

Модуль: Безпека користування соціальними мережами



Практична вправа:

«Двофакторна автентифікація облікового запису Facebook. Метадані фотозображень»



Навчальна мета заняття: навчитись налаштовувати двофакторну автентифікацію облікового запису Facebook та контролювати метадані фотозображень.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

Порядок проведення заняття

Двофакторна автентифікація облікового запису Facebook.

Створити, якщо немає, обліковий запис у соціальній мережі Facebook. Встановити для облікового запису Facebook двофакторну автентифікацію через Google Authenticator.

В обліковому записі перейти в «Налаштування та конфіденційність» – «Налаштування» – «Пароль і безпека» (рис. 1) – «Двохетапна перевірка» – «Використання двохетапної перевірки» – «Використовувати додаток для автентифікації» (рис. 2).

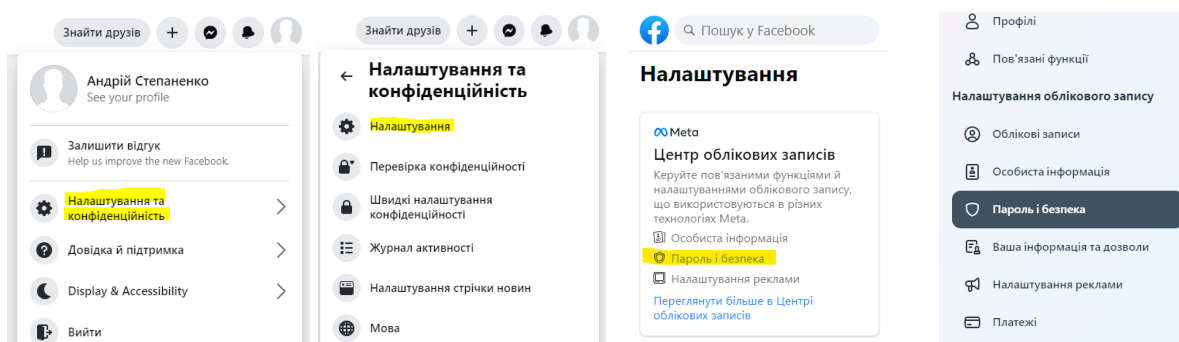


Рис. 1. Шлях до налаштувань «Пароль і безпека»

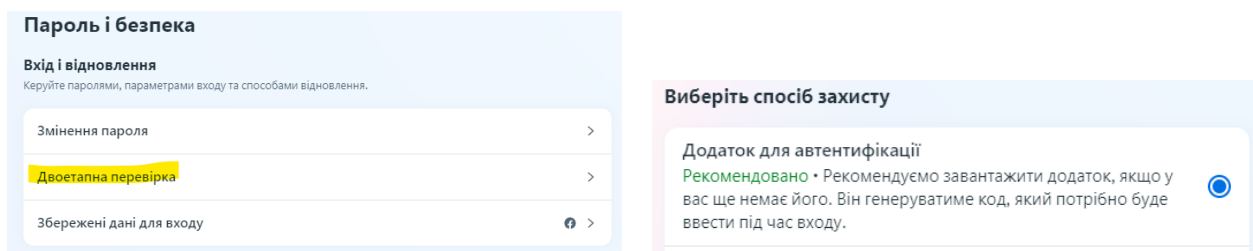


Рис. 2. Шлях до налаштування додатка автентифікації

Переконайтеся, що у власному смартфоні встановлений Google Authenticator (встановлюється з Google Play або App Store), увійти до «Використовувати додаток для автентифікації», зчитати додатком смартфона Google Authenticator QR-код та ввести код підтвердження (рис. 3).

