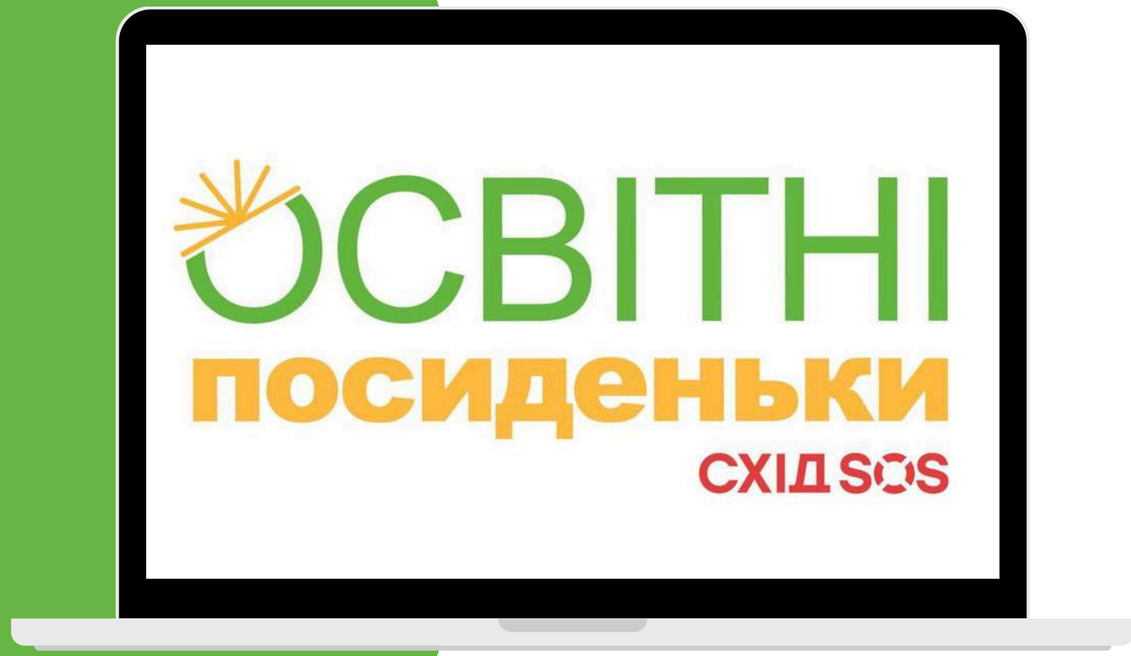
Тренінг з розвитку цифрових компетентностей

«Як зашторити вікна?»: безпека в Інтернеті та забезпечення приватності освітян й учнів

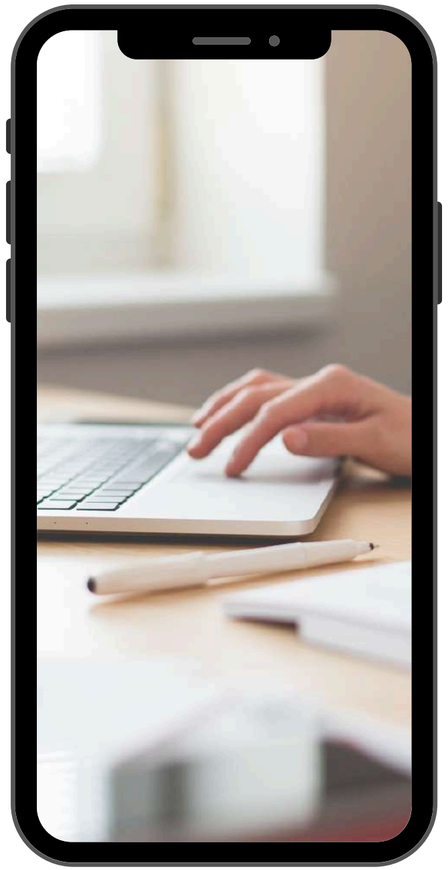


Дмитро Тельпіс

- Тьютор у проєкті Навчай для України «Освітній СУП»
- Ментор у проєкті з розвитку цифрових компетентностей «Girls4Tech»
- Запрошений лектор Одеського національного університету імені І. І. Мечникова
- Директор ГО “Софійський колегіум”

СХІД SOS

ОСВІТНІ посиденьки

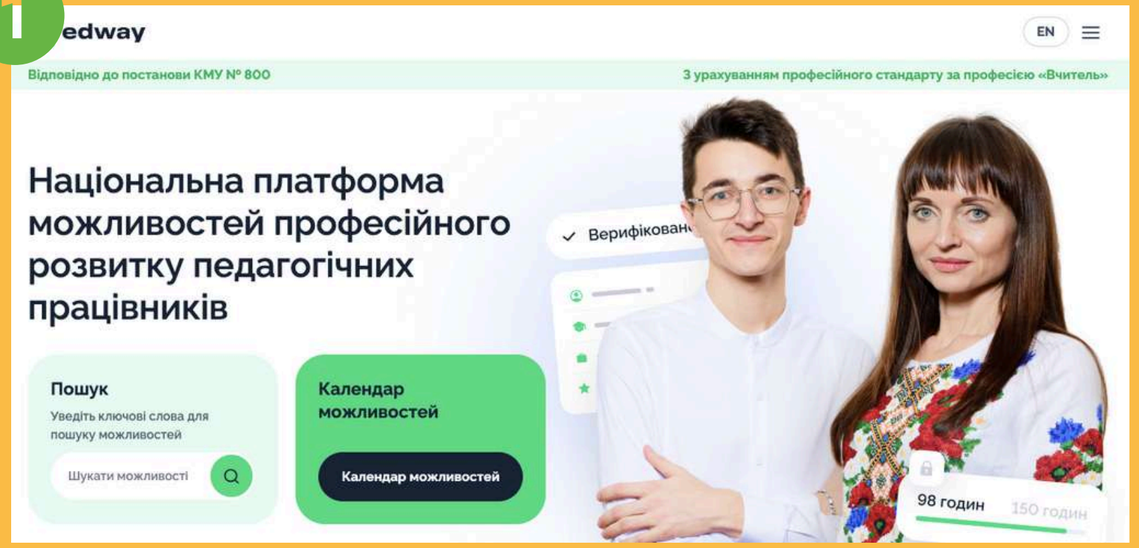


Долучіться до каналу

“ОСВІТНІ ПОСИДЕНЬКИ ОДЕСА”

