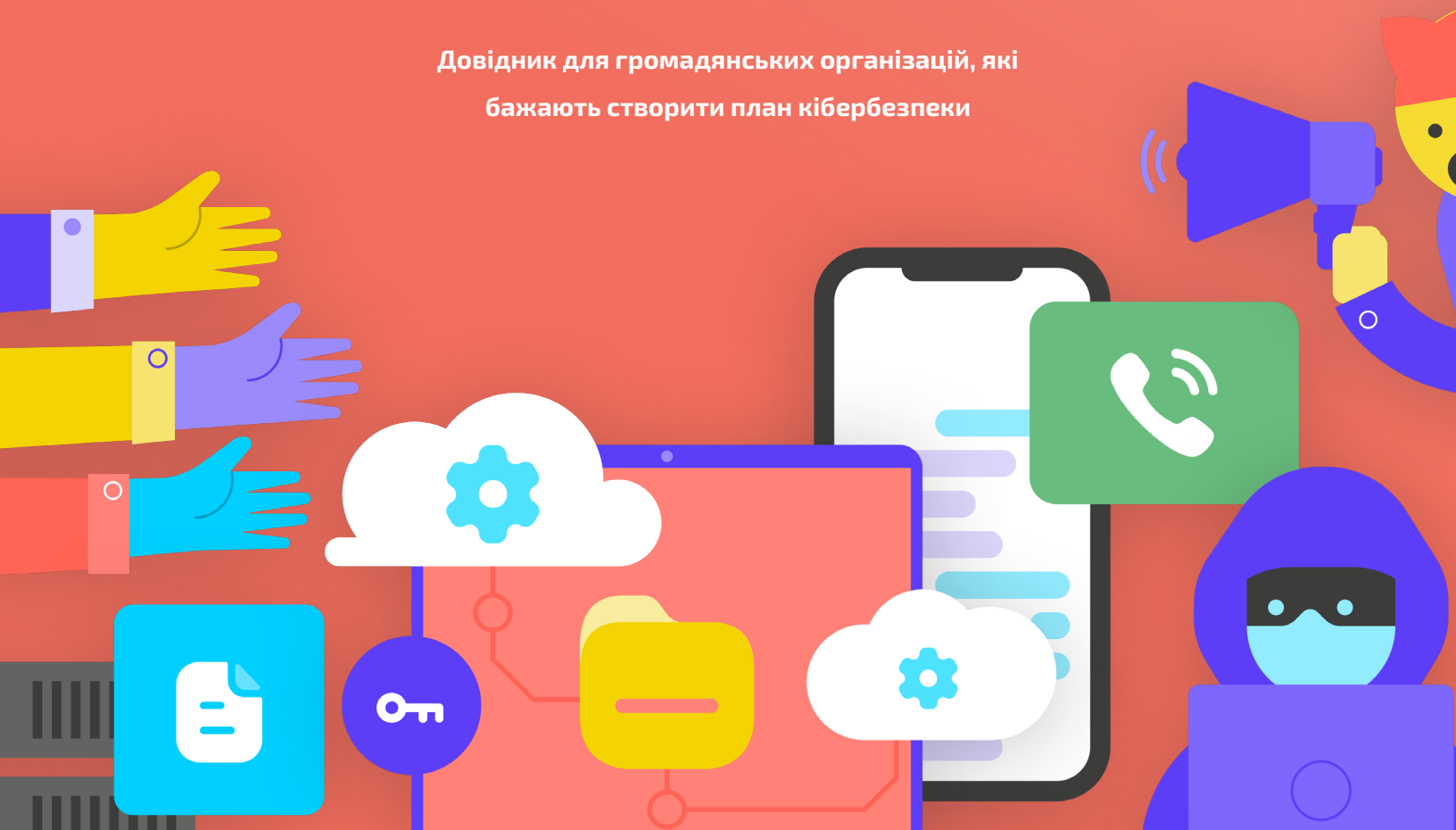
NDI
NATIONAL DEMOCRATIC INSTITUTE

Довідник із кібербезпеки

для

Громадських організацій

Довідник для громадянських організацій, які бажають створити план кібербезпеки



NDI
NATIONAL DEMOCRATIC INSTITUTE

Довідник із кібербезпеки

для

Громадських організацій

**Довідник для громадянських організацій,
які бажають створити план кібербезпеки**

Цей твір ліцензовано за міжнародною ліцензією Creative Commons Attribution-ShareAlike 4.0.
Щоб переглянути копію цієї ліцензії, відвідайте вебсайт http://creativecommons.org/licenses/by-sa/4.0/ або надішліть лист до Creative Commons, PO Box 1866, Mountain View, CA 94042 (Маунтін-В'ю, Каліфорнія, США).



Зміст

Пояснення умовних позначень 4

Перша десятка 6

Автори та подяка 7

Про укладачів Довідника 7

Для кого призначений цей Довідник? 8

Що являє собою план безпеки і навіщо він потрібен моїй організації? 8

Які активи має ваша організація і що ви хочете захистити? 9

Хто ваші супротивники, які їхні можливості та мотивація? 9

З якими загрозами стикається ваша організація? Наскільки вони вірогідні та який вплив вони можуть мати? 10

Створення плану кібербезпеки вашої організації 11

Формування культури безпеки 12

Інтегрування безпеки до вашої звичайної операційної структури 13

Отримання організаційної підтримки 14

Створення навчального плану 14

Міцна основа: захист облікових записів і пристроїв 16

Захищені облікові записи: паролі та двофакторна автентифікація 18

Захищені пристрої 26

Фішинг: поширена загроза для пристроїв та облікових записів 32

Безпечна комунікація і зберігання даних 37

Комунікація й обмін даними 38

Безпечне зберігання даних 50

Безпека в інтернеті 53

Безпечний перегляд вебсторінок 54

Безпека соціальних мереж 64

Робота вебсайтів онлайн 66

Захист мережі Wi-Fi 67

Захист фізичної безпеки 68

Захист фізичних активів 70

Що робити, коли все йде не так 74

Додаток А Рекомендовані ресурси 78

Додаток В Стартовий комплект плану безпеки 79

Пояснення умовних позначень

У Довіднику наведено кілька різних виділених елементів, які повторюються, і доповнюють основний текст. Нижче наведено коротке «пояснення умовних позначень», що допоможе зрозуміти основні елементи:



Конкретний приклад

Вказує на тематичні дослідження, які підкреслюють вплив певної теми на реальне життя громадських організацій на міжнародному рівні або в конкретній країні.



Додаткові поради

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



Реальні

Наводить поширені приклади інструментів тактики кібербезпеки, що використовуються в «реальному світі» як для добрих, так і для злочинних дій.



Вищий рівень

Вказує на тему просунутого рівня – інформацію, яку важливо розглянути вашій організації, але яка може бути дещо технічною або складною.



Елементи побудови плану безпеки

Вказує на «Елементи побудови плану безпеки», що є ключовими висновками кожного розділу Довідника.

1



Формування культури безпеки

2



Міцна основа: захист облікових записів і пристроїв

3



Безпечна комунікація і зберігання даних

4



Безпека в інтернеті

5



Захист фізичної безпеки

6



Що робити, коли все йде не так

Перша десятка

Ці десять елементів мають вирішальне значення для плану безпеки вашої організації. Якщо ви не знаєте, з чого почати, спочатку погляньте сюди.

1. **Проводьте регулярні тренінги з безпеки у вашій організації.**
2. **Остерігайтеся фішингу та створіть систему звітності.**
3. **Використовуйте шифрування для всіх видів зв'язку – за можливості, наскрізне.**
4. **Вимагайте встановлення надійних паролів і запровадьте менеджер паролів у всій організації.**
5. **За можливості вимагайте двофакторної автентифікації.**
6. **Переконайтеся, що всі пристрої та програмне забезпечення персоналу регулярно оновлюються.**
7. **Використовуйте безпечне хмарне сховище.**
8. **Використовуйте HTTPS і, за необхідності, VPN для доступу до інтернету.**
9. **Захистіть фізичні активи вашої організації.**
10. **Розробіть план реагування на інциденти організації.**

Автори та подяка

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:

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

Ми також хочемо відзначити чудові посібники, довідники, робочі зошити, навчальні модулі та інші матеріали, які розробила та веде Спільнота організаційної безпеки (OrgSec). Цей Довідник розроблено, щоб доповнити ці більш детальні матеріали та поєднати ключові уроки в єдиний, легкий для читання ресурс для громадських організацій, які хочуть розробити план 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, з 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**.

Ми також наполегливо рекомендуємо всім, хто читає цей Довідник, скористатися великою **бібліотекою** посібників із цифрової безпеки та ресурсів, що збираються й оновлюються фондом Open Technology Fund.

Про укладачів Довідника

National Democratic Institute for International Affairs **(NDI) – це некомерційна, позапартійна організація, розташована у Вашингтоні, округ Колумбія, 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 кібер-безпеки, 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.

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 — це не просто модне слово, а важлива концепція успіху організації та безпеки її співробітників. Особливо для громадських організацій, які працюють у сферах демократії, захисту громадських інтересів, вимоги підзвітності від уряду та відстоювання прав людини, безпека інформації (як онлайн, так і у реальному житті) є проблемою, що вимагає зосередженої уваги, пильності та інвестицій.

Ваша організація може опинитися – якщо вже не стала – об'єктом кібератаки. Ми не хочемо марно бити на сполох: це реальність навіть для тих організаційй, 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», каталогізує 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, що залишаються непоміченими або про які не повідомляється. Багато з них спрямовані на громадські організації, що працюють для підтримки демократії, вимоги підзвітності від уряду та відстоювання прав людини. Організації, що представляють жінок й інші маргіналізовані групи, часто стають об'єктами ціле спрямованої атаки.

Такі кібератаки мають серйозні наслідки. Такі погрози слід сприймати серйозно незалежно від того, чи хочуть зловмисники вкрасти ваші гроші, змусити вас мовчати, порушити діяльність вашої організації, зашкодити її репутації чи навіть викрасти інформацію, яка може призвести до психологічної чи фізичної шкоди ваших партнерів або співробітників. Хороша новина: вам не потрібно ставати програмістом або технічним спеціалістом, щоб захистити себе та свою організацію від поширених загроз. Однак слід бути готовими інвестувати зусилля, енергію та час у розробку та впровадження надійного організаційного плану безпеки. Якщо ви ніколи не думали про кібербезпеку у своїй організації, не мали часу приділити уваги цьому питанню або знаєте деякі основні аспекти, але вважаєте, що ваша організація може підвищити рівень своєї кібербезпеки, цей Довідник для вас. Незалежно від того, звідки ви, цей Довідник має на меті надати вашій організації важливу інформацію, необхідну для створення надійного плану безпеки - плану, що виходить за рамки простого викладення слів на папері й дає змогу втілити найкращі практики в життя.

Що таке план безпеки і навіщо він потрібен моїй організації?

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 вашої 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 вашій організації 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 вашій організації пройти такий процес. Якщо ви зможете отримати доступ до такого рівня професійних знань, це того варте, але навіть якщо ви не можете пройти повну оцінку, вам слід зустрітися з представниками своєї організації, щоб ретельно розглянути такі ключові питання.

1 Які активи має ваша організація і що ви хочете захистити?

Ви можете почати відповідати на ці запитання **шляхом створення каталогу всіх активів вашої організації**. 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 супротивники, які їхні можливості та мотивація?

«Супротивник» — це термін, що зазвичай використовується в організаційній безпеці. Простою мовою, супротивники — це суб'єкти (індивідууми чи групи), які зацікавлені в завданні цільової шкоди вашій організації, перешкоджанні вашій роботі та отриманні доступу або знищенні вашої інформації. Це ваші вороги. Приклади потенційних супротивників можуть включати фінансових шахраїв, конкурентів, місцеві чи національні органи влади або уряд, а також ідеологічно чи політично вмотивованих хакерів. Важливо скласти список своїх супротивників і критично подумати про те, хто може захотіти негативно вплинути на вашу організацію та співробітників. Хоча зовнішніх діячів (наприклад, іноземний уряд чи конкретну політичну групу) легко уявити супротивниками, пам'ятайте, що супротивниками 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 супротивником, наприклад, якщо випадково видалите важливі файли або надішлете приватні повідомлення не тій людині.

Мотиви супротивників, ймовірно, відрізнятимуться, як і їхні можливості, інтереси та стратегії. Чи зацікавлені вони в дискредитації вашої організації? Можливо, вони мають намір змусити вас замовчати? А може вони вважають вашу організацію конкурентом і хочуть отримати над вами перевагу? Важливо розуміти мотивацію супротивника, оскільки це може допомогти вашій організації краще оцінити загрози, які він може становити.

3 З якими загрозами зіштовхується ваша організація? 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 ваша організація могла 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 супротивників, аналіз минулих інцидентів безпеки, досвід інших подібних організацій і, звісно, наявність існуючих стратегій зменшення ризику, запроваджених вашою організацією.

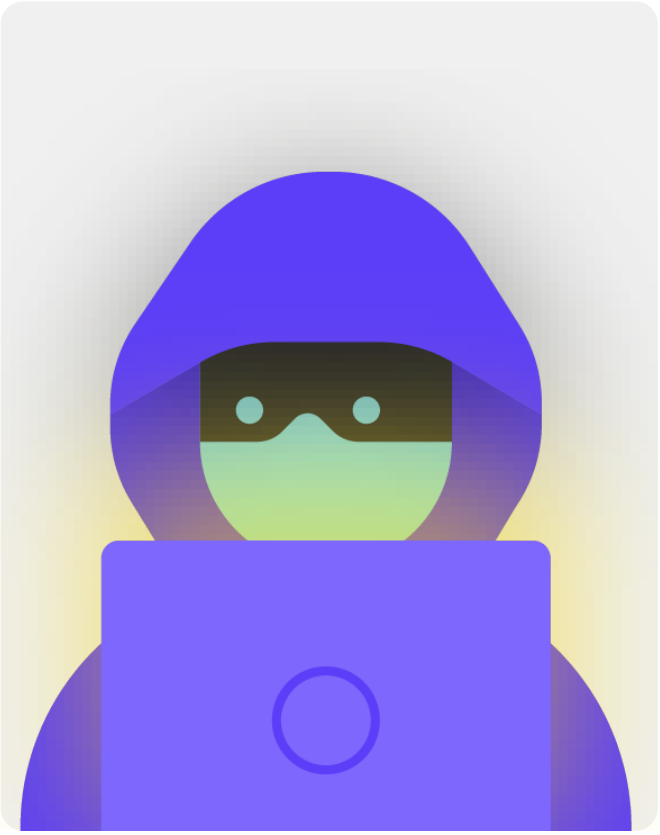
Щоб оцінити наслідки загрози, подумайте, що трапиться з організацією, якщо загроза справді виникне. Поставте такі запитання: «Якої шкоди, фізичної та психічної, завдасть загроза нам як організації та її співробітникам як людям?», «Наскільки тривалим буде ефект?», «Чи створить це інші шкідливі ситуації?» та «Як вона завадить здатності досягати цілей нашої організації 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: усунувши найбільші загрози, ви зробите багато, щоб захистити себе, своїх колег і свою організацію.



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 супротивників і загрози, які вони представляють), сама по собі може бути конфіденційною, тому важливо зберігати її захищеною.



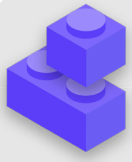
Створення плану кібербезпеки вашої організації

Хоча план безпеки кожної організації 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 найбільш значними витратами, пов'язаними із впровадженням ефективного плану безпеки, буде час, необхідний вам і вашій організації для обговорення, вивчення та реалізації вашого нового плану. Однак, враховуючи ризики, з якими може зіткнутися ваша організація, ці інвестиції будуть більше, ніж виправданими.

