Рекомендації з цифрової безпеки для юристок і юристів

Анастасія Апетик

1

Встановіть складний пароль.

Складний пароль складається з не менш ніж 16 символів (великі та малі літери, цифри та символи). Не рекомендую мати один і той же пароль для різних акаунтів.

Запам'ятати всі складні паролі від десятків акаунтів досить важко. Тому можна використовувати менеджери паролів:
Password (non-free)
Bitwarden (free & opensource)
Dashlane (non-free)
KeePassXC (free & opensource, DIY cloud sync)

Паролі від найбільш важливих акаунтів – соцмереж, якими часто користуєтеся, та пошти – доведеться запам'ятати. Крім того, рекомендую вимикати збереження паролів у браузерах.

Періодично змінюйте паролі, оновлюйте їх хоча б раз на пів року, а найкраще це робити кожні 3 місяці. Не слід вводити логіни й паролі в громадських місцях, де встановлено відеоспостереження. Якщо ви заходили в свій акаунт із чужого пристрою, змініть після цього пароль.

Перевірити, наскільки безпечний пароль, можна **тут.**

2

Встановіть двофакторку.

Двофакторна автентифікація – це метод контролю доступу до комп'ютера чи ґаджета, у якому для отримання доступу до інформації необхідно надати більше одного «доказу», що це саме ви хочете здійснити вхід на пошту чи в соцмережу. Наприклад, для входу в акаунт, окрім паролю, вам потрібно ввести код, який прийшов на пошту чи мобільний телефон. Або ж додатково пройти ідентифікацію обличчям чи відбитком пальця.

Як її встановити? Потрібно просто перейти за посиланням та налаштувати її:

Google
Facebook
Instagram

3

Оновлюйте програмне забезпечення системи.

Програмне забезпечення, яке працює у вашій мережі, часто потребує оновлення через виправлення. Дуже важливо робити ці оновлення вчасно, оскільки вони зазвичай виправляють уразливості, які програміст виявив у коді. Обов’язково використовуйте антивірусне програмне забезпечення. Користуйтесь виключно

ліцензованим програмним забезпеченням. Якщо ви не покупець ліцензованої програми, тоді ви самі є товаром для цього програмного софту, і він буде заробляти на ваших даних.

4 Зашифруйте свої дані.

Ви можете зашифрувати інформацію на жорстких дисках і знімних носіях. Це буде корисним, якщо сторонні особи відберуть чи викрадуть у вас комп'ютер або знімуть з нього жорсткий диск. Не ввівши спеціальний пароль, вони не зможуть прочитати вміст дисків. Уся інформація на диску для них буде виглядати, як абракадабра.

Для комп'ютерів Apple з OS X. Використовуйте програму FileVault, яка має функцію шифрування. На **офіційному сайті** компанії можна знайти інструкцію, як з нею працювати.

Для комп'ютерів з операційною системою Windows. У професійних версіях операційної системи (Enterprise, Pro, Ultimate Edition) від Microsoft є вбудована програма **BitLocker.** Для інших випадків є програма **VeraCrypt.** На розшифровку захищених нею даних у спецслужб, враховуючи сучасний розвиток технологій, піде не менше 40 років.

Для смартфонів. Інформація на iPhone, iPad і нових Android-пристроях шифрується за замовчуванням. На старих Android-пристроях можна ввімкнути шифрування вручну. Для цього треба зайти в розділ «Конфіденційність» основного меню, знайти пункт «Шифрування» і дотримуватися інструкцій.

5 Використовуйте найбільш захищені месенджери.

Насправді, зламати можна будь-який месенджер, але це справа великих ресурсів – фінансових, людських і часових. Некомерційна організація Electronic Frontier Foundation щороку формує рейтинг безпеки месенджерів. Захищеність месенджерів оцінюють за кількома критеріями: наприклад, чи може адміністрація сервісу ознайомитися з вмістом повідомлень і чи шифрується інформація на своєму шляху. Серед популярних месенджерів одним із найбільш захищених є Signal.

Ви запитаєте, а як же Telegram? Про безпечність Telegram можна судити **із цього відео.** Як бачите, використовуючи Telegram, можна дізнатися IP-адресу вашого співрозмовника. Про Viber рекомендую забути. Окрім слабкого захисту, відзначу, що сервери Viber знаходяться і в Росії. Також у YouTube є багато відео, де показано вразливість цього месенджера.

Якщо вам потрібно отримати чи надіслати документи, використовуйте краще власну пошту або Signal.

6

Використовуйте захищені з’єднання з Інтернетом.

Кіберзлочинці можуть перехоплювати особисту або конфіденційну інформацію, атакуючи незахищені з'єднання Wi-Fi (наприклад, громадські Wi-Fi, такі як у аеропортах та кав'ярнях). Переконайтеся, що пристрої, які використовуються для доступу до мережі, мають захищене з’єднання з Інтернетом. Якщо працюєте віддалено (наприклад, у офісі клієнта чи під час ділових поїздок), використовуйте власний модем або VPN (Virtual Private Network) – узагальнена назва мереж, які створюються поверх інших мереж із меншим рівнем довіри. Можу рекомендувати використовувати **ExpressVPN**.

