CyberLab
Комп'ютерна криміналістика

ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЦИФРОВОЇ ГІГІЄНИ

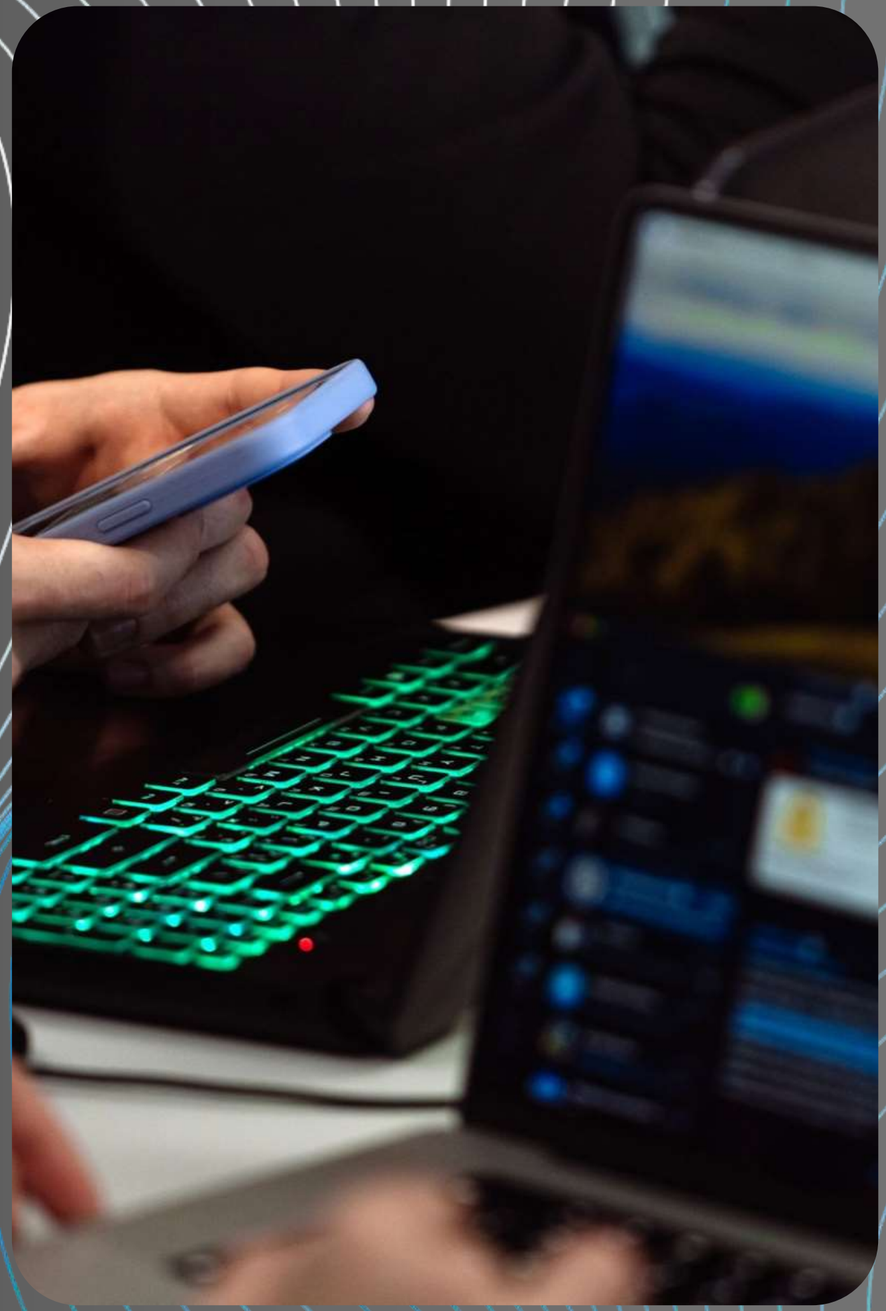
Лабораторія комп’ютерної криміналістики

F-7.5-1-

CyberLab
Комп'ютерна криміналістика

CyberLab

Єдина в Україні організація, що поєднує у своїй діяльності: впровадження систем управління інформаційною безпекою, участь у розслідуваннях кіберінцидентів, організацію навчання, проведення комп’ютерно–технічних експертиз та експертиз електронних комунікацій



Напрямки нашої діяльності

РОЗСЛІДУВАННЯ	Участь у розслідуваннях кіберінцидентів
ЕКСПЕРТИЗИ	Комп’ютерно–технічні експертизи та експертизи електронних комунікацій
БЕЗПЕКА	Впровадження систем управління інформаційною безпекою
НАВЧАННЯ	Популяризація кібербезпеки, проведення семінарів, тренінгів та практик стосовно цифрової криміналістики

CyberLab
Комп'ютерна криміналістика

Наші Досягнення

CyberLab активно займається популяризацією кібербезпеки та цифрової гігієни, організовує та приймає участь у різноманітних заходах, таких як конференції, семінари та тренінги

Спільні розробки CyberLab та SSG – ноутбук та захищений месенджер – стали переможцями на конкурсі Cybersecurity Startup Selection

Завдяки зусиллям CyberLab, вже впроваджені світові практики кібербезпеки в багатьох державних та недержавних організаціях

Реалії сьогодення

Від 24 лютого 2022 року інфраструктура інформаційно–комунікаційних технологій* (ІКТ) в Україні стала основним об’єктом атак, у тому числі кібератак.