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 у вашій організації.



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. Як для громадської організації, додаток **SOAP** («Захист організацій за допомогою автоматизованого формування політики») буде для вас безкоштовним і допоможе спростити й автоматизувати створення плану безпеки.

Також 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

Формування культури безпеки

Міцна основа: захист облікових записів і пристроїв

Безпечна комунікація і зберігання даних

Безпека в інтернеті

Захист фізичної безпеки

Що робити, коли все йде не так

Безпека залежить від людей, і щоб захистити свою організацію, ви повинні переконатися, що всі співробітники і волонтери, які беруть участь у її роботі, серйозно ставляться до кібербезпеки. Змінити культуру безпеки важко, але кілька простих кроків і серйозних розмов допоможуть створити атмосферу, що зміцнить стійкість вашого персоналу й організації перед обличчям загроз безпеці. Один із найпростіших, але найважливіших кроків для створення такої організаційної культури безпеки – це інформування про неї всередині вашої організації, лідери якої повинні завжди демонструвати дотримання цієї культури.

Інтегрування безпеки до вашої звичайної операційної структури

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

На таких зустрічах члени команди 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 члени команди 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 персоналу, 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 організації настільки сильна, наскільки сильна її 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 членам 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 організації, наприклад, під час оформлення співробітників на роботу, а також припинити доступ до систем під час їх звільнення. Безпека має бути не «ще однією річчю», про яку слід турбуватися, а радше ***невід'ємною частиною стратегії та діяльності*** організації.

Пам'ятайте про те, що всі плани безпеки слід вважати актуальними документами. Їх слід регулярно переглядати й обговорювати, особливо коли до організації приєднуються нові співробітники чи волонтери або змінюється контекст безпеки.

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

Отримання організаційної підтримки

Також частиною успішної культури безпеки є забезпечення організаційної підтримки 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 організаційної 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. Зараз багато донорів вимагають від одержувачів грантів мати надійну систему безпеки, тому доведення цієї вимоги до відома персоналу також може бути хорошим способом досягти більшої організаційної підтримки. Говорячи про безпеку, уникайте тактики залякування. Іноді загрози, з якими стикається ваша організація та її 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 весь персонал (і волонтерів) цим новим найкращим методам.

Обов'язкове проведення регулярного навчання, а також відвідування тренінгів та оцінювання результатів роботи персоналу, є 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.



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 персоналу, щоб повідомляти про проблеми та просити про допомогу.**
- **Оновлюйте план безпеки щорічно або після серйозних змін в організації.**



Міцна основа: захист облікових записів і пристроїв

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

Через них ви отримуєте доступ до конфіденційної інформації, спілкуєтеся всередині організації та зі сторонніми особами, а також зберігаєте в них особисту інформацію. Якщо вони не захищені, то все це та багато чого іншого можуть зазнати впливу загрози. 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 супротивник отримає доступ до облікових записів вашої організації в соціальних мережах, він може легко зашкодити вашій репутації та довірі до вас, підриваючи успіх вашої роботи. 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 супротивників. Хакери охоче виберуть найлегшу ціль і зламають особисті облікові записи чи домашні комп'ютери, якщо ваша команда використовує їх для спілкування та доступу до важливої інформації.

Безпечні облікові записи та громадянське суспільство

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 супротивників до складних інструментів злому паролів, найкращі методи захисту паролів і двофакторна автентифікація є обов'язковими елементами безпеки для громадських організацій. Про один з прикладів атаки на облікові записи громадянського суспільства Facebook повідомив у 2020 році. Відповідно до його звіту, хакерські групи в Бангладеш атакували облікові записи місцевих громадських активістів, журналістів і релігійних меншин. На жаль, хакерам вдалося зламати деякі з цих облікових записів Facebook, включно з адміністратором сторінки локальної групи у Facebook. Отримавши доступ до облікового запису адміністратора, хакери видалили решту адміністраторів, захопили та вимкнули сторінку, не даючи групі ділитися важливою інформацією та спілкуватися зі своєю аудиторією. Розслідування Facebook виявило, що облікові записи, ймовірно, були зламані різними способами, зокрема шляхом зловживання процесом відновлення облікового запису. Якби всі облікові записи використовували двофакторну автентифікацію, хакерам було б набагато складніше ефективно здійснити такі атаки.



Захищені облікові записи: паролі та двофакторна автентифікація

У сучасних умовах ваша 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 вебсайтів 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 надійного зберігання паролів і використання двофакторної автентифікації в усій організації.

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 вебсайтів. 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 вебсайтах, 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 для кожного в організації важливо використовувати довгий, випадковий, унікальний пароль для кожного з особистих і організаційних 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?

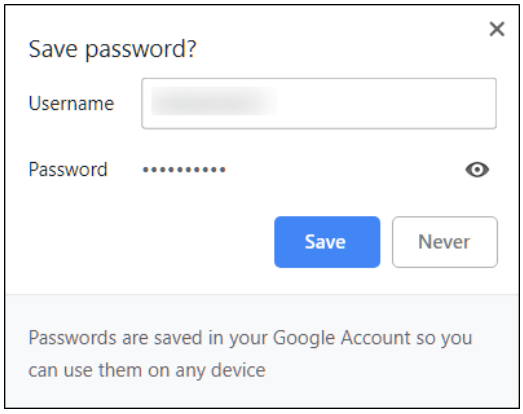
На жаль, існує багато поширених методів управління паролями, які не є безпечними. Зберігання паролів на аркушах паперу (якщо ви не зберігаєте їх під замком у сейфі) означає ризик фізичного викрадення, потрапляння на сторонні очі, легкої втрати чи пошкодження. Якщо ви зберігаєте паролі в документі на 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.

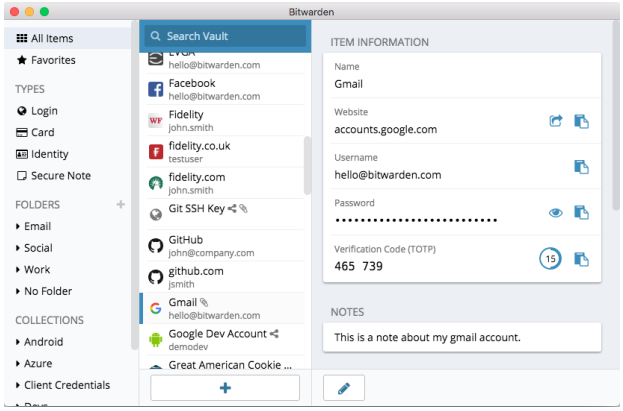
Чому слід довіряти менеджеру паролів?

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 підвищує ймовірність того, що люди у вашій організації продовжуватимуть неправильно створювати паролі та обмінюватися даними.

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 вашої організації. Менеджери паролів також включають специфічні для організації 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?

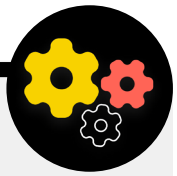
Існує багато надійних інструментів керування паролями, які можна налаштувати менш ніж за 30 хвилин. Якщо ви шукаєте надійний онлайн-варіант для своєї організації, до якого люди можуть отримати доступ із кількох пристроїв у будь-який час, 1Password (від 2,99 дол. США за користувача на місяць) або безкоштовний із відкритим кодом Bitwarden мають належну технічну підтримку та добрі хороші. 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 ваша організація надає спільний доступ до паролів, обов'язково скасуйте доступ до них (і змініть самі паролі) після звільнення співробітників. Наприклад, у колишніх співробітників не має бути доступу до пароля вашої організації 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 вебсайтів. 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 для вашої організації

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 загальноорганізаційного менеджера паролів не тільки забезпечують більший захист, але й зручність для персоналу. 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 вашій 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?

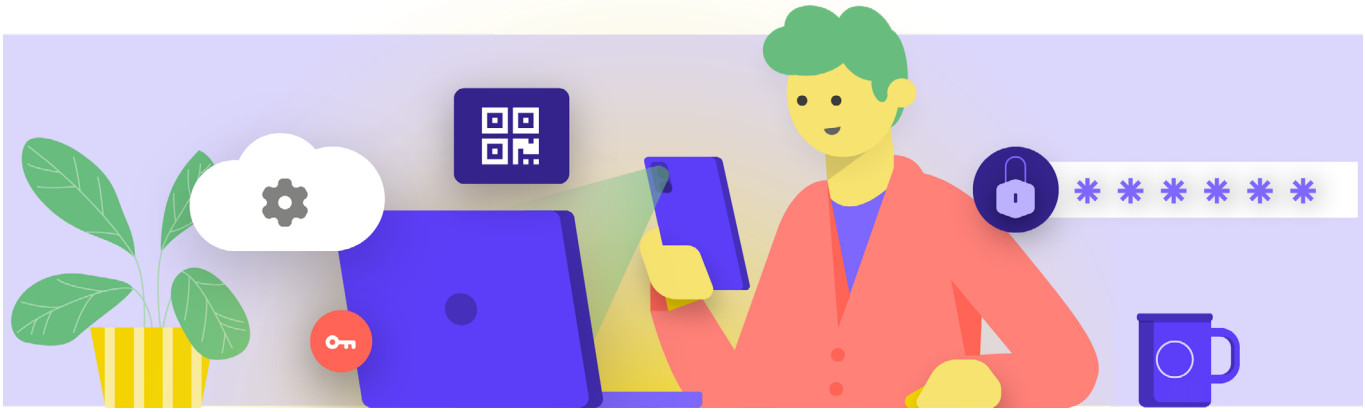
Яким би надійним не був захист паролів, хакери надто часто обходять паролі. Щоб захистити ваші облікові записи від деяких типових існуючих загроз, потрібен інший рівень захисту. Ось тут і вступає в гру багатофакторна або двофакторна автентифікація, що називається MFA або 2FA. Існує багато чудових посібників 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 вашій організації. 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). Вкрай важливо переконатися, що всі співробітники організації використовують 2FA у своїх облікових записах.

ЯК НАЛАШТУВАТИ ДВОФАКТОРНУ АВТЕНТИФІКАЦІЮ?

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** з деякими рекомендаціями, які ключі слід купувати. Майте на увазі, що один і той самий ключ безпеки можна використовувати для будь-якої кількості облікових записів. Хоча ключі безпеки є дорогими для багатьох організацій, такі ініціативи, як **Програма додаткового захисту Google** або **AccountGuard від Microsoft** надають ці ключі безкоштовно деяким групам ризику. Зв'яжіться з людьми, які надали вам Довідник, щоб дізнатися, чи можуть вони зв'язати вас із цими програмами або напишіть на адресу **cyberhandbook@ndi.org**.



Програми автентифікації

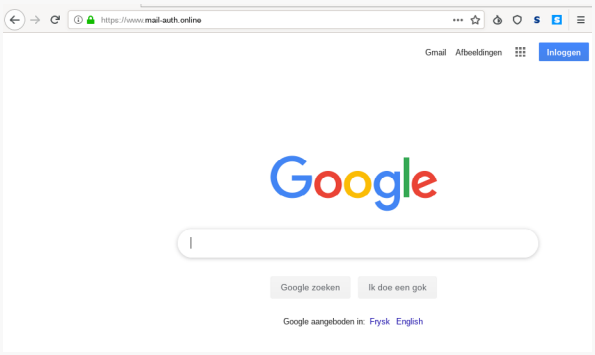
Другим найкращим варіантом 2FA є програми автентифікації. Ці служби дозволяють отримати тимчасовий двофакторний код входу через мобільний додаток або push-повідомлення на смартфоні. Деякі популярні та надійні варіанти включають Google Authenticator, Authy та Duo Mobile. Додатки Authenticator також чудові, 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 вебсайті. Вводіть коди входу лише на дійсних вебсайтах. 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 супротивник 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.

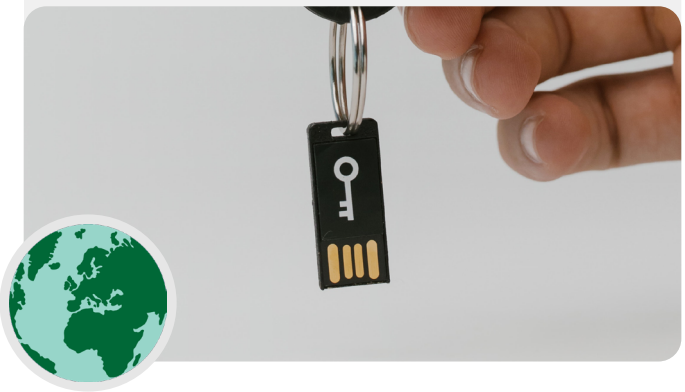
2FA і громадянське суспільство

Згідно з нещодавнім звітом Amnesty International, хакери, націлені на правозахисників в Узбекистані, використовували фішингові атаки, щоб обманом змусити користувачів надати паролі та двофакторні коди автентифікації для облікових записів електронної пошти через підроблені сторінки входу в Gmail. Такі атаки стають все більш поширеним способом «обійти» двофакторну автентифікацію. Важливо — навіть із 2FA — бути обережним із тим, де ви вводите коди. А ще краще усунути цей ризик, застосувавши фізичні ключі безпеки.



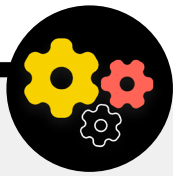
Ключі безпеки в реальному світі

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?

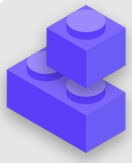
Якщо ви використовуєте ключ безпеки, поводьтеся з ним так само, як і з ключем від будинку чи квартири, якщо він у вас є. Одним словом, не губіть його. Так само, як і для ключа від будинку, завжди варто мати резервний ключ, зареєстрований у вашому обліковому записі, що зберігається у надійному місці під 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 вебсайтів (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 співробітники вашої організації знають про ці кроки, коли вони починають вмикати 2FA для всіх своїх облікових записів.



Застосування 2FA у вашій організації

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 ваших 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:

- **Вимагайте надійних паролів для всіх облікових записів організації; заохочуйте їх для особистих облікових записів співробітників і волонтерів.**
- **Запровадьте надійний менеджер паролів для організації (а також заохочуйте його використання для особистих облікових записів 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 звільняються з організації.**
- **Надсилайте паролі лише безпечно, наприклад через менеджер паролів вашої організації або програми з наскрізним шифруванням.**
- **Вимагайте 2FA для всіх облікових записів організації та заохочуйте персонал також налаштувати 2FA для всіх особистих облікових записів.**
  - За можливості, видайте фізичні ключі безпеки всьому персоналу.
  - 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 уважності до того, які типи пристроїв купує та використовує ваша організація та персонал. 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 супротивнику. 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 для організації, потенційні ризики для безпеки організацій, які виступають за демократію, права людини та підзвітність уряду, свідчать про необхідність вибору інших варіантів пристроїв, оскільки такий доступ до даних допомагає уряду Китаю та іншим урядам цілеспрямовано впливати на певних осіб і спільноти. Ваші супротивники можуть поставити під загрозу безпеку ваших пристроїв — і все, що ви робите на цих пристроях — шляхом отримання фізичного або «віддаленого» доступу до пристроїв.

Безпека пристроїв і громадянське суспільство

Деякі з найдосконаліших шкідливих програм були розроблені та застосовані по всьому світу для цільового впливу на громадські організації та правозахисників. В Індії, наприклад, Amnesty International повідомила, що у 2020 році принаймні дев'ять правозахисників стали мішенню шпигунських програм (типу шкідливого програмного забезпечення) на їхніх мобільних пристроях і комп'ютерах. Шпигунські програми були доставлені через серію фішингових електронних листів із посиланнями на заражені файли, надісланих через Firefox Send (програма для обміну файлами, яка більше не працює). Пристрої людей, які відкривали файли, заражалися програмним забезпеченням, що записувало аудіо, перехоплювало натискання клавіш і повідомлення, фактично поставивши їх під повний нагляд зловмисників. Такі атаки, що часто спрямовані на групи громадянського суспільства та їх окремих співробітників, на жаль, є поширеним способом для зловмисників отримати «віддалений» доступ до пристрою.



