**21 правило цифрової безпеки**

Важливо розуміти, що цифрова безпека – це процес. Ви не можете сьогодні  щось встановити, придбати якусь магічну кнопку, яка б дозволила захистити усі ваші дані, інформацію ваших друзів, колег і т.д. Ви постійно дізнаєтесь про нові загрози та про нові інструменти, які з’являються – щось використовуєте, а щось ні.

1. **Використовуйте ліцензійне програмне забезпечення скрізь, зокрема на телефонах і планшетах, робочих та домашніх комп’ютерах.**
2. **Регулярно оновлюйте все програмне забезпечення.**
Останнім часом Windows оновлюється та перезавантажується без вашого бажання: ви хочете попрацювати, а його не хвилює, що у вас конференція.
3. **Встановлюйте антивірусні програми та firewall (міжмережевий екран, фаєрвол)** Антивірус вирішує проблему зараження вірусами, а фаєрвол відслідковує міжмережеві зв’язки нашого комп’ютера та мережі Інтернет і, відповідно, допомагає нам захищатись від загроз ззовні. Користувачі Mac OS також повинні встановлювати антивірусні програми та фаєрвол, оскільки за 2017 рік кількість вірусів, які були створені для Mac, зросла набагато більше, ніж за останні 10 років. В основному це віруси, які зашифровують комп’ютер та вимагають гроші. Якщо у вас Windows, то можна використовувати вбудовані захисні програми Windows Defender або ж якісь інші – все залежить від того, кому ви довіряєте.
4. **Встановлюйте пароль на вхід у пристрій (телефон, планшет, комп’ютер).** Вам потрібен саме складний унікальний пароль. Складний унікальний пароль – це такий, котрий містить великі літери, маленькі літери, спеціальні символи, і розмір його загалом не менше 14 символів – це мінімальний стандарт, а ще краще 20 чи 30. Унікальність – це означає, що кожен обліковий запис повинен мати власний пароль. Тобто в Facebook у нас повинен бути один пароль, а на поштовій скриньці Gmail - зовсім інший.
5. **Використовуйте менеджер паролів.** Якщо ми створюємо для кожного облікового запису унікальні паролі, то з їх кількістю виникають труднощі. Ви можете використовувати той менеджер, який для вас є зручним і якому ви довіряєте. У користувачів Mac OS, наприклад, є вбудований менеджер Keychain, який автоматично зберігає паролі. LastPass – це онлайн менеджер паролів для тих облікових записів, які ви створюєте онлайн. KeePass - це офлайн менеджер, де ви самостійно забезпечуєте безпеку паролів.
6. **Не використовуйте ненадійні поштові сервіси, соціальні мережі, месенджери.** Ненадійні сервіси – це ті, які надавали інформацію про своїх користувачів, або ж вони поганої якості, тобто не використовують шифрування, або були скомпрометовані. В цьому випадку виходить, що наші дані захищені угодою користувача з будь-якою корпорацією.
7. **Розділяйте облікові записи.** Наприклад, у нас є поштові скриньки окремо для роботи і для дому. Якщо зламали нашу домашню скриньку, то не отримали доступ до робочої, і навпаки. Навіть, якщо ми комунікацію розділяємо між різними месенджерами: наприклад, частина переписки в WhatsApp, а частина в Viber – це вже захищає інформацію, тому що тим, хто атакує, треба отримати доступ до ще одного каналу комунікації.
8. **Блокуйте пристрої.** Наприклад, якщо ви йдете випити кави, то важливо заблокувати свій пристрій, щоб людина, яка йде повз ваш робочий стіл, не отримала доступ. На мобільному телефоні краще встановити відключення після 60 секунд, щоб він самостійно заблокувався, якщо ви його залишили на столі. Для Windows – це блокування клавішами Win+L, в Mac комп’ютерах ви просто блокуєте кришку, і він переходить в режим сну та запитує пароль.
9. **Використовуйте повнодискове шифрування пристроїв.** Якщо ви користуєтесь останніми моделями iPhone або телефонами преміум-класу з системою Android, то таке шифрування відбувається за замовчуванням.
10. **Видаляйте історію з браузера та кеш.** Коли ви працюєте в інтернеті, то сайти, на які ви заходите, відправляють на ваш комп’ютер невеличкі файли, щоб знати, що це були ви, та відповідно індексують усі ваші дії.  Наприклад, CCleaner – це програма, за допомогою якої можна видаляти такі тимчасові файли. Це потрібно для того, щоб людина, яка працюватиме на комп’ютері після вас, не могла подивитись, що саме ви шукали, тобто щоб ви були більш анонімними.