Лише за 6 місяців повномасштабної війни зафіксовано 1 123 кібератаки, спрямованих на всі сектори економіки України, включно з ІТ та телекомунікаціями, що підтверджує, що кібератаки стали повноцінною складовою війни і є доповненням кінетичних дій.

Війна спричинила значні збитки та руйнування інфраструктури ІКТ у понад 10 із 24 регіонів України.

На відновлення телекомунікаційного сектору необхідно 1,79 млрд дол.

НАЙПОШИРЕНІШІ МЕТОДИ КІБЕРАТАК:	
	Збір інформації (напр. – фішинг)
	Шкідливі програмні засоби
	Втручання
	Порушення доступності (напр. – DDOS–атаки)
	Інше

* інфраструктура інформаційно–комунікаційних технологій (ІКТ) – комплекс програмно–технічних засобів, організаційних систем та нормативних баз, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток засобів інформаційної взаємодії та інформаційного простору країни

Фішинг як метод

ФІШИНГ – масова розсилка електронних листів з метою отримання «цінних» даних.

Типові питання та форми фішингових листів :

- імена користувачів і паролі (зокрема, пропозиція зміни паролю);
- форми для введення певної «цінної» інформації;
- ідентифікаційні номери;
- фінансова інформація (номери банківських рахунків, PIN–коди, номери банківських карток, дівоче прізвище матері, дата народження, інше);
- персональні дані: номер мобільного телефону, адреса проживання, місце роботи, сімейний стан, віросповідання, тощо.

ФІШИНГОВИЙ ЛИСТ, як правило, професійно замаскований

Фішинг як метод

Загрози фішингу :

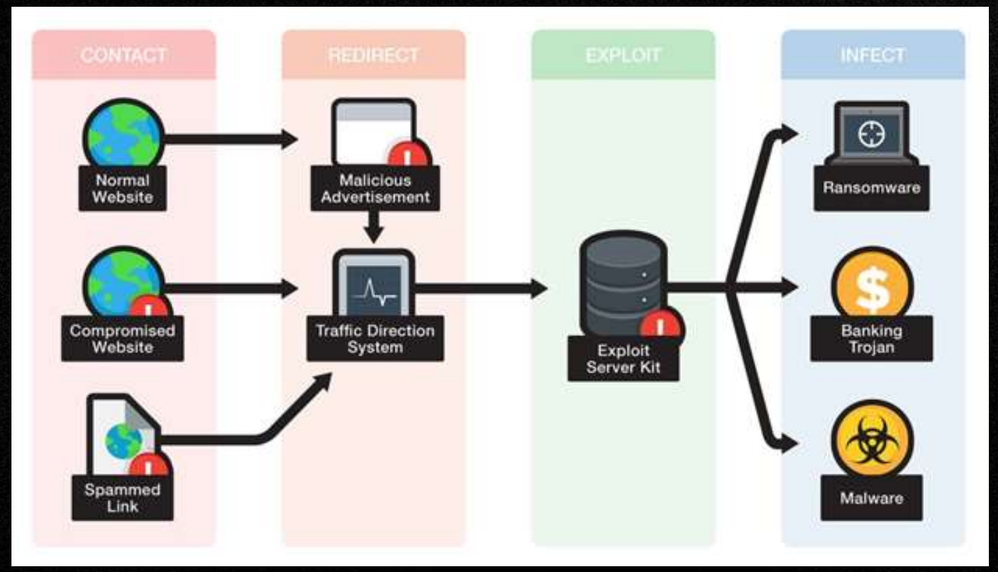
- Втрата контролю над електронною поштою (зловмисники постійно переглядають листи);
- Викрадення інформації стосовно авторизації;
- Втрата ВСІЄЇ інформації, яка міститься на комп’ютері;
- Маніпуляція з банківськими рахунками;
- Зловмисники отримують доступ до ВСЬОГО програмного забезпечення, що міститься на комп’ютері (бухгалтерські програми, месенджери, бази даних та ін.);
- Знищена чи змінена інформація.

Шкідливе програмне забезпечення (засоби), Malware– загальний термін для визначення різних форм програмного коду з деструктивними або небажаними функціями

Шкідливі програмні засоби

- Virus
- Trojan
- Worm
- Spyware
- Rootkit
- Ransomware
- Botnet
- Keylogger
- Bootkit
- Greyware
- Backdoor
- Adware
- Exploit
- Data stealer
- Logicbomb