ФІЗИЧНИЙ ДОСТУП ДО ПРИСТРОЮ ЧЕРЕЗ ВТРАТУ АБО КРАДІЖКУ

Щоб запобігти фізичному доступу, важливо забезпечити фізичну безпеку своїх пристроїв. Не дозволяйте супротивникам 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 безпеки або інші системи моніторингу, особливо якщо ваша організація належить до групи високого ризику. Нагадайте персоналу 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 обмежити 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», щоб розблокувати екран. Додаткові поради щодо блокування екрана містяться у Data Detox Kit від Tactical Tech. Використання надійних паролів на пристрої значно ускладнює супротивникам швидкий доступ до інформації на ньому в разі крадіжки чи конфіскації. За наявності надійного паролю можна активувати Face ID або розблокування відбитком пальця, але обов'язково вимкніть ці функції (залишивши надійний пароль на місці) перед будь-якими діями високого ризику, такими як протести чи перетин кордону, якщо ви та ваш персонал стурбований конфіскацією пристрою владою. Якщо пристрої, видані організацією, мають функцію «Знайти мій пристрій» на iPhone або на Android, зобов'яжіть співробітників активувати її. Заохочуйте персонал використовувати ці функції також на персональних пристроях. Якщо ці функції ввімкнено, власник пристрою (або довірена особа) може знайти пристрій або дистанційно стерти його вміст у разі викрадення, втрати чи конфіскації. На iPhone ви також можете налаштувати пристрій на автоматичне стирання після кількох невдалих спроб входу. Такі функції керування пристроєм стають критично важливими для організації, коли пристрій із конфіденційною інформацією втрачається або потрапляє в чужі руки.

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. Вам слід налаштувати на всіх пристроях організації функцію під назвою «**повнодискове шифрування**» за можливості. 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 націлена 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 та як би вони не поширювалися, шкідливі програми можуть зіпсувати комп'ютери, викрадати та знищувати дані, довести до банкрутства організації, порушувати конфіденційність і наражати користувачів на небезпеку. Одним словом, шкідливі програми дійсно небезпечні. Однак є кілька простих кроків, які ваша організація може зробити, щоб захиститися від цієї поширеної 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 вони точно пропустять 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.

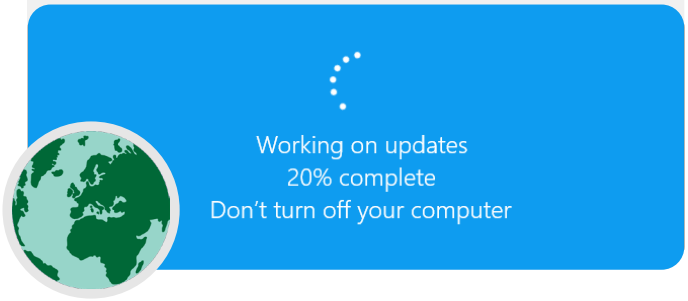
Якщо ви використовуєте Bitdefender або інший інструмент захисту від шкідливих програм у вашій організації, переконайтеся, що не запускаєте два інструменти одночасно. Багато з них визнають поведінку іншого підозрілою та зупинять його роботу, через що обидва працюють неправильно. Bitdefender або інші визнані 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 вебсайті відповідної програми. Як обговорювалося в розділі «Фішинг» Довідника, важливо бути уважним під час перегляду вебсайтів. Перевірте, куди веде посилання (навівши на нього курсор), перш ніж клацнути, подивіться на адресу вебсайту 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».

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.

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.



Заощаджуйте гроші та підвищуйте безпеку пристроїв за допомогою Tails у вашій організації

Дуже безпечним варіантом, для налаштування якого потрібні певні технічні навички, є операційна система Tails. Цією портативною операційною системою можна користуватися безкоштовно, і ви можете завантажити її прямо з USB, без використання ліцензованих операційних систем Windows або Mac. Tails також є хорошим вибором для тих, хто входить у групу надзвичайно високого ризику, оскільки ця система містить широкий спектр функцій для підвищення конфіденційності. Ці функції включають інтеграцію Tor (про яку йдеться нижче) для захисту вашого вебтрафіку та повне стирання пам'яті кожного разу, коли ви вимикаєте операційну систему. Ці функції, по суті, дозволяють починати з чистого аркуша кожного разу, коли ви перезавантажуєте комп'ютер. Tails також має режим збереження, який дозволяє зберігати важливі файли та налаштування протягом кількох сеансів, за необхідності.

Ще одним варіантом безкоштовної безпечної операційної системи є Qubes OS. Незважаючи на те, що Qubes не є найпростішим варіантом для технічно недосвічених користувачів, ця система розроблена для обмеження загрози шкідливих програм та є ще одним варіантом, який слід розглянути для досвідчених користувачів у вашій організації, особливо якщо витрати на ліцензування є проблемою.

Що робити, якщо ми не можемо дозволити собі легальне програмне забезпечення?

Придбання ліцензійних версій популярного програмного забезпечення, як-от Microsoft Office (Word, Powerpoint, Excel), для всієї вашої організації може бути дорогим, але обмежений бюджет не є виправданням завантажувати піратські версії програмного забезпечення або не оновлювати їх. Це не питання моралі – це питання безпеки. Піратське програмне забезпечення часто наповнене шкідливими програмами, і його часто неможливо виправити для усунення прогалин у безпеці. Якщо ви не можете дозволити собі програмне забезпечення, яке потрібне вашій організації, існує широкий вибір чудового безкоштовного програмного забезпечення з відкритим кодом LibreOffice (заміна стандартних програм Microsoft Office) або GIMP (заміна Photoshop), що може задовольнити ваші потреби. Також розгляньте можливість реєстрації через Tech Soup, організацію, що пропонує великі знижки на популярне програмне забезпечення для неприбуткових організацій. Навіть якщо ви можете дозволити собі законне програмне забезпечення та додатки, ваш пристрій все одно під загрозою, якщо основна операційна система нелегальна. Отже, якщо ваша організація не може дозволити собі ліцензії Windows, розгляньте дешевші альтернативи, як-от Chromebook, які є чудовим і простим у захисті варіантом, якщо ваша організація працює переважно в хмарному середовищі. Якщо ви використовуєте Google Docs або Microsoft 365, вам зовсім не потрібно багато програм для комп'ютера – безкоштовних редакторів документів і електронних таблиць у вебоглядачі більш ніж достатньо для майже всіх цілей. Іншим варіантом, якщо у вас є персонал із технічними навичками, є встановлення безкоштовної операційної системи на базі Linux (альтернатива операційним системам Windows і Mac з відкритим кодом) на кожному комп'ютері. Одним із популярних і досить зручних варіантів Linux є Ubuntu. Незалежно від того, яку операційну систему ви виберете, переконайтеся, що хтось в організації відповідає за регулярну перевірку співробітників, щоб переконатися, що вони встановили останні оновлення.

Коли ви приймаєте рішення про новий інструмент або систему, подумайте, як ваша організація може підтримувати їх технічно та фінансово протягом тривалого часу. Поставте собі такі запитання: Чи можете ви дозволити собі утримувати персонал, необхідний для безпечного обслуговування цього програмного забезпечення? Чи можете ви платити за подовження підписки? Чи маєте ви доступ до знижок від таких груп, як вищезгадана Tech Soup? Відповіді на ці запитання допоможуть переконатися, що ваші програмні та технологічні стратегії з часом будуть все більш успішними.



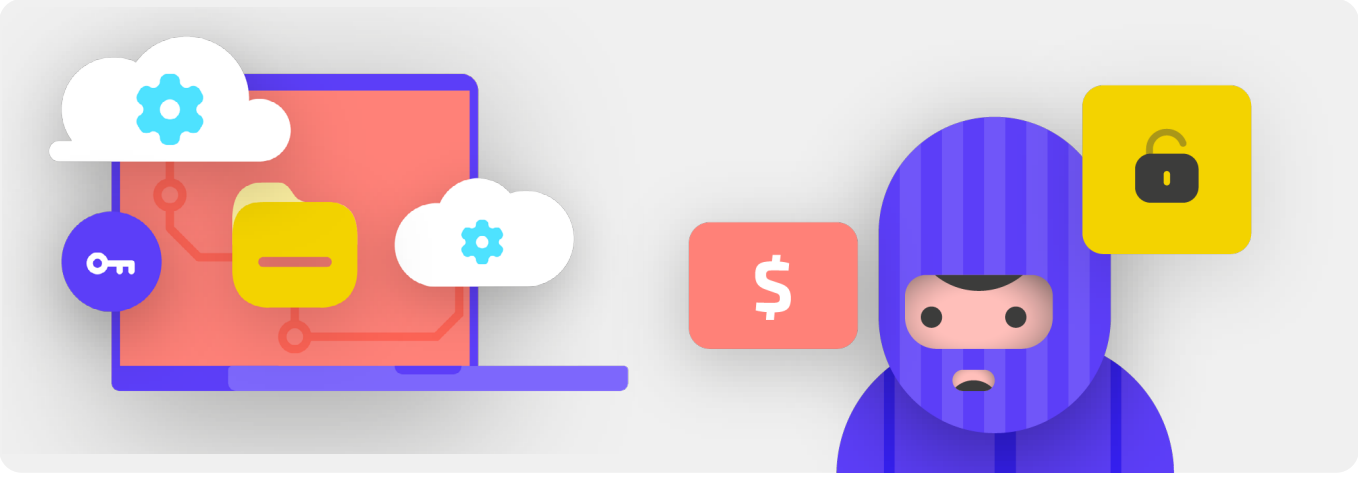
Захист пристроїв

- **Навчіть персонал ризикам, пов'язаним із шкідливими програмами, 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.
- **Переконайтеся, що всі пристрої використовують ліцензійне програмне забезпечення.**
  - Якщо вартість непомірно висока, перейдіть на безкоштовний альтернативний варіант.
- **Вимагайте захисту паролем усіх організаційних пристроїв, у тому числі персональних мобільних пристроїв, які використовуються для комунікації, пов'язаної з роботою.**
- **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 є найпоширенішою та найефективнішою атакою на організації в усьому світі. Цей метод використовується як дрібними шахраями, так і найбільш просунутими військовими спеціалістами на державному рівні.

Простими словами фішинг трапляється, коли супротивник 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 вебсайті, 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 вашій організації може вжити, щоб захиститися від більшості атак. Наведені нижче поради щодо захисту від фішингу підготовлено на основі поглибленого посібника з фішингу, розробленого Freedom of the Press Foundation. З ними слід ознайомити співробітників вашої організації (й інших контактних осіб) та інтегрувати їх у ваш план безпеки:

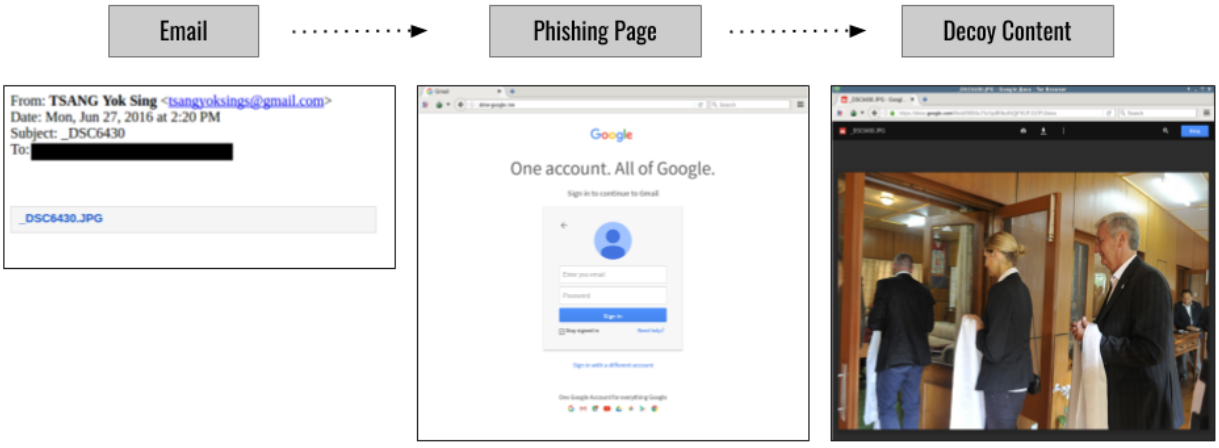
Іноді поле «від» містить фальшиві дані

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 громадянське суспільство

Складні, персоналізовані фішингові атаки щодня спрямовані на групи громадянського суспільства по всьому світу.

Один із прикладів такої атаки наведено в звіті The Citizen Lab за 2018 рік Шпигунство за бюджетні кошти: секрети фішингової операції, націленої на представників тибетського суспільства. Ця дуже недорога і проста, але неймовірно ефективна фішингова атака була спрямована проти тибетських правозахисників та інших активістів. Атака почалася з фішингового електронного листа (показаного ліворуч), надісланого зі стандартної адреси Gmail, що містив лише посилання на файл зображення. Після натискання посилання спрямовує ціль на підроблену сторінку входу в електронну пошту Google (на зображенні посередині), що використовується для викрадення логіну й паролю облікового запису. Якби жертви надали облікові дані на підробленій сторінці, їхні облікові записи було б легко зламано. Після введення імені користувача та пароля на підробленому вебсайті жертви перенаправляються на зображення (показане праворуч) делегатів на тибетській зустрічі. Зображення було додано як приманка, щоб змусити об'єктів фішингу повірити, що вони зайшли у свій справжній обліковий запис Google, і зменшити будь-які можливі підозри щодо шкідливого характеру електронного листа.



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.



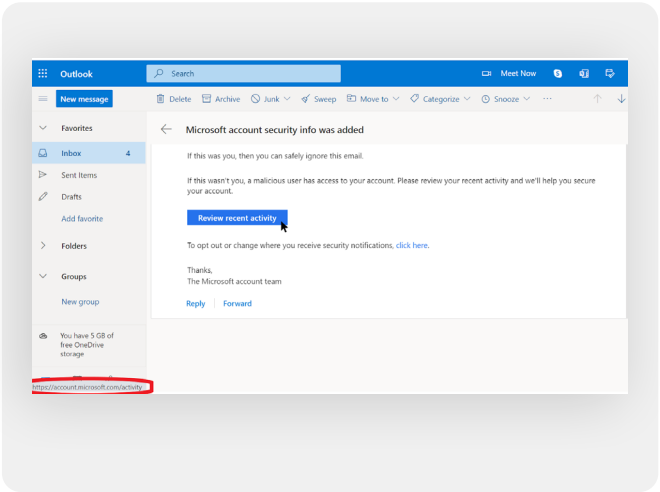
Захист від фішингу для вашої організації

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. Ще один просунутий варіант, який можна розглянути для застосування у вашій організації, — це служба фільтрації безпечної системи доменних імен (DNS). Організації можуть використовувати цю технологію для блокування дій персоналу для попередження випадкового доступу або взаємодії із шкідливим вмістом, що забезпечує додатковий рівень захисту від фішингу. Нові служби, як-от Gateway від Cloudflare надають такі можливості організаціям, не вимагаючи великих сум грошей (програма Gateway, наприклад, безкоштовна для 50 користувачів). Додаткові безкоштовні інструменти, в тому числі Quad9 із 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).

