Правила безпеки в інтернеті: 10 кроків

1. Електронна пошта та безпека в Інтернеті.

Переосмислюйте налаштування електронної пошти. Припустимо, що всі “безкоштовні” служби електронної пошти та веб-пошти (Gmail, тощо) є підозрілими. Будьте готові платити за таку послугу, як Fastmail, яка не розташована в США – хоча деякі з її серверів знаходяться в Нью-Йорку з резервними серверами в Норвегії. Також варто було б перевірити, чи ваша організація не передала свої електронні та інформаційні системи до сервісів Google або Microsoft – як це зробило багато організацій (включаючи газети та університети).

Реальна складність із електронною поштою полягає в тому, що, хоча існують способи зберігати вміст повідомлень приватними (див. Шифрування), “метадані”, що йдуть з повідомленням (так би мовити “конверт”), може бути видними, і немає спосіб їх шифрування через те, що вони потрібні системі інтернет-маршрутизації і доступні більшості служб безпеки без додаткового дозволу.

2. Шифрування.

Шифрування вважалося сферою винятково гіків та математиків, але багато чого змінилося останніми роками. Тепер це основне питання вашої безпеки в інтернеті. З’явилися різноманітні загальнодоступні інструменти шифруванням (і розшифровки) електронної пошти та файлів. Наприклад, GPG для пошти – це плагін з відкритим вихідним кодом для програми Apple Mail, який дозволяє легко шифрувати, дешифрувати, підписувати та перевіряти електронні листи за стандартом OpenPGP.

Для захисту файлів новіші версії операційної системи Apple OS X поставляються з FileVault, програмою, яка шифрує жорсткий диск комп’ютера. Ті, хто працює з Microsoft Windows, мають подібну програму. Це програмне забезпечення буде розбивати ваші дані, але не захистить вас від державних органів, які вимагають наявності вашого ключа шифрування відповідно до Положення про законодавство про розслідування (2000 рік), тому деякі шифрувальники рекомендують TrueCrypt, програму з дуже цікавими можливостями.

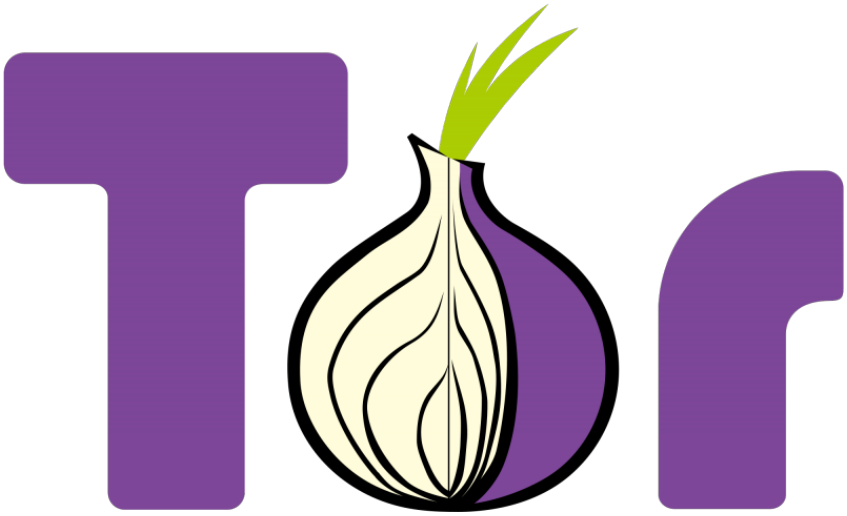
Правила безпеки в інтернеті:

3. **Веб-серфінг**

Оскільки, перегляд веб-сторінок напевно є тим, що користувачі Інтернету роблять найбільше, варто серйозно ставитися до безпеки та конфіденційності веб-браузера.

Якщо ви не вважаєте, що ваш клік-потік (журнал сайтів, які ви відвідуєте) насправді є державною власністю, можна подумати про використання вільнодоступних інструментів, таких як Tor Browser, щоб його приховати.

І, щоб захистити себе від надзвичайно нахабних комерційних компаній, які хочуть відслідковувати вашу поведінку в Інтернеті. Для цього ви повинні, як мінімум, налаштувати ваш браузер так, щоб він поставив перед ними багато бар'єрів та забезпечив інтернет безпеку для вас.



4. Хмарні сервіси та безпека в Інтернеті.

