

Анастасія Апетик

Про безпеку в інтернеті



Раніше, наш день починався з кави, тепер все починається зі смартфона.

Мабуть, саме так сказав би Стів Джобс, якщо був би поруч.

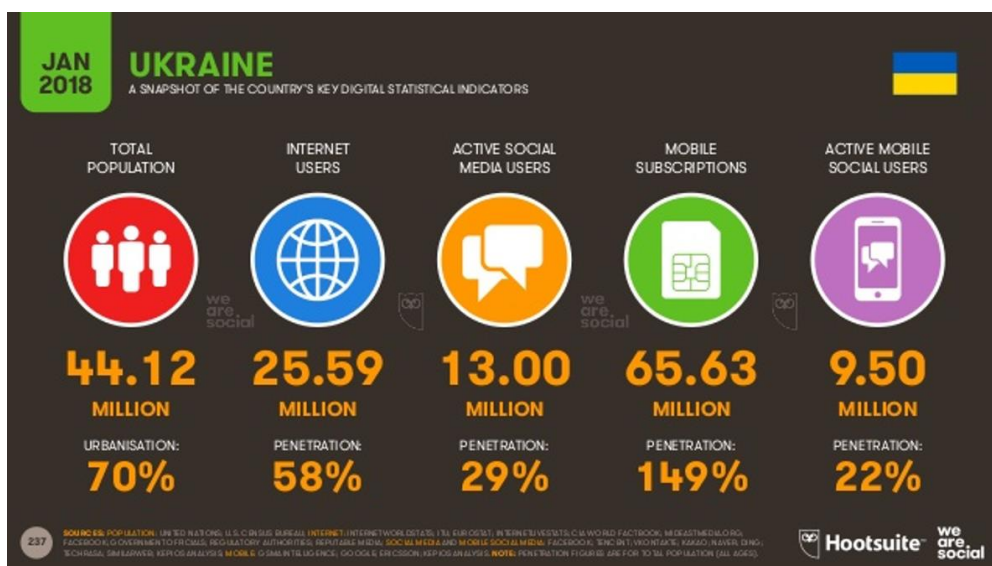
Поки ми їдемо на роботу, то майже не відриваємо очей від гаджетів: встигаємо переглянути всі соціальні мережі та відповісти друзям на нові меседжі.



Кібер-НЕ-безпека

За даними [дослідження компанії We Are Social та Hootsuite](#), у 2018 році в Україні зафіксовано **25,59** мільйонів інтернет-користувачів. Так, ми дуже просунуті, але все ще недостатньо захищені. Від кого?

Від кіберзлочинців. Кожен з нас може опинитися в ситуації інформаційної небезпеки.



Про що говорить офіційна статистика?

За даними [звіту голови Національної поліції у 2018 році](#), кіберполіцейські виявили **6 тисяч злочинів** із використанням ІТ технологій. Перенесення злочинної діяльності з вулиць у віртуальне середовище стає однією з найбільш негативних тенденцій розвитку злочинності в останні роки.

Чи можна захиститися від кіберзлочинців?

Можна. Але не думайте, що список паролів в блокноті може в цьому допомогти. Стереотипні принципи захисту даних тут не спрацюють. Треба використовувати сучасні засоби та кібертехнології.

Як створити безпечний пароль?

ТОП 5 порад від фахівців курсу кібербезпеки Ньюкаслського університету щодо обрання безпечного паролю:

Пароль має включати не менше **12 знаків**, і чим більше — тим краще.

Пароль має включати **великі та малі літери цифри та знаки**.

Використовуйте **«Кодову фразу»**, вона повинна бути відносно довгою (близько 20 символів), і складатись із випадкових слів, наприклад: **«Фіолетовий сніг#48Кандидат\$»**.

Очевидно, що такий пароль включає випадкові слова, цифри, символи, містить великі літери, і його складно буде вгадати.

P.S. Але я рекомендую придумати свій пароль і не використовувати цей.


Ніколи не записуйте Ваші паролі на аркуші!



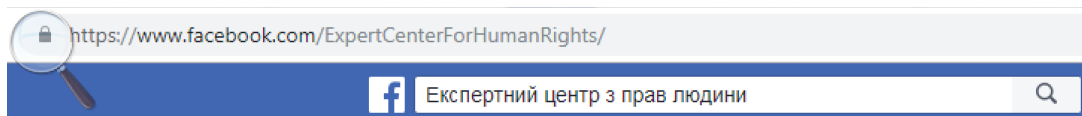
Як дізнатися, чи безпечний сайт?