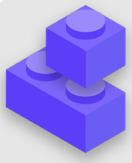
Перевірити посилання в електронному листі на мобільному пристрої, не натиснувши випадково, складніше, тому будьте обережні. Ви можете перевірити, куди веде посилання, на більшості смартфонів, довгим натисненням (утриманням) посилання, доки не з'явиться повна URL-адреса.
У разі фішингу через SMS і програми 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 вебсайти, незнайомі вам. Якщо ви сумніваєтеся, виконайте пошук сайту, взявши назву сайту в лапки (наприклад: «www.badwebsite.com»), щоб перевірити, чи це справжній вебсайт. 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 вебсайті, не робіть цього, якщо ви не впевнені на 100 відсотків, що електронний лист є непідробленим і спрямовує вас на відповідний вебсайт. Багато фішингових атак надають посилання, що спрямовують на підроблені сторінки входу в Gmail, Facebook або на інші популярні вебсайти. 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 у вашій організації отримує небажане вкладення, посилання, зображення, інше підозріле повідомлення чи дзвінок, важливо негайно повідомити про це спеціалісту з IT-безпеки вашої організації. Якщо у вас немає такої особи, слід призначити її під час розроблення плану безпеки. Співробітники 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.
Окрім того, щоб поділитися наведеними вище порадами з усіма співробітниками та волонтерами, ви також можете потренуватися розпізнавати фішинг за допомогою Тесту фішингу від Google.
Ми також наполегливо рекомендуємо організовувати регулярні тренінги з фішингу з персоналом, щоб перевірити обізнаність і заохотити людей бути пильними. Таке навчання може проводитися формально у формі регулярних організаційних зустрічей або більш неформально. Важливо, щоб усі в організації відчували себе комфортно, коли вони ставлять запитання про фішинг, повідомляють про фішинг (навіть якщо вони вважають, що могли зробити помилку, наприклад, натиснувши посилання), і що кожен може допомогти захистити вашу організацію від цієї загрози високого ризику і високої ймовірності.



Фішинг

- **Регулярно навчайте персонал 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 персоналу про найкращі практики, як-от:**
  - 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 в організації механізм звітності та призначити особу для отримання повідомлень про фішинг.
  - Винагороджувати за повідомлення, а не карати за невдачу.



Безпечна комунікація і зберігання даних

Комунікація й обмін даними

Щоб прийняти найкраще для вашої організації 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 повідомлення, передані в межах організації, можуть побачити супротивники. 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 й організацію залежно від характеру повідомлень і вмісту, яким ви ділитеся.

Безпечна комунікація та громадянське суспільство

Тисячі демократичних і правозахисних активістів і організацій щодня покладаються на захищені канали зв'язку, щоб зберегти конфіденційність розмов у складних політичних умовах. Без таких методів безпеки конфіденційні повідомлення можуть бути перехоплені та використані владою для дій, націлених проти активістів, і для розгону протестів. Один яскравий і добре задокументований приклад цього стався після виборів у Білорусі 2010 року. Як зазначено в цьому звіті Amnesty International, записи телефонних розмов та інші незашифровані повідомлення були перехоплені урядом і використані в суді проти відомих опозиційних політиків та активістів, багато з яких провели роки у в'язниці. У 2020 році в Білорусі під час чергового сплеску післявиборчих протестів тисячі протестувальників встановили зручні безпечні програми обміну повідомленнями, які були недоступні лише десять років тому, щоб захистити свої конфіденційні комунікації.



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 шляхом спостереження від Electronic Frontier Foundation надається практичне пояснення (з ілюстраціями) того, що означає шифрування:

Незашифровані повідомлення

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 супротивник 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 цьому зображенні).



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 супротивник 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 шляхом спостереження дані з якого наведено далі в адаптованій формі:

Шифрування транспортного рівня

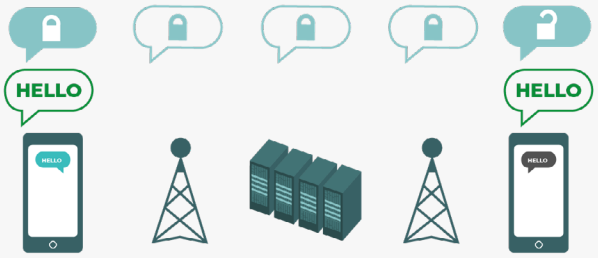
Шифрування транспортного рівня, також відоме як захист транспортного рівня (TLS), захищає повідомлення під час їх переміщення з вашого пристрою на сервери програми/служби обміну повідомленнями, а звідти — на пристрій одержувача. Це захищає їх від очей хакерів, які сидять у вашій мережі або у мережі інтернет-провайдера 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.

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.

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

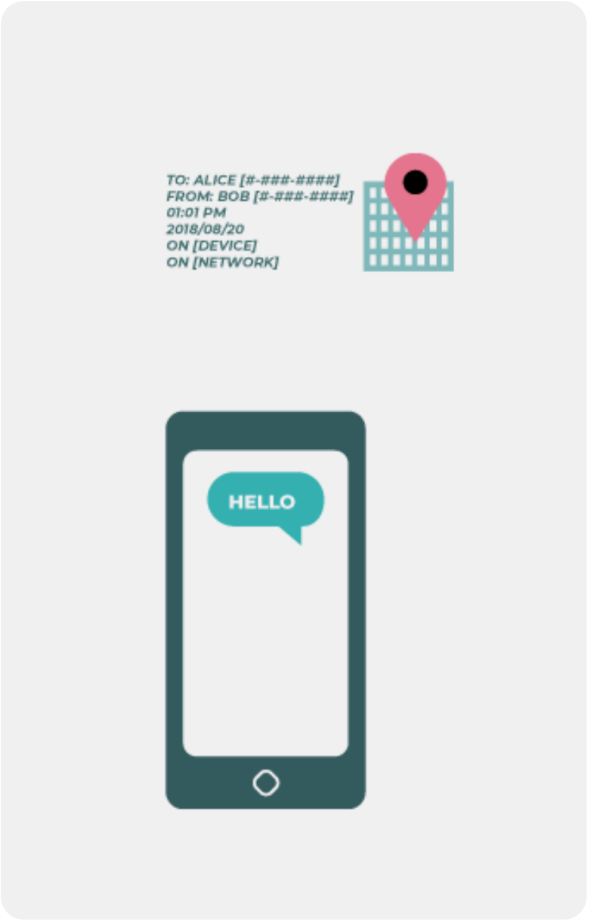
Якщо вам потрібно використовувати наскрізне шифрування або ви просто хочете застосувати найкращі методи незалежно від контексту загроз вашої організації, ось кілька прикладів надійних служб, які, **станом на 2022 рік,** пропонують обмін повідомленнями та дзвінки з наскрізним шифруванням. Цей розділ Довідника 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.

Рекомендовані засоби комунікації 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** • **OnionShare + додаток для обміну повідомленнями з наскрізним шифруванням, як-от Signal**

ЩО ТАКЕ МЕТАДАНІ І ЧИ ВАРТО ЗА НИХ ХВИЛЮВАТИСЯ?

З ким розмовляєте ви та ваші співробітники, а також коли і де ви розмовляєте з ними часто є такою само секретною інформацією, 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 шляхом 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.

Навіть мала частка метаданих може розповісти багато про діяльність вашої організації. Давайте подивимося, наскільки метадані насправді можуть бути відкритими для хакерів, державних установ і компаній, які їх збирають.

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 кілька співробітників вашої організації надіслали повідомлення відомому місцевому спеціалісту з питань цифрової безпеки. Однак тема повідомлень залишиться таємницею.

Вони знатимуть, що ви отримали електронний лист від лабораторії перевірки 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.

Вони знатимуть, що ви отримали електронний лист від місцевої правозахисної групи з темою «Скажіть уряду: припиніть зловживати владою!». Але вміст електронного листа не буде видимий для них.

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 про ризики (за наявності), якщо певні супротивники дізнаються, з ким спілкується ваша організація, коли ви з ними спілкувалися, а також (у випадку електронної пошти) загальну тему повідомлень вашої організації.

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.

А ЯК ЩОДО ЕЛЕКТРОННОЇ ПОШТИ?

Більшість постачальників послуг електронної пошти, як-от Gmail, Microsoft Outlook і Yahoo Mail, використовують шифрування транспортного рівня. Тому якщо ви маєте надсилати конфіденційний вміст електронною поштою та хвилюєтеся, що ваш постачальник послуг електронної пошти може бути зобов'язаний за законом надавати інформацію про ваші повідомлення уряду чи іншому супротивнику, ви можете розглянути можливість використання електронної пошти з наскрізним шифруванням. Однак майте на увазі, що навіть параметри електронної пошти з наскрізним шифруванням не оптимальні з точки зору безпеки, наприклад, вони не шифрують рядки теми електронних листів і не захищають метадані. Якщо вам потрібно повідомити дуже секретну інформацію, електронна пошта не найкращий варіант. Натомість оберіть варіанти безпечного обміну повідомленнями, наприклад, через Signal.

Якщо ваша організація продовжує використовувати електронну пошту, важливо запровадити єдину систему для всієї організації. Це допоможе обмежити поширені ризики, які виникають, коли співробітники використовують особисті адреси електронної пошти для своєї роботи, наприклад, слабкий захист облікових записів. Надавши співробітникам облікові записи електронної пошти, створені організацією, ви можете застосувати передові методи, як-от надійні паролі та 2FA, для будь-яких облікових записів, якими керує ваша організація. Якщо, за аналізом, проведеним вами попередньо, вашій електронній пошті потрібне наскрізне шифрування, як Protonmail, так і Tutanota пропонують плани для організацій. Якщо шифрування транспортного рівня підходить для електронної пошти вашої організації, можуть стати у нагоді такі варіанти, як Google Workspace (Gmail) або Microsoft 365 (Outlook).

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 ПАРТНЕРИ ТА КОЛЕГИ ВИКОРИСТОВУЮТЬ ІНШІ ПРОГРАМИ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ. 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. Будьте хорошим прикладом для осіб, із якими ви контактуєте. Якщо вам доводиться використовувати інші, менш безпечні системи, будьте уважні до того, що ви говорите. Уникайте обговорення секретних тем. Деякі організації можуть використовувати одну систему для загального спілкування в чаті, а іншу для обговорення з керівництвом найбільш конфіденційних питань. 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 персоналу 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 шляхом спостереження.

Використання додатків для чатів у реальному світі

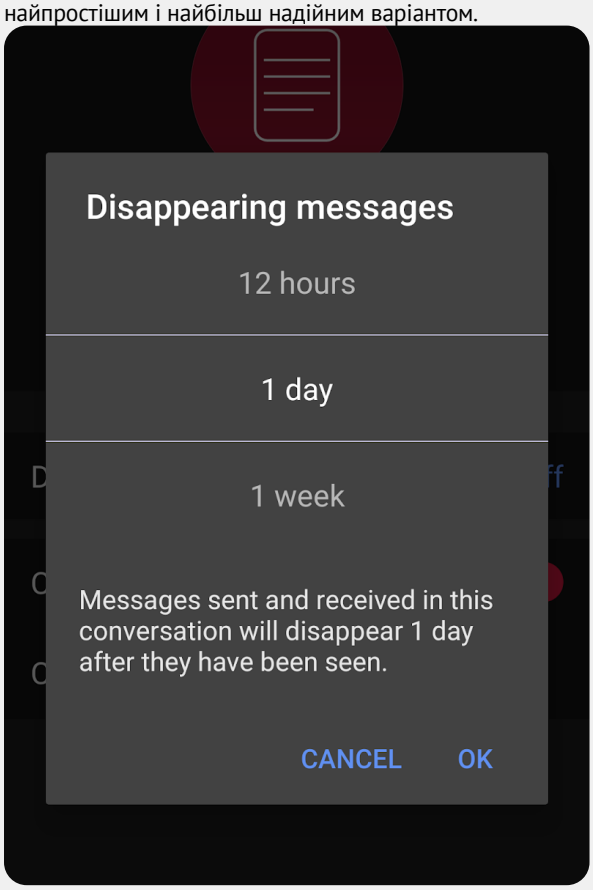
Щоб обмежити шкоду в разі втрати, викрадення чи конфіскації телефону, найкраще мінімізувати історію повідомлень, які зберігаються на вашому телефоні. Один із простих способів зробити це — увімкнути **«зникнення повідомлень»** для групових чатів вашої організації та заохочувати персонал зробити це також у своїх особистих чатах.

У Signal та інших популярних програмах обміну повідомленнями можна встановити таймер, щоб повідомлення зникали через певну кількість хвилин або годин після прочитання. Цей параметр можна налаштувати для окремого чату чи групи. Для більшості встановлення періоду зникнення в один тиждень дає достатньо часу, щоб знайти необхідну інформацію, не зберігаючи повідомлення, які вам ніколи не знадобляться, але які потенційно можуть бути використані проти вас у майбутньому. Пам'ятайте, що якщо у вас чогось немає, це неможливо вкрасти.

Щоб увімкнути зникнення повідомлень у Signal, відкрийте чат, торкніться імені людини/групи, з якою ви спілкуєтеся, натисніть зникаючі повідомлення, виберіть таймер і натисніть OK. Подібне налаштування є у WhatsApp.

У більш серйозних ситуаціях, коли необхідно негайно видалити повідомлення, можливо, через те, що телефон було вкрадено або ви надіслали повідомлення не тій особі, зверніть увагу, що Signal дозволяє видалити повідомлення для групи або окремої особи з усіх телефонів протягом трьох годин після надсилання шляхом простого видалення його з чату. Telegram залишається популярним у багатьох країнах, незважаючи на його обмеження шифрування, завдяки подібній функції, що дозволяє користувачам видаляти повідомлення з усіх пристроїв без обмежень.

Зважаючи на це, якщо ваша організація турбується про безпеку співробітників через повідомлення, які можна побачити на їхніх телефонах, то використання зникаючих повідомлень через короткий період часу, ймовірно, є найпростішим і найбільш надійним варіантом.



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

Зі збільшенням віддаленої роботи важливо мати безпечний варіант для великих групових відеодзвінків вашої організації. На жаль, наразі немає універсальних варіантів, які покривають всі потреби: зручність користування, підтримка великої кількості учасників і доступністьфункції співпраці, а також наявністьувімкненого наскрізного шифрування за замовчуванням.

Для груп до 40 осіб настійно рекомендується використовувати наскрізне шифрування Signal. До групових відеодзвінків у Signal можна приєднатися зі смартфона або за допомогою настільного додатка Signal на комп'ютері, що дозволяє ділитися екраном. 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.

Крім згаданих вище інструментів, **ця блок-схема**, розроблена Frontline Defenders, висвітлює деякі варіанти відеодзвінків і конференцій, які можуть бути корисними для вашої організації залежно від контексту ризику, з яким вона стикається.

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.

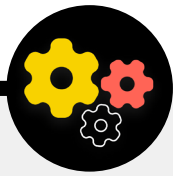
ЩО, ЯКЩО НАМ НАСПРАВДІ НЕ ПОТРІБНЕ НАСКРІЗНЕ ШИФРУВАННЯ ДЛЯ ВСІХ НАШИХ КОМУНІКАЦІЙ?

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 супротивником, Gmail не підходить), але ось кілька популярних і загалом надійних варіантів:

ЕЛЕКТРОННА ПОШТА	• **Gmail (через Google Workspace)** • **Outlook (через Office 365)** • Не розміщуйте власний сервер Microsoft Exchange для електронної пошти вашої організації. **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 Диск** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

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 у вашій організації таких пристроїв, як USB-накопичувачі, значно підвищує ймовірність встановлення шкідливих програм або крадіжки даних, а використання електронної пошти чи інших форм вкладень послаблює захист вашої організації від фішингових атак.