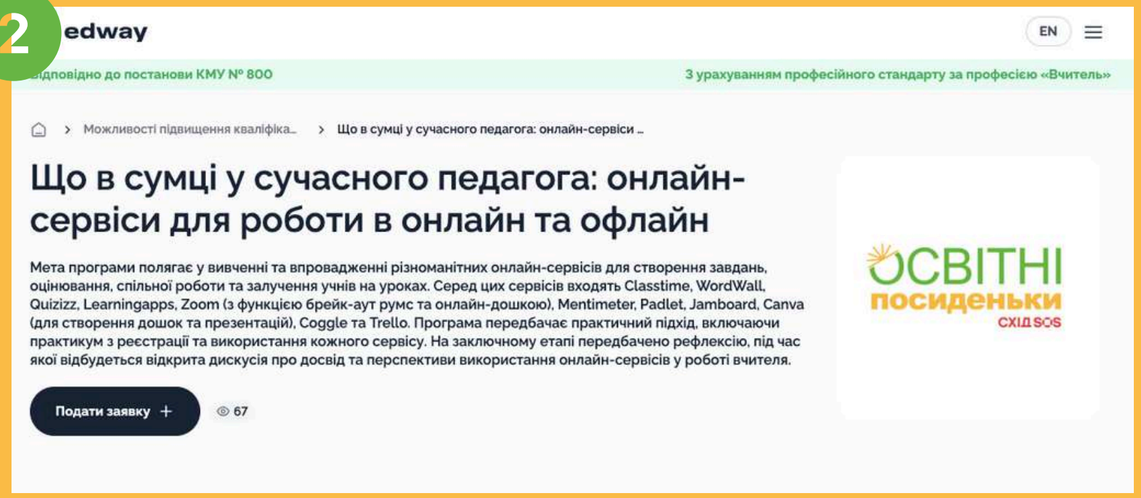
Як отримати сертифікат?

1



Зареєструйтесь на платформі Edway за ПОКЛИКАННЯМ

2



Подайте заявку за ПОКЛИКАННЯМ

Поговоримо про:

Актуальність цифрової безпеки та способи її забезпечення

Паролі та двофакторна автентифікація

Цифровий слід та його використання шахраями

Публікація персональних даних учнів: законодавчий аспект

СХІД SOS

ОСВІТНІ посиденьки

ЯКИЙ ТИ СЬОГОДНІ ПЕС ПАТРОН?

t.me/kryholam_today

КРИГОЛАМИ НА СЬОГОДНІ

@KRYHOLAM_TODAY

Безпека – це процес, а не мета.

І це завжди безперервний і нескінченний процес.

СХІД SOS

ОСВІТНІ посиденьки

Коли ви користуєтесь смартфоном або ноутбуком, ви працюєте з даними.

Дані бувають різних форм і видів: від текстових документів, відео, зображень та інших статичних медіафайлів до наборів координат або відеопотоків у реальному часі.

Загроза — це потенційна подія, яка може завдати шкоди нашим зусиллям із захисту даних. Загроза може надходити від особи (зловмисника) або групи осіб, але це також може бути й нещасний випадок: популярним прикладом є розлитий напій на ноутбук.

Ризик — це ймовірність того, що загроза відбудеться і зможе звести нанівець ваші зусилля щодо захисту ваших даних.

Безпека — це завжди баланс між зручністю та витраченими ресурсами (часом, грошима тощо).

СХІД SOS

ОСВІТНІ посиденьки

Принцип моделювання загрози

1. Що мені потрібно захищати?

2. Від кого я хочу це захистити?

3. Наскільки ймовірно, що актив буде атакований?

4. Що станеться, якщо мені не вдасться захистити актив?

5. Що я можу зробити, щоб уникнути наслідків?

6. Хто на моєму боці?

*Детальніше про принцип моделювання загрози читайте тут: https://ssd.eff.org/module/your-security-plan

Покращення безпеки. Програмне забезпечення

- **Постійно оновлюйте програмне забезпечення та не використовуйте програми, які не оновлювалися протягом тривалого часу;**
- **Використовуйте лише ліцензійне програмне забезпечення та не встановлюйте «зламані» програми, натомість шукайте дешевші або безкоштовні альтернативи;**
- **Не встановлюйте невідомі вам програми – завжди перевіряйте інформацію в інтернеті;**
- **Завжди майте принаймні одну резервну копію цінних даних.**

Покращення безпеки. Технічне оснащення

- **Подбайте про охолодження ваших пристроїв**
- **Не забувайте про гігієну! Важливо періодично чистити всі пристрої.**
- **Якщо на ваш смартфон потрапила волога, вимкніть його і дайте висохнути, за можливості вийміть акумулятор пристрою. Не підключайте акумулятор і не вмикайте пристрій, доки не будете на 100% впевнені, що він повністю висох.**
- **Якщо акумулятор вашого пристрою виглядає деформованим (набряклим, скрученим), не використовуйте його. Деформований акумулятор не безпечний.**

Покращення безпеки. Фізична безпека

- **Не залишайте мобільний пристрій без нагляду на тривалий час**
- **Увімкніть повне шифрування диска і завжди тримайте дані на своєму пристрої захищеними від несанкціонованого доступу**
- **Налаштуйте екран таким чином, щоб він вимикався через 2–5 хвилин відсутності активності і пропонував увести пароль після пробудження**
- **Візьміть собі за звичку завжди блокувати екран пристрою**
- **Пам’ятайте про підглядання через плече та підслуховування**

Шифрування диску та пристрою

Натисніть кнопку Пуск і виберіть пункт Налаштування > Оновити & Безпека > Шифрування пристрою

ЧИТАТИ більше про шифрування Bitlocker у Windows

Виберіть меню Apple > Системні налаштування, а потім натисніть Безпека та конфіденційність. Перейдіть на вкладку «Сховище файлів». Натисніть Заблоковано, а потім введіть ім’я адміністратора та пароль. Натисніть Увімкнути FileVault