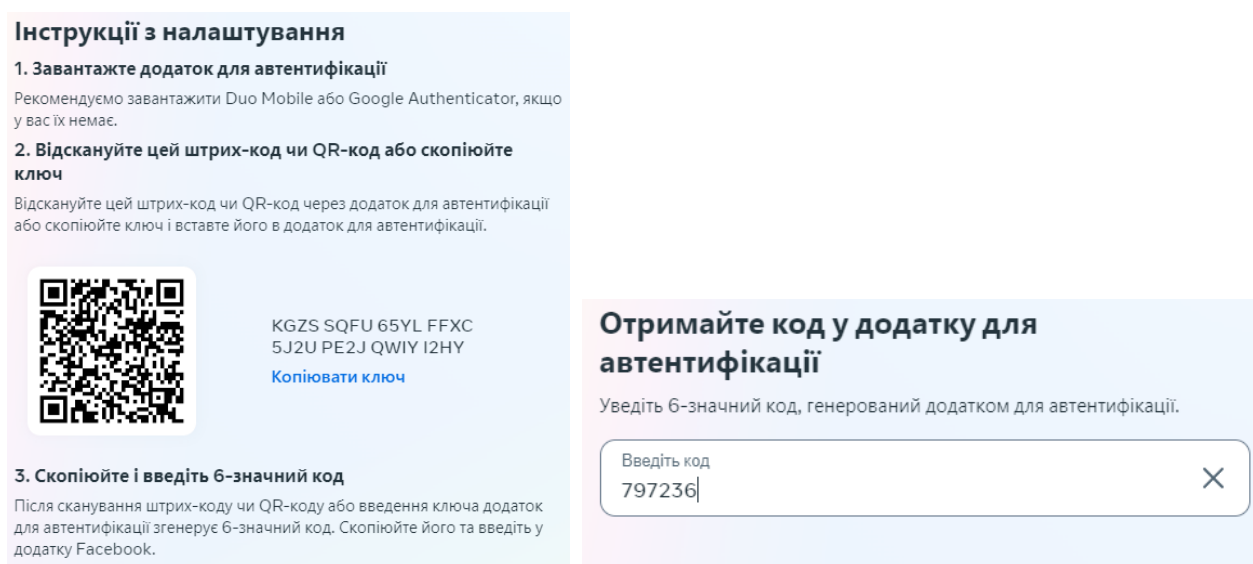
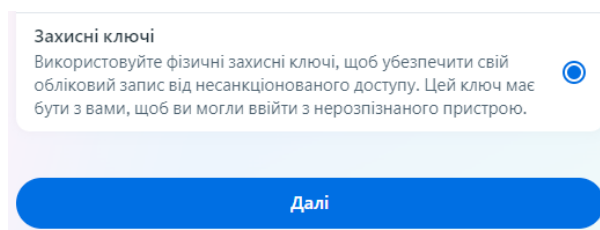


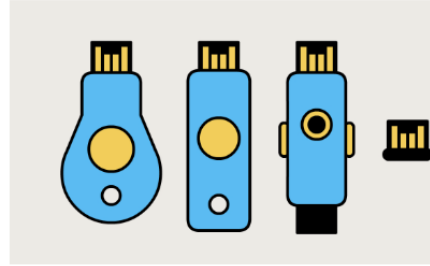
Рис. 3. Налаштування двохетапної перевірки

Після налаштування двохетапної перевірки повернутися у розділ «Використання двохетапної перевірки» – «Захисні ключі» – «Зареєструвати захисний ключ» (рис. 4) – Security key setup (Встановлення ключа безпеки) – Insert your security key into the USB port (Вставити ваш ключ безпеки в USB порт) – Скасувати (Cancel) (рис. 5). Далі обрати свій пристрій з ключами безпеки, який використовувався для автентифікації в акаунті Google і додатково ввести свій пароль (рис. 6).



Налаштуйте захисний ключ

Перш ніж використовувати захисний ключ для входу у Facebook, необхідно його зареєструвати. Переконайтеся, що захисний ключ під рукою.