Організаційні альтернативи обміну файлами

Якщо ви шукаєте безпечний варіант обміну файлами для вашої організації, який не вбудовано безпосередньо в платформу обміну повідомленнями (або, можливо, ви стикаєтеся з обмеженнями розміру файлу під час передачі великих документів), розгляньте варіант OnionShare. **OnionShare** — це інструмент із відкритим кодом, що дозволяє безпечно й анонімно ділитися файлами будь-якого розміру. Відправник встановлює додаток OnionShare (доступний на комп'ютерах Mac, Windows і Linux), завантажує файли, якими хоче поділитися, і генерує унікальне посилання. Це посилання, що можна відкрити лише у вебоглядачі Tor, потім можна передати через будь-який безпечний канал обміну повідомленнями (наприклад, Signal) призначеному одержувачу. Одержувач може відкрити посилання у вебоглядачі Tor і завантажити файл(-и) на свій комп'ютер. Зауважте, що файли настільки безпечні, наскільки безпечним і метод, за допомогою якого ви ділитеся посиланням. Про роботу Tor буде пояснено більш детально в наступному розділі «Вищий рівень» Довідника, але для цілей передачі файлів у вашій організації пам'ятайте про OnionShare як про безпечну альтернативу обміну великими файлами на USB-накопичувачах в офісі, якщо тільки у вас немає надійного постачальника хмарного сховища.

Якщо ваша організація вже інвестувала в менеджер паролів, як описано в розділі про паролі цього Довідника, і вибрала обліковий запис преміум-класу або груповий обліковий запис Bitwarden, **Bitwarden Send** — це ще один варіант безпечного обміну файлами. Ця функція дозволяє користувачам створювати безпечні посилання для обміну зашифрованими файлами через будь-який безпечний канал обміну повідомленнями (наприклад, Signal). Розмір файлу обмежено 100 МБ, але Bitwarden Send дозволяє встановити дату закінчення терміну дії посилань, захистити паролем доступ до спільних файлів і обмежити кількість відкривань вашого посилання.



Безпечна комунікація й обмін даними

- **Вимагайте використання надійних служб обміну повідомленнями з наскрізним шифруванням для конфіденційних повідомлень вашої організації (в ідеалі, для всіх комунікацій).**
  - Знайдіть час, щоб пояснити персоналу та стороннім партнерам, чому безпечний зв'язок такий важливий; це сприятиме успішному втіленню вашого плану.
- **Встановіть політику щодо того, як довго ви зберігатимете повідомлення та коли/чи організація використовуватиме «зникаючі» повідомлення.**
- **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.
- **Використовуйте для своєї організації хмарні служби електронної пошти, як-от Office 365 або Gmail.**
  - Не намагайтеся встановити власний сервер електронної пошти.
  - Не дозволяйте співробітникам використовувати особисті облікові записи електронної пошти для робочих цілей.
- **Часто нагадуйте організації про найкращі методи безпеки, пов'язані з обміном повідомленнями та метаданими у групі.**
  - Слідкуйте за тим, хто входить до групи повідомлень, чатів і ланцюжків електронних листів.

Безпечне зберігання даних

Для більшості громадських організацій одним із найважливіших рішень є місце зберігання їхніх даних.

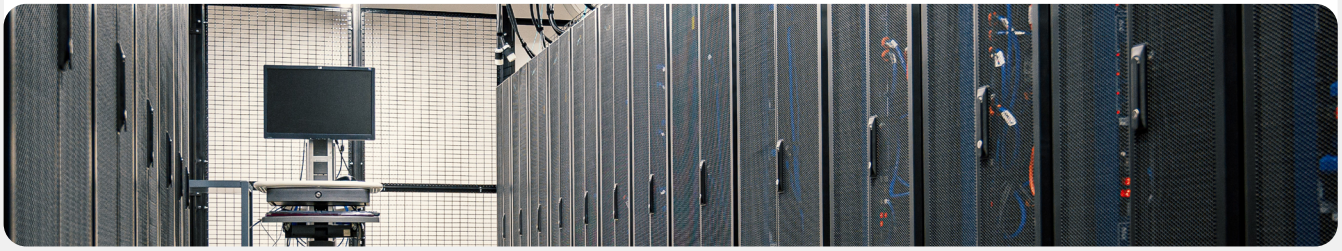
Де «безпечніше» зберігати дані: на комп'ютерах співробітників, на локальному сервері, на зовнішніх пристроях зберігання чи в хмарному сховищі? У 99% ситуацій найпростішим і найбезпечнішим варіантом є зберігання даних у надійних хмарних службах зберігання. Можливо, найпоширенішими прикладами є Microsoft 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.

Вибираючи інструмент або послугу для зберігання даних, переконайтеся, що ви довіряєте компанії чи групі, яка їх надає. Швидкий пошук у Google і консультація експертів із цифрової безпеки допоможуть вам перевірити надійність потенційного постачальника. Деякі запитання, про які слід пам'ятати: Чи продає або передає ця фірма ваші приватні дані? Чи є у цієї фірми належні штатні ресурси безпеки? Чи пропонує ця фірма функції безпеки (наприклад, 2FA), що допоможуть захистити ваш обліковий запис?



Зберігання даних і громадянське суспільство

Поява доступного (іноді безкоштовного) хмарного сховища даних спростила (і зробила більш безпечним) життя багатьох громадських організацій із обмеженими ресурсами. 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. Внаслідок атаки були вражені локальні сервери, що дозволило хакерам отримати доступ до організаційних облікових записів електронної пошти, встановити додаткові шкідливі програми на серверах і підключених системах жертв 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. Коротше кажучи, стратегію надійного хмарного зберігання буде набагато легше реалізувати та підтримувати з часом. Отже, замість того, щоб турбуватися про захист власного сервера, ви можете зосередитися на кількох простіших завданнях. Зберігання основної частини вашої інформації в хмарному середовищі допоможе подолати низку типових ризиків. Хтось залишив комп'ютер у ресторані чи телефон в автобусі? Дитина перекинула склянку соку на вашу клавіатуру, через що пристрій не працює? 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.

ЯКОГО ПОСТАЧАЛЬНИКА ХМАРНОГО СХОВИЩА ВИБРАТИ?

Двома найпопулярнішими варіантами хмарного сховища є Google Workspace (раніше відомий як GSuite) і Microsoft 365. Якщо ви та ваші співробітники вже використовуєте Gmail, має сенс зареєструвати вашу організацію в Google Workspace і зберігати дані на Google Диску за допомогою вбудованих програм Google Документи, Таблиці та Презентації для обробки текстів, електронних таблиць і презентацій. Так само, якщо ваша організація використовує Excel і Word, простим вибором буде зареєструватися в Microsoft 365, що надає вашій організації доступ до Outlook для електронної пошти та ліцензованих версій Microsoft Word, Excel, Powerpoint і Teams. Незалежно від того, якого постачальника ви виберете, безпечне зберігання даних у хмарному сховищі потребує впровадження належних налаштувань спільного доступу та навчання персоналу, щоб зрозуміти, як і коли ділитися (або не ділитися) папками та документами. Загалом, ви повинні налаштувати папки у своєму хмарному сховищі, щоб обмежити доступ лише для тих співробітників, яким це потрібно для роботи з певними файлами. Регулярно перевіряйте свою систему, щоб переконатися, що ви не надаєте надмірного доступу до будь-яких файлів (наприклад, не вмикаєте загальний спільний доступ за посиланням для файлів, що натомість має обмежуватися кількома людьми).

ЩО РОБИТИ, ЯКЩО МИ НЕ ДОВІРЯЄМО GOOGLE, MICROSOFT АБО ІНШИМ ПОСТАЧАЛЬНИКАМ ХМАРНИХ СХОВИЩ?

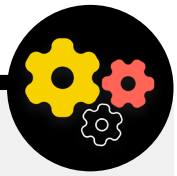
Якщо один із ваших супротивників (наприклад, іноземний чи місцевий уряд) може законним шляхом змусити Google або Microsoft (або іншого постачальника хмарного сховища) передати дані, тоді, можливо, немає сенсу вибирати їх як варіанти зберігання даних. Цей ризик може бути вищим, якщо вашим супротивником є, наприклад, уряд Сполучених Штатів, але набагато нижчим, якщо вашим противником є авторитарний режим. Майте на увазі, що Google і Microsoft мають політику щодо передачі даних лише тоді, коли це передбачено законом, і усвідомте, що ваша організація сама може бути підпадати під дію таких самих юридичних вимог з боку вашого власного уряду, якщо ви зберігаєте дані локально. У ситуаціях, коли хмарне сховище Google або Microsoft не підходить для вашої організації, варто розглянути альтернативний варіант **Keybase**. Функція «teams» у Keybase дозволить вашій організації обмінюватися файлами та повідомленнями за допомогою наскрізного шифрування в безпечному хмарному середовищі без необхідності покладатися на стороннього постачальника. Як результат, це може бути хорошим варіантом для безпечного зберігання документів і файлів вашої організації. Однак Keybase малознайомий більшості користувачів, тому майте на увазі, що використання цього інструменту, ймовірно, потребуватиме більше навчання та зусиль, ніж інші вищезгадані рішення. Зважаючи на це, якщо ви все ж вирішите діяти самостійно й взагалі не використовувати хмарне сховище, вкрай важливо, щоб ви інвестували час і ресурси в посилення цифрового захисту пристроїв вашої організації та переконалися, що локальні сервери правильно налаштовані, зашифровані та фізично захищені. Ви можете зекономити щомісячну ціну підписки, але це коштуватиме часу та ресурсів вашій організації, яка до того ж стане набагато вразливішою до атак.

РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ

Незалежно від того, чи ваша організація зберігає дані на фізичних пристроях чи у хмарному сховищі, важливо мати резервну копію даних. Майте на увазі, що 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 вашої організації на зовнішньому жорсткому диску, але обов'язково зашифруйте цей жорсткий диск за допомогою надійного пароля. 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.

Примітка: якщо ви користуєтеся послугами постачальника хмарного сховища у країні із спеціальними законами про локалізацію даних, зверніться до юристів, щоб краще зрозуміти, як хмарне сховище може відповідати місцевим вимогам. Багато постачальників хмарних сховищ, зокрема Google і Microsoft, тепер пропонують варіанти, які дозволяють деяким клієнтам вибирати, наприклад, географічне розташування своїх даних у хмарному сховищі.



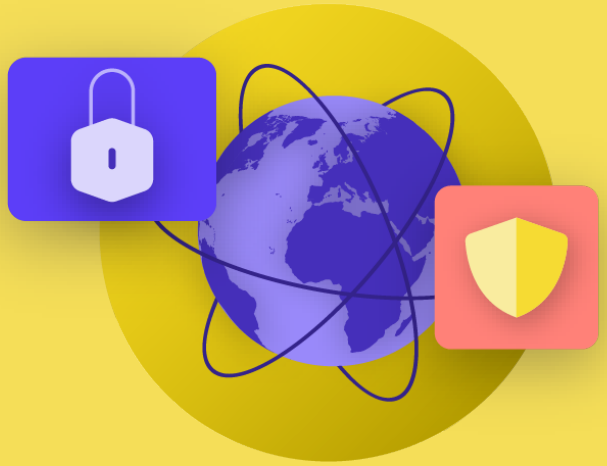
Покращення безпеки облікових записів організації у хмарному сховищі

Якщо ваша організація вирішить налаштувати домен у Google Workspace або Microsoft 365, майте на увазі, що обидві компанії пропонують підвищений рівень безпеки (у багатьох випадках безкоштовно) для громадських організацій. Програма розширеного захисту Google і AccountGuard від Microsoft надають ще більш надійну безпеку для всіх облікових записів вашої організації у хмарному сховищі та допоможуть вам значно зменшити ймовірність ефективного фішингу й пошкодження облікового запису. Якщо ви вважаєте, що ваша організація відповідає вимогам участі у програмі, і зацікавлені в реєстрації вашої організації в будь-якому з планів, відвідайте веб-сайти, посилання на які наведені вище, або зв'яжіться з cyberhandbook@ndi.org



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 весь персонал тому, як правильно надавати спільний доступ до документів (і не надавайте зайвого доступу).
- **Якщо ваша організація вирішить зберігати дані локально, інвестуйте у кваліфікований IT-персонал.**
- **Зберігайте резервні копії даних у безпеці — зашифруйте резервні копії жорстких дисків або інших резервних пристроїв.**



Безпека в інтернеті

Формування культури безпеки

Міцна основа: захист облікових записів і пристроїв

Безпечна комунікація і зберігання даних

Безпека в інтернеті

Захист фізичної безпеки

Що робити, коли все йде не так

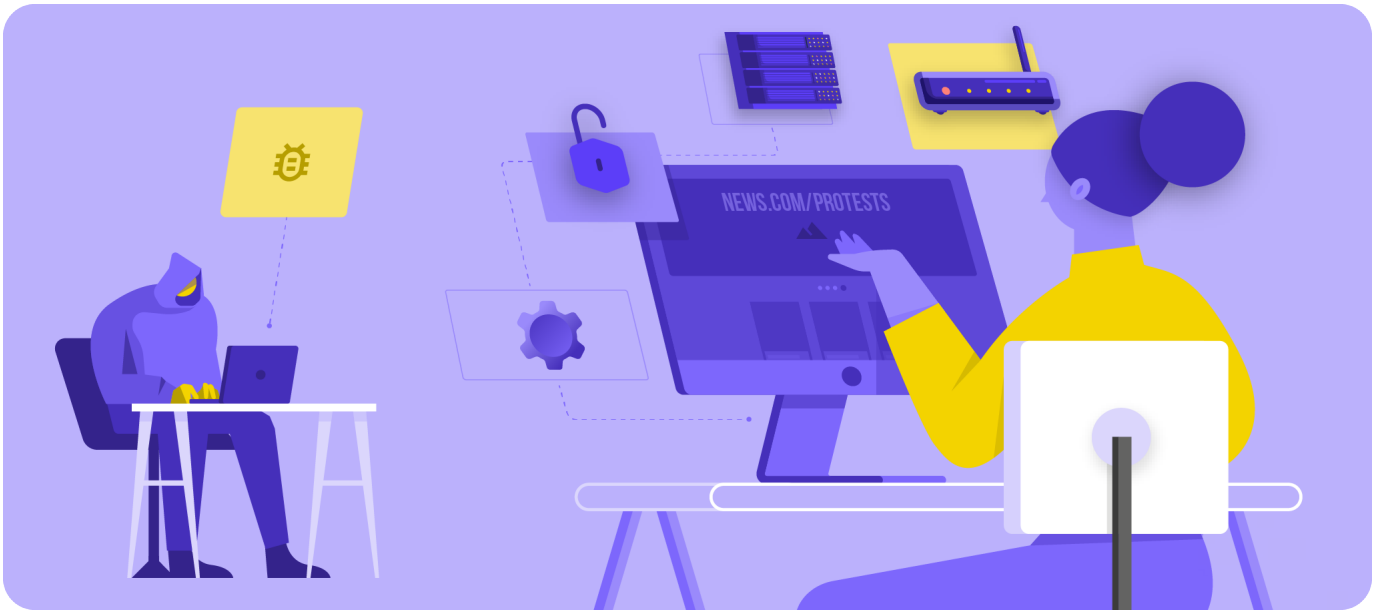
Коли ви користуєтеся інтернетом на своєму телефоні чи комп'ютері, ваша активність може багато розповісти про вас і вашу організацію.

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 вебсайтів, які ви відвідуєте, подалі від сторонніх очей. Блокування або обмеження доступу до певних вебсайтів 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 вебсайтів: 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 вебсайті (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 вебсайту, який ви відвідуєте, і будь-яка організація, з якою він обмінюється даними, і, звичайно, (5) сам вебсайт, який ви відвідуєте, має доступ до великої кількості потенційно конфіденційної інформації.



