майстерня політик

DOVIDKA.INFO

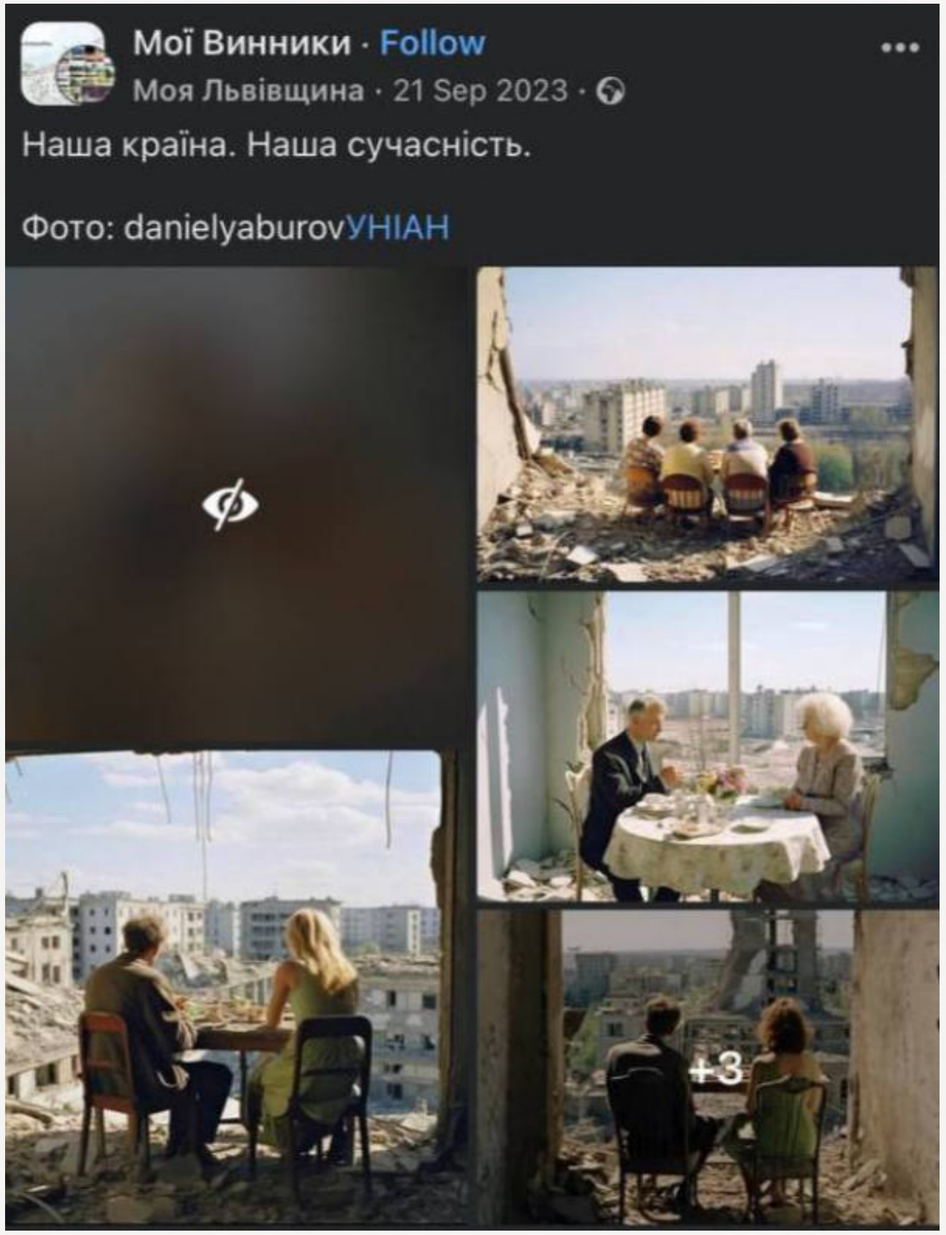
11 КЛАС. ТРЕНІНГ № 7

ІНФОРМАЦІЙНА ВІЙНА

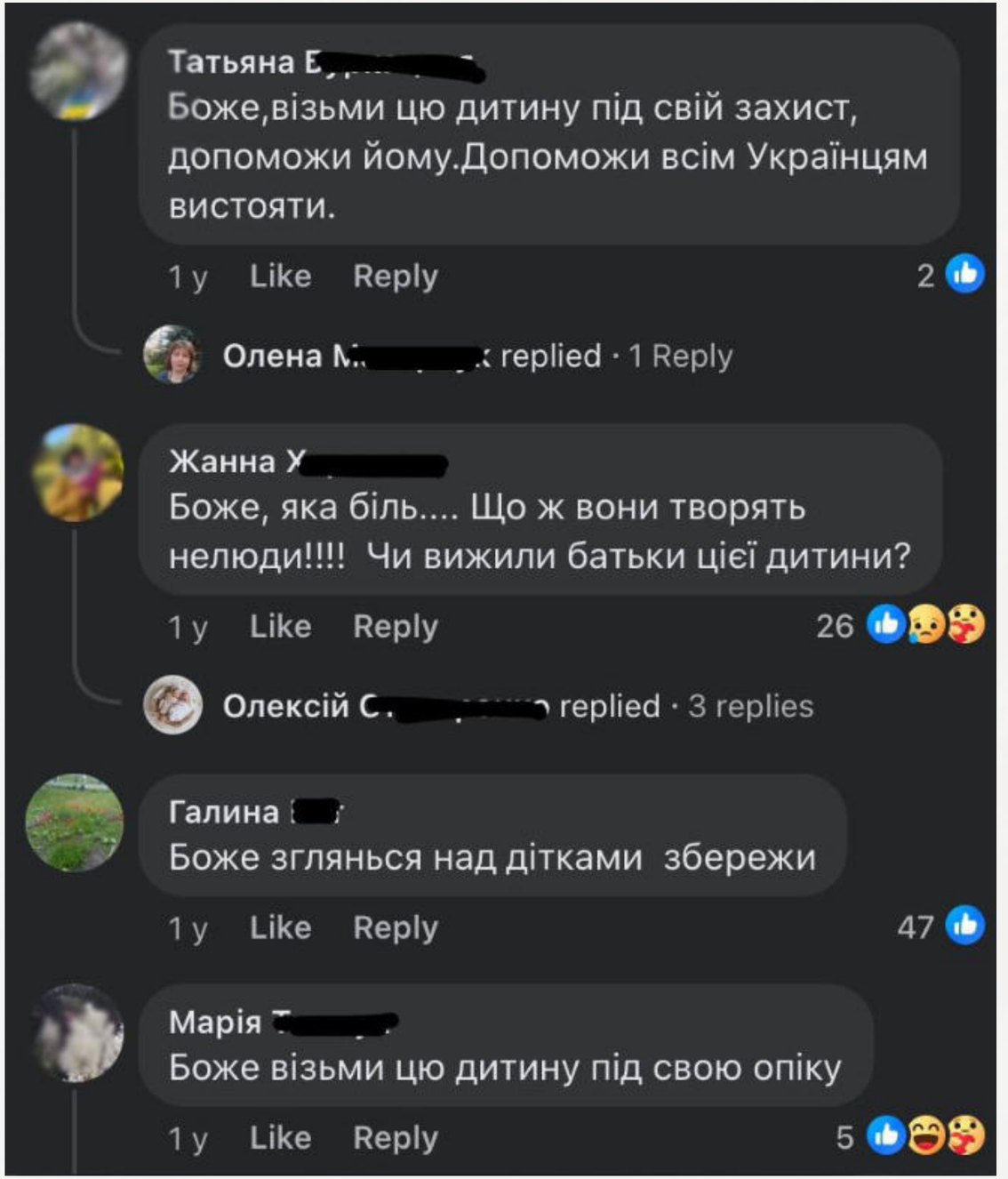
Урок 1

Роль штучного інтелекту в інформаційній війні

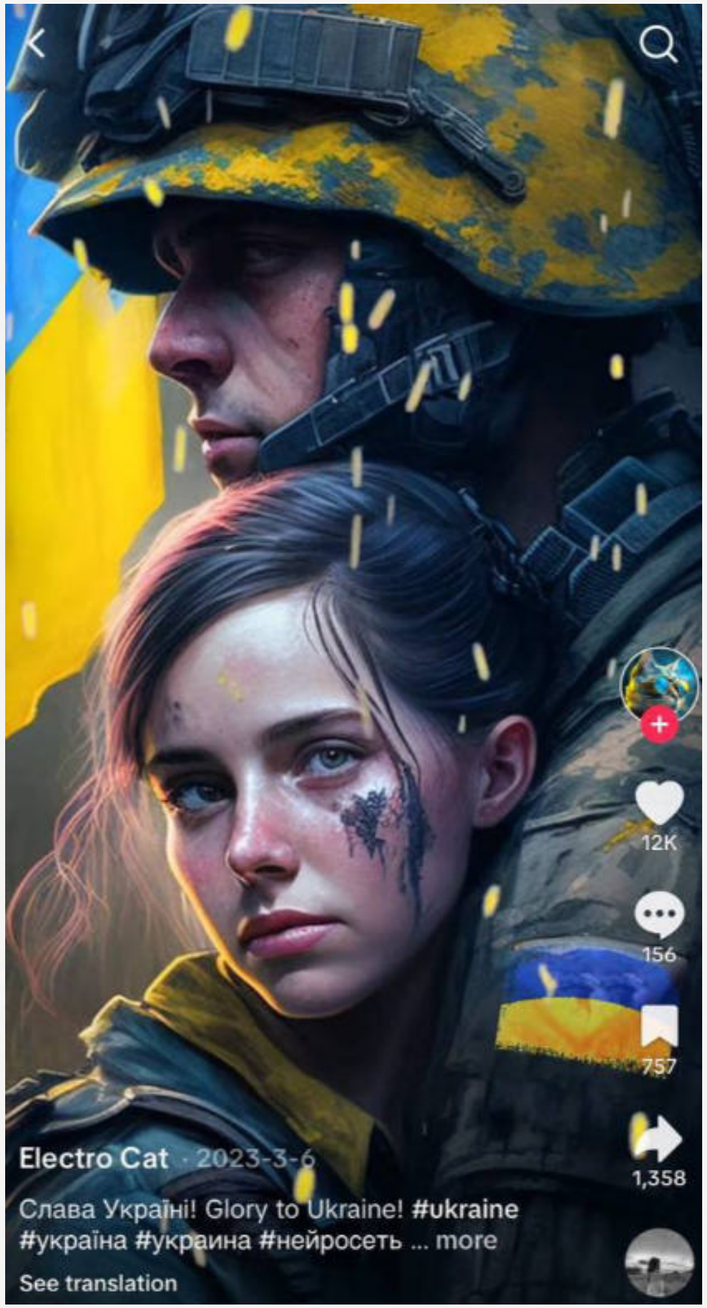
Джерело зображення: [*Рубрика*]



Джерело зображення: [Рубрика]



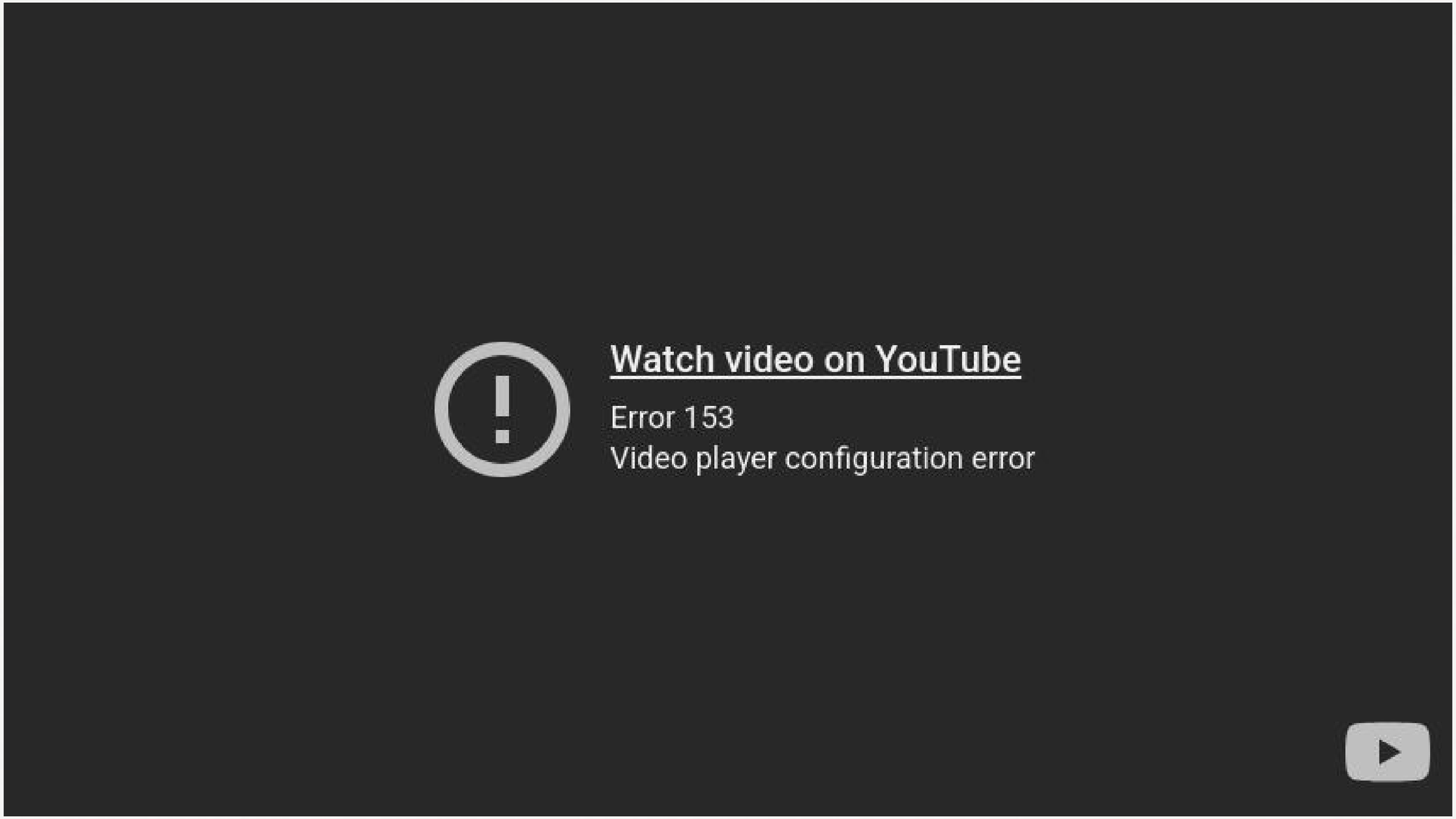
Джерело зображення: [Рубрика]