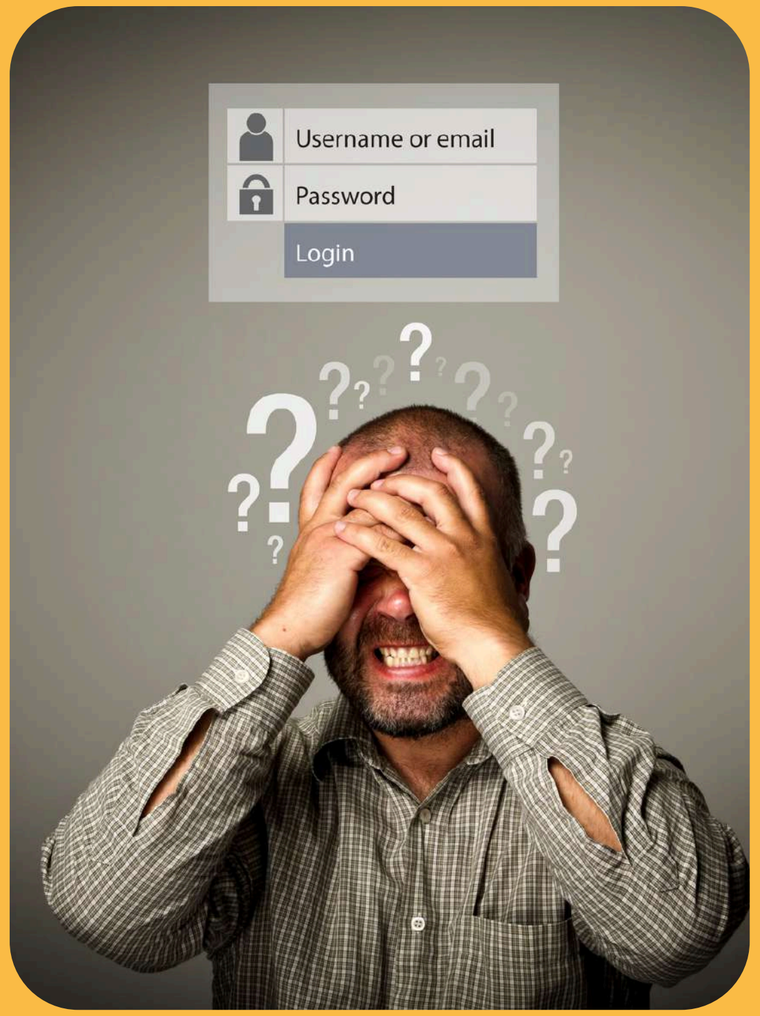
СХІД SOS

ОСВІТНІ посиденьки

Надійний пароль

- **Не використовуйте паролі**, що містять ваше ім’я, день народження або будь-яку іншу особисту інформацію, яку легко вгадати;
- **Поєднуйте літери** з цифрами, малі літери з великими, також можна використовувати деякі символи в паролях, наприклад: ?!#;
- Використовуйте **мінімум 12 символів**;
- **Ніколи не використовуйте один і той самий пароль у всіх акаунтах**. Якщо хтось викраде один пароль, він спробує підібрати його до інших акаунтів.

Двофакторна автентифікація



Двофакторна автентифікація – один із найдієвіших способів захисту облікових записів: електронної пошти, месенджерів, акаунтів у соцмережах та інших.

Якщо хтось намагатиметься увійти до вашого акаунту з незнайомого пристрою – наштовхнеться на додаткову перепону, а ви отримаєте сповіщення про таку спробу входу.

СХІД SOS

ОСВІТНІ посиденьки

Додатковим фактором для перевірки може бути підтвердження:

- через код, надісланий у смс;
- через дзвінок на мобільний;
- через лист на e-mail;
- через надсилання сповіщення
- через код, згенерований за допомогою спеціальних мобільних додатків тощо.

Як встановити двофакторну автентифікацію:

1. Увійдіть у потрібний акаунт.
2. Зайдіть у розділ меню “Налаштування”, а потім “Безпека”.
3. Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (може називатися також – двоетапна перевірка).
4. Виконайте всі необхідні дії за запропонованою інструкцією.

Пароль на флешці

Щоб встановити пароль на флеш-накопичувачі:

1. Відкрийте меню «Пуск» >→ «Параметри» (значок у вигляді шестерні) та перейдіть до розділу «Облікові записи».
2. Виберіть у бічному меню «Варіанти входу», розкрийте пункт «Пароль» і натисніть «Додати».
3. Заповніть поля, користуючись підказками системи, наприкінці клацніть «Готово».

Менеджер паролів

Менеджер паролів – це програма, яка дозволяє зберігати всі ваші паролі в безпечному, зашифро-ваному сховищі. Це сховище можна відкрити лише за допомогою головного пароля, який захищає всі інші паролі.

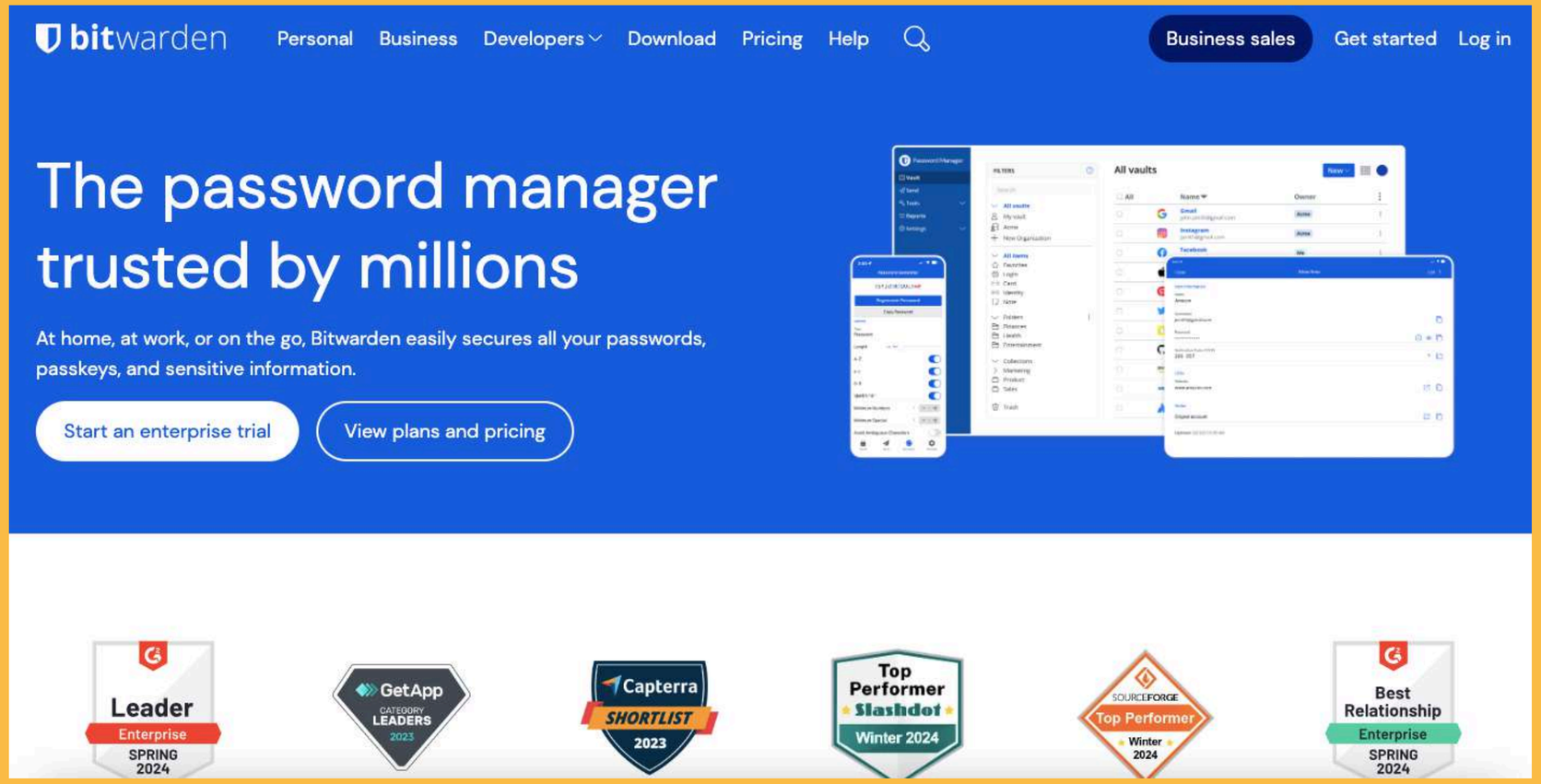
Існує дві великі групи менеджерів паролів:

Хмарний – зашифрований вміст зберігається в хмарі, що дозволяє синхронізувати його на різних пристроях;
Офлайн – зашифрований вміст зберігається локально на вашому пристрої.