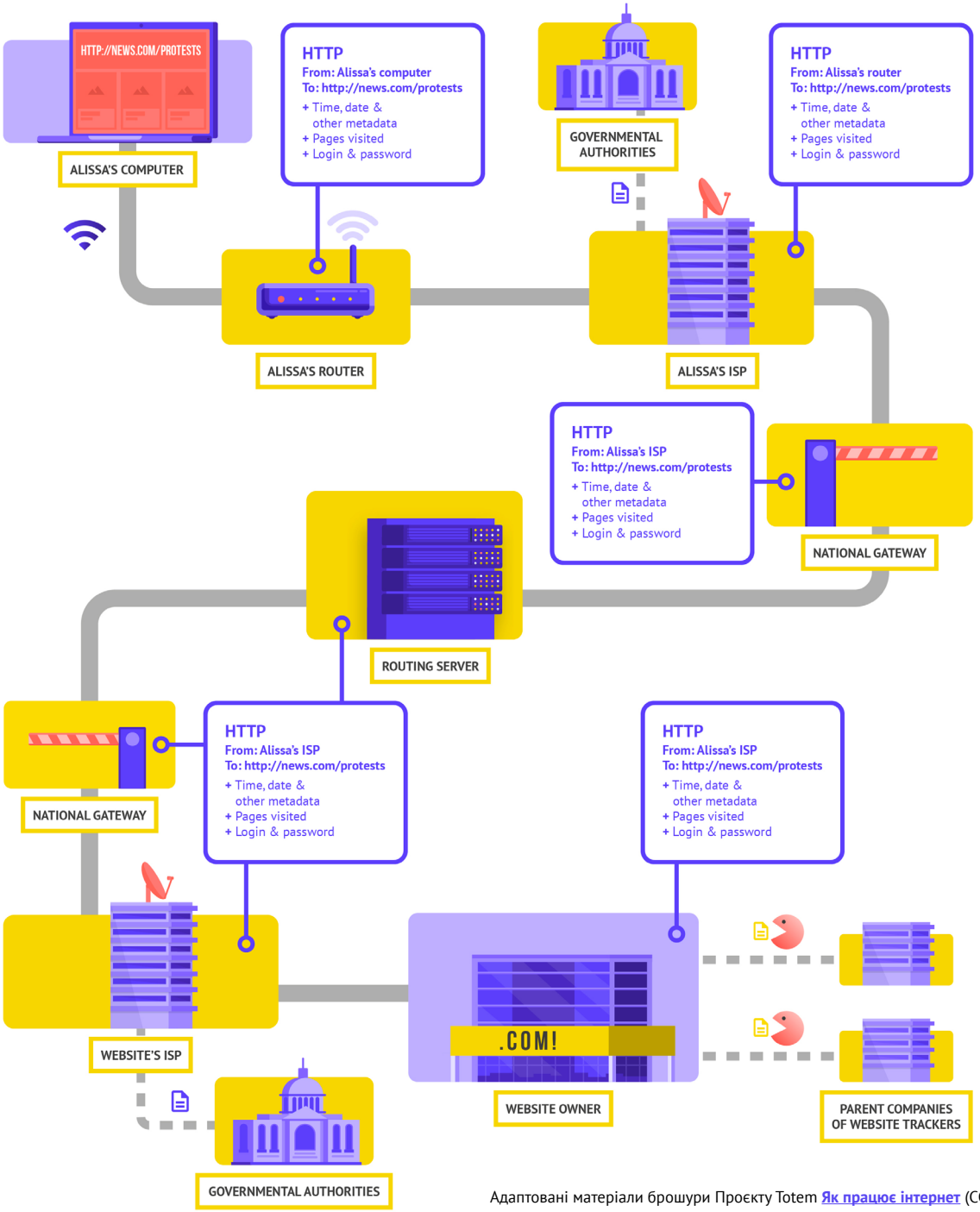
Стеження, цензура та громадянське суспільство

Уряди все більше використовують свій вплив і владу над постачальниками послуг інтернету та іншою локальною інфраструктурою інтернету, щоб перешкодити окремим особам і групам громадянського суспільства отримати доступ до інформації в інтернеті. У деяких випадках такі збої в роботі інтернету спрямовані на припинення роботи ключових комунікаційних платформ і платформ обміну інформацією, зокрема соціальних мереж і сайтів новин. Наприклад, у відповідь на протести, спричинені військовим переворотом, військові М'янми наказали мобільним операторам тимчасово вимкнути всю мережу мобільної передачі даних у країні. Це сталося незабаром після цілеспрямованого блокування Facebook, Twitter та Instagram. Окрім блокування доступу до інтернету та вебсайтів, уряди та хакери на державній службі по всьому світу використовують все більш доступні технології стеження для моніторингу активності громадян в інтернеті. Наприклад, згідно до звіту «Свобода в мережі у 2020 році» від Freedom House уряд Уганди співпрацював із китайською технологічною компанією Huawei **для стеження за діячами опозиції та громадськими активістами** напередодні та після спірних президентських виборів у країні.

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



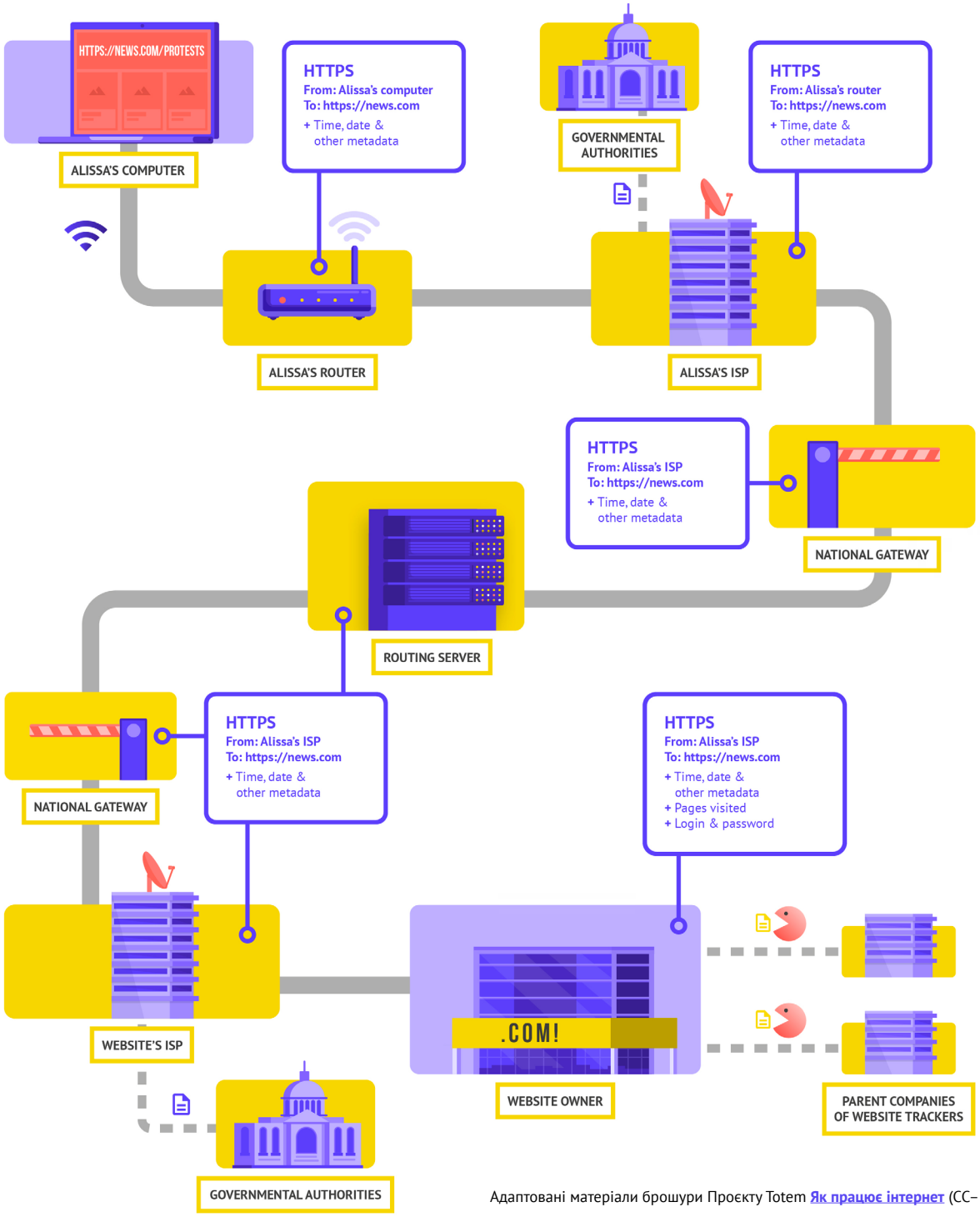
Розглянемо реальний приклад того, як виглядає перегляд вебсторінок без шифрування.



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

Під час перегляду вебсторінок без шифрування всі ваші дані є відкритими. Як вказано вище, зловмисник може побачити, де ви перебуваєте, що ви переходите на news.com, переглядаєте сторінку про протести у вашій країні, і побачить ваш пароль, який ви надаєте для входу на вебсайт. Така інформація в чужих руках не лише ставить під загрозу ваш обліковий запис, але й дає потенційним супротивникам достатнє уявлення про те, що ви робите або про що думаєте.

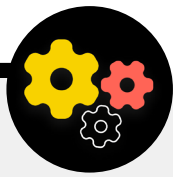
Використання HTTPS («s» означає «безпечний») означає, що використовується шифрування. Це надає вам набагато більший захист. Подивимося, як виглядає перегляд вебсторінок через HTTPS (тобто із шифруванням):



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

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 вебсайт 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 вебсайт може бути небезпечним, не ігноруйте його. Це означає, що щось не так. Це може бути нешкідливим, наприклад, у вебсайта прострочений сертифікат безпеки, або сайт може бути зловмисно фальсифікований або підроблений. У будь-якому випадку важливо дослухатися попередження та не переходити на такий вебсайт. 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 вебсайтів 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 вебсайти, які ви відвідуєте, ви можете використовувати зашифровану DNS.

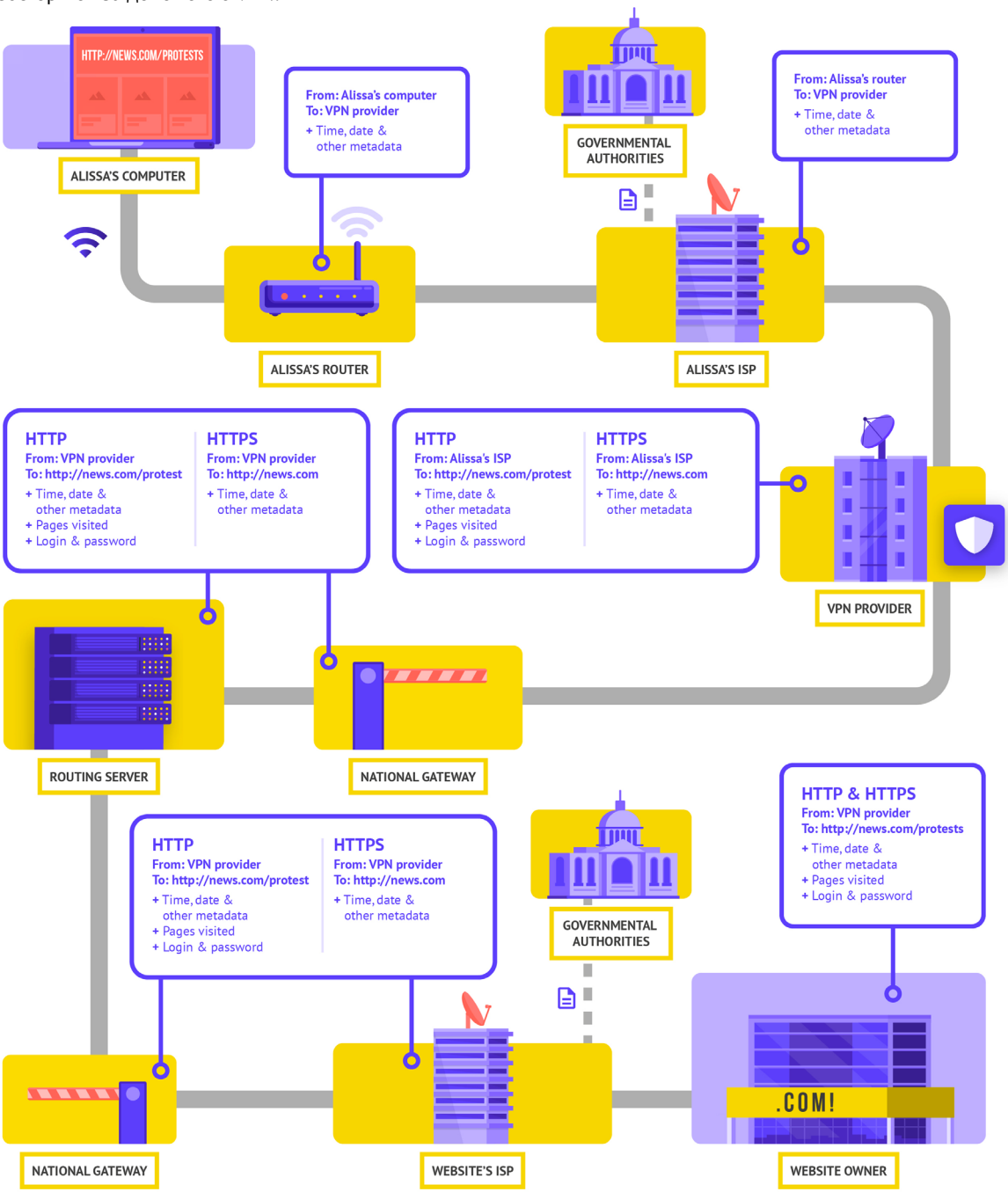
Якщо вам **цікаво знати**, DNS означає «Система доменних імен» (Domain Name System). По суті, це телефонна книга інтернету, яка перетворює зручні для людини доменні імена (наприклад, ndi.org) на адреси зручних для всесвітньої мережі інтернет-протоколів (IP). Завдяки цій системі люди використовують вебоглядачі 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 вебсайтів, які ви відвідуєте, ця проста у використанні функція може допомогти персоналу 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. Разом із тим важливо використовувати HTTPS і переконатися, що ви довіряєте VPN, яку використовує ваша організація. Ось приклад того, як виглядає перегляд вебсторінок за допомогою VPN:



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

Детальний опис VPN міститься у Посібнику із самозахисту шляхом 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.

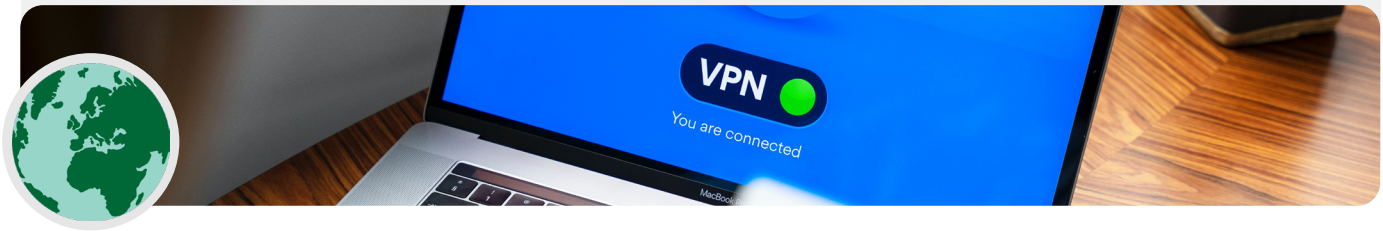
Чому би просто не скористатися безкоштовною VPN? Коротка відповідь полягає в тому, що більшість безкоштовних VPN, включно з тими, які попередньо встановлені на деяких смартфонах, мають значний прихований недолік. Як і всі компанії та постачальники послуг, мережі VPN повинні якимось чином фінансуватися. 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.