Джерело зображення: [Рубрика]

ЧИ ЧУЛИ ВИ ПРО ВІДЕО ЧИ АУДІО,
ЯКІ ВИЯВИЛИСЯ НЕ ТИМ, ЧИМ ЗДАВАЛИСЯ?

ШТУЧНИЙ ІНТЕЛЕКТ - ЦЕ АЛГОРИТМИ, ЯКІ МОЖУТЬ ОБРОБЛЯТИ ВЕЛИЧЕЗНІ ОБСЯГИ ДАНИХ, ГЕНЕРУВАТИ ТЕКСТ, ЗОБРАЖЕННЯ, ВІДЕО ТОЩО.


Watch video on YouTube
Error 153
Video player configuration error

10:17-17:42

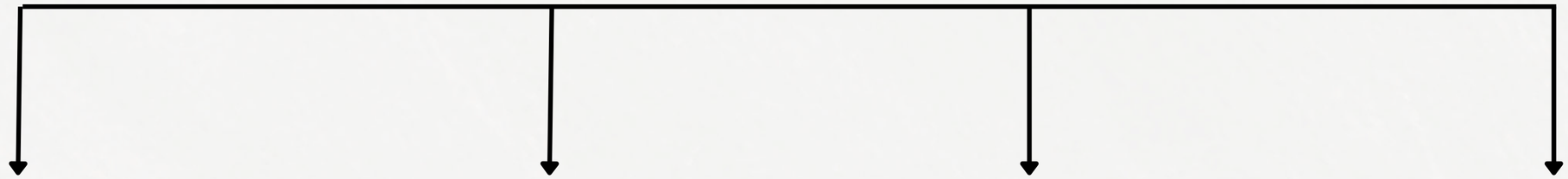
КРИТЕРІЇ ДЛЯ ГРУПОВОЇ РОБОТИ

1. Джерело
2. Якість зображення
3. Голос
4. Анотації
5. Підписи
6. Метадані
7. Інше

РИЗИКИ ВІД КОНТЕНТУ, ГЕНЕРОВАНОГО ШІ

1. Зниження довіри
2. Маніпуляція настроями
3. Втручання в особисте життя
4. Спотворення фактів

ЗАСОБИ ЗАХИСТУ ВІД КОНТЕНТУ, ГЕНЕРОВАНОГО ШІ



Медіаграмотність

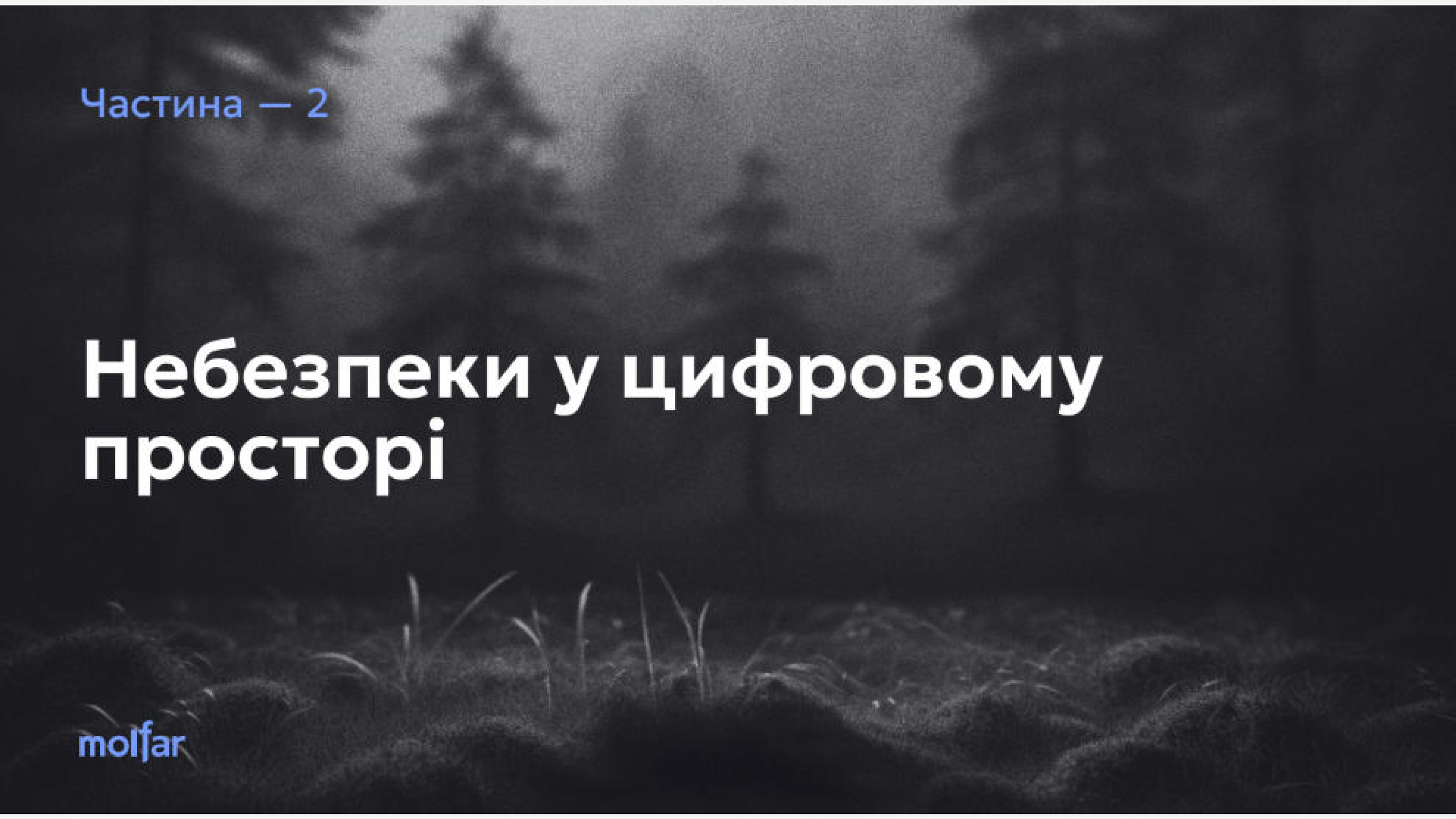
Перевірка джерел

Скепсис щодо емоційного контенту

Використання фактчекінгових ресурсів

Урок 2	Кібербезпека в умовах інформаційної війни

Джерело блоку презентації про кібербезпеку:
OSINT-агенція Molfar


Частина — 2
Небезпеки у цифровому просторі
molfar

Що таке кібербезпека і для чого вона потрібна?

Це сукупність методів захисту персональної та іншої чутливої інформації в Інтернеті.

До кібербезпеки можна віднести протидію хакерським атакам або отриманню персональних даних зловмисниками

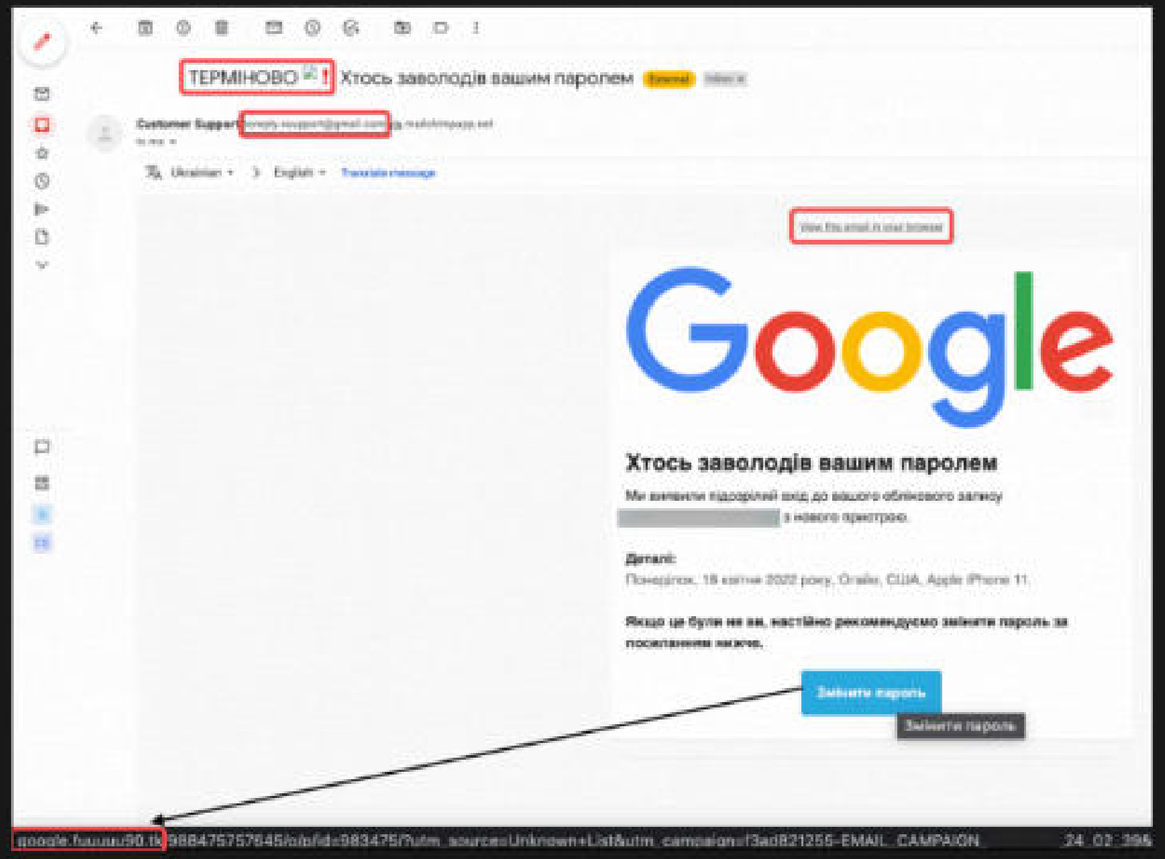
Найпоширенішими хакерськими атаками є DDoS, фішинг та встановлення вірусних програм-шантажистів.

molfar

Фішинг (англ. риболовля)

Вид онлайн шахрайства, де вас намагаються спіймати на гачок і отримати доступ до ваших:

- соцмереж
- робочих і особистих онлайн сховищ
- банківської інформації



Ознаки:

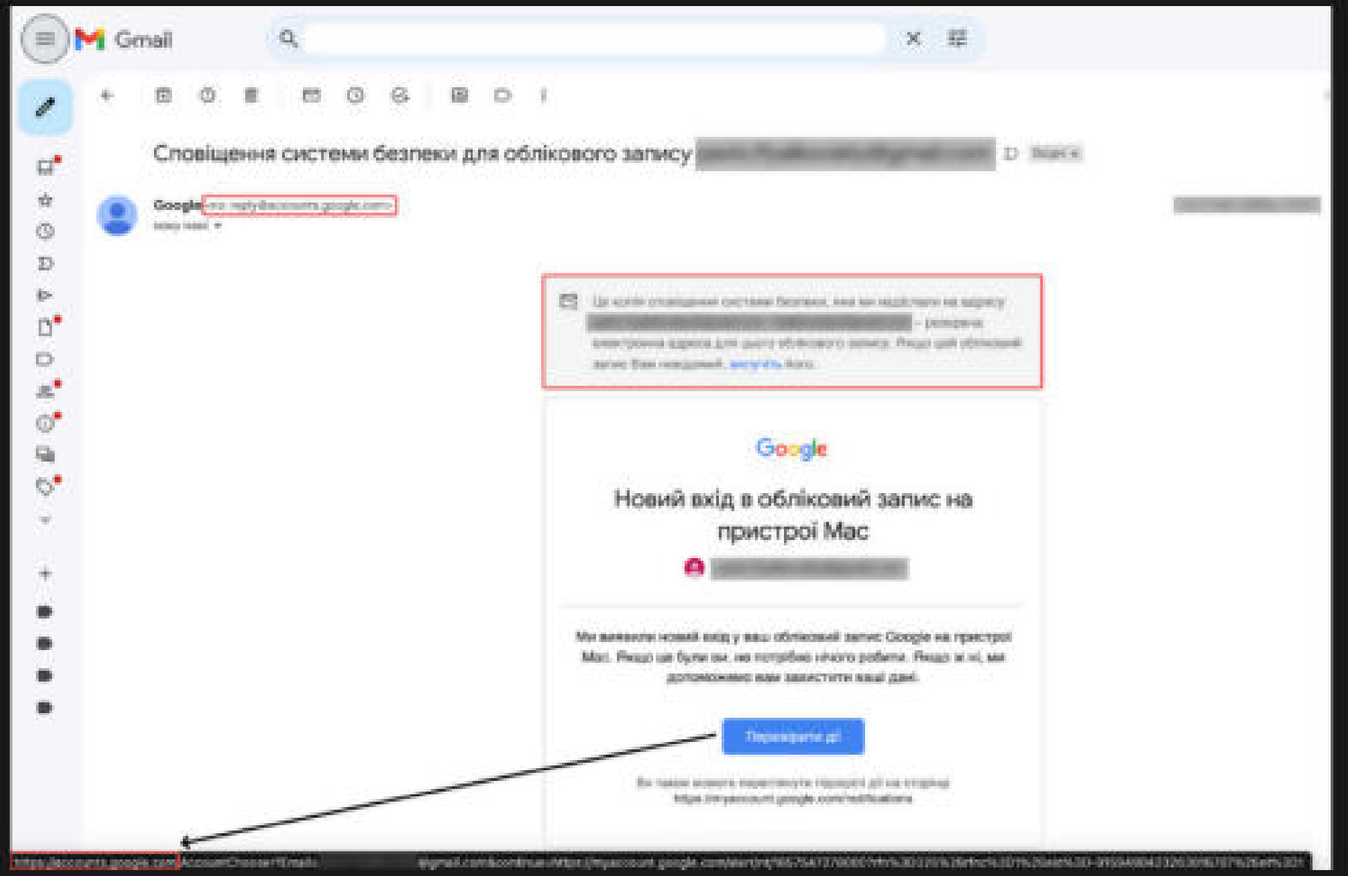
- Провокаційні повідомлення
- “Ви додані до чорного списку, терміново необхідне підтвердження особистості”
- Розмиті формулювання у листах
- “Шановний власник облікового запису”
- Повідомлення від “друзів”
- Прохання надати або оновити персональні дані

Як мало б бути?

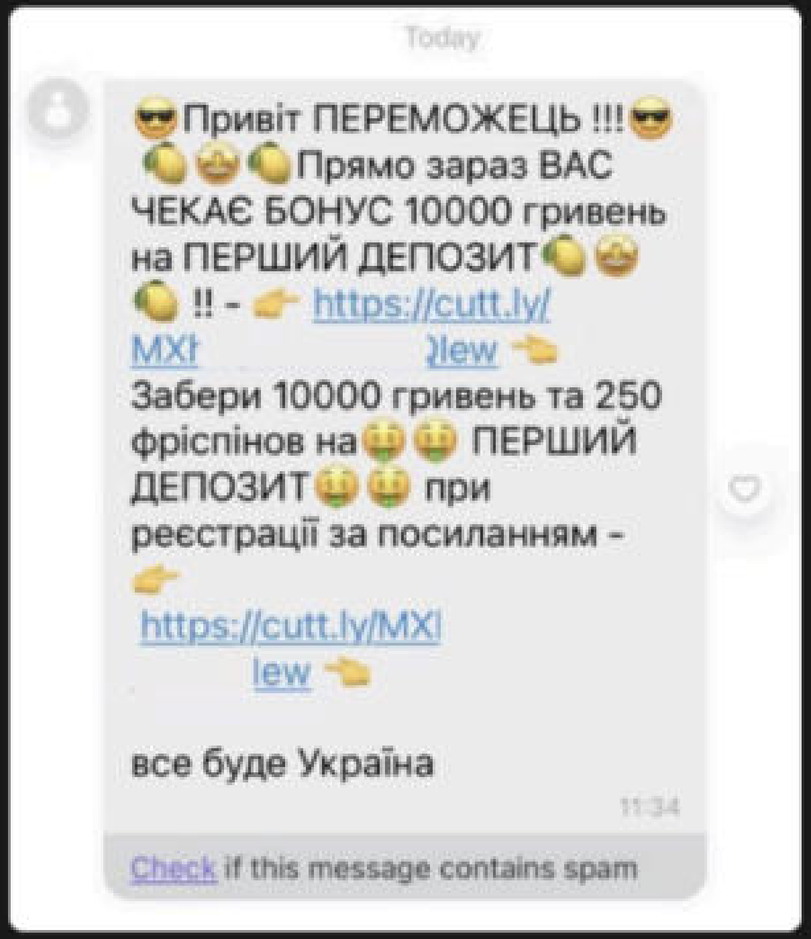
- лист від accounts.google.com ☑️
- копії листів надіслані вашим резервним обліковим записам ☑️
- дублювання вірної адреси в посиланні ☑️
- https ☑️

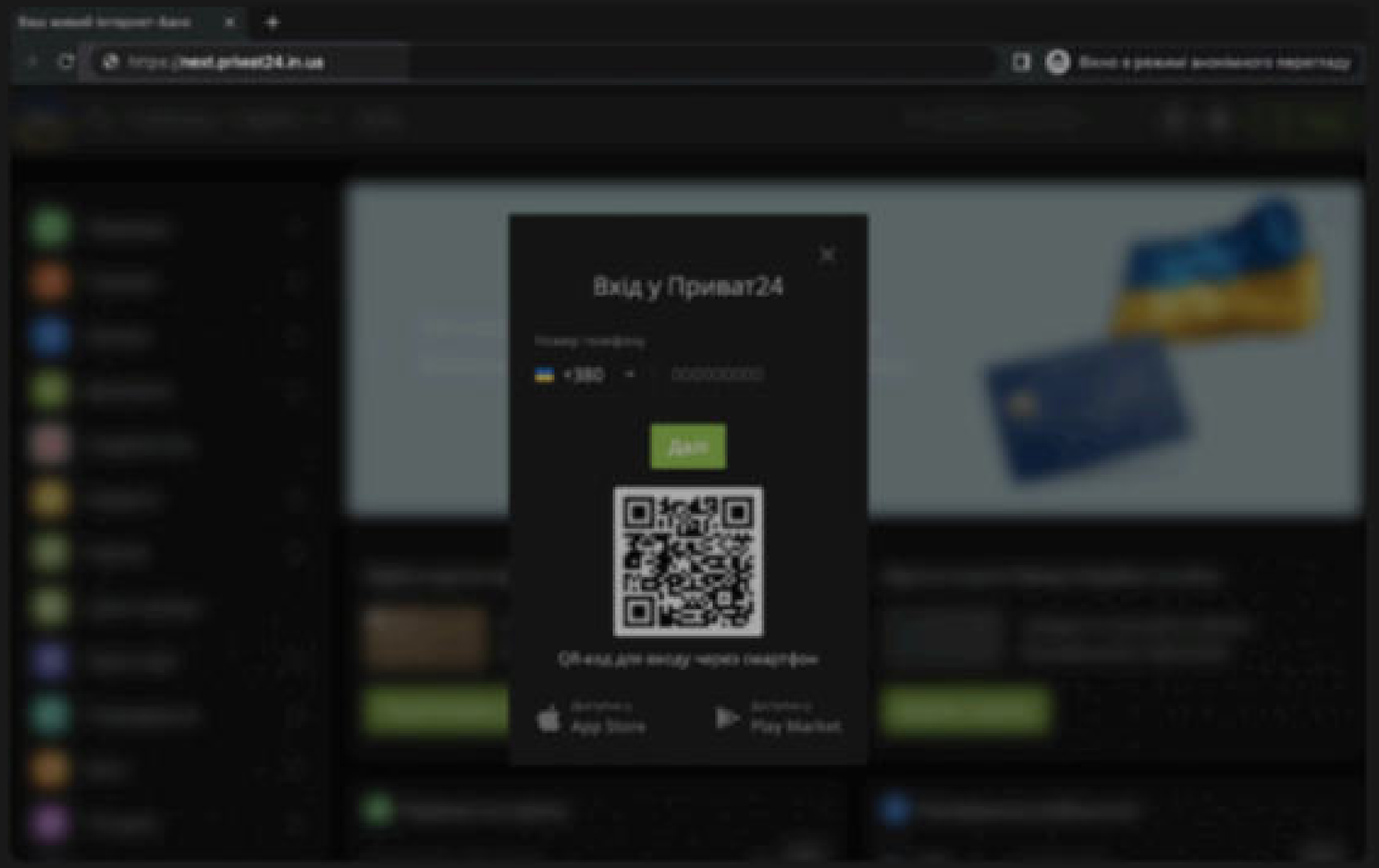
Правила протидії:

- Уникати використання персональної пошти.
- Не відповідати на незнайомі і підозрілі листи.
- Не відкривати файли у підозрілих листах.



Які ще бувають приклади фішингу?

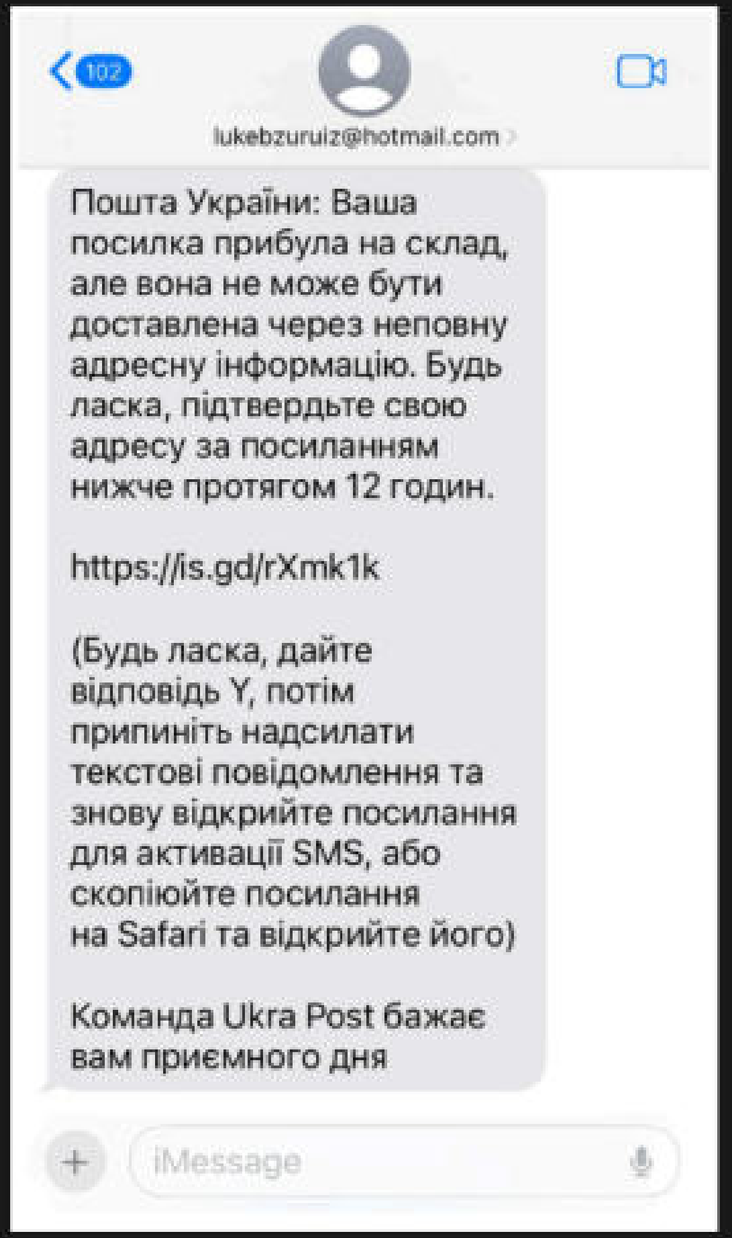




molfar

Пошта України

Приходить SMS від "пошти України" з вимогою підтвердити свою адресу протягом певного часу. Для цього просять перейти за фішинговим посиланням.



molfar

Фішинг із «запитом від СБУ»

Від: Сичевко Іларіон Гордиславович <[redacted]@dk0wua.de>
Надіслано: 18 січня 2024 р. 15:33
Кому: [redacted]
Тема: [WARNING - ENCRYPTED ATTACHMENT NOT VIRUS SCANNED] [DKIM Failure] Запит документів (ЦУ СБУ)