СХІД SOS

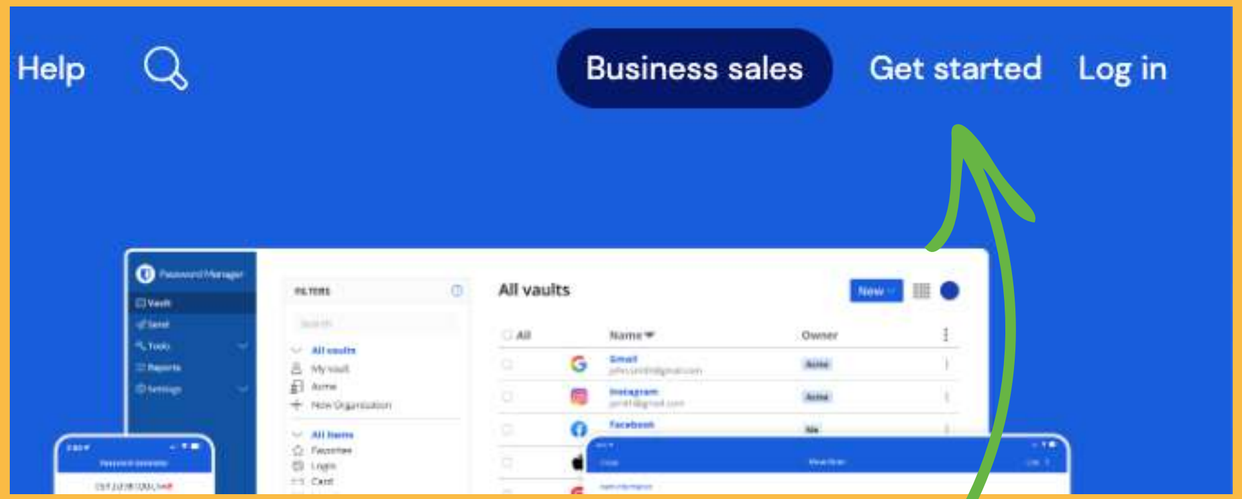
ОСВІТНІ посиденьки

Bitwarden



ПОКЛИКАННЯ НА СЕРВІС

Bitwarden: реєстрація



Реєструватись тут

Адреса е-пошти (обов'язково)

Адреса е-пошти буде використовуватися для входу.

Назва

Як до вас звертатися?

Головний пароль (обов'язково)

Важливо: Головний пароль неможливо відновити, якщо ви його втратите! Мінімум 12 символів

Введіть головний пароль ще раз (обов'язково)

Підказка для головного пароля

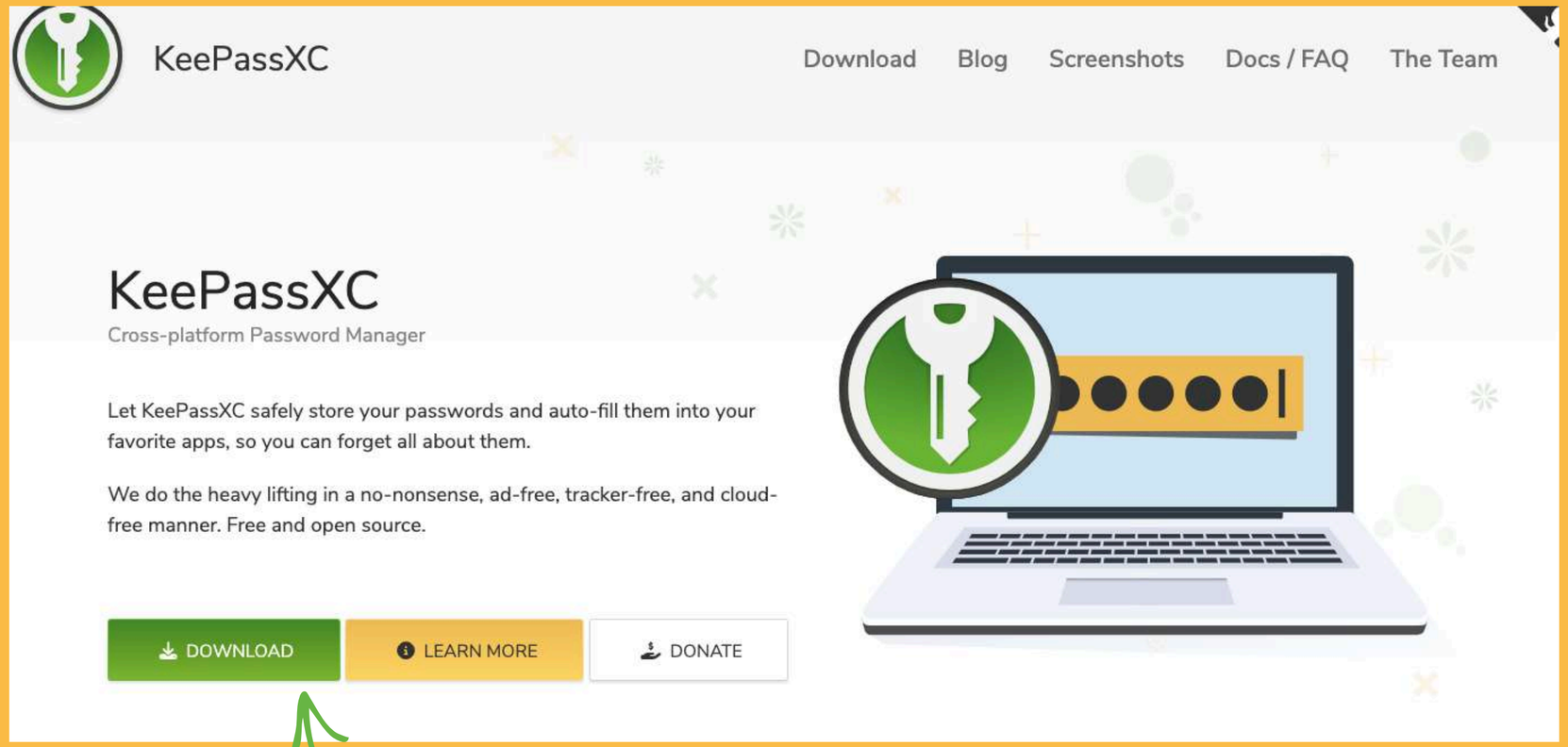
Якщо ви забудете головний пароль, підказка може допомогти вам згадати його.