Зареєструвати захисний ключ

Рис. 4. Налаштування автентифікації через захисні ключі

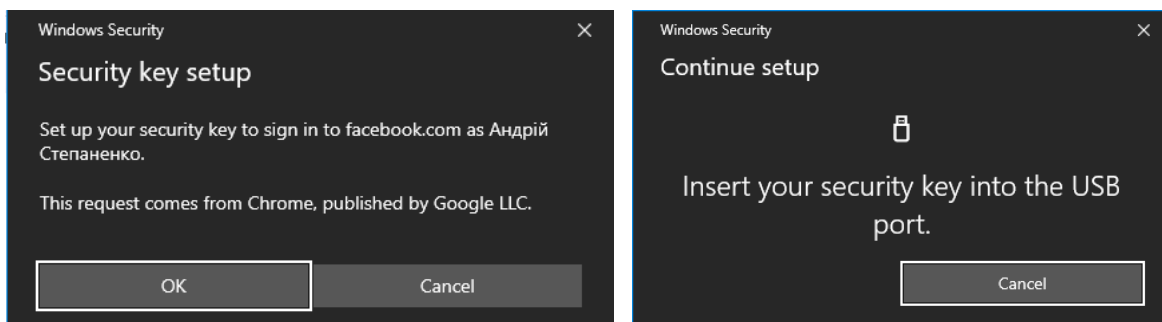


Рис. 5. Продовження налаштування автентифікації через захисні ключі

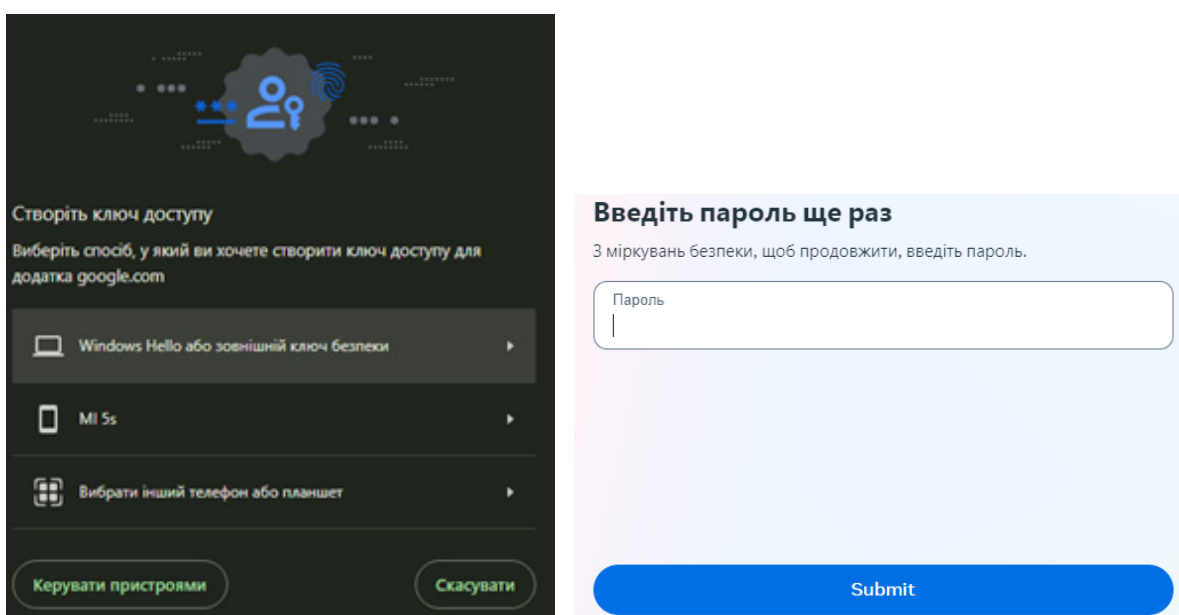


Рис. 6. Вибір свого пристрою з ключами безпеки

Повернутись у розділ «Пароль і безпека» і переглянути проблеми з безпекою, виконавши перевірку додатків, пристроїв і надісланих електронних листів (рис. 7).

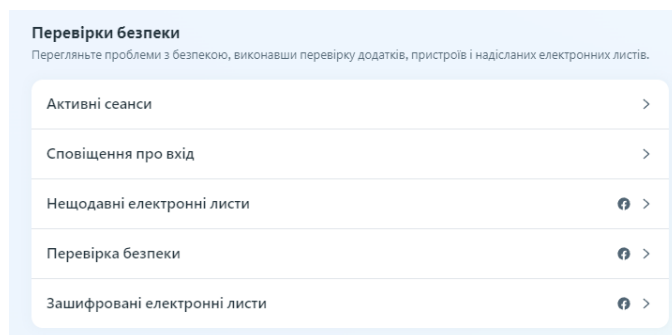


Рис. 7. Перевірка безпеки облікового запису

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двохетапної автентифікації та пристрою з ключами.

Метадані фотозображень.

В особистому смартфоні включити GPS, підійти до вікна у приміщенні й дочекатися встановлення координат свого місцезнаходження, перевіривши цей факт запуском додатку «Карти», де відобразиться точне місцезнаходження смартфона.

Зробити кілька фотознімків фотокамерою смартфона, підключити смартфон до комп'ютера та завантажити фотозображення на комп'ютер. Або скопіювати на комп'ютер підготовлені файли фотозображень з метаданими. Перевірити наявність метаданих у файлах фотозображень та видалити їх.

Завантажити, встановити і запустити утиліту перегляду та редагування метаданих «AnalogExif» (<https://sourceforge.net/projects/analogexif>). Відкрити у AnalogExif фотозображення, переглянути метадані, двічі клацнути на поле Location та скопіювати у буфер координати (рис. 8).

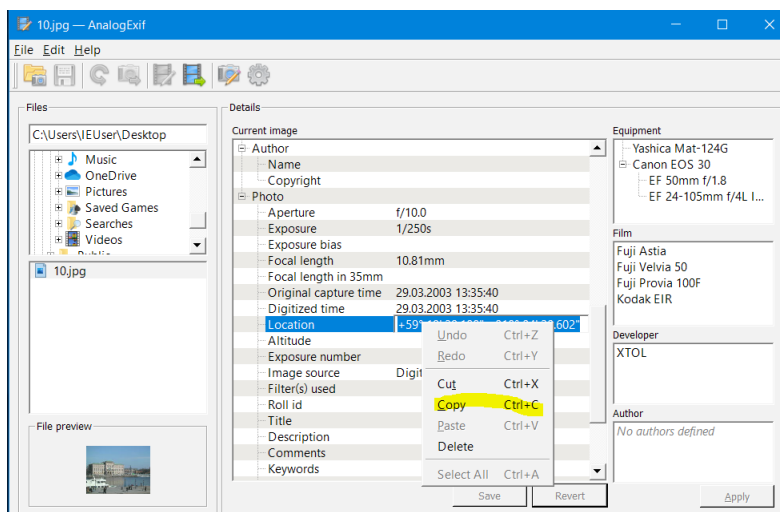


Рис. 8. Перегляд метаданих фотозображення

Відкрити веб-браузер Google Chrome, вставити координати в адресний рядок і здійснити пошук місця фотозйомки (рис. 9).