Центральне управління СБУ

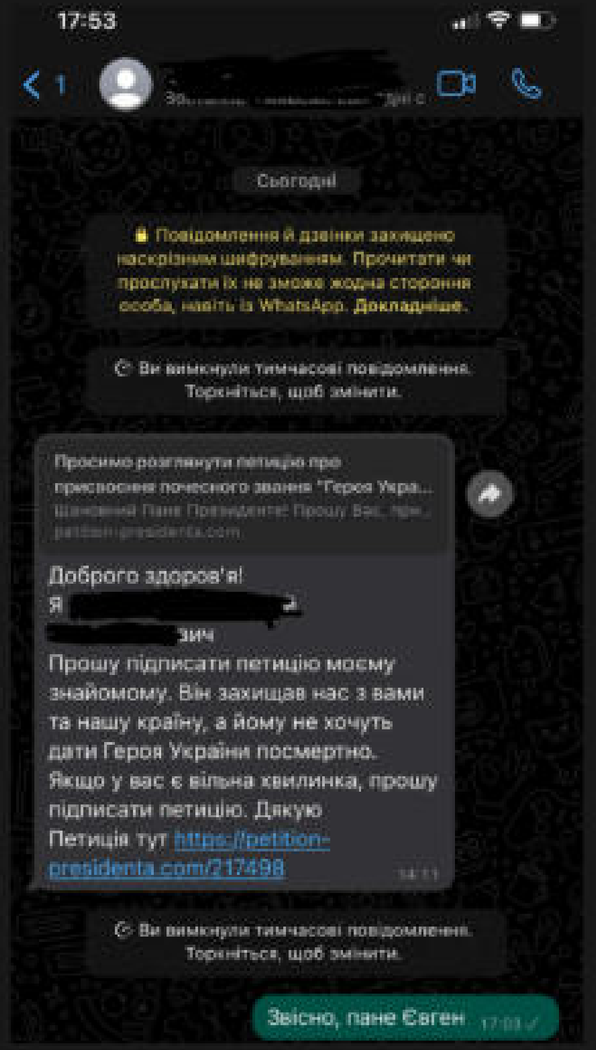
01601, м. Київ 1, вул. Малопідвальна, 16
Служба безпеки України
Вихідний номер листа: 510381661 от: 18 Січня 2024
Отримувач листа: [redacted]
Категорія - електронно

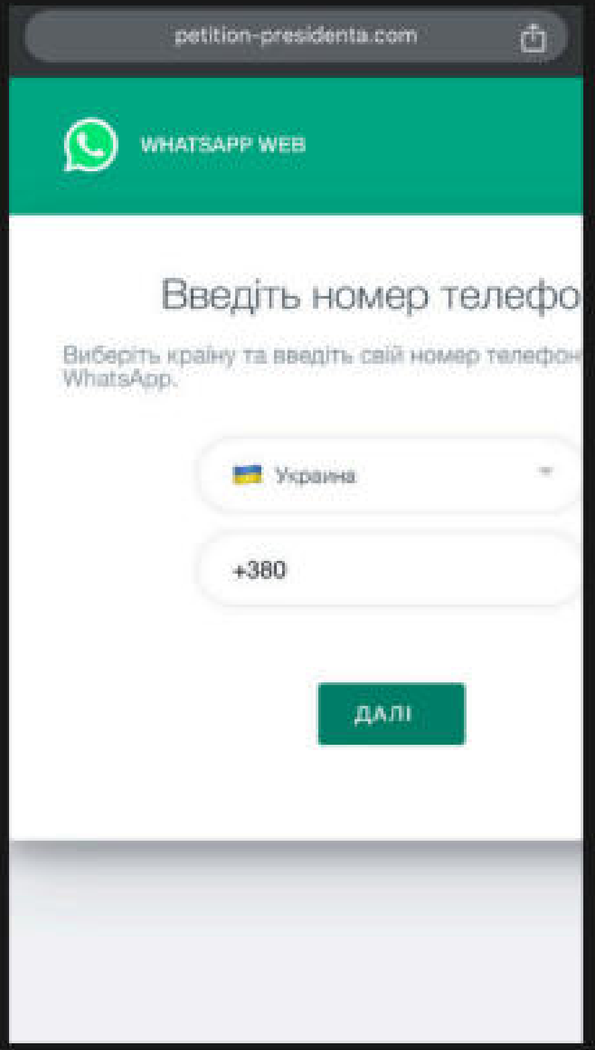
Здрастуйте, Центральним Управлінням СБУ проводитися до слідчої перевірки за фактом легалізації доходів у рамках порушеної кримінальної справи № 5124831398373 згідно з пунктом 3 статті 25 закону про «Службу Безпеки України» нам необхідно отримати відомості про Ваші контрагенти та Ваші фінансово-господарські взаємовідносини зазначені у запиті. На запит прошу відповісти письмово на адресу: 01601, м. Київ 1, вул. Малопідвальна, 16 Служба безпеки України для ПВБ .
У разі не надання інформації в строк до 25 січня 2024 року, ми будемо змушені викликати Вас на допит.

Сичевко Іларіон Гордиславович

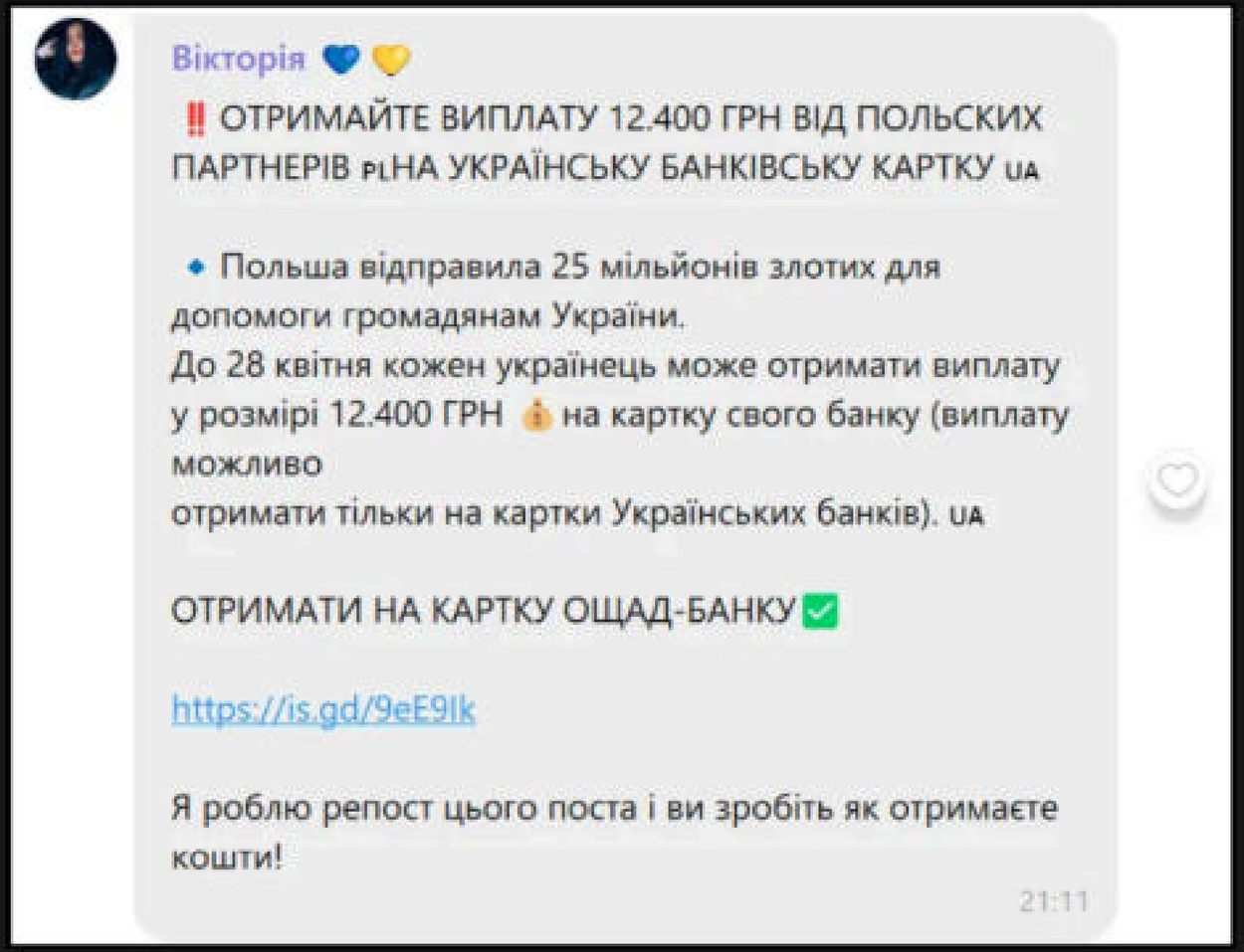
Співробітник 2 відділу
контррозвідувального забезпечення об'єктів
критичної інфраструктури та
протидії фінансуванню тероризму
01601, м. Київ 1, вул. Малопідвальна, 16
Служба безпеки України

Сайт петицій для фішингу



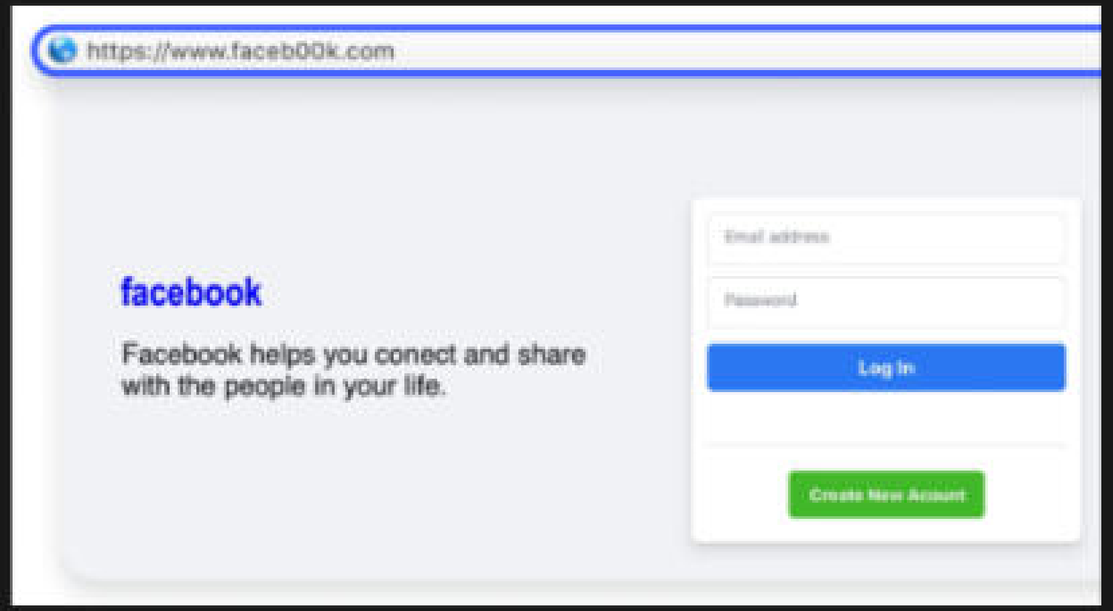


«Отримайте виплату від польських партнерів»



Перевірка адреси посилання

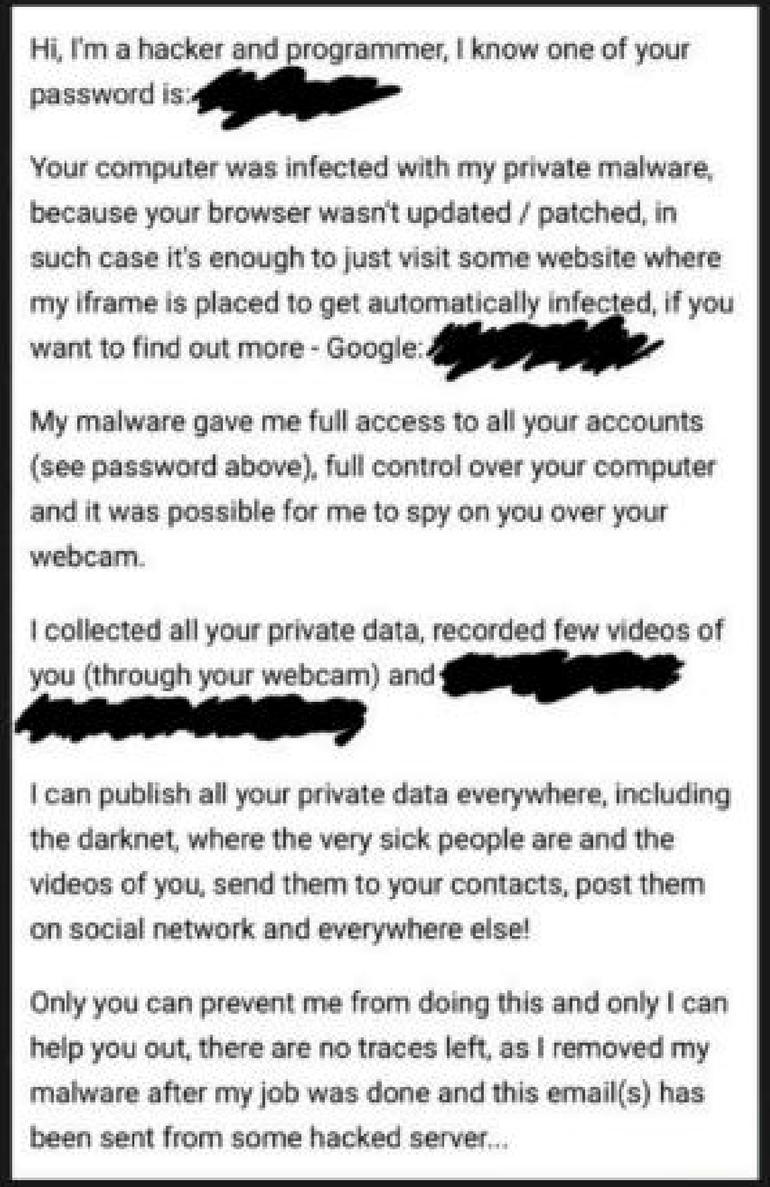
- скорочення посилань;
- додають зайві символи, фрази та цифри;
- URL-кодування: літера “M” стає “%6D”;
- відмінність посилання від вказаного у листі;
- зміна літер на схожі, без візуальної зміни;
- google - google. В оригінальному домені – англійська маленька літера l (ел), у фейковому — велика i (ай);
- checkshorturl.com — перевірка на скороченість посилання;
- urlvoid.com, safeweb.norton.com, transparencyreport.google.com - перевірка надійності.



