



Організація з безпеки та
співробітництва в Європі



**Міністерство
внутрішніх справ
України**

Безпека користування соціальними мережами

ЗМІСТ

Загальні правила безпеки
в соціальних мережах

Паролі та 2FA (MFA)

Налаштування правил
конфіденційності

ОБСЕ



Робота в групах

Група 1 – переваги використання соціальних мереж та месенджерів

Група 2 – ризики користування соціальними мережами та месенджерами

Група 3 – правила безпеки під час користування соціальними мережами та месенджерами





Ризик публікації особистої інформації в соціальних мережах

1. Мері відвідала весілля друзів декілька тижні тому назад. Невдовзі Мері отримує електронний лист із фотографіями з події, нібито від одного із гостей даного весілля...

2. Єва прибула у місце своєї відпустки. Раптом їй надходить електронний лист, начебто від авіакомпанії, якою вона летіла на відпочинок...



Ризик комунікації з незнайомими користувачами

Кетфішинг (з англ. *catfish* - сом, дослівно «Ловля сома», «риболовля на сома») - це вид шахрайства, коли людина створює вигаданий несправжній акаунт чи сторінку в соціальних мережах або на сайтах знайомств, зазвичай націлюючись на конкретну жертву з метою компрометації, отримання фінансової вигоди тощо.

Загальні правила безпеки в соціальних мережах

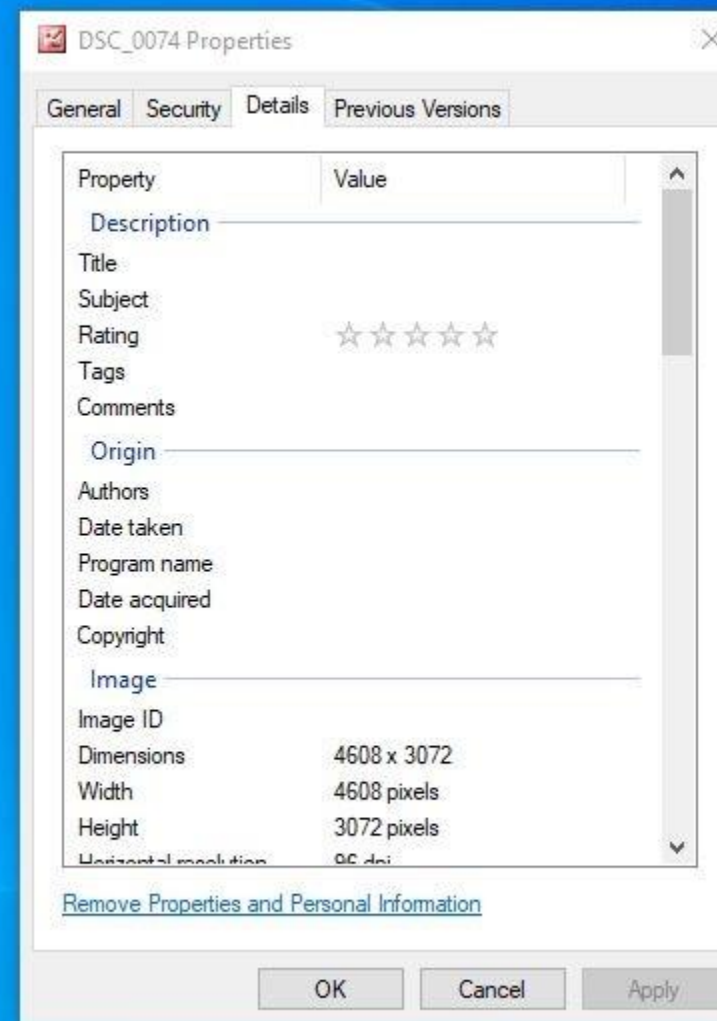
1. Налаштуйте 2FA
2. Складні та надійні паролі
3. Ретельно обирайте друзів і підписників
4. У разі необхідності надсилайте адміністрації скарги

5. Пам'ятайте, що моніторинг соціальних мереж є підготовчим етапом до успішної фішингової атаки і не тільки...
6. Для реєстрації використовуйте резервні е-пошти, номери телефонів (**не використовуйте корпоративні**).
7. Не використовуйте аккаунт соціальної мережі для реєстрації на інших сервісах.