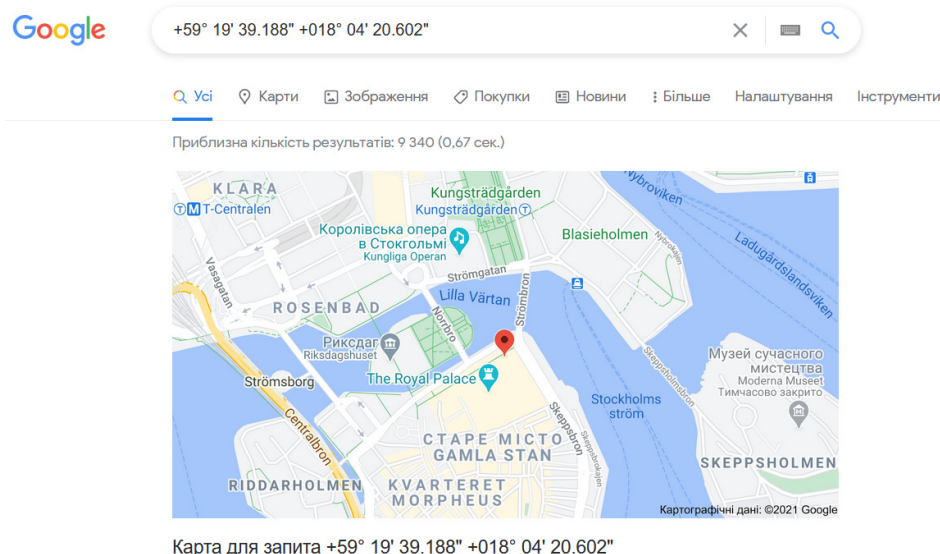


Рис. 9. Пошук місця фотозйомки за координатами з метаданих фотозображення

У Провіднику файлів через контекстне меню (клацнути правою кнопкою миші) подивитися «Властивості файлу фотозображення», перейти у вкладку «Докладно» та клацнути на «Видалити властивості та особисті відомості» – «Вибрати всі» – «ОК» (рис. 10).

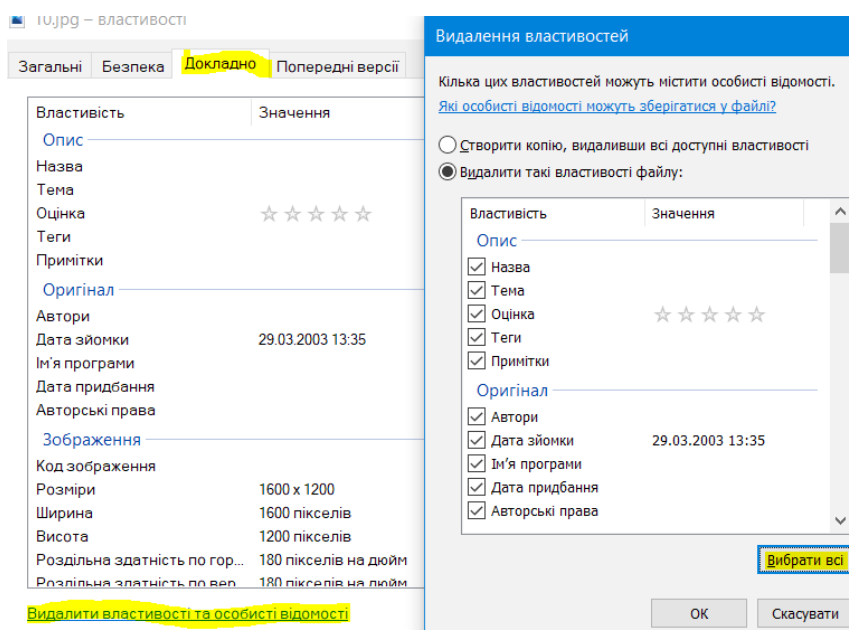


Рис. 10. Видалення метаданих фотозображень

Знову відкрити у AnalogExif фотозображення та переконатися, що метадані відсутні та можна їх безпечно завантажувати у соціальні мережі.