11. **Не зазначайте очевидні відповіді для відновлення доступу до свого облікового запису.** Якщо таємне питання для відновлення паролю – дівоче прізвище вашої мами, то ця інформація є загальнодоступною, її можна знайти в соціальних мережах та легко отримати доступ до вашої скриньки.
12. **Не використовуйте для відновлення доступу незахищені поштові скриньки.** Якщо у вас є добре захищена поштова скринька на Gmail, а інша скринька на Mail.ru, і вони пов’язані між собою функцією відновлення, тоді потенційно ви є вразливими.
13. **Користуйтесь секретними месенджерами, якщо вирішили вести таємну переписку.** Наприклад, Viber, Signal, таємні чати в Telegram. Одна із важливих складових – це не лише передача зашифрованої комунікації, але й її зберігання. Якщо ви комусь передали таємну інформацію, то вона є у вас і у вашого колеги. Відповідно, якщо ви не хочете, щоб це в подальшому було виявлено, краще відразу видаляти інформацію. В деяких месенджерах є певний час для видалення повідомлення: наприклад, ви встановлюєте його на 1 хвилину, після чого повідомлення автоматично видаляється.
14. **Використовуйте месенджери з шифруванням від пристрою до пристрою – Signal, WhatApp, Viber, а в Telegram - секретний чат.** В такому випадку у сервіс-провайдера немає можливості читати вашу переписку.
15. **Не клікайте на підозрілі посилання.**
16. **Не ловіться на фішинг.** Фішинг - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.
17. **Робіть резервні копії важливих файлів в хмарних сховищах.** Хмарні сховища – це Google Диск, Dropbox. Статистично є дуже ймовірним, що може трапитись пошкодження жорсткого диску або флешки без можливості відновлення. Якщо ви користуєтесь Gmail поштою, то можете використовувати Google Диск. Якщо у вас є таємні файли, то ви можете їх попередньо зашифрувати, а потім завантажити в хмарне сховище.
18. **Робіть двофакторну авторизацію для важливих облікових записів.** Facebook, Dropbox, Microsoft, Yandex Диск, ВКонтакте, Gmail – скрізь, де це можливо, краще застосовувати двофакторну авторизацію. Це означає, що, окрім паролю, який ви знаєте, вам потрібно зазначити другий фактор – це може бути або СМС-повідомлення, або локально згенерований код на вашому телефоні через Google автентифікатор. В Росії були випадки, коли ФСБ перехоплювала СМС-повідомлення та зламувала двофакторну аутентифікацію, тому там краще користуватись Google автентифікатором.
19. **Використовуйте технології VPN (Virtual Private Network — віртуальна приватна мережа) при підключенні до публічного Wi-Fi.** VPN – це тунель від вашого ПК до іншого комп’ютера, а потім до мережі Інтернет. По суті, це створення надійного тунелю, що захищає ваші дані в ненадійній мережі. Наприклад, є VPN-сервіс TunnelBear – це соціально відповідальний бізнес, тому, якщо ви напишете, що ви активіст чи журналіст з Україні, то вони нададуть вам знижку. VPN-сервіс можна створити самостійно (купуєте сервер, підключаєте Open VPN). Якщо ми не можемо зробити це власноруч, то купуємо підписку на VPN. В браузері Opera є VPN, який пересилає ваш веб-трафік через сервери Opera. Відмінність полягає в тому, що стандартний VPN пропускає увесь трафік. Наприклад, ви підключаєтесь до публічного Wi-Fi, заходите в поштову скриньку, на сайт новин і т.д. Люди, які тут працюють, бачать, що користувач №1 увійшов в соціальну мережу, потім почитав новини – увесь трафік відкритий через точку доступу. Якщо ви бажаєте приховати цю інформацію, то купуєте VPN та користуєтесь в таких випадках.
20. **Використовуйте мережу Tor, якщо хочете бути анонімними.** Якщо ви звичайний користувач і вам майже нічого не потрібно приховувати, то VPN буде достатньо. Tor (The Onion Router) – це інструмент анонімності, а VPN – інструмент безпеки.
21. **Змінюйте дефолтний пароль на домашньому Wi-Fi-роутері.** Дефолтні паролі – це паролі за замовчуванням. Ваш роутер підключений до мережі Інтернет. Якщо на ньому стандартні паролі, як от «admin» або номер вашого телефону, то до нього може підключитись зловмисник. Наприклад, років 5 тому молдавська телекомунікаційна мережа роутерів перейшла в  невеликий ботнет – це коли у вас є доступ до пристроїв, і ви можете віддалено наказувати, що їм робити. Таким чином можна змусити всіх одночасно зайти на один сайт, і він вже не буде доступним. Якщо я можу підключитись до вашого роутера, то зможу комусь щось надіслати від вашого імені.

**Тож подумайте про свою безпеку завчасно. І вона у Ваших руках!**