Шкідливі програмні засоби

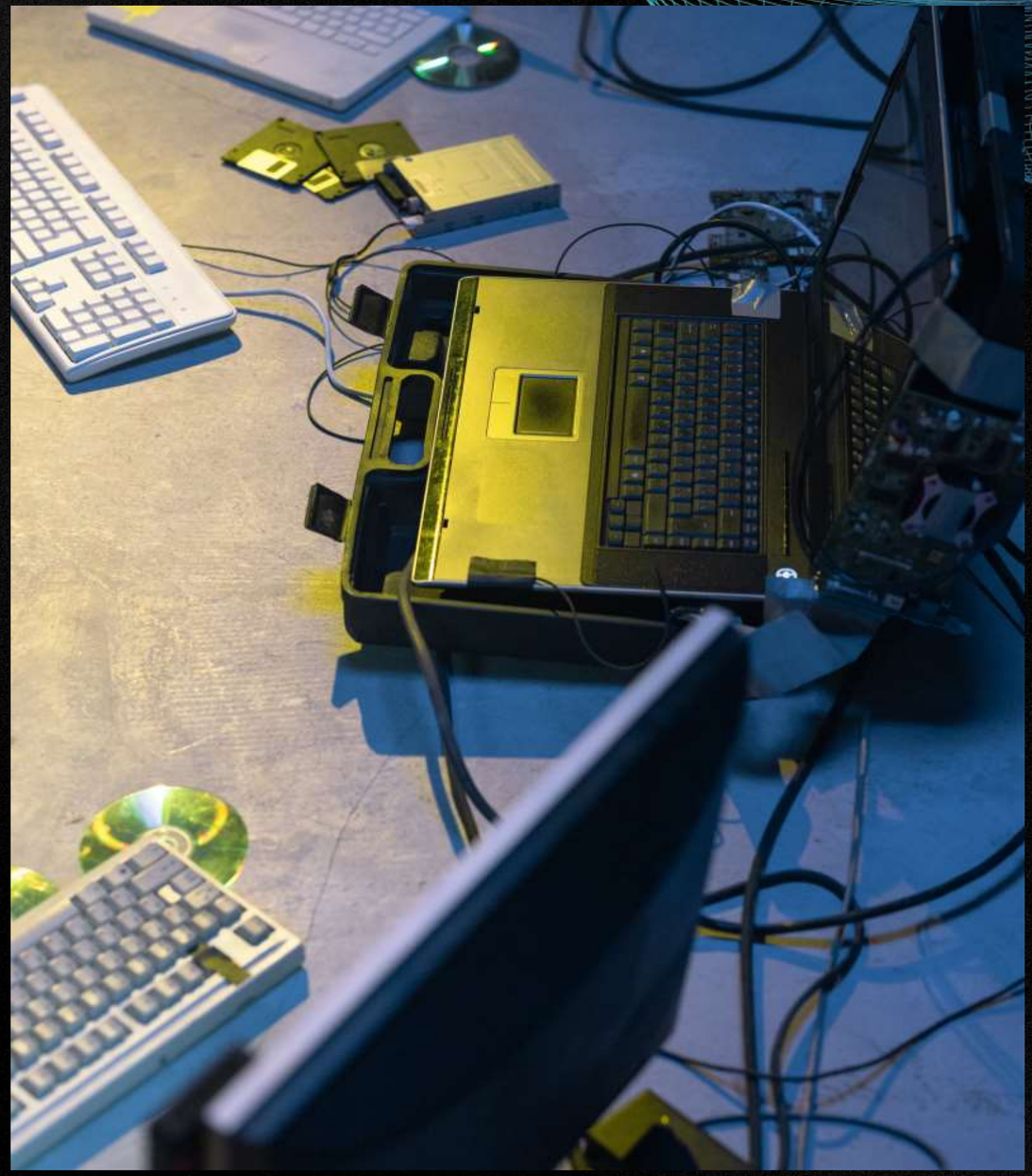


Способи поширення шкідливого програмного забезпечення:

- Фішинг, включаючи направлені атаки
- Атаки drive-by (сумнівні сайти)
- Експлойткіти (вразливості програмного забезпечення)
- USB накопичувачі та інші змінні носії
- Мережа (спільні ресурси, Wi-Fi)
- Ручне встановлення (RDP, VNC, Teamviewer,...)
- Через інші, в тому числі легальні, шкідливі продукти
- Сплановані атаки на веб-ресурси типу wateringhole (зараження онлайн-платформ)

Втручання

Несанкціоноване втручання в роботу електронно–обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ст. 361 КК України)