7

Використовуйте віддалені (хмарні) сховища даних.

Якщо ви втратили будь-який зі своїх пристроїв, ви не втратите інформацію. Сховище Google Drive прив'язане до вашого Google-акаунта. На ньому можна встановити двофакторну автентифікацію та подивитися журнал відвідувань, а також увімкнути сповіщення про вхід з невідомих пристроїв. Google Drive самостійно не шифрує дані. Для цього будуть потрібні сторонні сервіси – наприклад, VeraCrypt. У користувачів техніки Apple є сховище даних iCloud. Доступ до нього також можна захистити двофакторною автентифікацією.

8

Вводьте важливу інформацію тільки на сайтах із захищеним з'єднанням.

Будь-яку інформацію – від введення логіна та пароля до номера банківської карти й вашого прізвища – варто надсилати тільки з ресурсів, де ввімкнений HTTPS. Це зашифрований спосіб передачі інформації. Від звичайного протоколу HTTP він відрізняється тим, що будь-які дані, які ви відправляєте на сайт, шифруються. Так вони стають недоступними для перехоплення.

Подивіться на початок адреси вашого сайту в рядку браузера. Бачите зелений замочок і абревіатуру HTTPS? Якщо їх немає, то передача даних від вашого пристрою до сайту не зашифрована – цю інформацію можна перехопити.

Google Chrome автоматично вмикає HTTPS на всіх сайтах, де він передбачений. На більшості банківських сайтів HTTPS також працює за замовчуванням. У Facebook – теж.

9 Не під’єднуйте до вашого пристрою невідомі носії (флешки, SD-карти, смартфони) навіть для підзарядки.

Не варто під’єднувати будь-які невідомі USB-пристрої до вашого комп'ютера. Навіть у ліхтарика, який працює від USB-порту, може бути носій пам'яті, що містить шкідливий софт. Не варто заряджати свої телефони та планшети деінде. Ви можете під’єднати пристрій до зараженого комп'ютера, який отримає доступ до даних на вашому пристрої або завантажить на нього шкідливі програми. Не варто без крайньої необхідності користуватися громадськими зарядними пристроями, які виглядають, як кіоск або ящик з дротами. Невідомо, до чого саме ви таким чином під’єднаєтеся. Краще пошукати звичайну електричну розетку та скористатися власною зарядкою.

10 Увімкніть функцію віддаленого видалення даних з телефону.

У разі втрати або крадіжки телефону ви зможете стерти всі персональні дані з його пам’яті віддалено. Вам не доведеться переживати про втрату всіх своїх даних, якщо ви дотримувалися попередніх порад і регулярно створювали резервні копії. Детальніше дізнатися про те, як віддалено стерти дані з **iPhone** та з пристроїв на **Android**, можна за вказаними посиланнями.

11 Встановіть TeamViewer.

Це програма, що є комплексним рішенням для віддаленого доступу, віддаленого моніторингу та віддаленої підтримки. Вона сумісна практично з усіма стаціонарними комп’ютерами та мобільними платформами, зокрема Windows, macOS, Android та iOS.

12 Дізнавайтеся більше про цифрову безпеку.

Так, технології не стоять на місці, вони змінюються та розвиваються в геометричній прогресії. Тому заплануйте проходження тренінгів, вебінарів чи онлайн-курсів з цифрової безпеки, ніби це ваш обов’язковий візит до лікаря.

Анастасія Апетик

юристка, експертка з інформаційних прав та безпеки Експертного центру з прав людини

Про авторку

Ексюристка Національної поліції України.
Авторка першого в Україні онлайн-курсу «Цифрові права та безпека для дітей».
Експертка україно-естонської програми «Resilient Ukraine 2018-2020» International Centre for Defence and Security.
Модераторка заходів у сфері безпеки на міжнародних, всеукраїнських майданчиках та платформах.
Розробляє політики приватності та конфіденційності для організацій, сайтів і мобільних додатків.

Тренерський досвід

Проводить тренінги та розробляє методичні матеріали для представників суду, поліції, органів місцевого самоврядування, адвокатури та громадськості у сфері інформаційних прав та безпеки.
Розробила методичні матеріали та провела понад 50 тренінгів для працівників поліції у сфері дотримання прав людини.
Спікерка понад 90 публічних національних та міжнародних заходів.

Публікації

Кому потрібні наші дані?

Як інструменти стеження за COVID-19 порушують права людей?

Безпека чи відповідальність? Коментуємо проект “Білої книги для штучного інтелекту”

Чи допомагає Big Data захищати права людини?

Приватність, здоров’я чи безпека — що обрати в умовах карантину?

Дизайн – Ярослав Турбіль

Ілюстрації – Freepik