Кейси з паролями

Скамери беруть зламані бази паролів і на їх базі роблять розсилки.

Паролі справжні, хоча і не актуальні.



Hi, I'm a hacker and programmer, I know one of your password is: [redacted]

Your computer was infected with my private malware, because your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: [redacted]

My malware gave me full access to all your accounts (see password above), full control over your computer and it was possible for me to spy on you over your webcam.

I collected all your private data, recorded few videos of you (through your webcam) and [redacted]

I can publish all your private data everywhere, including the darknet, where the very sick people are and the videos of you, send them to your contacts, post them on social network and everywhere else!

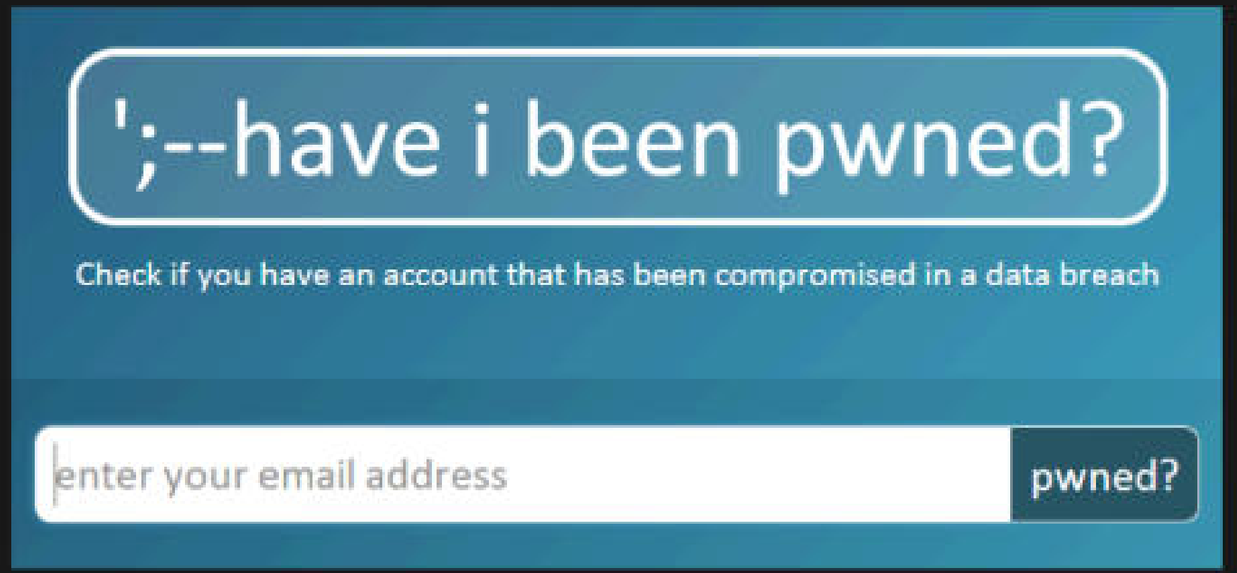
Only you can prevent me from doing this and only I can help you out, there are no traces left, as I removed my malware after my job was done and this email(s) has been sent from some hacked server...

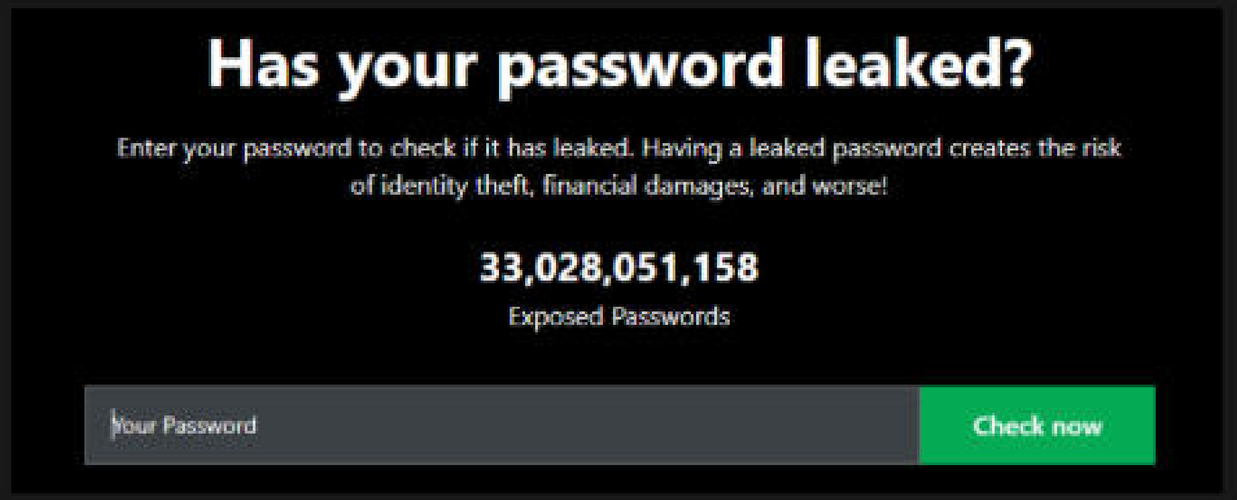
Кейси з паролями

Have I Been Pwned

Перевірте свою пошту на те, чи були злиті паролі від неї у різних сервісах.

Також перевірте чи був злитий ваш пароль, наприклад через **CyberNews**.

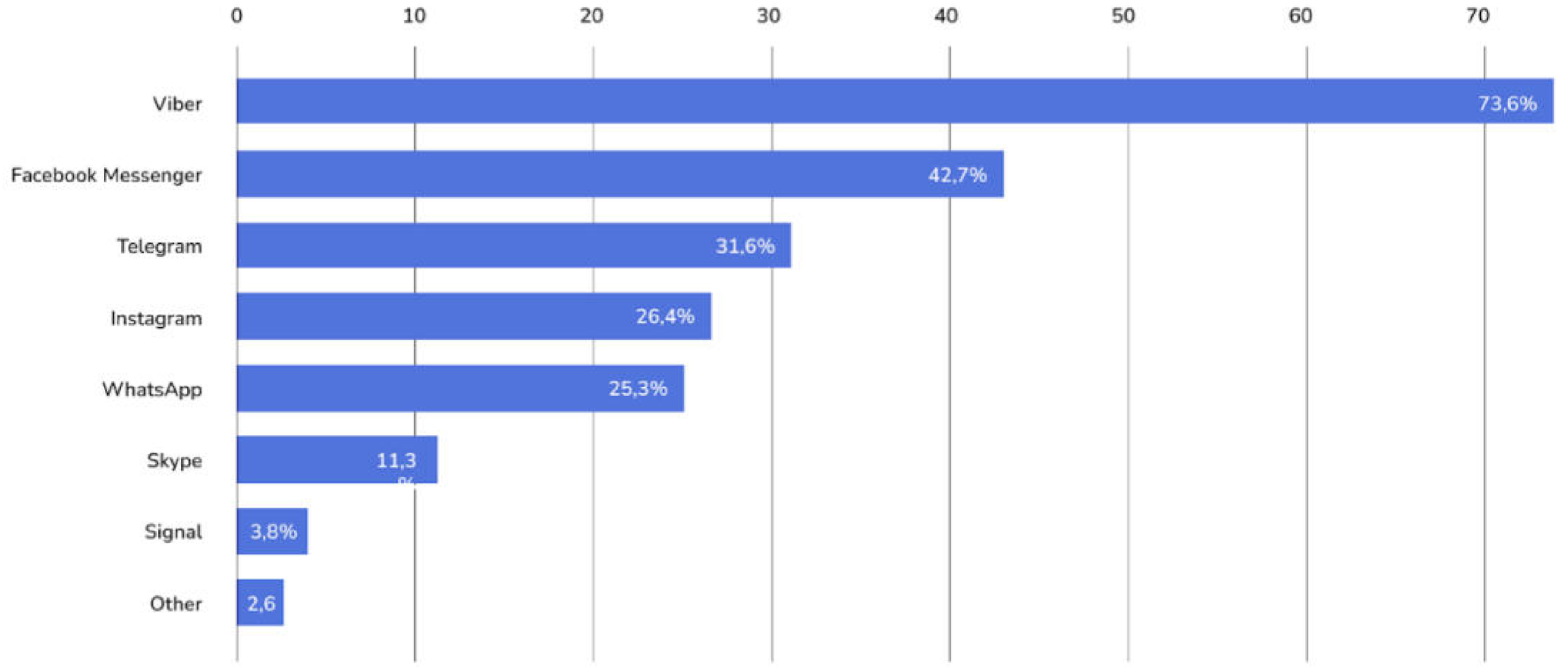




molfar

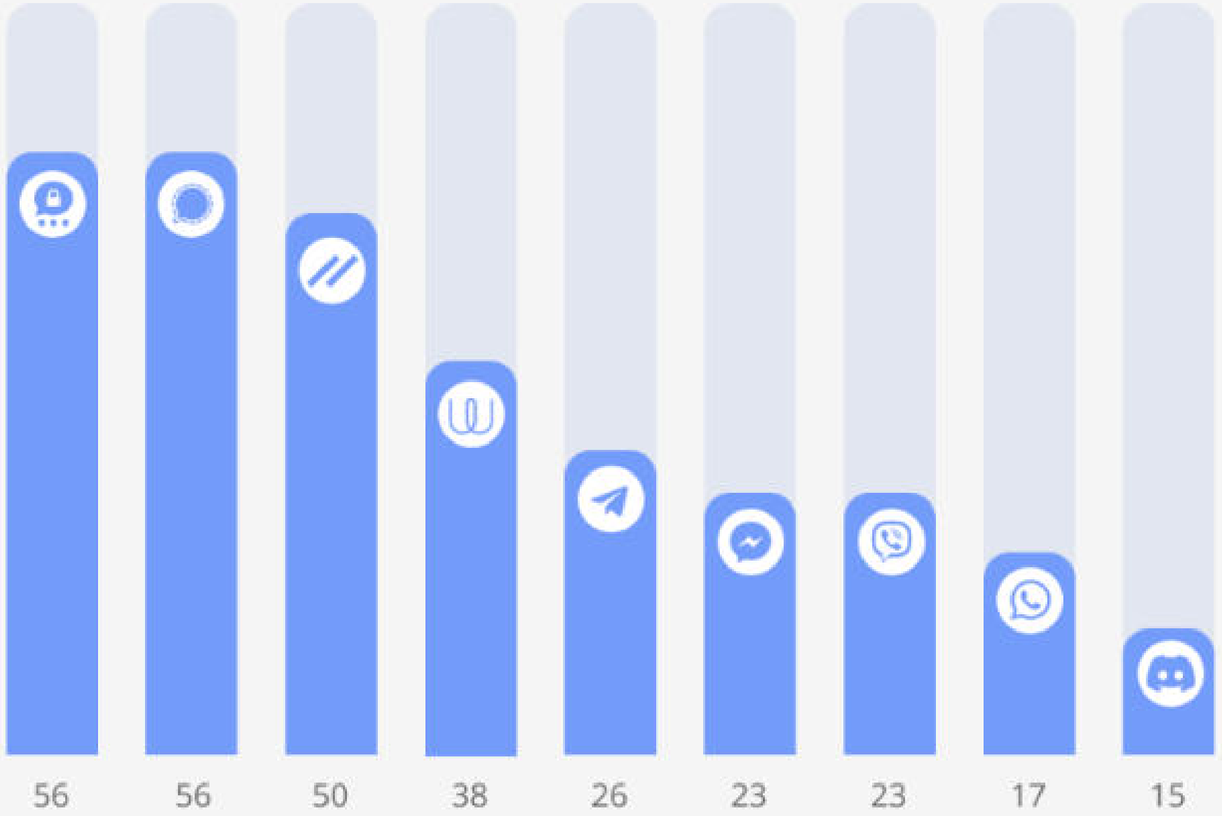
Протестуймо надійність пароля

Найпопулярніші додатки для спілкування в Україні



Рейтинг безпеки месенджерів

molfar



Криптографія

Threema, Wickr, Signal та Wire мають надійні криптографічні протоколи та алгоритми. Решта месенджерів не шифрують метадані та не хешують особисту інформацію.