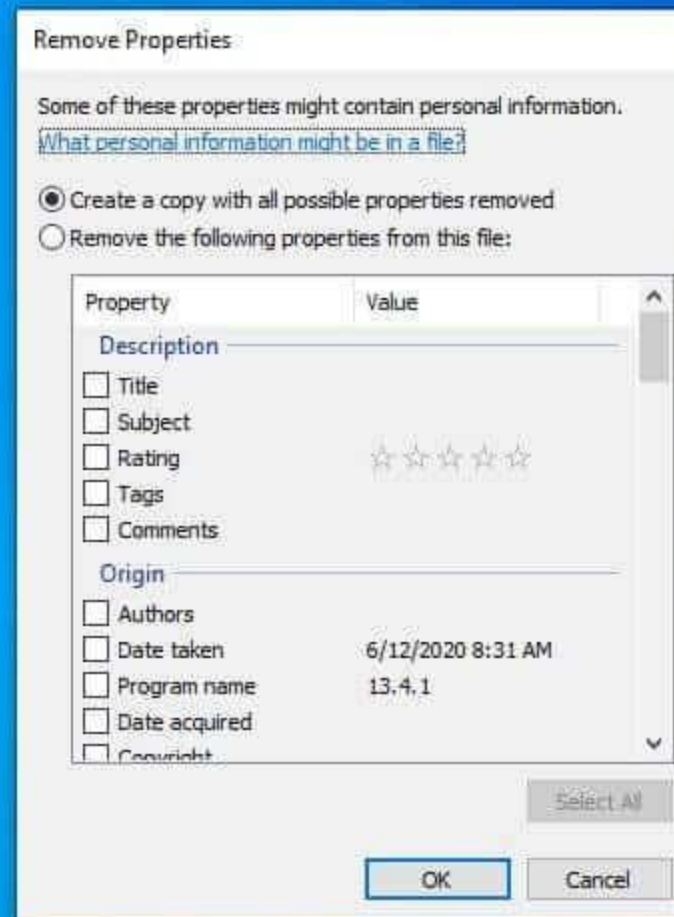
Контролюйте метадані файлів

Метадані - це дані про дані (про їх склад, зміст, статус, походження, місцезнаходження, якість, формати, обсяг, умови доступу, авторські права тощо). Щодня ми надсилаємо електронні повідомлення чи файли. У кожного такого послання є не тільки зміст, але й дата та час відправлення, вказівка відправника та одержувача, тип вкладення, його обсяг та інші характеристики.

1. Натиснути правою кнопкою миші по файлу і обрати “Властивості”, потім “Докладно”.
Виберіть пункт «Видалити властивості та особисту інформацію».



**2. Натиснути кнопку
Створити копію з усіма
можливими віддаленими
властивостями.
Вибираємо ОК та все.**





Паролі та 2FA (MFA)



- Пароль має бути складним та унікальним
- Не менше 12 символів
- Різні символи: великі та малі літери, цифри, спецсимволи
- Не «словниковий» пароль

1. <https://raw.githubusercontent.com/duyet/bruteforce-database/master/2151220-passwords.txt>

2. <https://haveibeenpwned.com/Passwords>

3. Google it

4. Вбудовані сервіси з перевірки витоків паролів

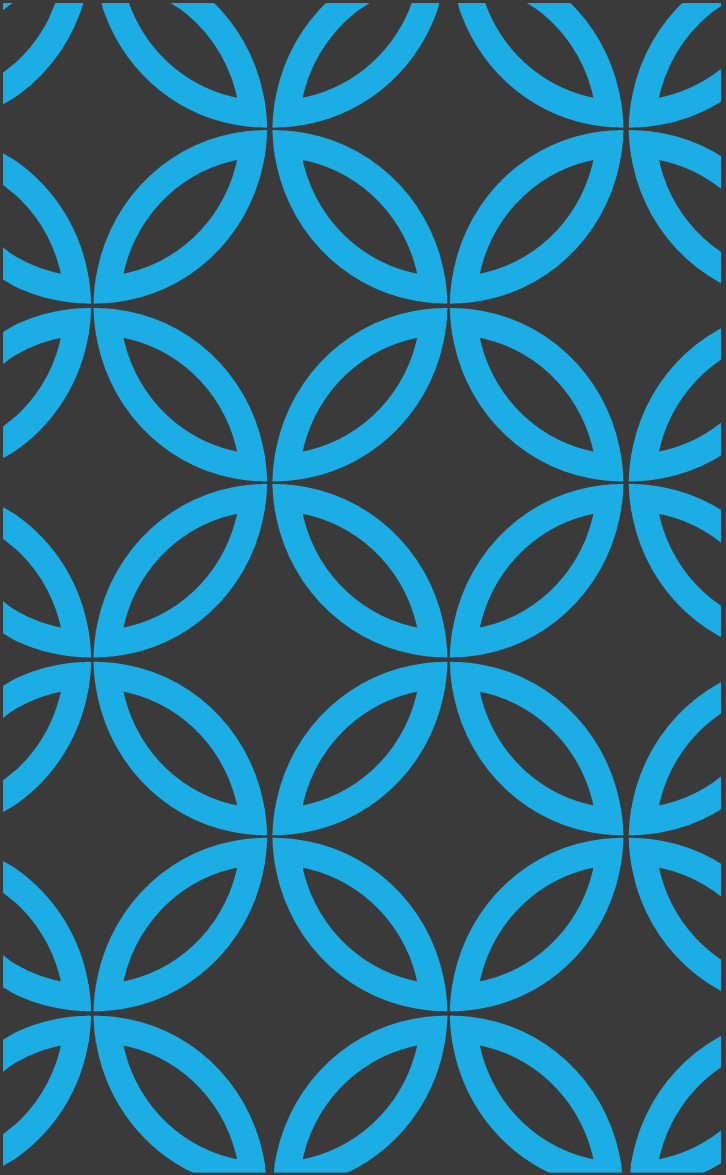
- Періодично змінювати паролі
- Парольна фраза (легко запам'ятати)