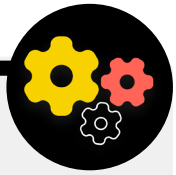


Отже, яку VPN слід використовувати?

Якщо використання VPN має сенс для вашої організації, є такі надійні варіанти, як TunnelBear і ProtonVPN. Ще один варіант — налаштувати власний сервер за допомогою Опису Jigsaw. У цьому випадку немає компанії, що керуватиме вашим обліковим записом, але натомість ви повинні налаштувати власний сервер. Якщо ваша організація велика, ви можете розглянути бізнес-VPN, що надає функції керування обліковим записом, наприклад план Teams від TunnelBear. Для певних кваліфікованих організацій у сфері громадянського суспільства та прав людини TunnelBear надає кредити на безкоштовне користування VPN (зазвичай це коштує близько 3 доларів на місяць). Якщо ви вважаєте, що ваша організація відповідає вимогам і вас цікавить ця тема, зв'яжіться з нами за адресою cyberhandbook@ndi.org для отримання додаткової інформації.

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 персоналу використовувати VPN, важливо також переконатися, що співробітники залишають VPN увімкненою. Це може здатися очевидним, але VPN, що встановлена, 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 являють собою обидва інструменти, чому ви можете використовувати один або інший і як обидва можуть вплинути на вашу організацію.

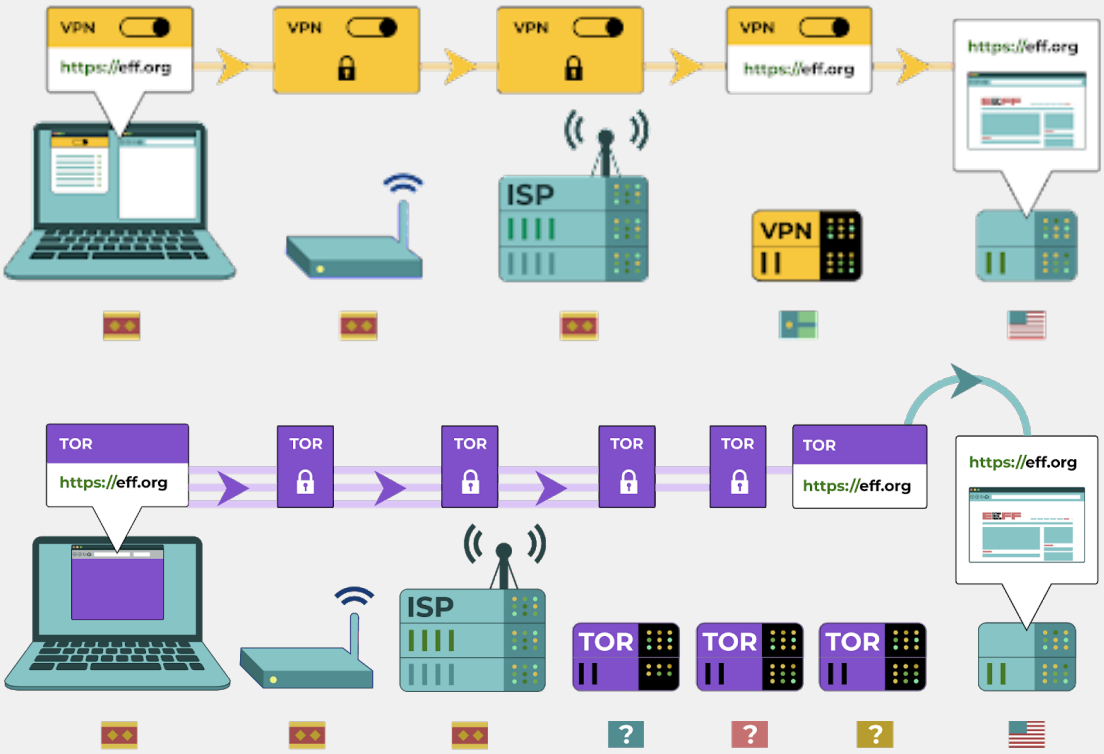
Tor — це протокол для анонімної передачі даних через інтернет шляхом маршрутизації повідомлень або даних через децентралізовану мережу. Ви можете дізнатися більше про те, як працює Tor тут, але коротко кажучи, він направляє ваш трафік через кілька точок на шляху до місця призначення таким чином, щоб 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 і тому може зацікавити супротивників, які можуть стежити за вашим інтернет-трафіком.

Отже, чи варто вашій організації використовувати Tor? Відповідь: це залежить від багатьох речей. Для організацій, що знаходяться у групі ризику, найпростішим і найзручнішим є надійний VPN, що належним чином використовується всіма співробітниками в будь-який час. В епоху все більшого використання VPN у всьому світі малоймовірно, що це може сприйматися як індикатор ризику. Однак якщо ви не можете дозволити собі надійну VPN або працюєте в середовищі, де VPN регулярно блокуються, Tor може стати хорошим варіантом, якщо він є законним, для обмеження стеження й уникнення цензури в інтернеті.

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

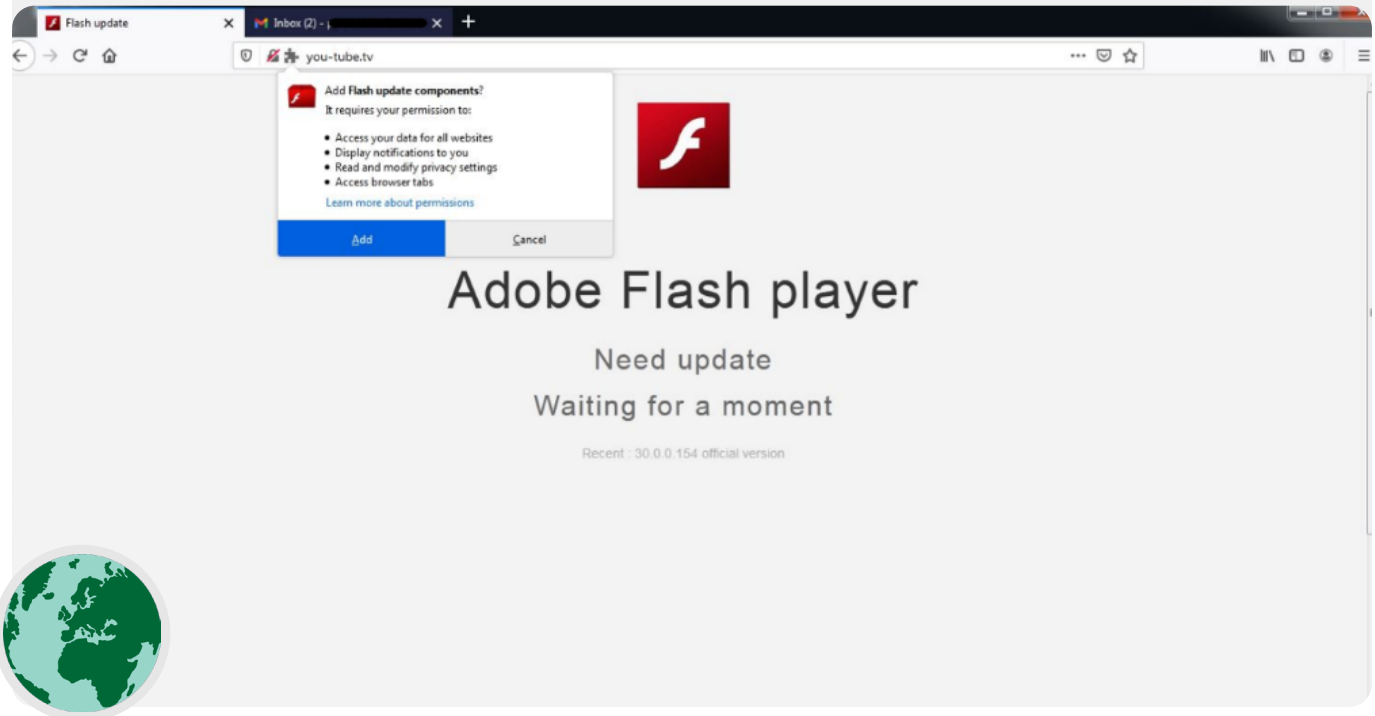
Окрім занепокоєння з приводу послуг VPN із поганою репутацією, головне, що слід розглянути, це те, чи може використання VPN або Tor привернути небажану увагу або, у деяких регіонах, суперечити закону. Хоча ваш інтернет-провайдер не знатиме, які сайти ви відвідуєте під час використання цих служб, він може побачити, що ви підключені до Tor або VPN. Якщо це незаконно там, де працює ваша організація, або 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. Однак, оскільки використання VPN стає все більш поширеним, це менш ризикований варіант. За замовчуванням постійне використання VPN є найкращим вибором, якщо це законно та можливо.

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 вебсайти 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

На тибетських громадських активістів було здійснено цільову атаку на початку 2021 року за допомогою вміло розробленого шкідливого додатку для вебоглядача, що викрадав їхню електронну пошту та дані про перегляд вебсторінок. Додаток під назвою «Flash update components» було представлено користувачам, які відвідували вебсайти, на які вели посилання з фішингових електронних листів. 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.



Безпека соціальних мереж

Ваша організація може розкрити багато інформації – іноді більше, ніж вона хотіла б, – 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 вашої організації, але й у деяких випадках особистих облікових записів співробітників, а також їхніх родин і друзів.

Безпека соціальних мереж і громадянське суспільство

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 доклали таких значних зусиль, щоб заробити кілька тисяч доларів на притулку для тварин, ви можете уявити, якої шкоди можуть завдати досвідчені супротивники, якщо вони отримають доступ до облікових записів вашої організації або успішно видадуть себе за вас в інтернеті.

Окрім злому облікових записів, групи громадянського суспільства й окремі користувачі в багатьох країнах також стикаються з неприємними наслідками контенту, розміщеного в соціальних мережах. До прикладу в Замбії у 2020 році поліція затримала 15-річного школяра за нібито наклеп на президента у дописі у Facebook. Дитину, яка опублікувала повідомлення під псевдонімом, було ідентифіковано за номером телефону, який використовувався для реєстрації облікового запису, та адресою інтернет-протоколу (IP).



РОЗРОБІТЬ ОРГАНІЗАЦІЙНУ ПОЛІТИКУ ЩОДО СОЦІАЛЬНИХ МЕРЕЖ

Припустіть, що будь-який допис, опублікований у соціальних мережах, може стати загальнодоступним, і розробіть відповідну політику організації щодо соціальних мереж. Ця політика повинна відповідати на такі питання: Хто має доступ до ваших облікових записів у соціальних мережах? Кому дозволено публікувати дописи та хто має затверджувати дописи? Якою інформацією слід/не слід ділитися в соціальних мережах? Якщо ви публікуєте фотографії, інформацію про місцезнаходження чи іншу ідентифікаційну інформацію про ваш персонал, партнерів або відвідувачів події, чи запитували ви їхнього дозволу та чи враховували вони ризики? 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 ваших особистих і організаційних облікових записів:

- 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 повинні люди знаходити вас або вашу організацію 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, і 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 вашої організації в соціальних мережах настільки безпечні, наскільки безпечні «пов'язані» з ними облікові записи. Це особливо важливо пам'ятати для Facebook, де сторінкою вашої організації може керувати пов'язаний із кимось особистий обліковий запис.

ПЕРЕСЛІДУВАННЯ В ІНТЕРНЕТІ

На жаль, багато організацій стикаються зі значним переслідуванням 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.

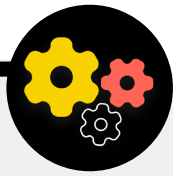
Коли ваша організація розробляє політику щодо соціальних медіа, важливо знати про цю динаміку. Передбачте у своєму плані безпеки структуровану підтримку співробітників, які стикаються з негативними повідомленнями, дошкульними образами та погрозами в соціальних мережах як на роботі, так і в особистому 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 вебсайтів онлайн

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

Для сторінок у соціальних мережах це означає захист облікових записів надійними унікальними паролями та двофакторною автентифікацією. Для вашого вебсайту 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. Якщо ви є громадською організацією чи іншою некомерційною організацією, ви, швидше за все, можете отримати безкоштовний захист від DDoS, що значно ускладнить зловмисникам задачу знищити ваш вебсайт. Кілька варіантів включають Проєкт Galileo від Cloudflare, Проєкт Shieldвід Google або послугу Deflect від eQualitie.



Безпечне розміщення вебсайту вашої організації

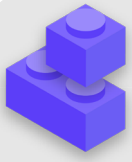
Вебсайти розміщуються на комп'ютерах, і їм загрожує ризик злому, як і вашим власним пристроям. За можливості вашій організації слід скористатися перевагами існуючих служб хостингу, таких як Wordpress.com, Wix та інші, які організують безпеку вебсайту за вас. Якщо ви читаєте цей довідник, ваша організація також, скоріше за все, має право на безкоштовне безпечне розміщення сайту на Wordpress від eQualitie через їх послугу хостингу eQPress. Це чудовий варіант для громадських організацій із наявними вебсайтами на Wordpress або якщо ваша організація захоче створити новий вебсайт. Якщо потрібен більш складний вебсайт або якщо вам потрібно самостійно розмістити свій вебсайт, 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 вебсайтів. Незалежно від того, які інструменти ви використовуєте для розміщення свого вебсайту, 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 вебсайту, вам слід розглянути можливість вибору так званого «статичного сайту» або плоского веб-сайту. На відміну від динамічних вебсайтів, вебсайти цих типів зменшують площу атаки для хакерів і мають більшу стійкість до атак.

Захист мережі WiFi

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. Також подумайте про створення гостьової мережі у вашому офісі, якщо в будівлю входять і виходять відвідувачі, які користуються інтернетом.



Безпека в інтернеті

- **Проводьте регулярне навчання персоналу щодо важливості дотримання основних заходів безпеки в інтернеті.**
- **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 у контексті вашої організації, виберіть надійну мережу, навчіть персонал її використанню та переконайтеся, що вона постійно використовується.**
- **Розробіть і розішліть співробітникам чітку організаційну 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 співробітників, які постраждали від них.**
- **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 вебсайтів.**
- **Використовуйте надійного постачальника вебхостингу.**
- **Використовуйте надійний пароль і гостьову мережу для офісного Wi-Fi.**



Захист фізичної безпеки

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. До них входять друковані документи; офіс або робочі приміщення вашої організації; і, звичайно, ви самі, ваші співробітники та волонтери.

Стеження, цензура та громадянське суспільство

На жаль, фізичні напади на громадські організації не є рідкістю і часто мають значні наслідки як для фізичної, так і для інформаційної безпеки. Однією з поширених тактик ворогів для придушення діяльності ГО є рейдерські напади та закриття офісів – як для залякування персоналу, так і в деяких випадках для викрадення чи конфіскації інформації та технічного обладнання. Такі загрози часто спрямовані проти груп меншин і правозахисних груп, а також громадських організацій, що просувають демократію та самоврядування. Наприклад, офіси громадської організації LGBT+ Rights Ghana, що на початку 2021 року відкрила перший у країні громадський центр для місцевої ЛГБТКІ+ спільноти, погрожували спалити. Зрештою, було проведено рейдерський напад і представництво було закрито поліцією. Такі рейди не лише впливають на фізичну роботу організації, а й можуть змусити її персонал почуватися в небезпеці.

