YouVenture

Кібербезпека: Як захистити свої дані та гроші в цифровому світі

Чи справді ви в безпеці в інтернеті?

Уявіть, що одного ранку ви прокидаєтеся, відкриваєте телефон і бачите повідомлення: "Ваш акаунт заблоковано через підозрілу активність". Паніка. Ваші паролі зламані, гроші списані, і зловмисники мають доступ до всіх ваших особистих даних. Це не сценарій для кіно, а реальність тисяч людей щодня. Більшість навіть не підозрює, що їхні паролі вже давно злиті в даркнет. Чи входите ви до цього списку?

Цей гайд допоможе вам дізнатися, які загрози існують, як захистити свої акаунти, уникнути шахрайства та зробити свою цифрову безпеку неприступною фортецею. Наприкінці ви знайдете тест для швидкої перевірки своєї безпеки та тест, який допоможе зрозуміти, наскільки ви вразливі.

Найбільші загрози в інтернеті

Кожен користувач стикається з небезпеками в мережі. Давайте розглянемо найпоширеніші способи атак і що робити, щоб не потрапити в пастку.

1. Фішингові сайти. Вас просять підтвердити логін у Facebook, але сайт виглядає трохи інакше? Це підробка. Фішингові сайти копіюють дизайн відомих платформ, крадучи ваші дані. Завжди перевіряйте URL перед введенням пароля.

2. Зламані акаунти. Чи знаєте ви, що один і той самий пароль для різних сайтів – це смертельний вирок вашій безпеці? Якщо один сайт зламають, зловмисники зможуть зайти в усі ваші акаунти.

3. Витік паролів. Перевірте, чи ваші паролі вже злиті: зайдіть на сайт *haveibeenpwned.com* і введіть свою електронну пошту.

4. Злами через Wi-Fi. Безкоштовний Wi-Fi в кав'ярні – пастка для хакерів. Вони можуть "прослуховувати" трафік і отримати доступ до ваших даних.

5. Шахрайські SMS та дзвінки. "Ваша картка заблокована" – це класичний обман. Ніколи не переходьте за посиланнями в підозрілих повідомленнях і не передавайте дані картки телефоном.

Як захистити себе: 5 простих кроків

Ви можете витратити всього 10 хвилин, щоб захистити свої дані. Це елементарні речі, які вбережуть вас від більшості атак.

1. Використовуйте менеджер паролів. Не запам'ятовуйте десятки комбінацій – використовуйте LastPass, Bitwarden або 1Password. Вони збережуть ваші паролі та запропонують унікальні.

2. Увімкніть двохфакторну аутентифікацію (2FA). Це захист навіть у разі зламу пароля. Google Authenticator або SMS-підтвердження – це ваш друг.

3. Перевіряйте посилання перед натисканням. Наведіть курсор на лінк перед тим, як перейти. Справжній сайт чи підробка?

4. Використовуйте VPN та шифрування. VPN приховає ваш трафік від хакерів, особливо в публічних Wi-Fi.

5. Уникайте публічних Wi-Fi без VPN. Коли ви підключаєтесь до відкритої мережі, ви ніби залишаєте свій ноутбук без пароля в людному місці.

Практичні інструменти та перевірка безпеки

Настав час протестувати вашу цифрову безпеку. Використовуйте ці сервіси:

✓ **Перевірка паролів**: haveibeenpwned.com.

✓ **Менеджери паролів:** Bitwarden, LastPass, 1Password.

✓ **Антивіруси**: Malwarebytes, Kaspersky, Norton.

✓ **Безкоштовні VPN:** ProtonVPN, Windscribe.

Збережіть цей список – він може врятувати ваші дані!

Тест "Чи вразливий ваш акаунт?"

1. Чи використовуєте ви один і той самий пароль для кількох акаунтів?
2. Чи є у вас двохфакторна аутентифікація?
3. Чи перевіряли ви свої паролі на витоки?
4. Чи використовуєте менеджер паролів?
5. Чи часто ви підключаєтесь до публічних Wi-Fi?

Якщо у вас більше 2 негативних відповідей – ви у групі ризику!

Час діяти.

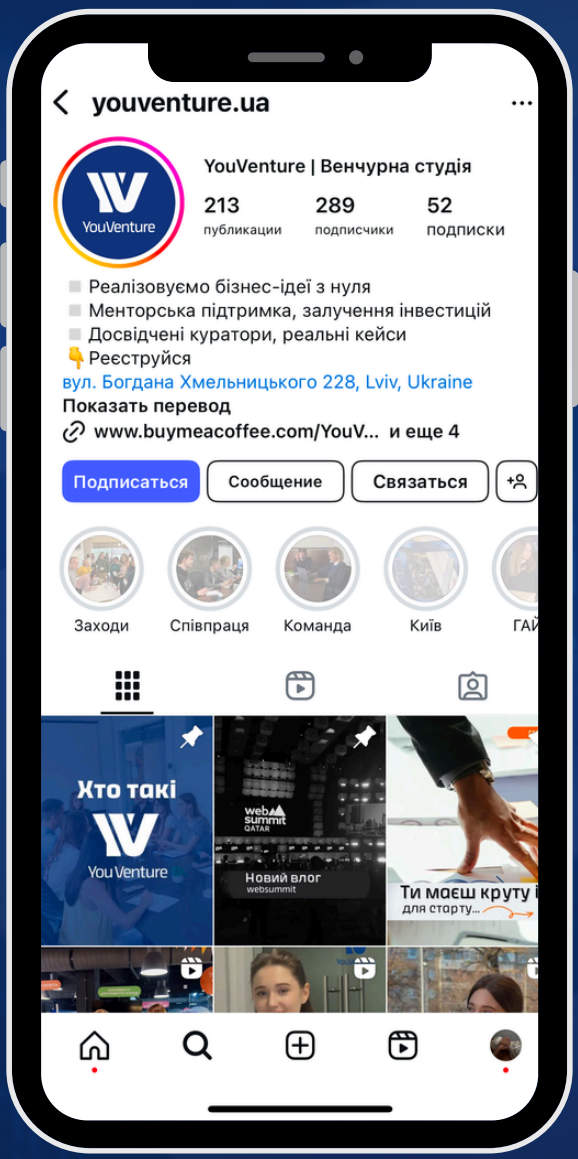
Ви дізналися, як захистити себе. Але що далі?

Кібербезпека – це лише частина сучасного цифрового світу. Якщо вам цікаво, як не тільки захистити себе, а й заробляти в інтернеті, створювати стартапи та розвивати бізнес, тоді вам до YouVenture ! Ми навчимо вас:

- ✓ **Як будувати бізнес із нуля**
- ✓ **Як залучати інвестиції**
- ✓ **Як монетизувати цифрові навички**
- ✓ **Як масштабувати власний проєкт**

Готові стати частиною майбутнього? Долучайтесь прямо зараз!

YouVenture



youventure.eu
info@youventure.eu
+38 068 646 77 10