Функціональність

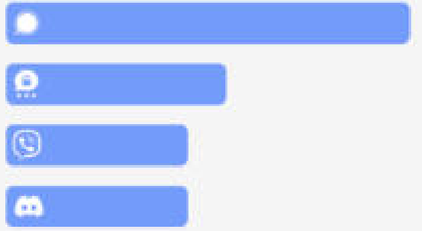
Threema володіє найкращою функціональністю: власні сервери, анонімна реєстрація, додавання контактів без сервера каталогів.

Безпека даних

Лише Threema та Wickr не збирають і не відправляють контактні дані під час анонімного використання.

Інше

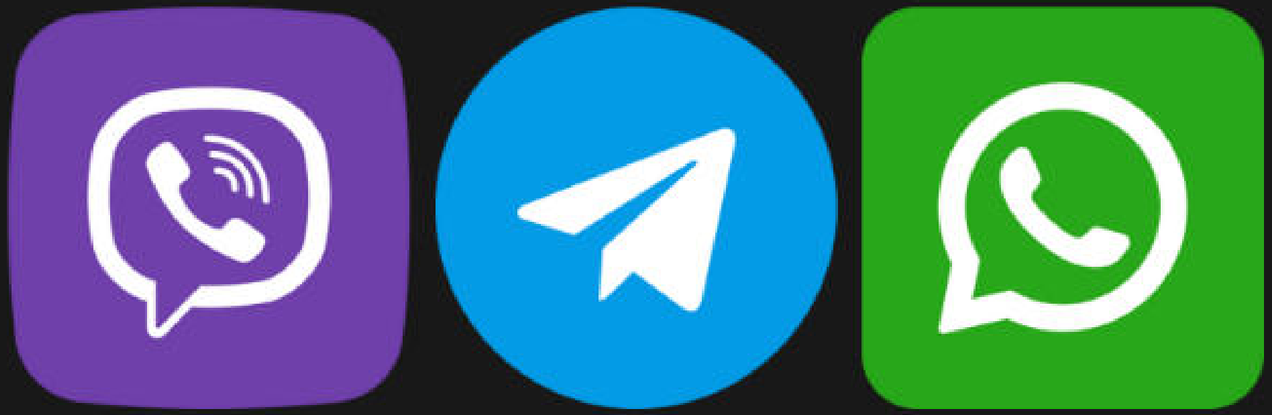
Signal — єдиний месенджер, який проводить аудит безпеки кожен рік, починаючи з 2014 року.



Месенджери

Viber, Telegram або WhatsApp — зручні, проте доволі небезпечні месенджери.

Саме через ці месенджери частіше за все вербують або проводять спроби заволодіння даними.



Месенжери: пам’ятайте про баланс

Завжди пам’ятайте про баланс зручності та секретності інформації.

Насправді для побутового спілкування з вашими близькими та друзями — вам підійде і Telegram.

Проте для спілкування з вашими родичами-військовими, краще використовувати секьюрний месенджер, наприклад Signal. Це допоможе забезпечити безпеку військового.

Декілька порад, які допоможуть підвищити рівень конфіденційності в Telegram

- **Локація.** Переконайтеся, що функція “Люди поблизу” вимкнена. Для цього перейдіть у “Контакти” > “Знайти людей поблизу” > “Не показувати мене”. Ця опція повинна за замовчуванням бути вимкнена.
- **Номер телефону.** Перейдіть у налаштування Telegram > розділ “Приватність і безпека” > “Номер телефону”. Там виберіть опцію, щоб ніхто не міг бачити ваш номер мобільного телефону.
- **Відвідування.** Перейдіть у налаштування Telegram >“Приватність і безпека” > “Відвідини й стан у мережі”. Звідти виберіть пункт, щоб ніхто не бачив онлайн ви чи офлайн.
- **Фото.** Перейдіть до налаштувань Telegram > “Приватність і безпека” > “Фотографія профілю”. Звідти виберіть лише “Мої контакти”.
- **Телефонні дзвінки.** В розділі “Приватність і безпека” > “Виклики”, на питання про те, хто може вам зателефонувати, виберіть “Ніхто”.
- **Повідомлення.** У тому ж таки розділі, в пункті “Пересланні повідомлення”, теж натисніть “Ніхто”, щоб була відсутньою можливість пересилати будь-які з ваших меседжів.
- **Групи.** Розділ “Групи та канали” повинен висвічуватися, що лише “Мої контакти” мають право додавати вас до якихось груп і каналів.
- **Свята “двофакторка”.** Увімкніть її в розділі “Приватність і безпека”.

Безпека в Signal: деякі рекомендації для безпечного використання

- **Налаштуйте зникаючі повідомлення:** Налаштування → Конфіденційність → Зникаючі повідомлення → Увімкнути.
- **Перевірте підключені пристрої:** Налаштування → Прив’язані пристрої.
- **Активуйте PIN, щоб упередити повторну реєстрацію вашого номера:** Налаштування → Обліковий запис → Блокування реєстрації.
- **Вимкніть відображення викликів в історії дзвінків телефона:** Налаштування → Конфіденційність → Вимикаємо показ викликів на Телефоні iOS.
- **Увімкніть захист екрана:** Налаштування → Конфіденційність → Блокування екрана.
- **Регулюйте вміст сповіщень:** Налаштування → Сповіщення → Показувати (обираємо).
- **Приховайте свій номер телефону (краще встановіть нікнейм):** Налаштування → Конфіденційність → Номер телефону.
- **Ретранслюйте виклики через сервери Signal, щоб не світити IP:** Налаштування → Конфіденційність → Додаткові функції → Завжди ретранслювати дзвінки.
- **Приховайте екран у перемикачі застосунків:** Налаштування → Конфіденційність → Приховувати екран.

Як блокувати (спам-) виклики від невідомих номерів без застосунків?

iPhone

Можна стишити та перевести виклики від невідомих абонентів на голосову пошту.
Для цього клікаємо **Налаштування → Телефон → Стишувати невідомі**.

Android

- Щоб заблокувати дзвінки з незнайомих номерів тиснемо **Контакти → Налаштування → Блокування номерів** активуємо блокування невідомих номерів.
- Щоб стишити дзвінки тиснемо **Налаштування → Не турбувати → Увімкнути**. Потім **Дозволити дзвінки** та обираємо **Усі контакти**.

* Інструкція на Android може варіюватися на різних моделях пристроїв.

Watch video on YouTube

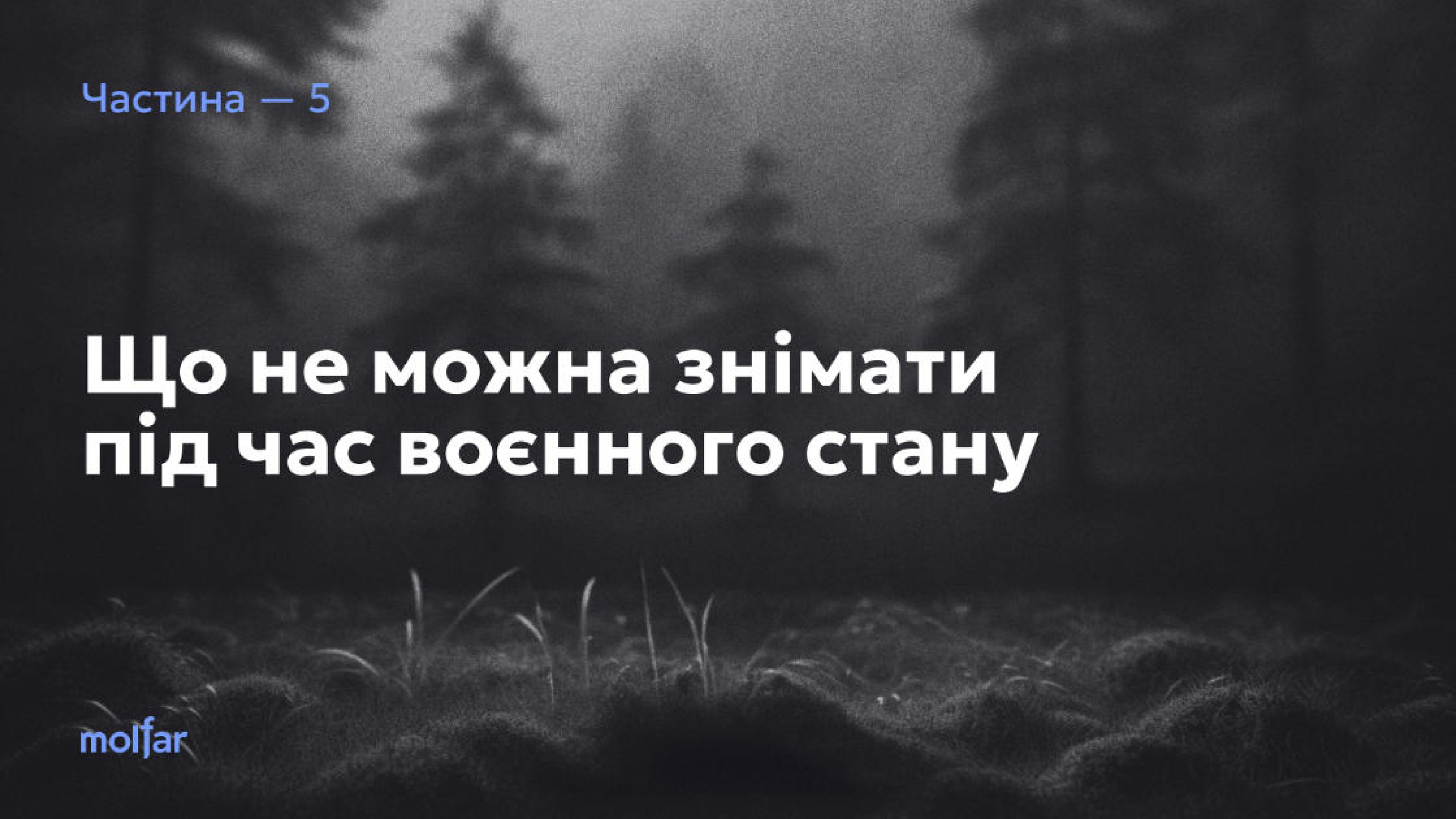
Error 153

Video player configuration error

Watch video on YouTube

Error 153

Video player configuration error



Частина — 5

Що не можна знімати під час воєнного стану

molfar

- Номер військової частини та назву військового об'єкта, елементи геральдики, сині таблички

- Блокпости та місця дислокації військових

- Номери та позначки на військовій техніці та цивільних машинах, що паркуються на території військового об’єкта

- Позначки на службових автівках інших служб, наприклад, пожежників

- Обличчя працівників інших служб, оскільки через них можна ідентифікувати місце знімання

- Вид з вікна військової будівлі

- Об’єкти на горизонті, за якими можна дізнатися локацію

- Техніку, яка є в нас в одиничних екземплярах

- Обличчя військових
- Прізвище, звання та знаки військового підрозділу
- Якщо у відео людина називає якусь чутливу інформацію (місце дислокації, кількість техніки, плани тощо), то окрім вирізання звуку, треба замалювати губи (чорним прямокутником), бо по губах можна прочитати інформацію

- Нестандартні об’єкти які можна знайти за допомогою пошуку по картинках в інтернеті та визначити місце дислокації військових

- Специфічні позначки на будівлях, адреси будівель: знаки можуть видати інформацію про дислокацію військових у будівлях

- Загальні відеоплани, де можна підрахувати кількість техніки, боєприпасів: з цією інформацією ворог може коригувати свої плани наступу та розвідки

- Досі активне державне/комунальне підприємство, де знаходяться працівники: є ризик деанону та ракетної/артилерійської атаки на об’єкт

- Документи, плани та карти з планами: з цією інформацією ворог може коригувати плани наступу та розвідки

- Квадрокоптерні знімання місцевості біля дислокації військових: такі кадри можуть видати місце дислокації військових, бронетехніки, систем ППО тощо

- Місця виробництва боєприпасів та налаштування техніки, у тому числі дронів та їх вибухових компонентів
- Роботу військової техніки, за краєвидом можна дізнатися координати дислокації техніки та військових
- Місця прильотів та роботу ППО

Watch video on YouTube

Error 153

Video player configuration error

Які правила особистої безпеки під час публікацій будь-який фотографій в соцмережах?