одна ручка та дві книжки

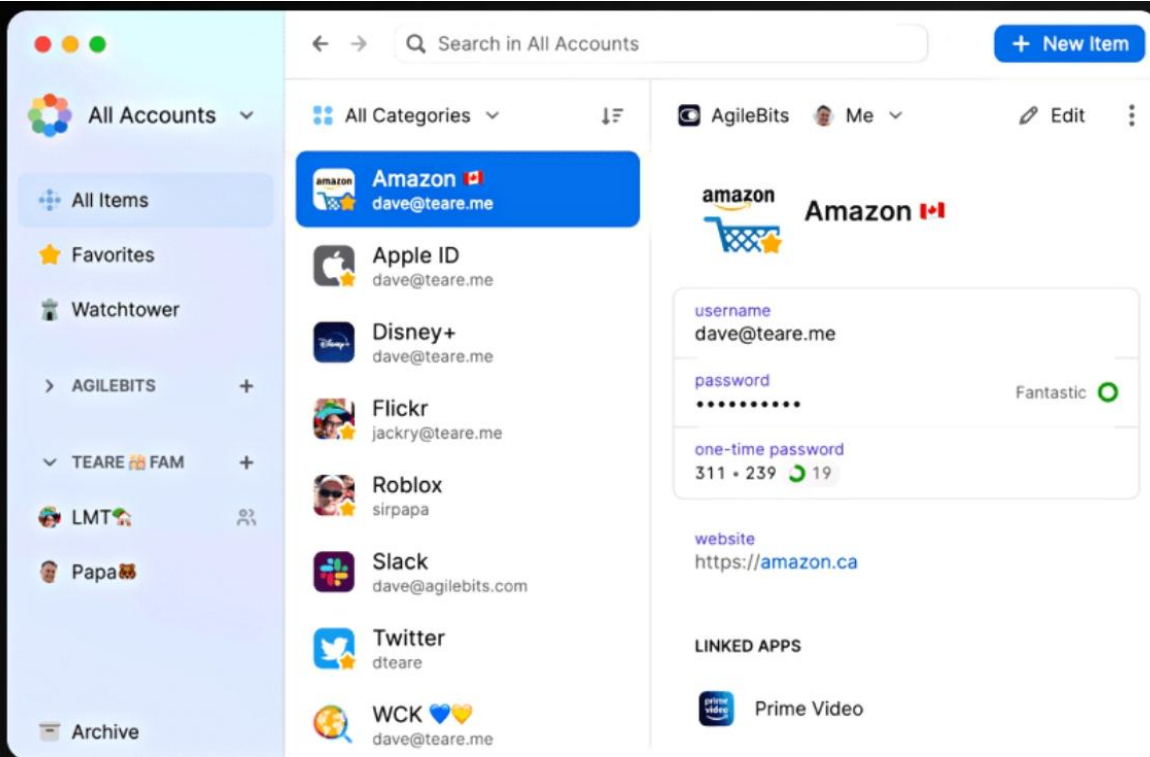
1. Перетворити на парольну фразу

2.

1Ru4ka@2kn!_!>|<k!_!



МЕНЕДЖЕРИ ПАРОЛІВ



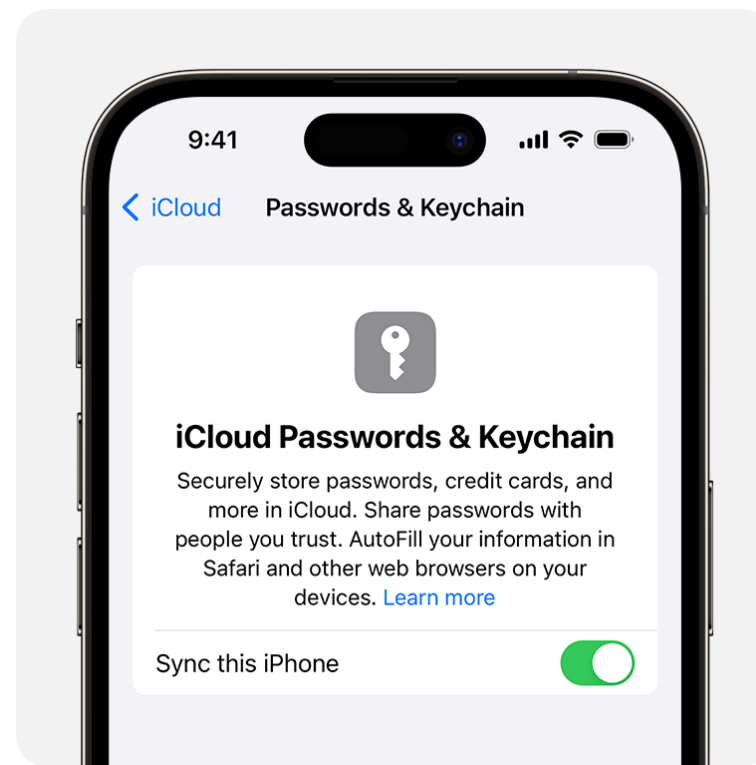
Джерело: 1Password

Якщо ви використовуєте менеджер паролів, всі ваші паролі безпечно зберігаються в одному місці і вам не потрібно запам'ятовувати декілька складних паролів. Вам лише потрібен один головний пароль, аби увійти в менеджер паролів.

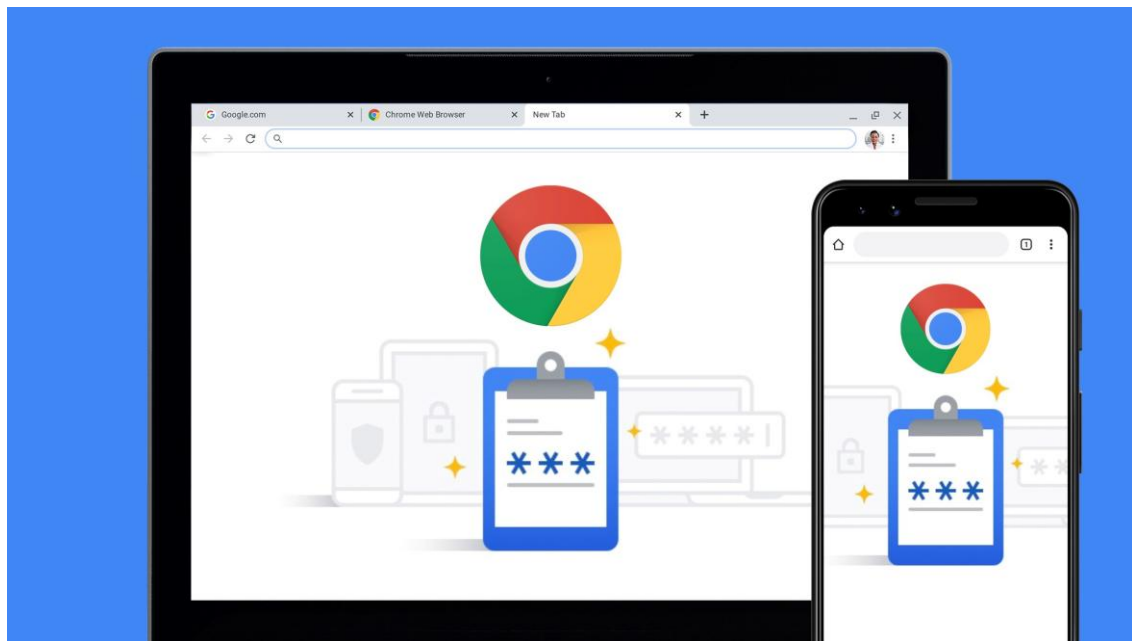


LastPass...