Правила безпеки в інтернеті стверджують, що вам слід уникати всіх хмарних сервісів (Dropbox, iCloud, Evernote тощо). Ваша позиція повинна полягати в тому, що будь-що, що зберігається в таких системах, потенційно доступне для інших. І якщо ви повинні довіряти їм дані, переконайтеся, що дані зашифровані. Правила безпеки в Інтернеті: 10 способів збереження ваших особистих даних – хмарні сервіси

5. **Зберігання та архівування файлів.**

Все більша кількість людей, використовує власні служби хмарних технологій, використовуючи продукти, такі як PogoPlug та Transporter, які надають послуги типу Dropbox, але на підключених до Інтернету дисках, якими ви володієте та керуєте. І якщо ви зберігаєте конфіденційні дані на USB-накопичувачу, переконайтесь, що він зашифрований за допомогою TrueCrypt.

6. Соціальні мережі.

Кібер-злодії полюють в Інтернеті не лише за даними ваших платіжних карток. Видаліть свій обліковий запис Facebook. Тоді ви будете почуватися в безпеці. А якщо ви повинні використовувати його, не додавайте свою дату народження в свій профіль. Навіщо надавати особисті дані злодіям? І пам'ятайте, що незалежно від ваших налаштувань конфіденційності, ви не маєте контролю над інформацією про вас, яка відкрита вашими "друзям".

7. Дані про місцезнаходження.

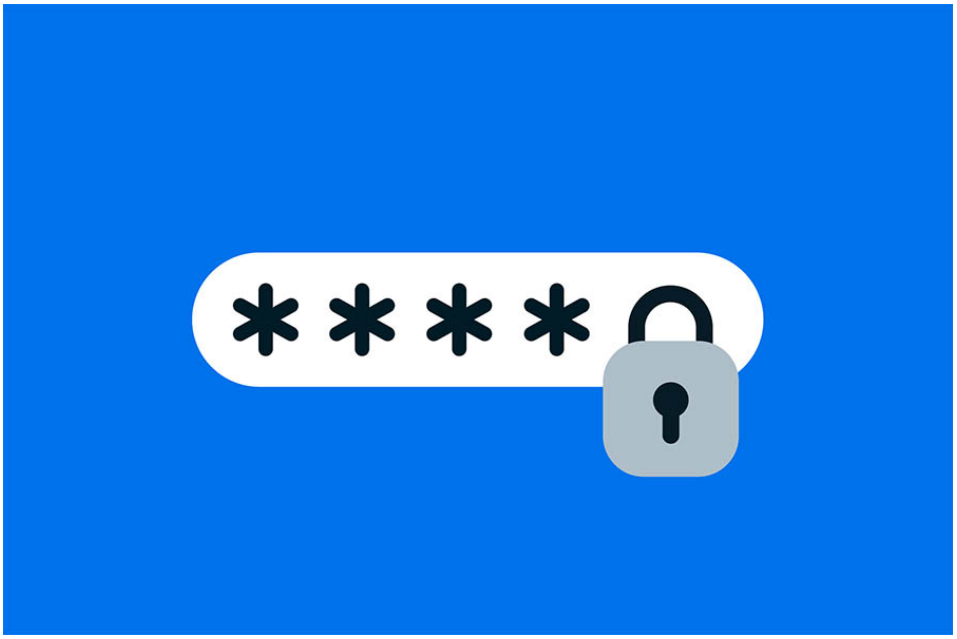
Уникайте використання таких служб, як FourSquare (і подібних), для яких потрібна інформація про місцезнаходження.

8. Бездротові послуги.

Правила безпеки в інтернеті радять вимкнути Bluetooth за умовчуванням на всіх своїх мобільних пристроях. Увімкніть його лише тоді, коли вам явно потрібно його використовувати. Аналогічно, будьте обережні, використовуючи відкритий wifi в громадських місцях. Насамперед, переконайтеся, що будь-який сайт, з яким ви взаємодієте, використовує HTTPS, а не незашифровані HTTP-з'єднання. Хтось поруч може використовувати Firesheep, щоб побачити все, що ви робите.

9. Особиста безпека.

Забудьте про пароль, придумайте парольну фразу – тобто безглузде речення, яке ви пам'ятаєте, – і зробите деякі перетворення (перший і третій літери кожного слова), щоб ви могли згенерувати сильний пароль від нього кожен раз. Або скористайтеся програмою керування паролями, як-от LastPass або 1Password. І якщо служба пропонує багатофакторну аутентифікацію, скористайтеся нею.



Правила безпеки в Інтернеті: безпечний пароль

10. Пошукові системи та безпека в Інтернеті.

Всі великі пошукові системи відстежують вашу історію пошуку та створюють профілі на вас, щоб надавати персоналізовані результати на основі вашої історії пошуку. Якщо ви хочете вийти з цього “фільтрувального міхура”, вам потрібно перейти до пошукової системи, яка не відстежує ваші запити. Найбільш очевидним є химерно названий, але досить ефективний DuckDuckGo.