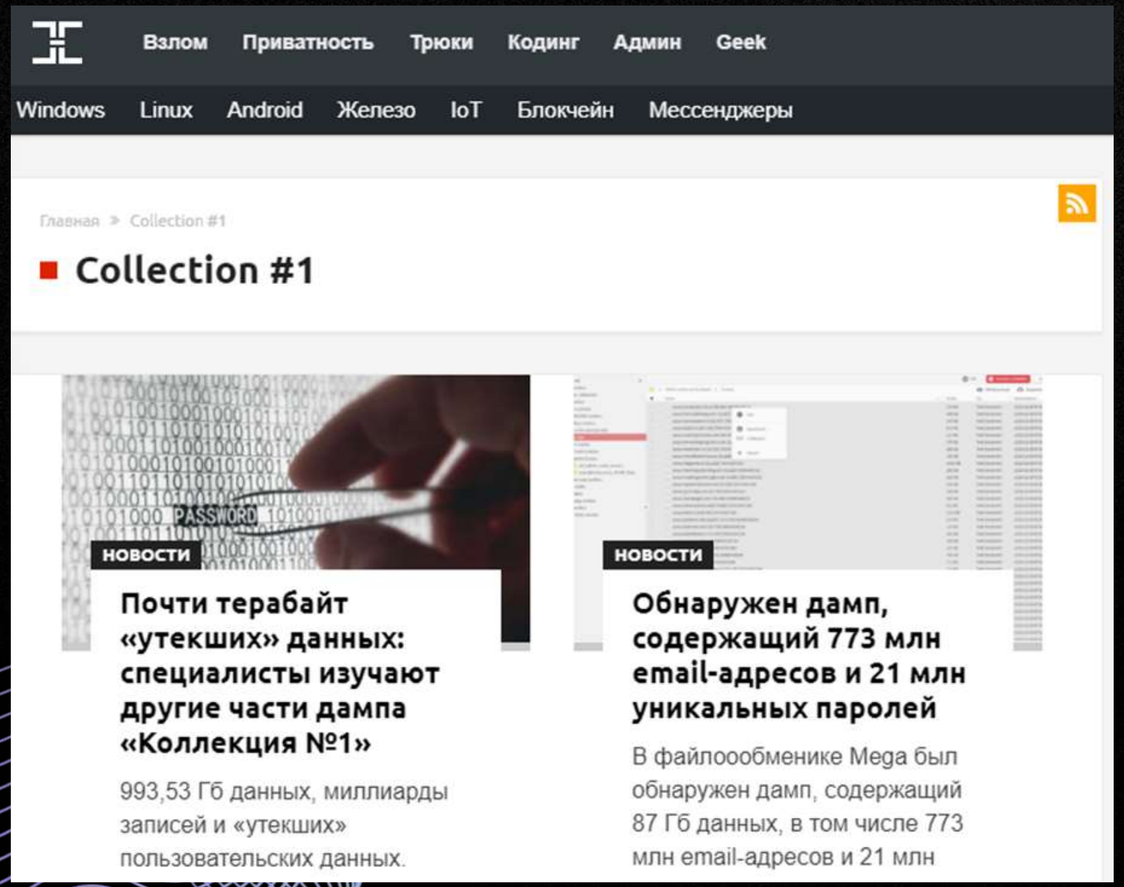


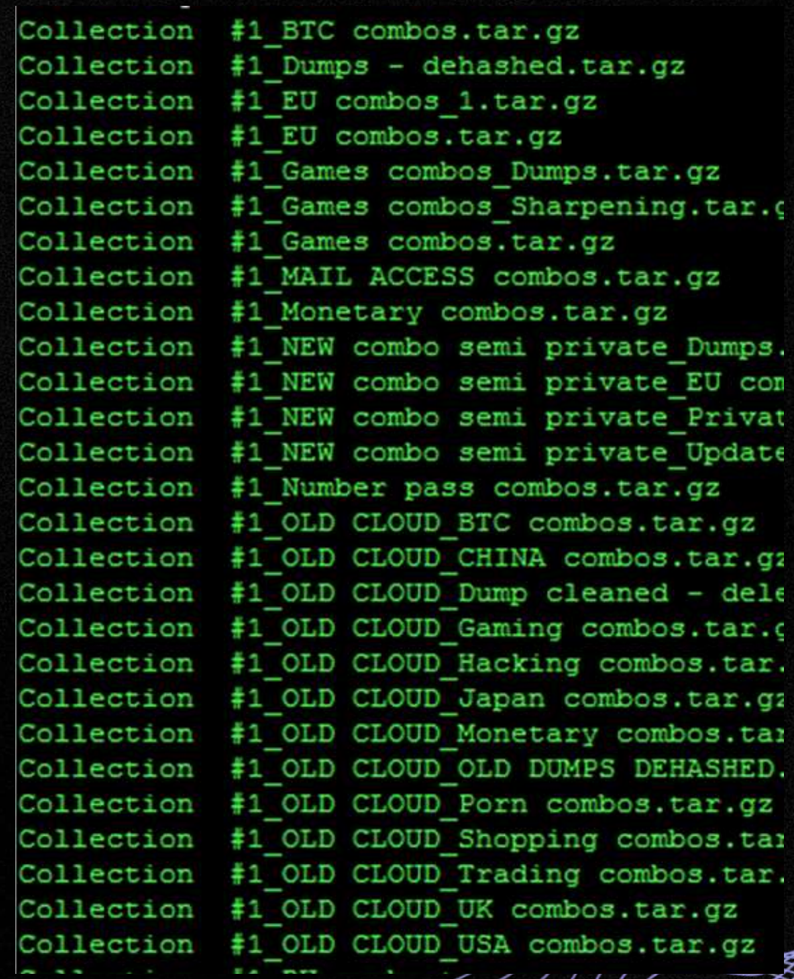
Інструменти для втручання

- витоки із зламаних сервісів
- використання ШПЗ
- брутфорс (підбір методом «грубої сили») паролей
- фішинг
- вразливості програмного забезпечення
- фізичний доступ
- використання спеціальних засобів
- Зловживання службовим становищем в розрізі Указа Президента України від 1 лютого 2022 року № 37/2022

Витоки із зламаних сервісів містять мільярди записів «логін–пароль»

Підбирати пароль не потрібно: все вже зламано до нас!