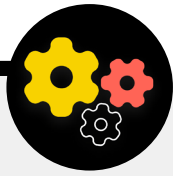


Захист фізичних активів

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 надійні замки (і міняйте їх, коли змінюється персонал) в офісі та/або вдома. Крім того, подумайте про придбання сейфа для ноутбука або шафи, що замикається, щоб захистити пристрої протягом ночі. Камери відеоспостереження стали набагато дешевшими, а прості версії, призначені для домашнього використання, стали широкодоступними. 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 супротивнику.

Якщо ризик злому або рейдового нападу на офіс високий, зберігайте найбільш конфіденційні дані організації подалі від офісу, у безпечному хмарному сховищі (що розглядалося вище), або фізично перемістивши їх у маловідоме місце. 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 інвентарний перелік всього обладнання організації. Якщо у вас немає переліку всіх ваших пристроїв, важче відстежити, що могло бути втрачено, якщо один із них викрадуть.



Налаштування власної системи безпеки офісу

Якщо повна система безпеки офісу виходить за рамки бюджету вашої організації, і вас особливо турбує конфіденційність, ви можете спробувати креативний варіант, як-от Додаток Haven від Проєкту Guardian, щоб повідомити вас про можливе проникнення в офіс. Haven — це додаток для смартфонів, що може перетворити будь-який телефон Android на детектор руху, звуку, вібрації та світла. Ви можете встановити додаток на кількох дешевих пристроях Android у різних точках офісу, щоб сповіщати вас про несподіваних гостей і небажаних зловмисників і записувати їх. Додаток Haven також може бути корисним для встановлення в готельному номері чи квартирі, якщо ви належите до групи підвищеного ризику. Найкраще мати повну систему безпеки, але якщо вона недоступна і ви хочете дізнатися більше про те, як користуватися додатком Haven, відвідайте веб-сайт проекту.

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 цих даних можуть бути дуже конфіденційними: роздруківки бюджетів, списки учасників, конфіденційні листи від донорів і нотатки з 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. Якщо ви вважаєте, що ваша організація піддається високому ризику злому або рейдерського нападу, зберігайте конфіденційну інформацію в маловідомому місці.
Наскільки це можливо, постарайтеся позбутися непотрібної друкованої інформації. Пам'ятайте: якщо у вас чогось немає, це неможливо вкрасти. Встановіть політику організації щодо права власності на паперові нотатки й обов'язково заберіть паперові нотатки від співробітників, якщо вони вирішать піти з організації або їх звільнять (так само, як ви забираєте комп'ютер або телефон, виданий організацією). 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.

ПОЛІТИКА ЩОДО ОФІСУ

Хоча для багатьох «офісні» реалії суттєво змінилися після початку пандемії COVID-19, для вашої організації все таки важливо встановити чітку політику щодо доступу до офісу. 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 питання, на яке потрібно відповісти, — хто отримує ключ від офісу. Лише довірений персонал повинен мати ключі, а замки слід міняти, коли персонал звільняється, та/або на більш-менш регулярній основі. Протягом дня будь-які двері, які залишаються незамкненими, повинні постійно перебувати в полі зору людини, якій довіряють в організації. Також подумайте, чи має організація довірчі стосунки з вашим орендодавцем і прибиральником. 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 персонал покине офіс наприкінці дня.

Чи дозволено гостям заходити в офіс? 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 вашої організації також можуть вплинути на ваш персонал. 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. Для організацій, які працюють із політично активними жінками або підтримують їх Інструмент планування безпеки від NDI **#Think10** є корисним ресурсом для тих, хто може зазнавати підвищеного особистого ризику внаслідок своєї діяльності.

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 ж таки **Практичний посібник щодо переслідування в інтернеті** від PEN America містить ідеї щодо того, як організації можуть підтримувати персонал під час та після криз, а **Комплексний посібник із безпеки** від Tactical Tech містить необхідні відомості про те, як організації зазвичай реагують у часи серйозної загрози.

БЕЗПЕКА ПІД ЧАС ПОДОРОЖІ

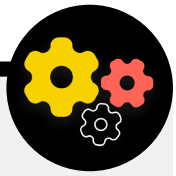
Подорожі – до іншої країни чи до сусіднього міста – часто посилюють ризики фізичної інформаційної безпеки. Загалом можна з упевненістю припустити, що для вас і ваших пристроїв не має прав на конфіденційність під час перетину кордону. Таким чином, було б гарною ідеєю включити організаційну політику щодо 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 «стертя даних» ці пристрої готові до підключення до звичайних мереж WiFi вдома чи в офісі.

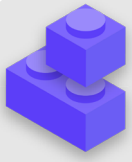
Підготуйте персонал до того, що робити, якщо його допитають представники влади або зупинять під час перетину кордону. Подумайте, як можна обмежити кількість інформації, з якою співробітник подорожує, якщо це важливо, і створіть протоколи повідомлення про стан справ для персоналу, який подорожує до ризикових регіонів. 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. 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 персонал, який подорожує, міг безпечно заряджати пристрої через USB.



Безпечне бронювання подорожей для вашої організації

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. Книга завдань організаторів від Tactical Tech містить чудовий робочий аркуш, який допоможе вашій організації продумати ключові питання, пов'язані з безпекою подорожей, **посилання тут**.



Захист вашої фізичної безпеки

- **Нагадайте персоналу про необхідність постійного фізичного захисту пристроїв.**
- **Перевірте та захистіть усі шляхи, якими люди можуть проникнути у ваше приміщення – двері та вікна.**
- **Розробіть політику для гостей і доступу до офісу.**
- **Використовуйте надійні замки та міняйте їх, за необхідності.**
- **Розгляньте можливість встановлення камери чи іншої системи безпеки офісу.**
- **Встановіть і використовуйте подрібнювач паперу.**
  - Виділіть певний час персоналу 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.**
- **Розробіть організаційну політику щодо подорожей.**
- **Переконайтесь, що співробітники знають, що робити в екстрених випадках під час подорожі. Зокрема підготуйте персонал до того, що робити в разі затримання на кордоні чи контрольно-пропускному пункті.**
- **Перед будь-якими місцевими, національними чи міжнародними поїздками нагадайте персоналу обмежити інформацію, що зберігається на пристроях.**
- **Пам'ятайте про додаткові дані, які створюються та передаються під час організації подорожей або заходів.**



Що робити, коли все йде не так

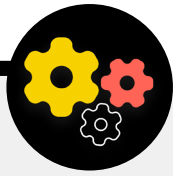
Отже, ви знаєте, як і що треба робити. Ви запровадили політику та навчили всіх в організації найкращим методам захисту безпеки. Навіть попри всю цю важку роботу дуже ймовірно, що щось піде не так.

Всяке трапляється. Коли відбувається щось не те, важливо мати план реагування на інцидент. Реагування на інциденти є важливою, і часто недооціненою, частиною плану безпеки вашої організації. Цей план може перетворити атаку, руйнівну для репутації вашої організації, на неприємну вибоїну на дорозі. Майте на увазі, що ви можете відреагувати на інцидент, лише якщо знаєте про нього. Дуже важливо мати сильну організаційну культуру безпеки та заохочувати персонал 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 вебсайти 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 будемо робити, якщо хтось із наших співробітників зазнає фізичної небезпеки або буде заарештований? 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 будемо робити, якщо комп'ютер або телефон співробітника буде втрачено або вкрадено?

Відповіді на ці й інші запитання відрізнятимуться залежно від організації, але важливо продумати їх разом, чітко сформулювати й поділитися планом, щоб кожен у вашій організації 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 активізацію мережі підтримки – широкої мережі союзників, що може включати друзів і родичів, громаду, місцевих союзників, урядові ресурси, національну або міжнародну підтримку, наприклад, від НУО та журналістів. 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 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 вплив інциденту на репутацію вашої організації та будьте готові відповідним чином відреагувати. Переконайтеся, що керівник з питань комунікації організації (у деяких організаціях це може бути адміністратор сторінки Facebook або облікового запису Twitter) знає про інцидент і може стежити за соціальними мережами чи іншими медіа на предмет можливого реагування. 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. Першим кроком може бути пошук довіреного юридичного консультанта, який знається на законах і правилах вашої країни чи місцевості. 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. Під час складання плану реагування на інциденти настійно рекомендуємо скористатися чудовими ресурсами, розробленими, щоб допомогти громадським організаціям та іншим групам високого ризику зорієнтуватися у реагуванні на інциденти. 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 організаційний 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 організації знають про те, як ви будете спілкуватися та які технічні заходи будуть вжиті у випадку інциденту.**
- **Знайдіть час, щоб дізнатися про засоби правового захисту й усвідомити свої зобов'язання.**
- **Будьте готові надати персоналу організації необхідну емоційну та соціальну підтримку після інциденту.**

Додаток A
Рекомендовані ресурси

- Комплексний посібник із безпеки від Tactical Tech; Creative Commons Attribution-ShareAlike 4.0 Міжнародна ліцензія
  - 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 ; Creative Commons Attribution 3.0 US License
  - Роздатковий матеріал із моделювання загроз
- Freedom of the Press Foundation's Phishing Prevention and Email Hygiene Guide ; Creative Commons Attribution 4.0 International License
- Керівництво зі встановлення додатку Signal від Freedom of the Press Foundation; Creative Commons Attribution 4.0 Міжнародна ліцензія
- Посібник із самозахисту шляхом спостереження (SSD) від Electronic Frontier Foundation; Creative Commons Attribution 3.0 Ліцензія США
  - 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; Creative Commons Attribution 4.0 Міжнародна ліцензія
- Керівництво з безпеки виборів щодо двофакторної автентифікації від Center for Democracy and Technology ; Creative Commons Attribution 4.0 Міжнародна ліцензія
- Двофакторна автентифікація для початківців від Martin Shelton; Creative Commons Attribution 4.0 Міжнародна ліцензія
- 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
  - Захистіть свою інформацію від фізичних загроз
- SANS Ой! Бюлетень: Зупиніть цю шкідливу програму
- Доступ до пристроїв і даних, коли особиста безпека під загрозою від Apple
- Global Cyber Alliance Кібербезпека для соціально відповідальних організацій

Додаток B
Стартовий комплект плану безпеки

Використовуйте наступний стартовий комплект, щоб робити нотатки, коли ви та ваша організація читаєте Довідник і вивчаєте матеріал, а також обміркуйте питання, що виникають, із колегами, щоб ініціювати продуктивну дискусію.

Обов'язково посилайтеся на ключові «елементи побудови» в кожному розділі Довідника, щоб забезпечити охоплення важливих тем під час створення плану безпеки. До кінця Довідника елементи побудови, 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 комунікація і зберігання даних



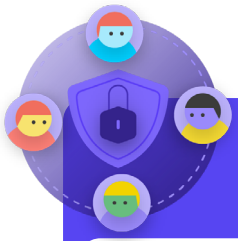
Безпека в інтернеті



Захист фізичної безпеки



Що робити, коли все йде не так



Формування культури безпеки

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Коли запланувати розмову для розгляду плану безпеки з усією організацією?
- У які дні чи години організації краще запланувати регулярні обговорення та навчання з питань безпеки?
- Які кроки може зробити керівництво, щоб продемонструвати належне дотримання безпеки та виконання плану безпеки? Яку роль можуть відігравати інші співробітники організації в справі безпеки?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:



Міцна основа: захист облікових записів і пристроїв

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як ви будете впроваджувати заходи із захисту облікових записів, як-от менеджер паролів і 2FA, в усій організації? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваша організація гарантуватиме безпеку й оновлення пристроїв? Чи потрібен організації план боротьби з неліцензійним програмним забезпеченням або неліцензійним комп'ютерами?
- Коли доцільно провести навчання для всього персоналу щодо небезпеки фішингу, шкідливих програм і застосування найкращих методів захисту пристроїв?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

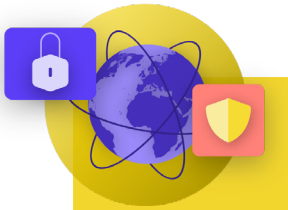


Безпечна комунікація і зберігання даних

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як ваша організація запровадить наскрізне шифрування повідомлень для безпечного зв'язку? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваша організація запровадить безпечне рішення для обміну файлами як усередині організації, так і з третіми сторонами? З якими перешкодами ви можете зіткнутися під час впровадження?
- Як ваша організація 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:

- Як ваша організація впроваджуватиме вимоги щодо безпечного веб-перегляду, наприклад, HTTPS, надійний браузер і, за необхідності, VPN для персоналу?
- Якими будуть ключові елементи політики вашої організації щодо соціальних мереж? Як вони будуть впроваджуватися?
- Як ваша організація захищатиме свої вебсайти та свої ресурси в інтернеті?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

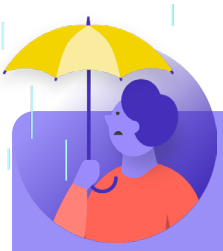


Захист фізичної безпеки

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як організація поширюватиме та запроваджуватиме свою політику відвідування офісу та доступу до нього?
- Хто відповідає за підготовку персоналу до запобігання проблемам із фізичною та цифровою безпекою, з якими вони можуть зіткнутися під час відряджень?
- Які кроки може зробити персонал, щоб зберегти свої пристрої в безпеці як в офісі, так і під час подорожі?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:



Що робити, коли все йде не так

ПИТАННЯ ДЛЯ РОЗГЛЯДУ:

- Як організація 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 організація зможе забезпечити ці ресурси в разі інциденту?

ВАШІ ПРИМІТКИ ТА ІДЕЇ:

Додаток C
Цитування зображень

Сторінка 17: Збірка CNP, «Security Protection Anti-Virus Software cms», 2014, цифрове зображення, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Купуйте%20роялті%20безкоштовно%20в%20Alamy&utm_medium=вплив&irgwc=1.

Сторінка 24: Cottonbro, «Person Holding Black and Silver Key», 2020, цифрове зображення, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

Сторінка 26: Blogtrepreneur, «Malware Infection», 2016, цифрове зображення,, Flickr, https://www.flickr.com/photos/143601516@N03/.

Сторінка 29: «Microsoft Loading Screen», цифрове зображення, Kompass, 23 вересня 2019 р. 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, цифрове зображення, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

Сторінка 33: "Human right protection survey lure," цифрове зображення, Mandiant, листопад 2021, https://www.mandiant.com/sites/default/files/2021-11/PeriscopeCambodia2.png.

Сторінка 38: Andrew Keymaster, «People Gathering on Street During Daytime Photo», 2020, цифрове зображення, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.

Сторінка 39: Surveillance Self-Defense, «No Encryption in Transit», цифрове зображення, Electronic Frontier Foundation, 17 січня 2019 р.
https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Сторінка 40: Surveillance Self-Defense, «4.Transport-layer-alternate», цифрове зображення, Electronic Frontier Foundation, 17 січня 2019 р., https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, «6. End-to-end Alternate», цифрове зображення, Electronic Frontier Foundation, 17 січня 2019 р., https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.

Сторінка 42: Surveillance Self-Defense, «9._endtoendencryptionmetadata», 2019, цифрове зображення, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Сторінка 50: Brett Sayles, «Server Racks on Data Center», 2020, цифрове зображення, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

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

Сторінка 60: Стефан Кодерс, «laptop-screen-vpn-cyber-security», 2020, цифрове зображення, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

Сторінка 62: Surveillance Self-Defense, «Using the Tor Browser», цифрове зображення, Electronic Frontier Foundation, 25 квітня 2020 р. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

Сторінка 64: Nathan Dumlao, «White Samsung Android Smartphone on Brown Wooden Table», 2020, цифрове зображення, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.

Сторінка 69: Matt Artz, «Two Broken 6-Pane On White Painted Wall Photo», цифрове зображення, Unsplash, 1 жовтня 2017 р., https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE