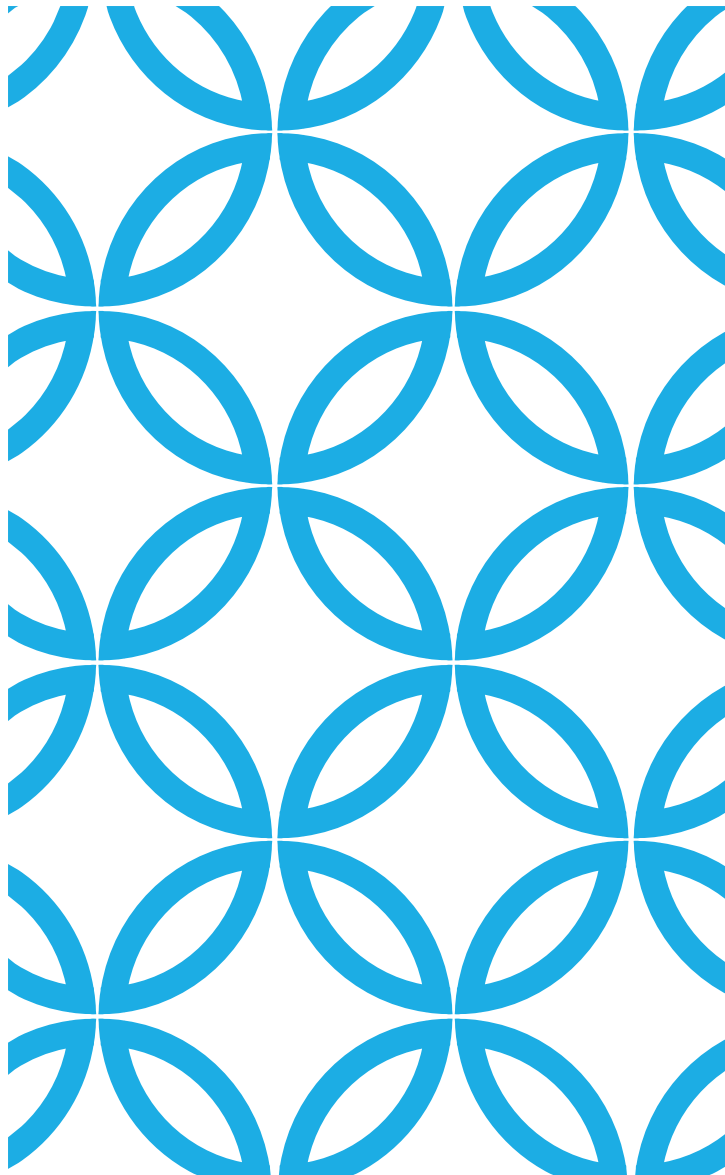




ЗБЕРІГАННЯ ПАРОЛІВ НА МОБІЛЬНИХ ПРИСТРОЯХ



ЗБЕРІГАННЯ ПАРОЛІВ У
БРАУЗЕРАХ?



ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ



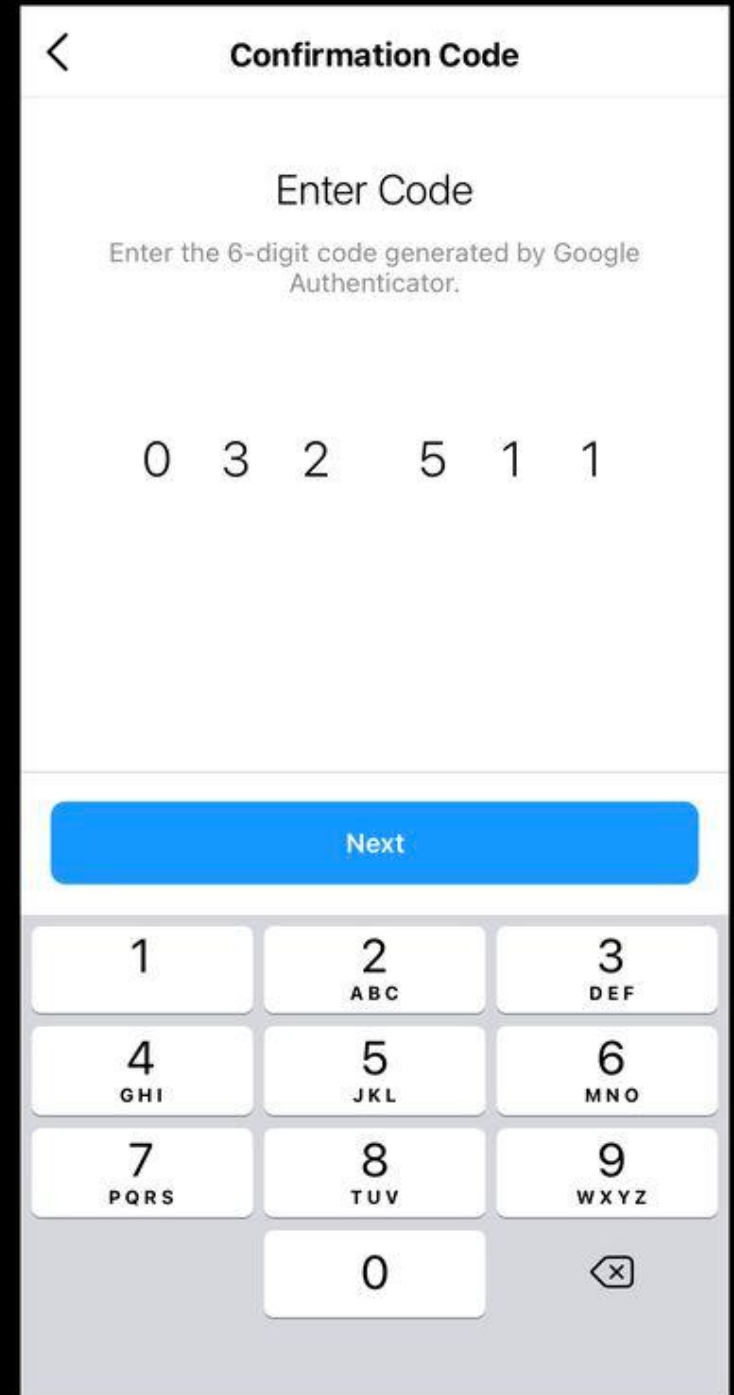
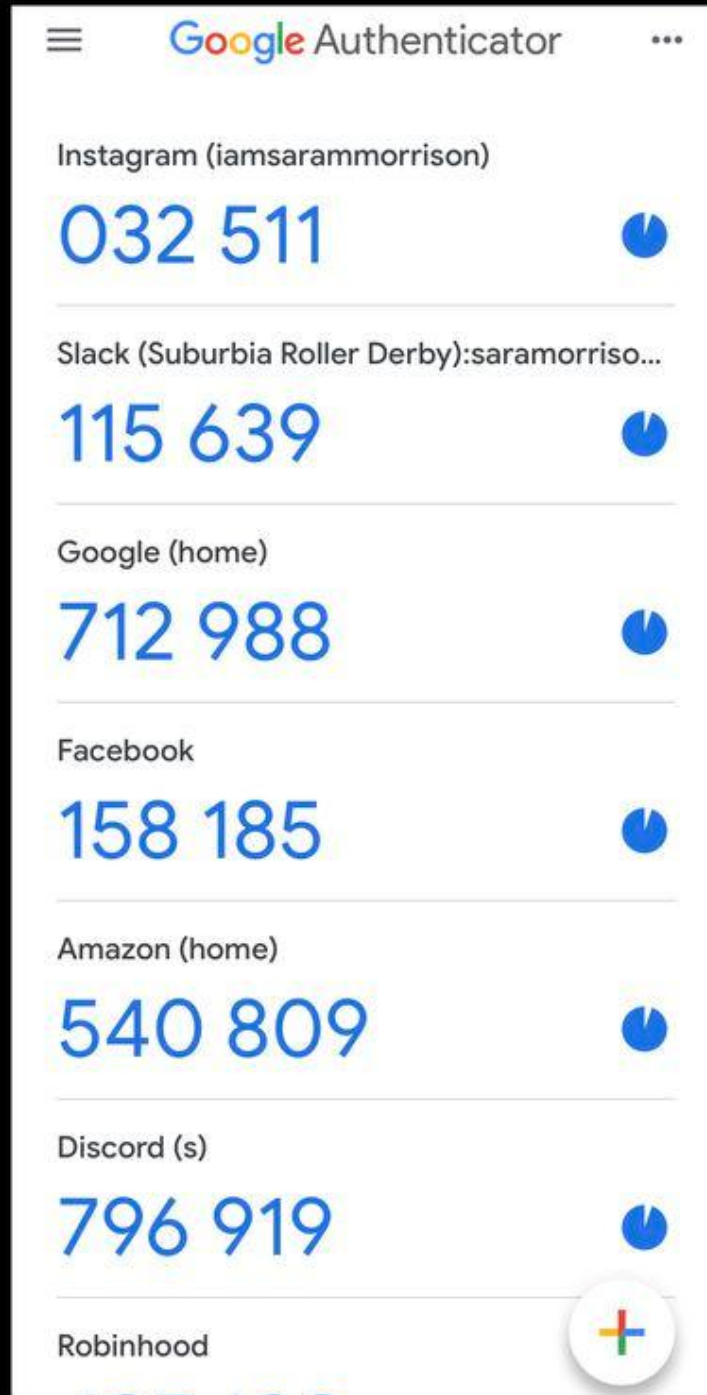
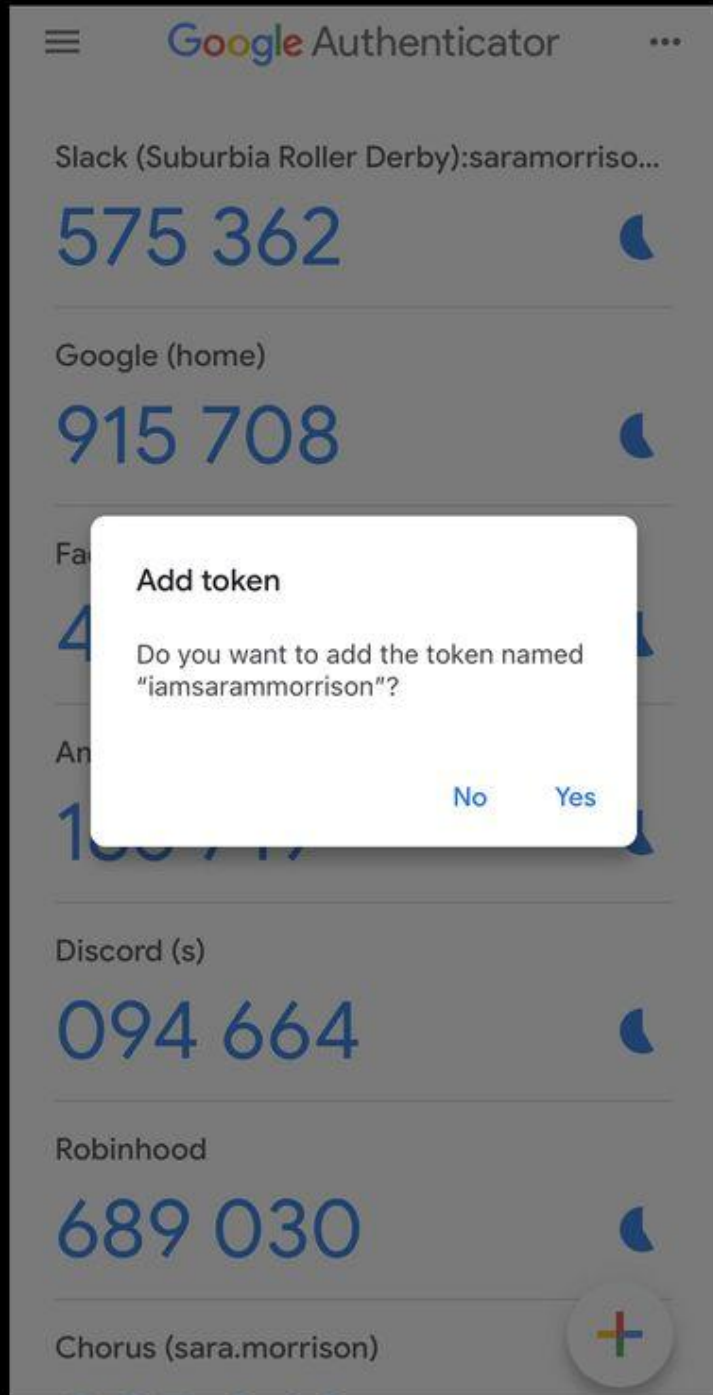
***Використання автентифікації
через SMS не рекомендовано***



Microsoft Authenticator



GOOGLE AUTHENTICATOR



Резервні коди

Резервні коди можна використовувати, коли телефон недоступний. Резервні коди нижче можна використовувати для підтвердження входу лише один раз. Якщо ви використали всі резервні коди, ви можете згенерувати новий набір.

Збережіть ці коди та зберігайте їх десь у безпеці

xvnwra5h

6eg5idaj

4w3kg6bh

qdl76jhg

d5knwdm

uoskbx

dr5q

k2d

039442

ВСТАВИТИ

Скасувати

Згенерувати

ПІСЛЯ
УВІМКНЕННЯ
ДВОФАКТОРНОЇ
АВТЕНТИФІКАЦІЇ
ОБОВ'ЯЗКОВО
ЗБЕРЕГТИ
РЕЗЕРВНІ КОДИ

AUTHY



Authy | Two-factor Authentication | X +

https://authy.com

Authy

APP FEATURES ▾ 2FA GUIDES HELP BLOG DEVELOPERS ▾ DOWNLOAD

Enable 2FA for your favorite sites.

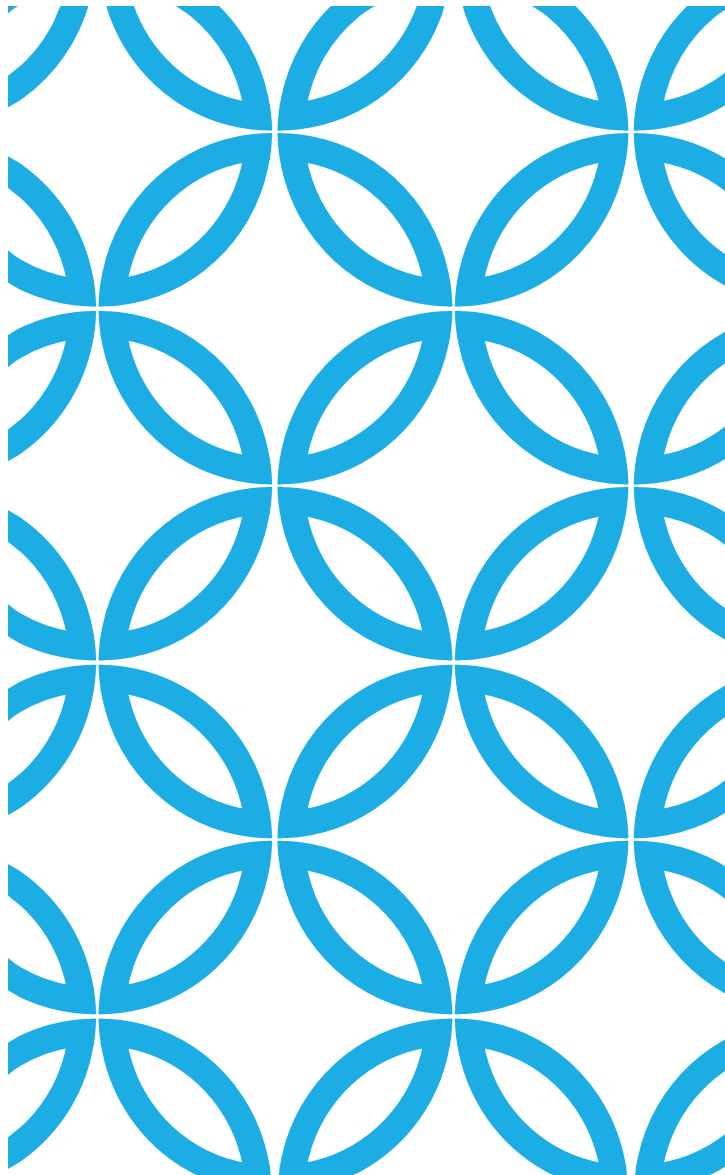
Go beyond the password and protect yourself from hackers and account takeovers. Download our free app and follow our guides:

Search for 2FA guides...

IDENTITY MANAGEMENT	TASK MANAGEMENT	COMMUNICATION	CRYPTOCURRENCIES	RETAIL
 RoboForm Password Manager	 Grammarly	 Fastmail	 Bittrex	 Arduino
VIEW GUIDE	VIEW GUIDE	VIEW GUIDE	VIEW GUIDE	VIEW GUIDE

VIEW ALL 2FA GUIDES LEARN ABOUT 2FA

Powered by Twilio

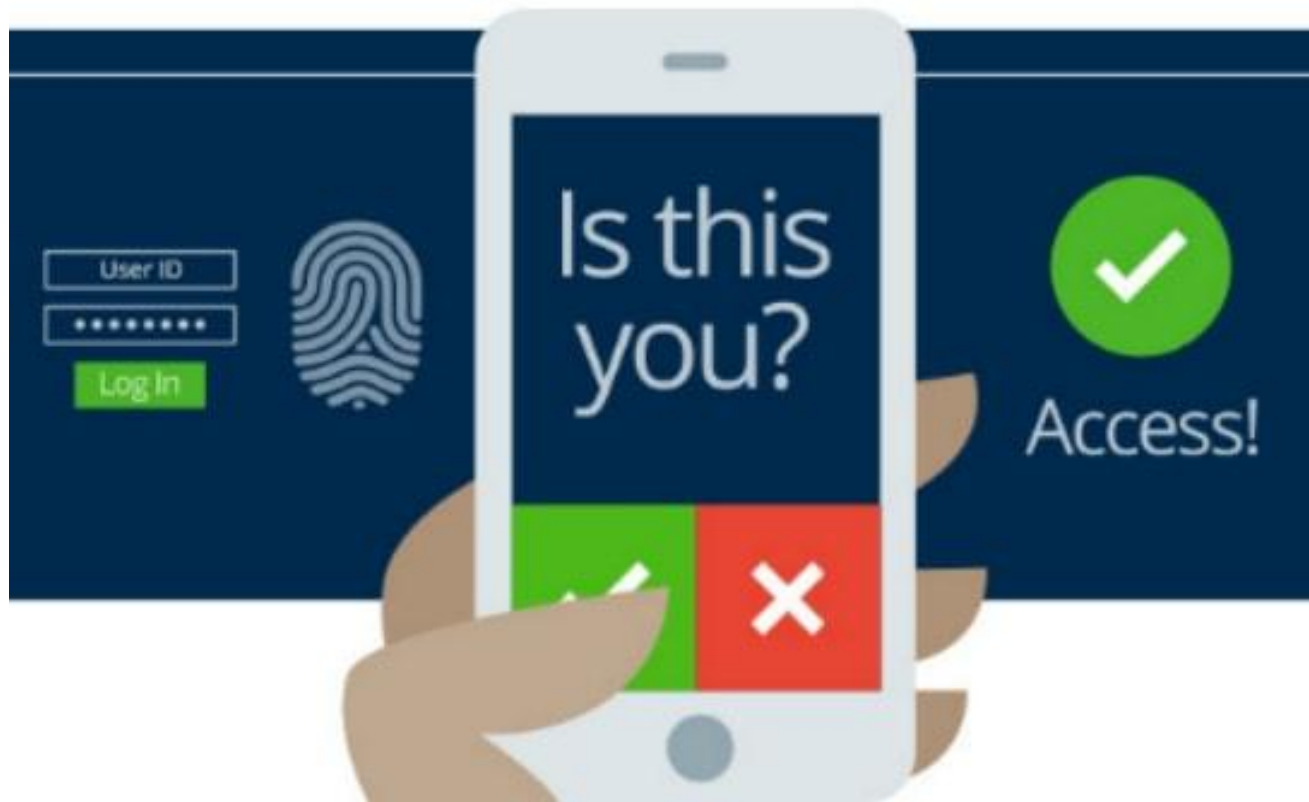


АПАРАТНІ ПРИСТРОЇ АВТЕНТИФІКАЦІЇ



YubiKey vs.
smartphone

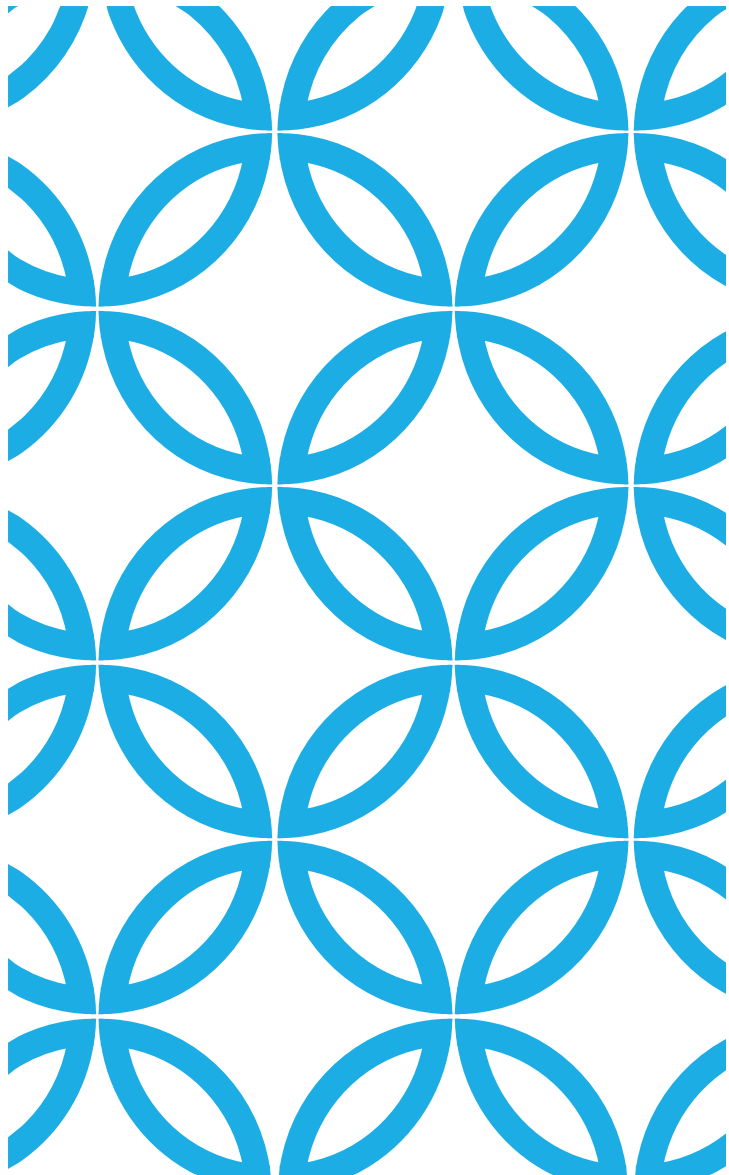




Двофакторна автентифікація (2FA)

*Вправа.
Увімкнення двофакторної
автентифікації*

<https://2fa.directory/int>

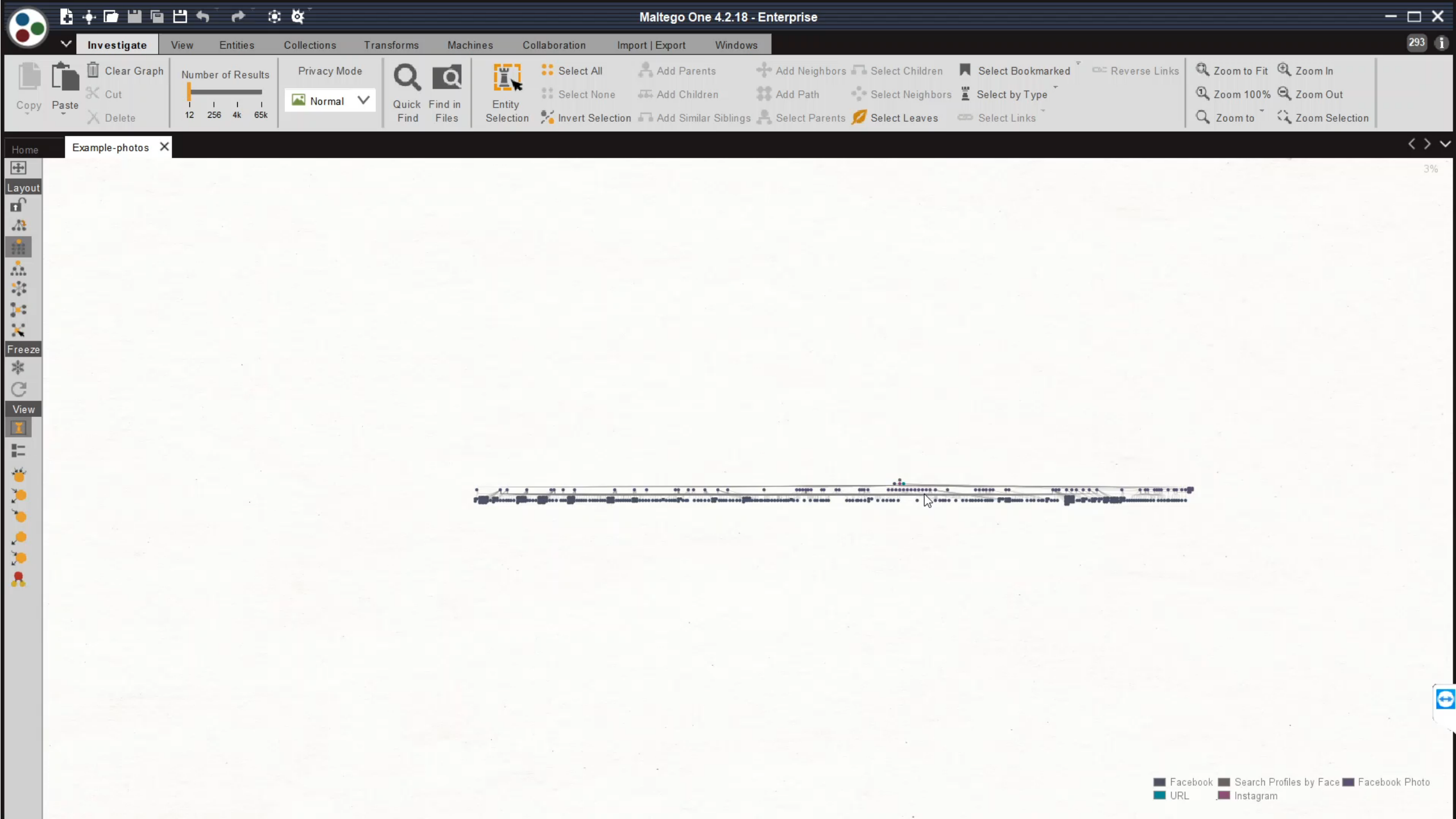


НАЛАШТУВАННЯ ПРАВИЛ КОНФІДЕНЦІЙНОСТІ

The Facebook logo, consisting of the word "facebook" in a bold, blue, sans-serif font. A thin blue vertical line is positioned to the left of the letter 'f'.

facebook

<https://www.facebook.com/settings?tab=security§ion=approvals>





Організація з безпеки та
співробітництва в Європі



**Міністерство
внутрішніх справ
України**

Дякую за увагу!