☑ Перевірити відомі витоки даних для цього пароля

☐ Позначивши цей прапорець, ви погоджуєтеся з: Умови користування, Політику приватності

Створити обліковий запис

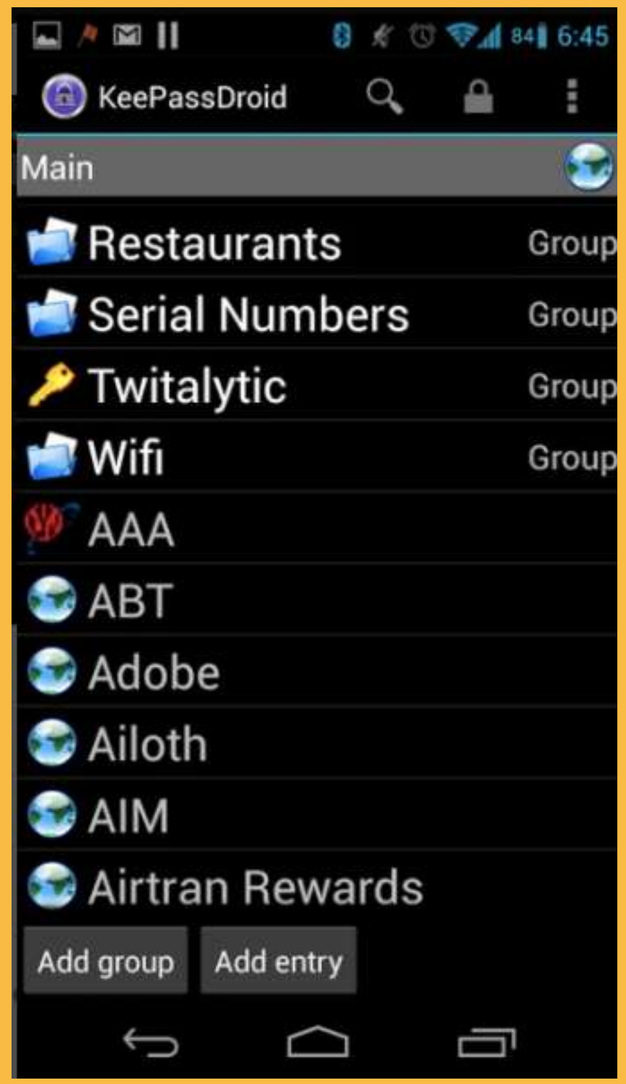
KeePassXC



ПОКЛИКАННЯ НА СЕРВІС

Завантажити тут

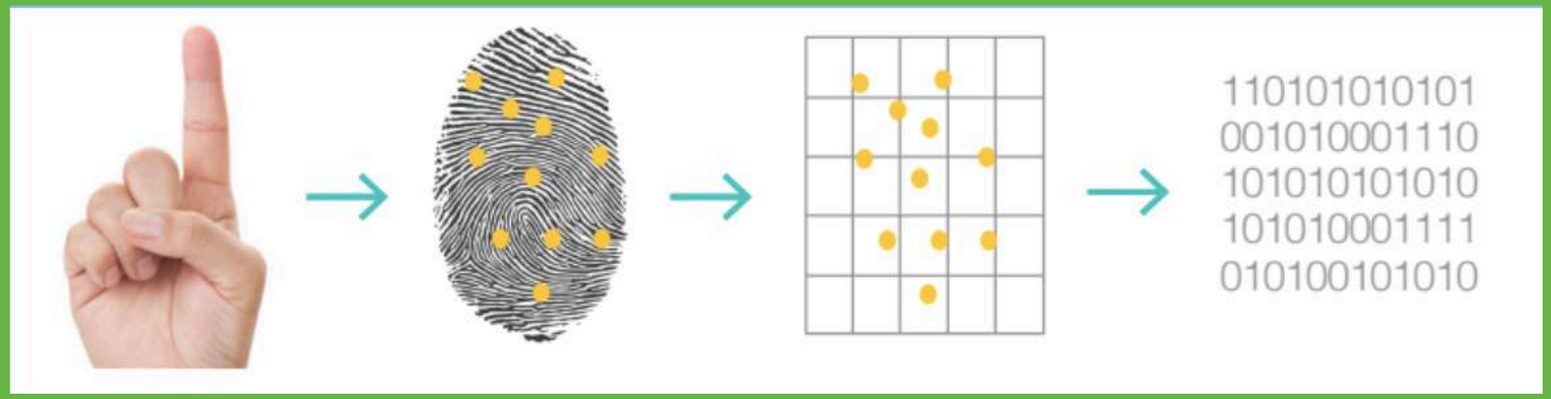
KeePassDroid

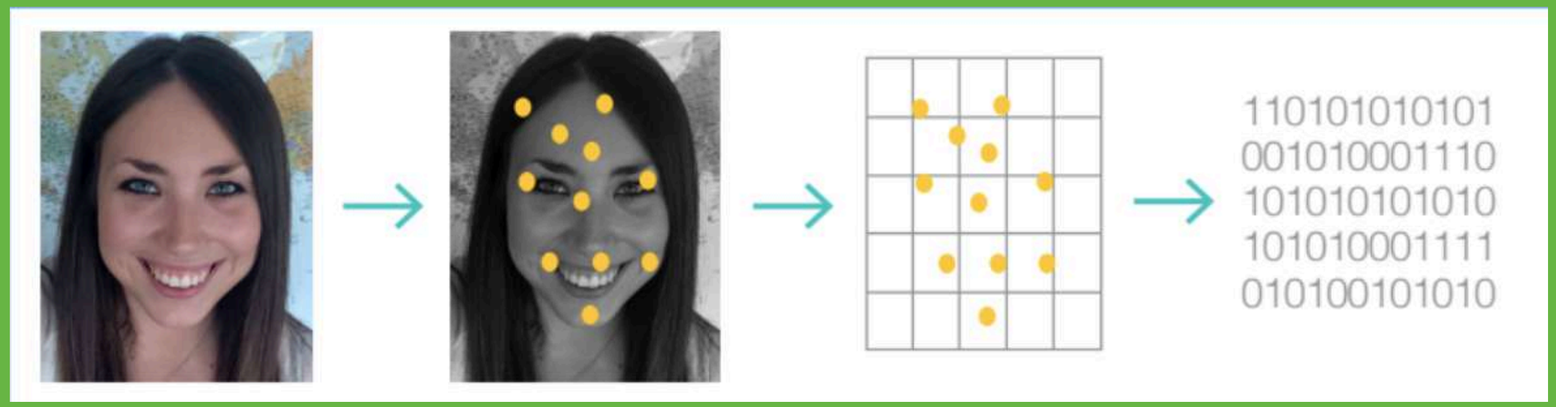


KeePassDroid – менеджер паролів для платформ Android, який працює з тим самим типом зашифрованих файлів, що й KeePassXC.

ПОКЛИКАННЯ НА СЕРВІС

Біометрія





Біометрія – вимірювання унікальних характеристик, насамперед для ідентифікації особи.

СХІД SOS

ОСВІТНІ посиденьки

Біометрія

Цифровий слід

Цифровий слід – це слід даних, які ви створюєте під час користування Інтернетом.