Коли ви заходите на сайт і бачите лінк, який починається із «**https://**» — це означає, що такий сайт є захищеним. HTTP (Hyper Text Transfer Protocol) — протокол передачі даних у мережі, а літера s означає **secure**, тобто «безпечно».

Звертайте увагу на те, щоб не повідомляти сайт, в адресному рядку якого відсутній значок замочок,  про свої паролі. Таке з'єднання вважається не захищеним.

Безпечне з'єднання виглядає так:



Електронна скринька та Ваша безпека

Ми часто отримуємо на електронні поштові скриньки невідомі повідомлення, автори яких просять відповісти чи перейти за посиланням, чи навіть, завантажити якісь файли.

Наприклад, вчора я отримала повідомлення такого характеру:

🇺🇦 англійский ▾ > русский ▾ [Перевести сообщение](#)

Good day,

My Name is Johann Reimann and i have something important to discuss with you but only with your permission i will proceed.

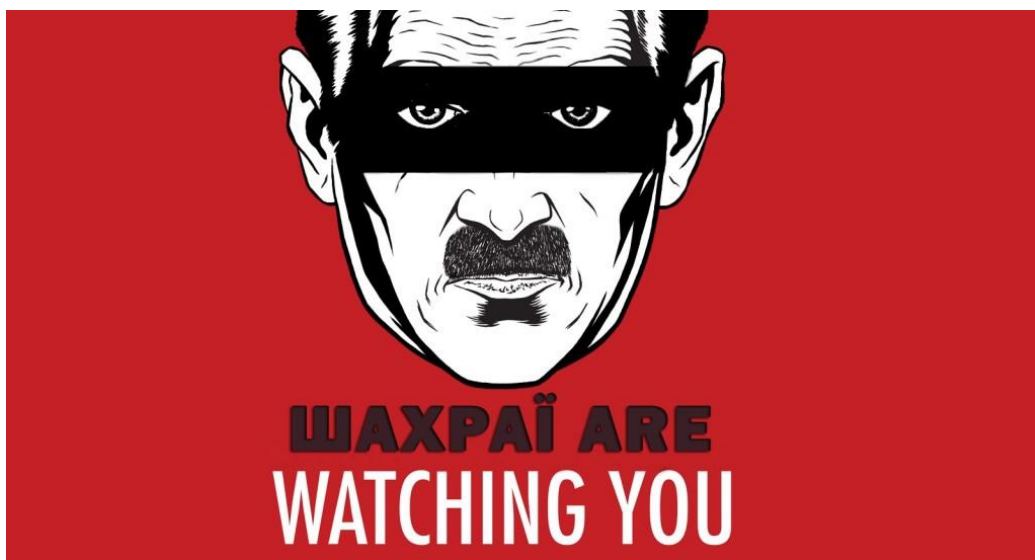
Regards
J. Reimann

Люди, що займаються шахрайством, можуть надсилати електронні листи, які нагадують повідомлення від банку з проханням підтвердити номер вашого рахунку. Вас попросять як найшвидше відреагувати на лист, завантажити додаток чи перейти за посиланням, а також надати:

- Ім'я користувача та паролі
- Номери банківських рахунків
- PIN-коди чи особистий ідентифікаційний номер
- Номери кредитних карток
- Дівоче прізвище матері
- Дату Вашого дня народження

Бачили щось подібне? Такий вид атаки називається **фішингом**.

«А якщо я випадково потрапив на фішингову сторінку?...»



З метою крадіжки особистої інформації користувачів фішингова сторінка копіює зовнішній вигляд іншої (як правило — офіційної) сторінки, ми стереотипно реагуємо, оскільки звикли довіряти подібним документам. Якщо так сталось, що ви вже перейшли за посиланням, зазначеним у листі, та виявилось, що сторінка є фішинговою, захистити себе можна шляхом повідомлення компанії **Google**, яка відповідає за безпечний перегляд.

Для цього достатньо заповнити форму:

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=ru

Як ще можна навчитися кібербезпеці?

Хочете отримати більш ґрунтовні знання у сфері кібербезпеки? Рекомендую пройти безкоштовний онлайн курс:

<https://www.netacad.com/courses/security/introduction-cybersecurity>

І щоб завершити розмову про паролі на веселій, проте освітній ноті, пропоную переглянути 3-хвилинне відео, на якому Едвард Сноуден разом із Джоном Олівером розмірковують, якими мають бути паролі:

<https://www.youtube.com/watch?v=vzGzB-yYKcc>



Якщо Ви ще не переконались у необхідності кібербезпеки, можливо, це відео призведе до деяких коректив.



Expert Center for
Human Rights