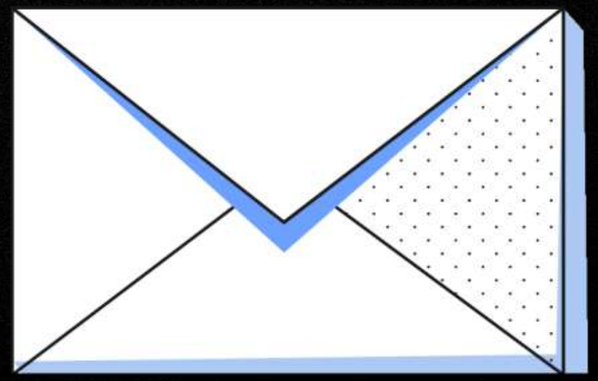




Основні цілі кібератак

- Електронна пошта, в тому числі Хмарні сховища;
- Мобільні пристрої;
- Комп’ютерна техніка, сервери;
- Комп’ютерні мережі, в тому числі і бездротові мережі Wi–Fi;
- Засоби відеоспостереження.

Електронна пошта



Способи зламу:

- брутфорс (підбір методом «грубої сили») паролей;
- дані витоків;
- соціальна інженерія;
- фішинг;
- шкідливе програмне забезпечення;
- локальні мережі та бездротові мережі Wi–Fi;
- фізичний доступ.

Складність паролю

Підбір паролів на сучасному обладнанні

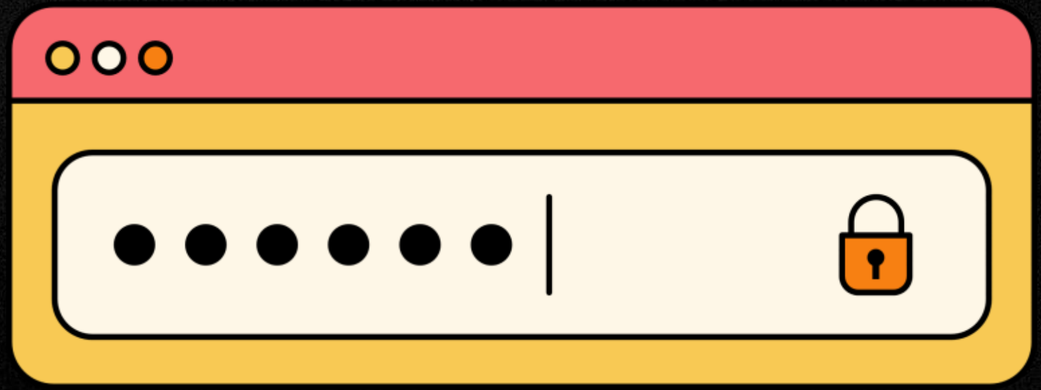
Довжина менше 8 символів – хвилини
Довжина 8 символів – максимум 2 години
Довжина 9–10 символів – дні і тижні

На сьогодні мінімальна довжина паролю
повинна бути **12** або більше символів

Потрібно змінювати паролі щонайменше
раз на три місяці

Для запам'ятовування – використання парольних фраз

Використання менеджерів паролів



Електронна пошта – рекомендації

Мінімізація ризиків:

постійна зміна паролей (бажано раз на три місяці);

двофакторна автентифікація (при наявності);

використання «складних» паролей;

різні паролі від різних сервісів;

заборонено повідомляти свій пароль «стороннім» особам;

не зберігати пароль у відкритому доступі (на клаптику папері чи у файлі на комп’ютері. Бажано не зберігати у браузері);