Він охоплює все: від веб-сайтів, які ви відвідуєте, до електронних листів, які ви надсилаєте, і публікацій у соціальних мережах, з якими ви взаємодієте. По суті, кожна окрема дія, яку ви виконуєте в Інтернеті, залишає цифровий слід, сприяючи вашому загальному цифровому сліду.

Цифровий слід

Активний цифровий слід

Ваш активний цифровий слід це всі цифрові сліди, які ви свідомо залишаєте в Інтернеті. Щоразу, коли ви публікуєте фотографію в Instagram, пишете допис у блозі, коментуєте відео на YouTube або надсилаєте електронний лист, ви робите свій внесок у свій активний цифровий слід.

Пасивний цифровий слід

Це дані, зібрані про вас без вашої безпосередньої ініціативи. Це стосується вашої історії веб-перегляду, даних про місцезнаходження, які відстежуються програмами, або файлів cookie на веб-сайтах, які ви відвідуєте.

Цифровий слід

Плюси

Персональний брендинг

Мережа

Вплив

Спеціальний досвід

Мінуси

Питання конфіденційності

Інтернет-репутація

Кіберзалякування та шахрайство

Фішинг

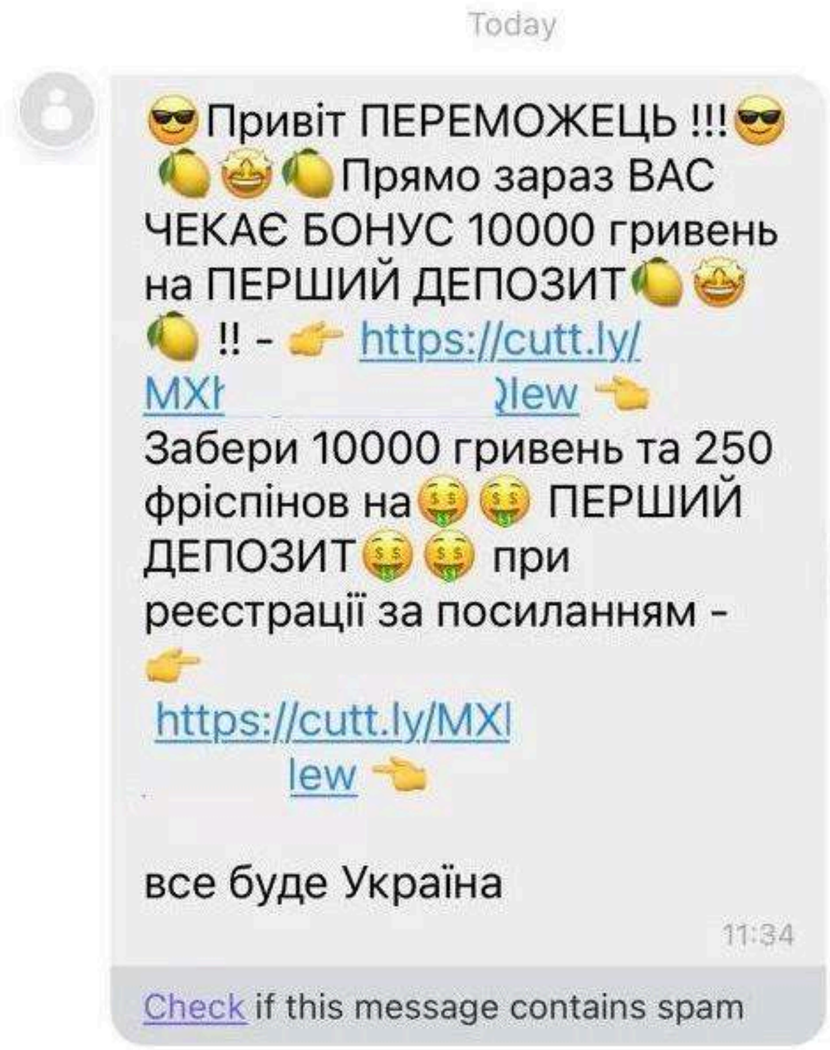
Фішинг — це один з різновидів шахрайства в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів.

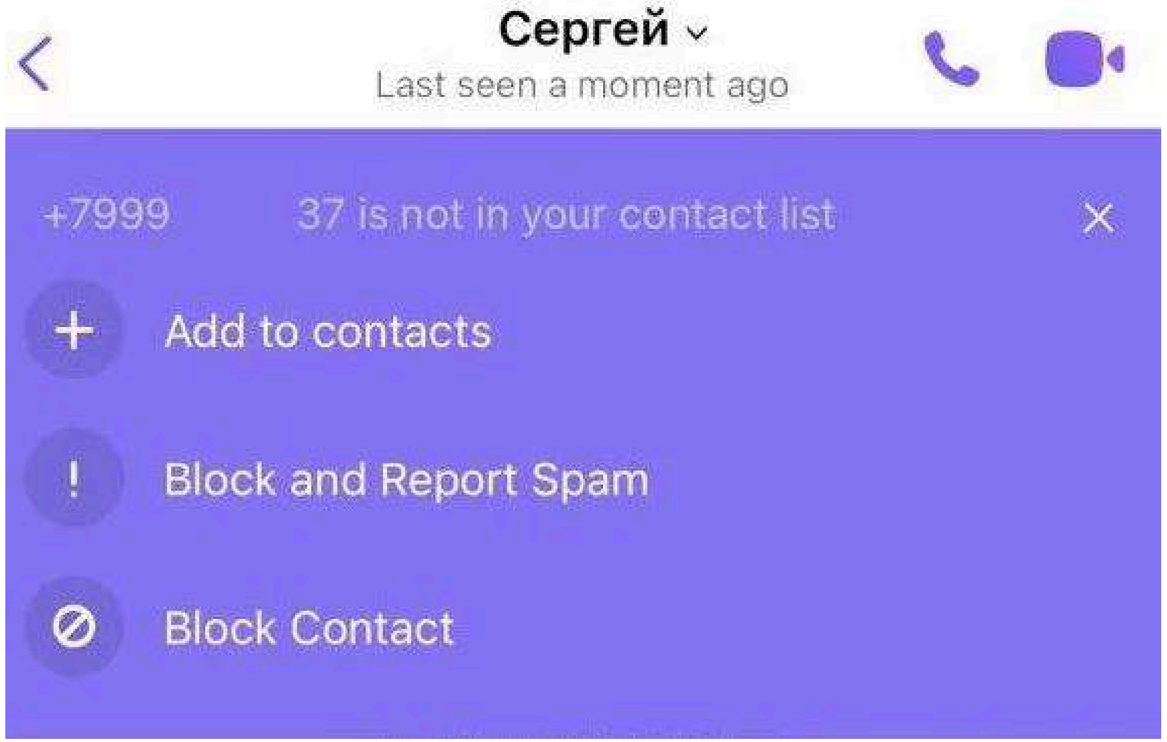
Шахраї «вивуджують» дані користувачів під різними пристойними приводами: перевірка авторизації на сайті, необхідність «відписатися» від спаму в електронній пошті, оплата покупки за низькою ціною або з великою знижкою, необхідність встановити новий додаток.