Формуємо 5-7 правил кібербезпеки

Моя перша дія сьогодні для поліпшення власної кібербезпеки — це...

Урок 3	Розвідка на основі відкритих джерел (OSINT): цілі та завдання

ЯК МОЖНА ПЕРЕВІРИТИ, ЧИ СПРАВЖНЄ ФОТО, ЯКЕ ВИ ПОБАЧИЛИ В СОЦМЕРЕЖІ?

ЧИ МОЖНА ДІЗНАТИСЬ, ДЕ ПЕРЕБУВАЮТЬ РОСІЙСЬКІ ВІЙСЬКОВІ, ЯКЩО ВИ МАЄТЕ ЛИШЕ КОМП’ЮТЕР ТА ІНТЕРНЕТ?

Watch video on YouTube

Error 153

Video player configuration error

НАВІЩО НАМ ДОСЛІДЖУВАТИ РОСІЯН ТА РОСІЯНОК, ПРИЧЕТНИХ ДО ВІЙНИ В УКРАЇНІ?

ЩО ВИ ВЖЕ ЗНАЄТЕ ПРО OSINT?
В ЯКИХ СФЕРАХ, ОКРІМ ФІКСАЦІЇ РОСІЙСЬКИХ ЗЛОЧИНІВ, OSINT МОЖЕ БУТИ КОРИСНИМ?

OSINT (розвідка на основі відкритих даних) — це процес пошуку, аналізу та інтерпретації відкритих даних, які можна отримати легально й етично для певних аналітичних або дослідницьких цілей.

ФУНКЦІЇ OSINT

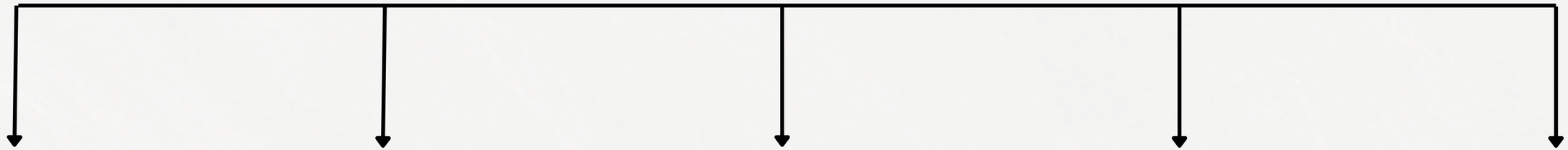
1. Відстежувати потенційні загрози безпеці
2. Здійснювати перевірку або розслідування щодо конкретних осіб
3. Перевіряти достовірність фактів
4. Підтверджувати або спростовувати інформацію з різних джерел
5. Виявляти перші сигнали кібератак
6. Аналізувати конкурентне середовище
7. Оцінювати надійність партнерів чи інших осіб

Характеристика	Стандартний пошук / дослідження	Розвідка на основі відкритих джерел (OSINT)
Мета	Загальне розуміння теми, отримання знань.	Підтримка ухвалення конкретного рішення (наприклад, підтвердження особи, викриття зв'язків).
Методологія	Довільна.	Суворо структурована, базується на розвідувальному циклі.
Критичний етап	Збір інформації.	Верифікація та аналіз джерел.
Вихідний продукт	Реферат, стаття, набір фактів.	Аналітичний звіт, висновок.

ДЖЕРЕЛА OSINT

1. Традиційні медіа
2. Інтернет-ресурси
3. Архіви вебсторінок
4. Онлайн-бази даних
5. Соціальні мережі
6. Супутникові знімки
7. Цифрові метадані
8. Deep web

ТИПИ OSINT



SOCMINT
(Social Media Intelligence - розвідка за соціальними мережами)

HUMINT
(Human Intelligence - агентурна розвідка)

GEOINT
(Geospatial Intelligence — розвідка геопросторових даних)

FININT
(Financial Intelligence — фінансова розвідка)

SIGINT
(Signals Intelligence — радіоелектронна розвідка)

SOCMINT
(Social Media Intelligence - розвідка за соціальними мережами)

- Розслідування Bellingcat щодо російського спеціального загону швидкого реагування «Ахмат».

- Розслідування про збиття росією літака MH17 у 2014 році.

GEOINT
(Geospatial Intelligence — розвідка геопросторових даних)

- Візуалізація розгортання військ росії перед повномасштабним вторгненням.
- Перший супутниковий знімок зруйнованої Каховської ГЕС від “Схем”.

SIGINT
(Signals Intelligence — радіоелектронна розвідка)

- Волонтерський проєкт Monitor: це україномовні OSINT-зведення про активність ворожої авіації та загрозу ракетних обстрілів в Україні.

Аналогічний ресурс існує й у додатку Telegram, однак через кращу захищеність додатку WhatsApp рекомендуємо користуватися каналом у WhatsApp.

HUMINT
(Human Intelligence - агентурна розвідка)

- «Список 31» (депортація дітей). «Схеми» + «Ти як?» встановили маршрут вивезення 31 дитини, ідентифікували причетних осіб, використали свідчення батька дітей та документи з верифікованого витоку пошти воєнного злочинця Дениса Пушиліна.
- Спецоперація Головного управління розвідки “Синиця”: українські розвідники переманили російського пілота бойового гелікоптера Мі-8 на бік України.

Watch video on YouTube

Error 153

Video player configuration error

Мініпрактикум “Знайди локацію”

ЕТАП 1: ЗВОРОТНИЙ ПОШУК (10 ХВ)

1. **ПОШУК:** ВИКОНАЙТЕ ЗВОРОТНИЙ ПОШУК ЗОБРАЖЕННЯ ЗА ДОПОМОГОЮ ЩОНАЙМЕНШЕ ДВОХ РІЗНИХ ІНСТРУМЕНТІВ (НАПРИКЛАД, TINEYE ТА GOOGLE LENS).
2. **НАЙДАВНІШЕ ДЖЕРЕЛО:** ЗНАЙДІТЬ НАЙРАНІШЕ ДЖЕРЕЛО АБО ОРИГІНАЛЬНУ СТОРІНКУ (ЗАЗВИЧАЙ ВІКІСХОВИЩЕ, FLICKR АБО ОСОБИСТИЙ БЛОГ ФОТОГРАФА / ФОТОГРАФКИ) ТА ЗАФІКСУЙТЕ ДАТУ ПУБЛІКАЦІЇ.
3. **ЧОМУ ЦЕ ВАЖЛИВО?** НАЙРАНІШЕ ДЖЕРЕЛО З НАЙВИЩОЮ РОЗДІЛЬНОЮ ЗДАТНІСТЮ НАЙІМОВІРНІШЕ Є ОРИГІНАЛОМ, ЩО ДОПОМАГАЄ У ВЕРИФІКАЦІЇ.
4. **ОБ'ЄКТ:** ВИЗНАЧТЕ НАЗВУ ОБ'ЄКТА ТА ЙОГО ЗАГАЛЬНЕ МІСЦЕЗНАХОДЖЕННЯ.

Мініпрактикум “Знайди локацію”

ЕТАП 2: ГЕОЛОКАЦІЯ ТА ВЕРИФІКАЦІЯ (10 ХВ)

1. **ГЕОПІДКАЗКИ**: УВАЖНО ПРОАНАЛІЗУЙТЕ ЗОБРАЖЕННЯ. ЗВЕРНІТЬ УВАГУ НА:
   - АРХІТЕКТУРУ / ЛАНДШАФТ — ТИПОВІ ЕЛЕМЕНТИ БУДІВЕЛЬ, РОСЛИННІСТЬ.
   - ТРАНСПОРТ — НОМЕРНІ ЗНАКИ, МОДЕЛІ АВТОМОБІЛІВ, ТРАМВАЇ.
   - ВИВІСКИ / СИМВОЛІКУ — ПРАПОРИ, ЛОГОТИПИ.
2. **МАПА**: ВИКОРИСТОВУЙТЕ НАЗВУ ОБ'ЄКТА ТА ЗНАЙДЕНІ ПІДКАЗКИ, ЩОБ ЗНАЙТИ ТОЧНЕ МІСЦЕ НА GOOGLE MAPS АБО GOOGLE STREET VIEW.
   - ЗАВДАННЯ: ЗІСТАВТЕ УНІКАЛЬНІ ДЕТАЛІ НА ФОТО (ВІКНО, ДЕРЕВО, ЛІХТАРНИЙ СТОВП) З ТИМ, ЩО БАЧИТЕ НА STREET VIEW.
   - ВИЗНАЧТЕ ТОЧНУ АДРЕСУ АБО КООРДИНАТИ.

Мініпрактикум “Знайди локацію”

ЕТАП 3: ПРЕЗЕНТАЦІЯ (5 ХВ)

КОЖНА ПАРА КОРОТКО ПРЕДСТАВЛЯЄ:

- ЯКІ ІНСТРУМЕНТИ ВИКОРИСТОВУВАЛИ?
- ЯКЕ НАЙДАВНІШЕ ДЖЕРЕЛО ЗНАЙШЛИ ТА КОЛИ ВОНО БУЛО ОПУБЛІКОВАНЕ?
- ТОЧНУ ГЕОЛОКАЦІЮ (АДРЕСУ, МІСТО).
- ЯКІ ПІДКАЗКИ ВИЯВИЛИСЯ НАЙКОРИСНІШИМИ?

Урок 4	Аналіз соцмереж

SOCMINT (Social Media Intelligence) — це збір та аналіз інформації, що є у відкритому доступі на платформах соціальних медіа (Facebook, Instagram, X / Twitter, Telegram тощо). Це лише один із доменів OSINT, але ключовий для розуміння публічної думки, зв'язків та переміщень людей.

SOCMINT:
ПАСИВНИЙ VS. АКТИВНИЙ ЗБІР

Пасивний збір:
це збір даних без прямої взаємодії з цільовим об'єктом

Активний збір:
це взаємодія з цільовим об'єктом

Watch video on YouTube

Error 153

Video player configuration error

ЧОМУ МИ ВИКОРИСТОВУЄМО НІКНЕЙМИ?

WhatsMyName: пошук акаунтів за нікнеймом

Molfar: ТОП-10 OSINT-інструментів 2024 року

ЕТИЧНИЙ АСПЕКТ

1. **Принцип приватності**

2. **Умови платформ**

GOOGLE DORKS (АБО GOOGLE HACKING)

це не окремий інструмент, а метод використання спеціальних операторів (команд), які дозволяють користувачеві / користувачці фільтрувати мільярди проіндексованих Google сторінок для пошуку дуже специфічної та цільової інформації, недоступної через звичайний пошук.

КЛЮЧОВІ ОПЕРАТОРИ ДЛЯ SOCMINT

Оператор	Призначення	Пояснення для учнів та учениць	Приклад використання (SOCMINT)
site:	Обмеження пошуку доменом	Дозволяє Google шукати інформацію лише на вказаному вебсайті чи соціальній мережі, ігноруючи решту	Щоб знайти публічні профілі людини на Facebook: site:facebook.com «Іван Петренко» Київ
" "	Точна відповідність (Exact Match)	Дозволяє шукати точну фразу чи ім'я, а не окремі слова. Виключає небажані варіації.	Щоб знайти публікації з точною фразою: site:facebook.com «Я люблю OSINT»

ДОДАТКОВІ КОРИСНІ ОПЕРАТОРИ

Оператор	Призначення	Приклад використання
-	Виключення слова / фрази	Дозволяє виключити зі списку результатів нерелевантне слово. Наприклад: технічні характеристики БТР -США site:mil.in.ua
**OR або `	Пошук альтернатив	Пошук альтернатив Наприклад: новини танки OR БМП site:armyinform.com.ua

Урок 5	GEOINT: що нам кажуть знімки та тіні?

GEOINT (Geospatial Intelligence) — це аналіз інформації про об'єкти на Землі, отриманої з супутникових знімків, мап, 3D-моделей та геолокаційних даних. У OSINT GEOINT використовується для підтвердження місця та часу фото чи відео.

КЛЮЧОВІ МЕТОДИ GEOINT В OSINT

Метод	Суть	Основне завдання
Геолокація	Порівняння візуальних підказок на фотографії (будівлі, знаки, рослинність, рельєф) з картографічними даними (Google Maps, Google Earth).	Знайти точні GPS-координати місця знімання.
Темпоральний аналіз	Використання даних про положення Сонця (тіні) або історичних супутникових знімків.	Визначити дату та час фільмування (чи відповідає заявленим).

Watch video on YouTube

Error 153

Video player configuration error

GOOGLE EARTH PRO (ВІЗУАЛЬНА ВЕРИФІКАЦІЯ)

Google Earth - безплатна програма, яка надає потужні можливості для GEOINT, які виходять за межі звичайних Google Карт:

- 3D-моделювання;
- історичні знімки.

SUNCALC (АНАЛІЗ ТІНЕЙ)

SunCalc — це простий візуальний онлайн-інструмент, який показує траєкторію руху Сонця та напрямок тіней у будь-якій точці земної кулі на будь-яку дату.