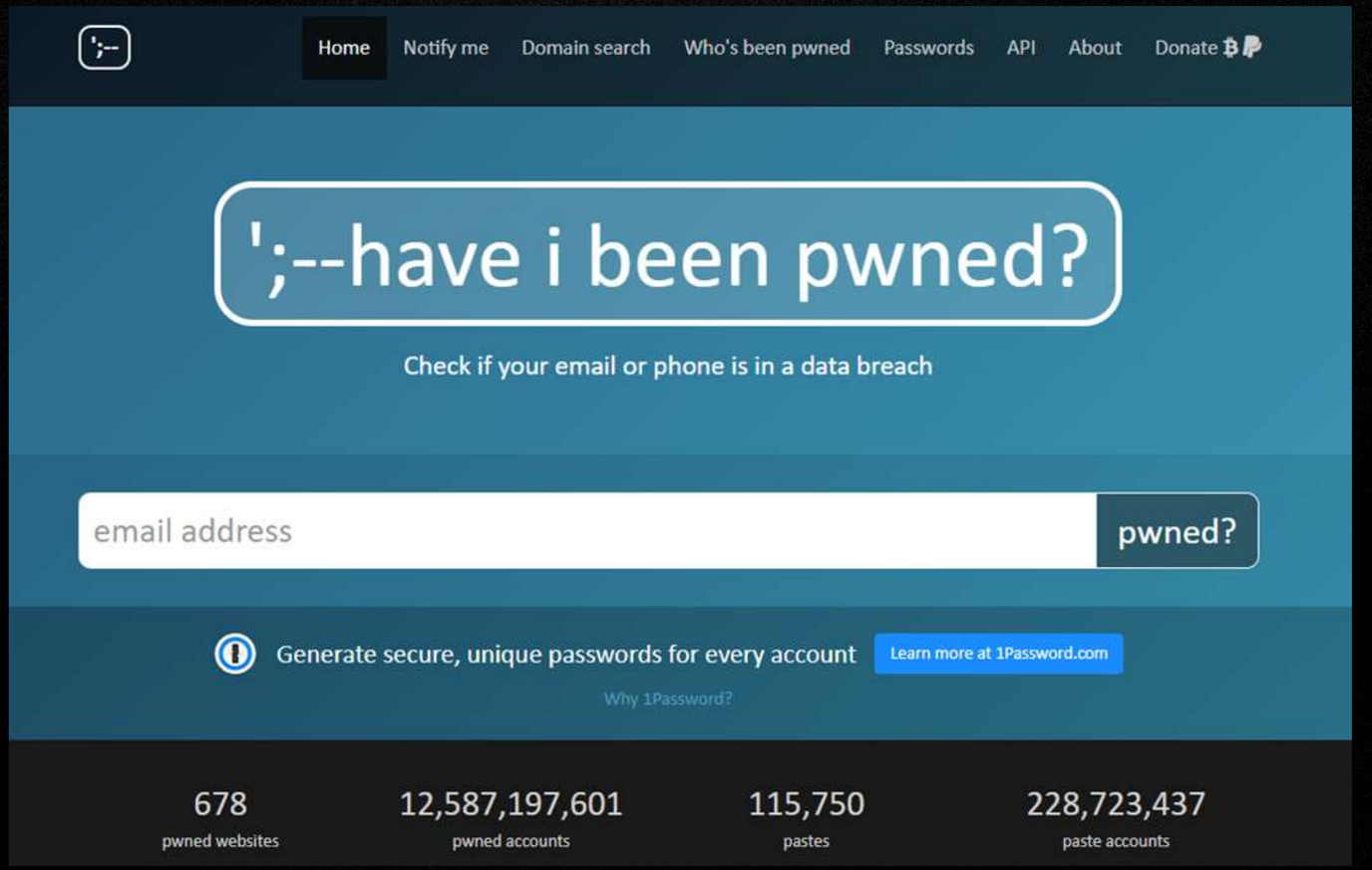
постійно перевіряти комп’ютерну техніку на наявність/відсутність ШПЗ;

шкідливе програмне забезпечення;

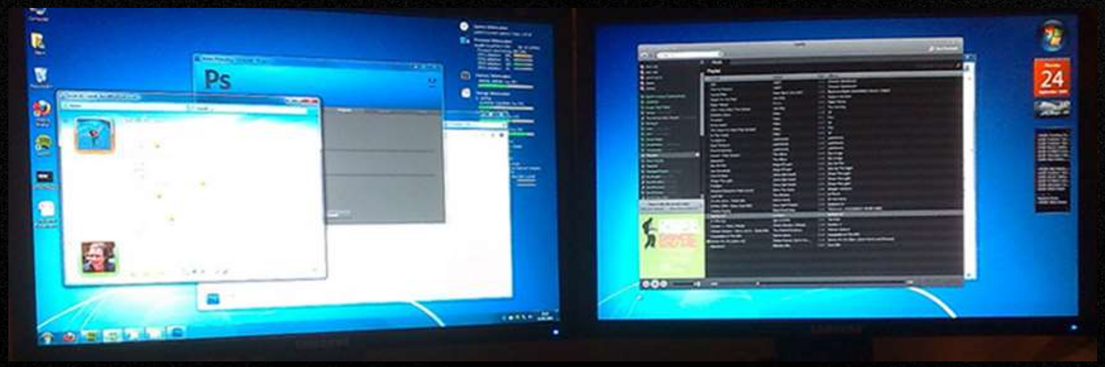
встановити пароль на доступ до операційної системи.

Перевірка компрометації

https://haveibeenpwned.com/



Несанкціонований доступ до комп’ютера. Результати розслідування



Віддалене керування комп'ютером

Хакер має повний доступ до комп'ютера:

- встановлює необхідні програми для моніторингу дій користувача (кейлоггер та ін.)
- вивчає режим роботи користувача та слідкує за його діями
- встановлює програми для емуляції апаратного ключа (фактично «копія» ключа підключена до комп'ютера хакера)
- має можливість прихованої роботи одночасно з користувачем в паралельній сесії

Комп’ютерна техніка, сервери

Дії користувача на мінімізацію ризику:

обов’язкова наявність антивірусного програмного забезпечення;

цифрова гігієна в мережі Інтернет;

пароль на доступ до операційної системи;

використання ліцензійного програмного забезпечення;

заборона завантаження програмного забезпечення з сумнівних сайтів чи через Торенти;

рекомендовано не зберігати паролі в браузері;

встановлення необхідності зберігання критичної інформації

Мобільний пристрій – персональний комп’ютер

Операційні системи мобільних пристроїв:

- Android
- IOS
- ОС Windows
- Blackberry OS
- інші

Що зберігає мобільний телефон

Дії користувача на мінімізацію ризику:

Телефонна книга

Архів дзвінків

Переписка (повідомлення)