СХІД SOS

ОСВІТНІ посиденьки

Фішинг





СХІД SOS

ОСВІТНІ посиденьки

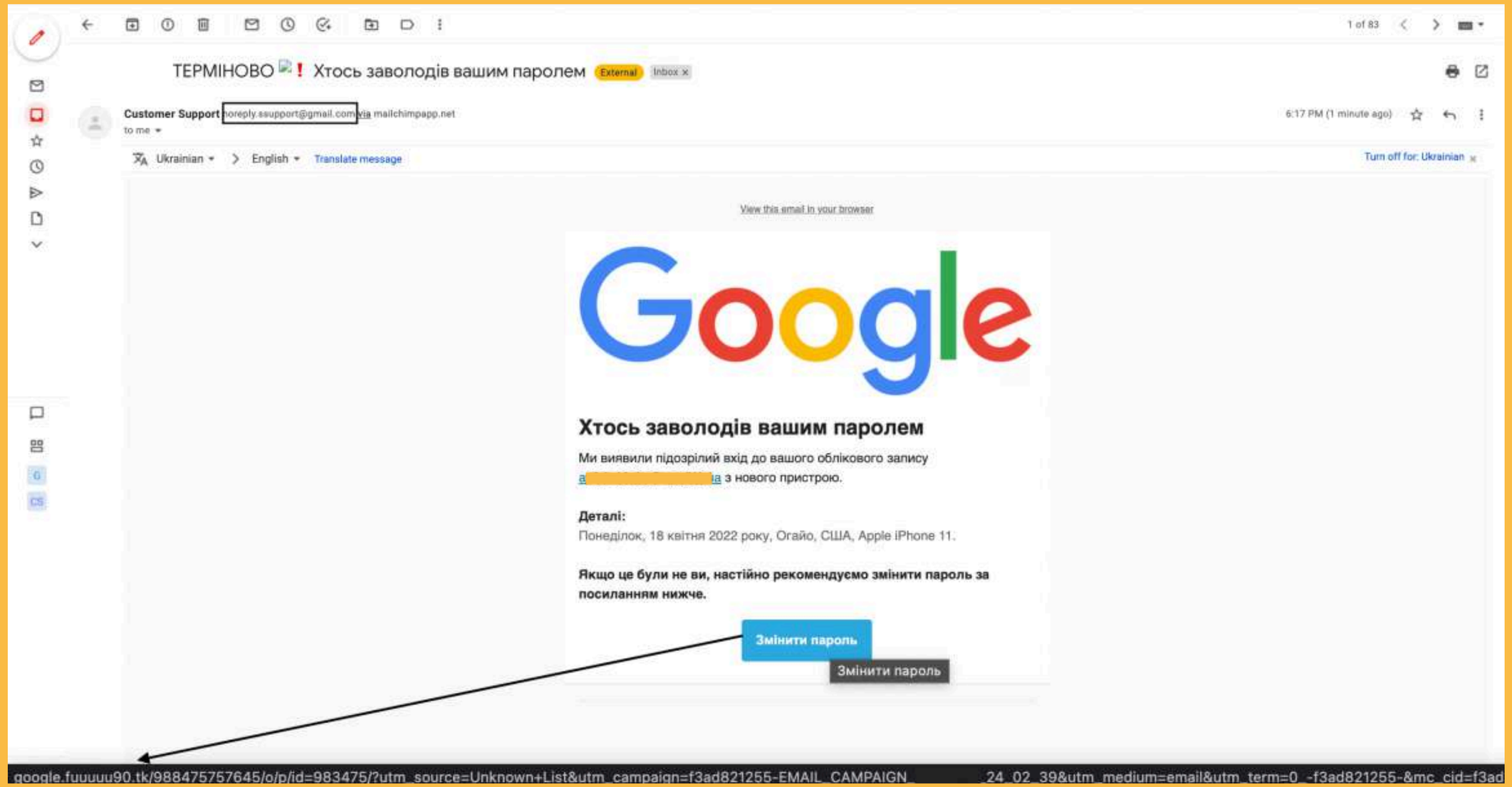
Найпоширеніші технології фішингу

- Розсилка підроблених електронних листів, з проханням підтвердити логін і пароль
- Переможці інтернет-аукціонів
- Фіктивні благодійні організації
- Створення фішингових інтернет-магазинів

СХІД SOS

ОСВІТНІ посиденьки

На що звернути увагу?



Фішинг

Голосова версія фішінгу називається вішинг.

Тут мова йде вже про телефонне шахрайство, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації. Він також може включати в себе змушення жертви перевести гроші на банківський рахунок зловмисника.

Як захиститися від фішингу

Нікому і ні за яких обставин не можна передавати конфіденційні дані

Звертайте увагу на адресний рядок на посиланні переходу

Остерігайтеся заходити на банківські вебакаунти через точки доступу громадського Wi-Fi

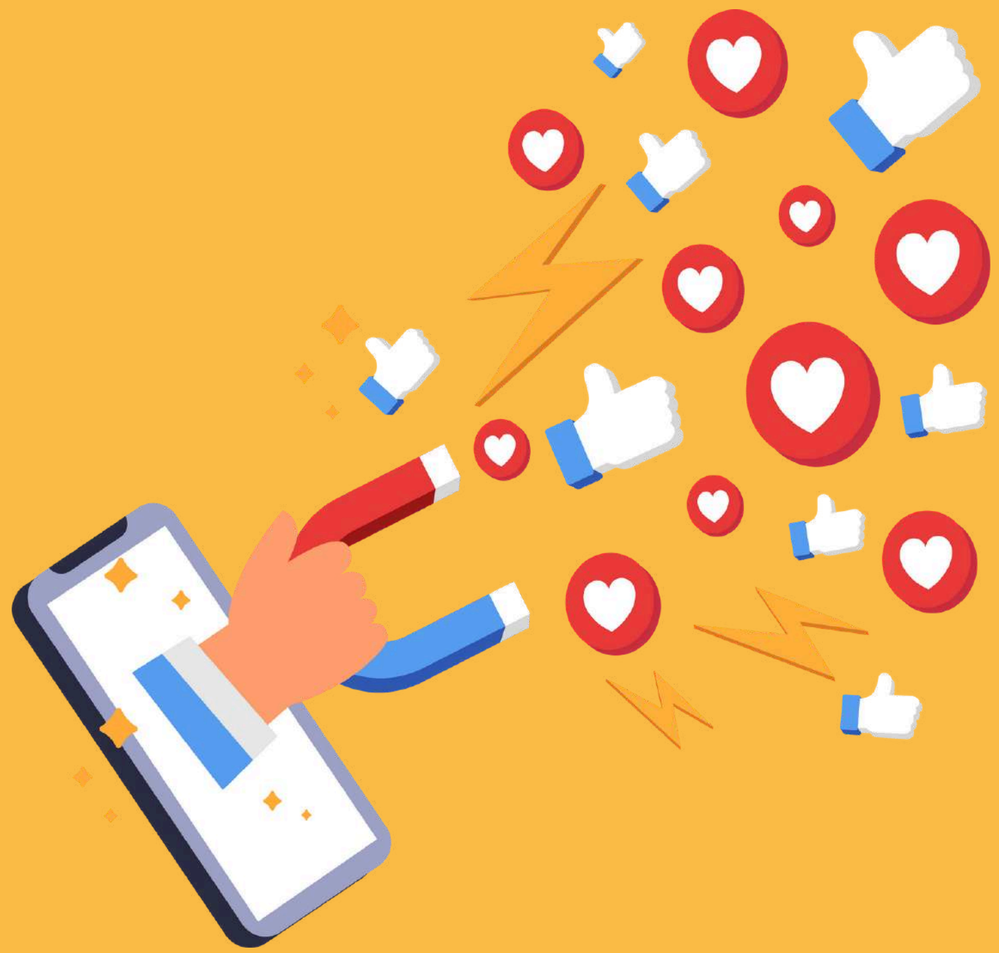
Встановіть хороший антивірус з останньої базою антивірусів