ДЖЕРЕЛО: SUNCALC

Урок 6	Аналіз фінансових даних

FININT (FINANCIAL INTELLIGENCE)

це збір та аналіз відкритої, офіційної інформації, що стосується фінансової та майнової діяльності організацій та публічних осіб. FININT — це не хакерство, не злам і не доступ до банківських рахунків. Це легальна робота виключно з тими даними, які держава зобов’язана публікувати для забезпечення прозорості та боротьби з корупцією.

FININT ДОЗВОЛЯЄ ПЕРЕВІРИТИ:

- Чи існує компанія взагалі (її статус і реєстрацію)?
- Хто її справжній власник / власниця (засновник/ засновниця, кінцевий бенефіціар / кінцева бенефіціарка)?
- Чи має компанія борги або судові позови?
- Яким майном володіють публічні службовці / службовиці та їхні родичі й родички (за допомогою декларацій)?

ЄДИНИЙ ДЕРЖАВНИЙ РЕЄСТР (ЄДР)

Найважливіше і найнадійніше джерело для перевірки будь-якої юридичної особи в Україні. Воно вкрай цінне для OSINT, оскільки містить офіційні, перевірені державою дані.

Що шукаємо: наявність реєстрації, точну назву, статус (зареєстровано, у стані припинення, банкрутство), ПІБ керівника / керівниці, основні види діяльності (КВЕД).

Чому це важливо: жодна легальна компанія чи ФОП не може діяти без коректної реєстрації в ЄДР. Перевірка статусу допомагає уникнути співпраці з фірмами-одноденками або такими, що перебувають у процесі ліквідації.

РЕЄСТР ДЕКЛАРАЦІЙ НАЗК

Інструмент для забезпечення прозорості та доброчесності влади. Він є публічним і доступним для пошуку за ПІБ декларанта / декларантки.

Що шукаємо: річні доходи, володіння нерухомістю, автомобілями, цінним майном, фінансові зобов'язання, а також інформацію про членів / членкинь сім'ї.

Чому це важливо: це дає змогу виявляти можливі конфлікти інтересів або ознаки незаконного збагачення, порівнюючи офіційні доходи публічного службовця / службовиці з його / її фактичними активами.

Комерційні платформи

YOUCONTROL

OPENDATABOT

Урок 7	Інструменти OSINT

КЕЙС: «НЕНАДІЙНИЙ ЗАБУДОВНИК»

Сценарій: у місцевих новинах та соціальних мережах (SOCMINT) активно поширюється інформація про те, що велика будівельна компанія «ЛідерБуд» два тижні тому зупинила роботи на новому житловому комплексі в місті. Клієнти й клієнтки хвилюються, а компанія видалила зі свого сайту всі відгуки.

Завдання: розробити план верифікації надійності компанії та перевірки її репутації

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	Юридичний статус компанії: чи не перебуває вона у стані припинення або банкрутства?	FININT	ЄДР (Єдиний державний реєстр)
2	Історія репутації: які публічні заяви про терміни будівництва розміщували на сайті компанії до скандалу?	SOCMINT	Google Dorks
3	Перевірка місцевості: чи дійсно роботи зупинені?	GEOINT	Google Earth Pro (огляд свіжих супутникових знімків)
4	Пошук негативу: чи були судові позови, пов'язані з цією компанією?	FININT (Агрегатори)	YouControl / Opendatabot (для демонстрації)
5	Аналіз соцмереж: що люди говорять про компанію зараз на форумах / сторінках, які не пов’язані з компанією?	SOCMINT	Google Dorks (site:facebook.com "ЛідерБуд")

Урок 8	Військові професії. Особливості професій, пов'язаних із сучасними цифровими технологіями, медіа та аналізом даних

LOBBY X

ПЛАТФОРМА З ПРАЦЕВЛАШТУВАННЯ
ТА РЕКРУТИНГОВА АГЕНЦІЯ

ВАКАНСІЇ ДЛЯ ДОСЛІДЖЕННЯ НА ПЛАТФОРМІ:

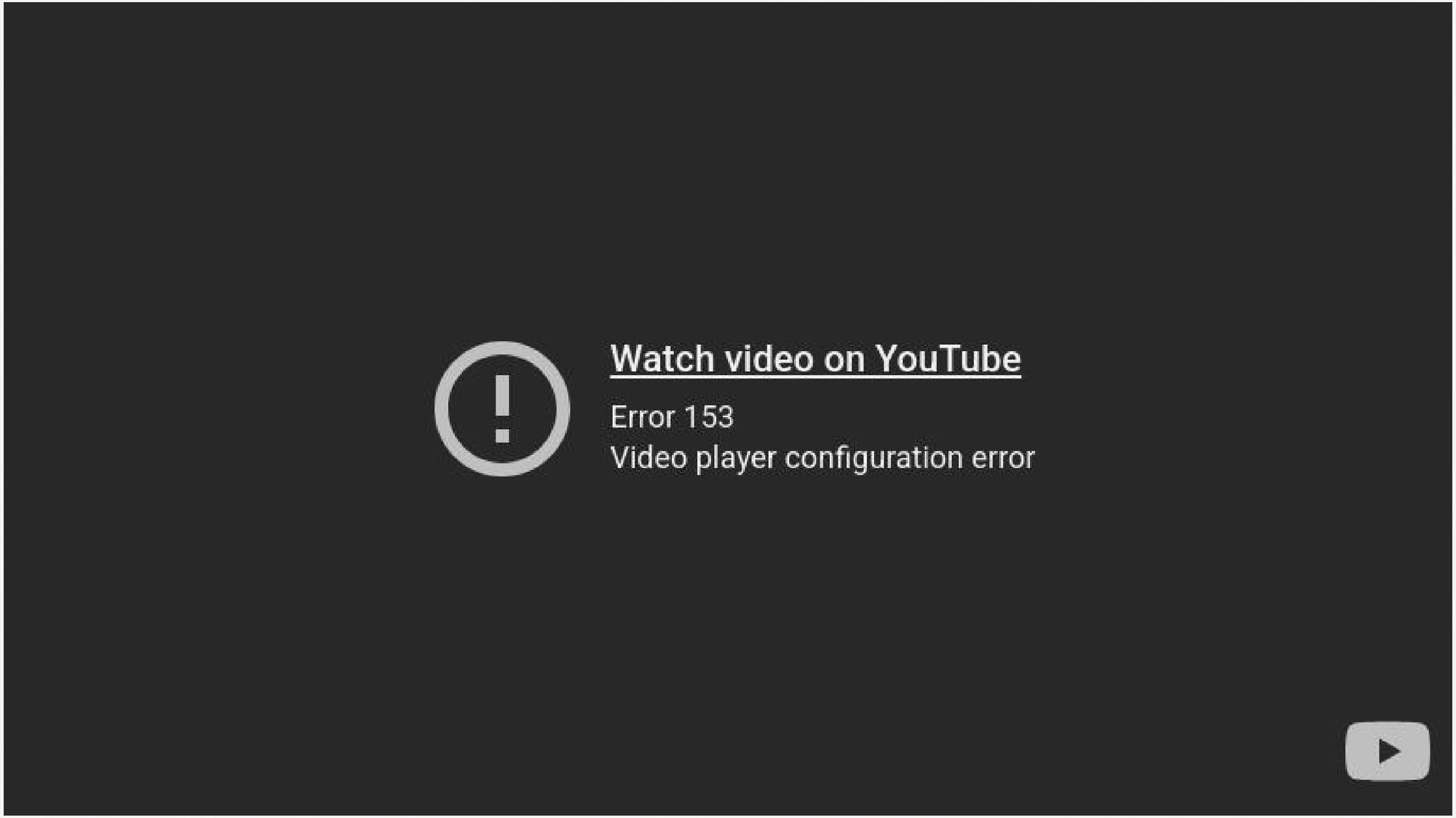
1. ДЕШИФРУВАЛЬНИК / ДЕШИФРУВАЛЬНИЦЯ.
2. АНАЛІТИК / АНАЛІТИКИНЯ.
3. ПРЕСОФІЦЕР / ПРЕСОФІЦЕРКА.

LOBBY X

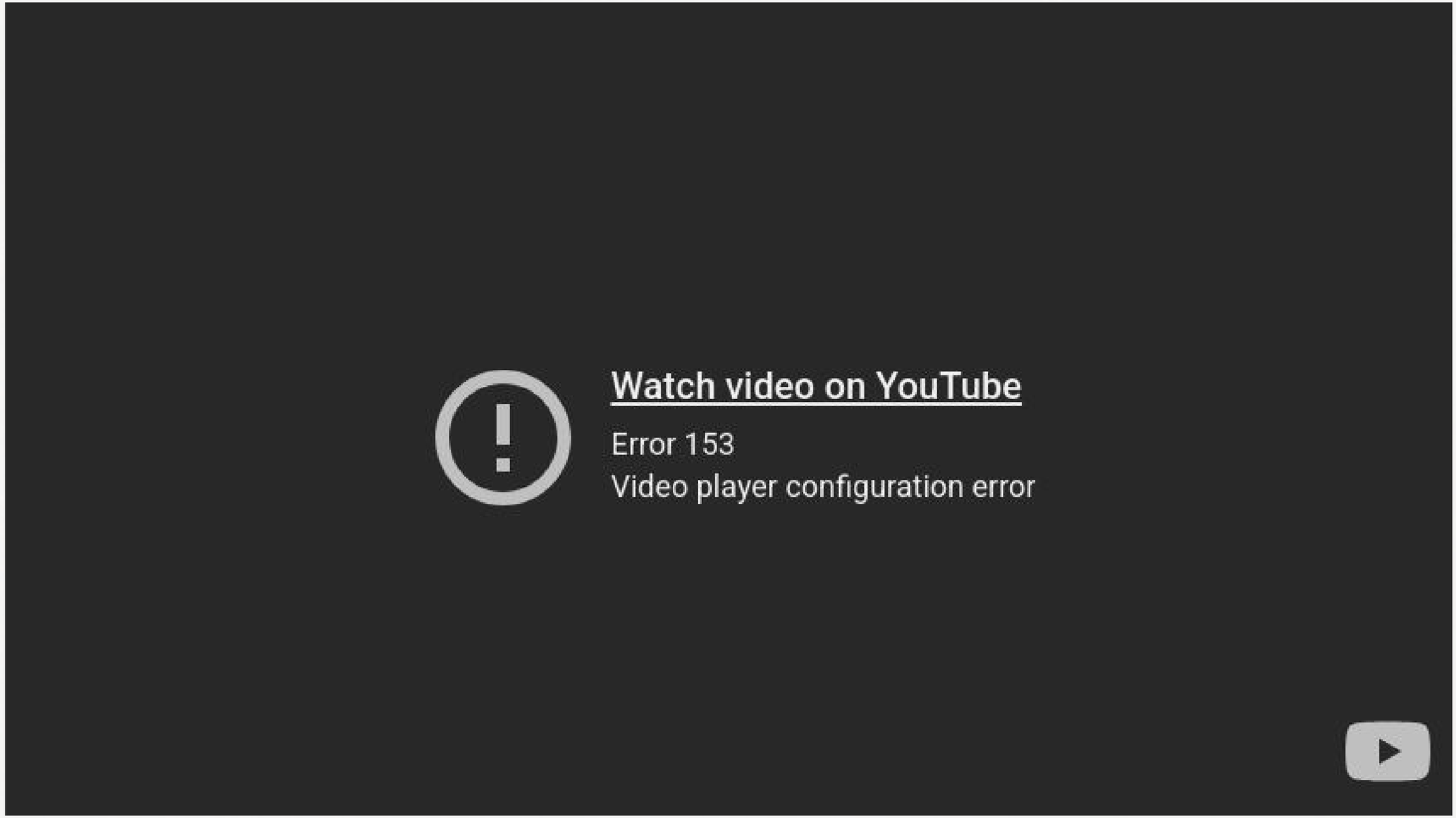
ПЛАТФОРМА З ПРАЦЕВЛАШТУВАННЯ
ТА РЕКРУТИНГОВА АГЕНЦІЯ

ВАКАНСІЇ ДЛЯ ДОСЛІДЖЕННЯ НА ПЛАТФОРМІ:

1. ДЕШИФРУВАЛЬНИК / ДЕШИФРУВАЛЬНИЦЯ.
2. АНАЛІТИК / АНАЛІТИКИНЯ.
3. ПРЕСОФІЦЕР / ПРЕСОФІЦЕРКА.


Watch video on YouTube
Error 153
Video player configuration error

(01:28-5:50)


Watch video on YouTube
Error 153
Video player configuration error

(13:37–19:17)

ОБОВ’ЯЗКИ ПРЕСОФІЦЕРА / ПРЕСОФІЦЕРКИ

1. Комунікація з журналістами / журналістками
2. Створення власного контенту
3. Ведення соціальних мереж
4. Інформаційний захист

СТАТТЯ «ЩО РОБИТЬ ПРЕСОФІЦЕР У ЗСУ?»