При відвідуванні банківських сайтів, стежте, щоб було встановлено захищене з'єднання HTTPS

Завжди звертайте увагу на дизайн сайту

Перевіряйте листи з невідомих адрес, які «тиснуть на емоції» або мають екстрений характер

Збір даних у соцмережах

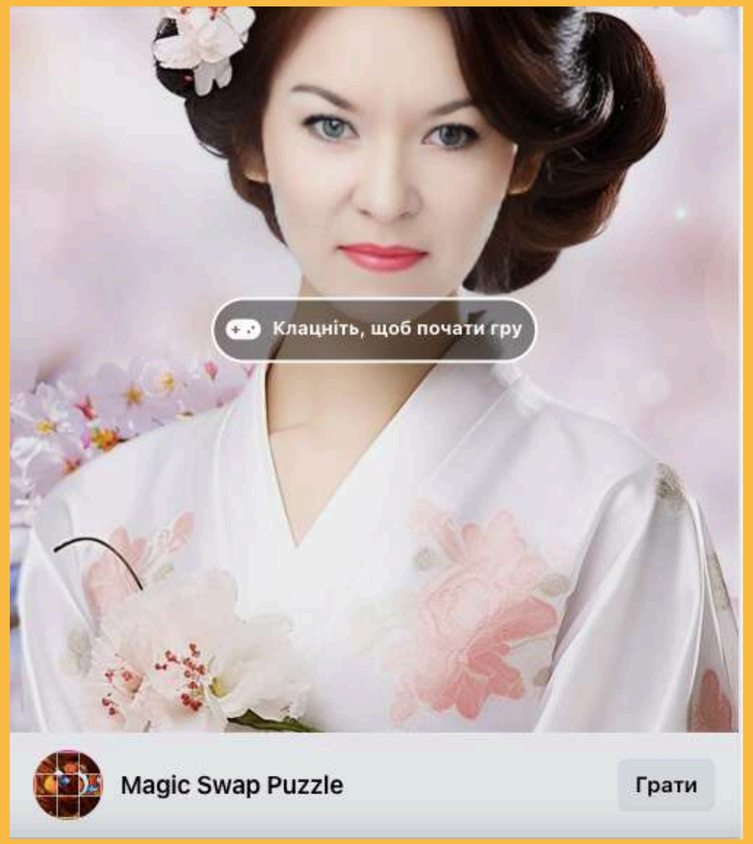


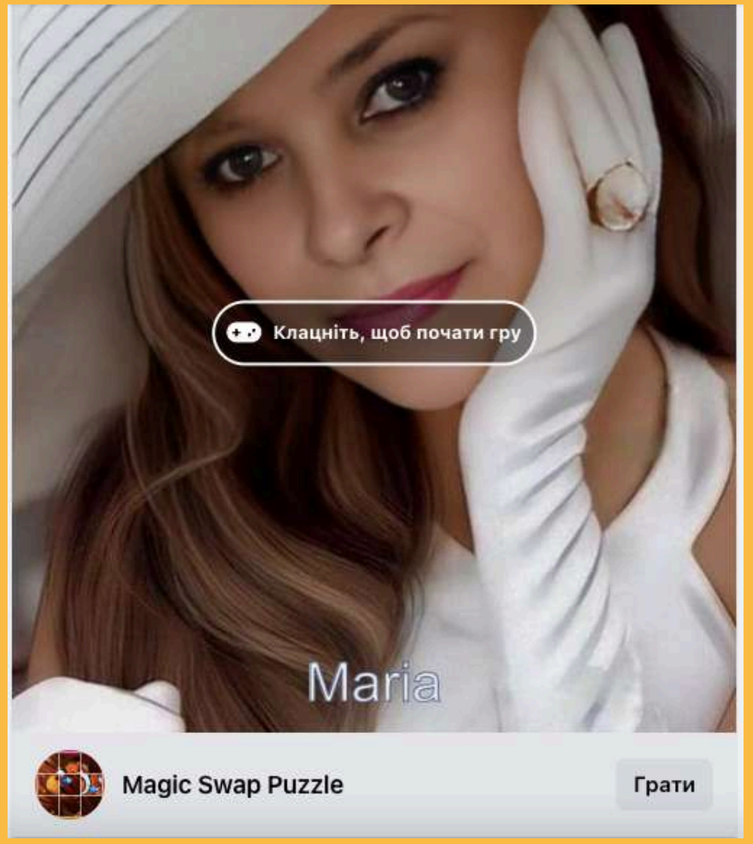
Як приймається рішення, яку рекламу вам показати?

Дані, які збираються

- ім'я
- вік
- місце користування
- інтереси
- фотографії
- взаємодії з іншими користувачами

Збір даних у соцмережах





СХІД SOS

ОСВІТНІ посиденьки

VPN

VPN — це віртуальна приватна мережа, яка дозволяє отримати доступ до Інтернету більш безпечно та конфіденційно, а також дає можливість обійти цензуру чи обмеження вмісту.

VPN працює шляхом створення зашифрованого з’єднання між вашим комп’ютером/пристроєм і сервером VPN.

ЧИТАТИ детальніше про VPN

Захист персональних даних: законодавча база

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

- Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 року
- Конституція України
- Закон України "Про захист персональних даних"
- Закон України "Про доступ до публічної інформації"
- Кодекс України про адміністративні правопорушення
- Наказ Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року № 1/02-14 "Про затвердження документів у сфері захисту персональних даних"
- Роз'яснення Міністерства юстиції України від 21 грудня 2011 року "Деякі питання практичного застосування Закону України "Про захист персональних даних""
- Роз'яснення Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року "Роз'яснення до Типового порядку обробки персональних даних"

Захист персональних даних: законодавча база

За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності (стаття 182 Кримінального кодексу України).

СХІД SOS

ОСВІТНІ посиденьки

Наступна зустріч відбудеться за анонсом в телеграм-каналі

“ОСВІТНІ ПОСИДЕНЬКИ ОДЕСА”