Фото– відеозображення

Додатки, в тому числі месенджери

Логіни та паролі

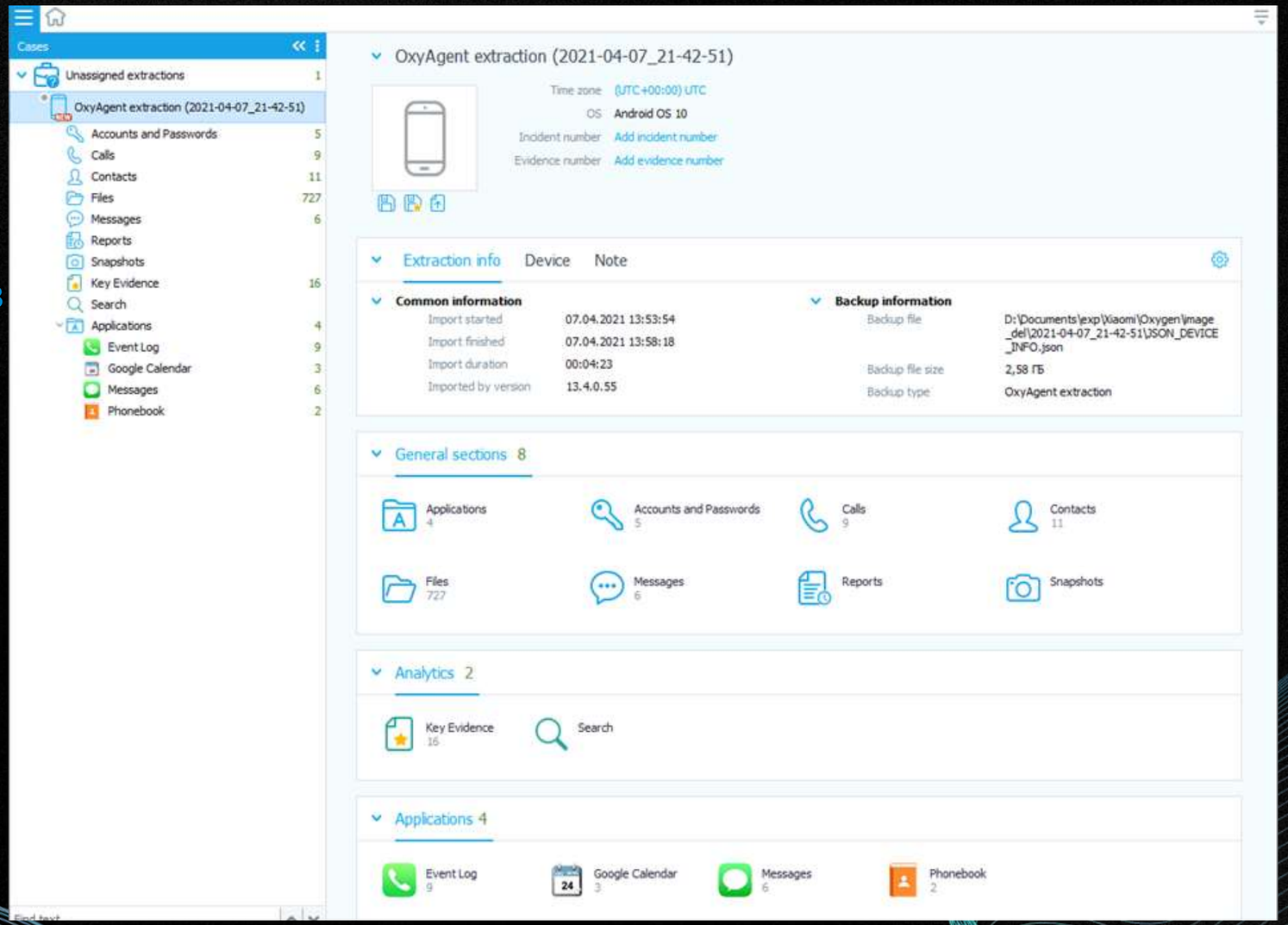
Геолокація пристрою

Доступ до віддалених сервісів (розумний дім, системи відеонагляду, тощо

Електронна пошта

Що зберігає мобільний телефон

Типовий набір вилучених даних з мобільного телефону

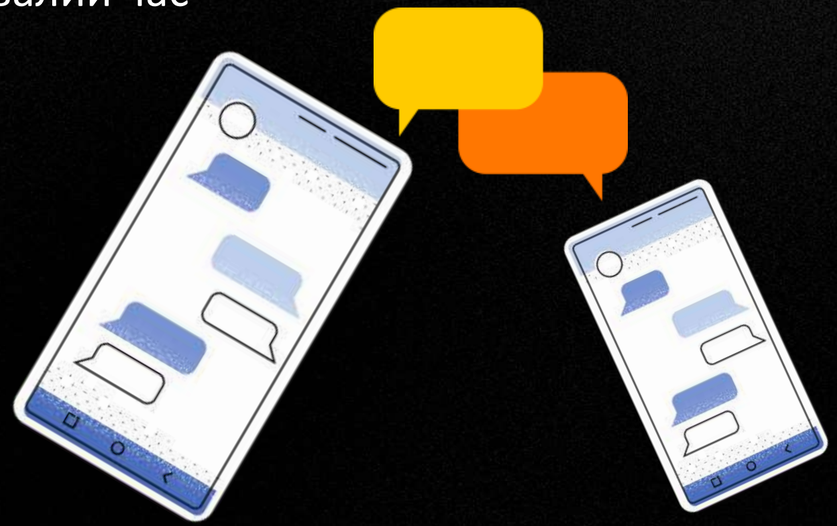


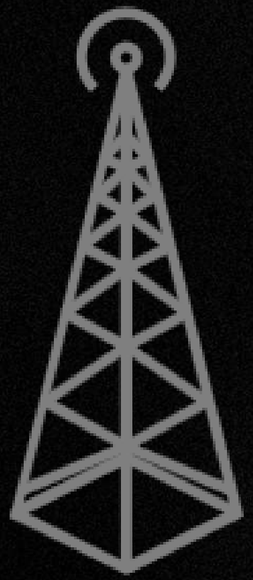
Мобільний зв’язок

Оператор має повний доступ до голосових дзвінків та SMS–повідомлень

На запит правоохоронних органів, надається інформація про абонента

Інформація про абонента зберігається у оператора тривалий час





Обмежте себе у «вирішенні питань» через GSM–зв’язок

Не пишіть сумнівних повідомлень

НЕ ДОКУМЕНТУЙТЕ СЕБЕ

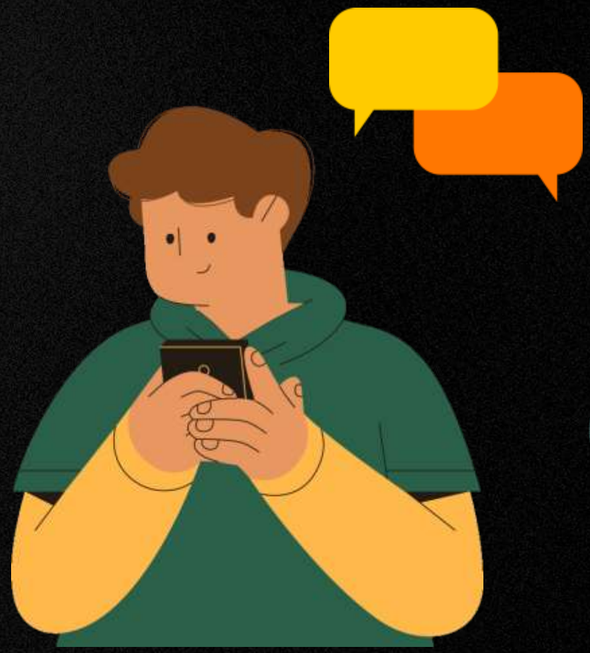
Захищений зв’язок

Інтернет зв’язок

Використання захищених VPN підключень

Обмежене використання публічного Wi-Fi

Власні Wi-Fi точки для спілкування



Мобільний зв’язок

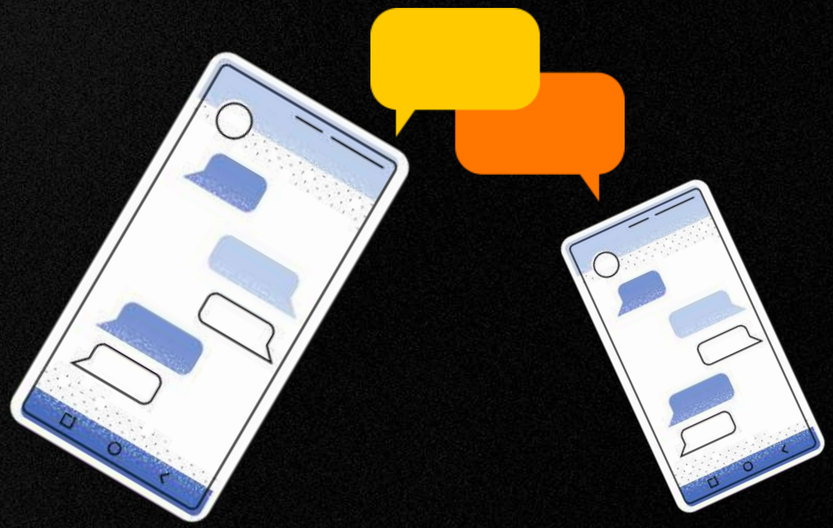
Окремі мобільні пристрої

Контроль історії переписки

Використання псевдонімів, а не номерів телефону

Обов'язково:
шифрування каналів зв'язку
приховування місця розташування

Програми для обміну повідомленнями



Типовий месенджер:

Дані на клієнтах в НЕ шифрованому вигляді (або наявний ключ дешифрування)

Можливий доступ до даних на сервері (розробник має ключі дешифрування)

Канал зв'язку використовує шифрування

Більш захищені месенджери

Signal

Threema

Wickr

Особливості

Легка ідентифікація абонента

Можливість встановлення геолокації

Легке відновлення «видалених» даних

Захист даних майже відсутній

Програми обміну повідомленнями

Інші способи отримання доступу

Зняття інформації з транспортних телекомунікаційних мереж

Ухвала про тимчасовий доступ

Отримання доступу до токенів авторизації

Маніпуляції з SIM-картками

Фізичне втручання

Перевіряйте інформацію яку зберігаєте

Сторонні додатки

ЗАГРОЗИ

Доступ до даних

Викрадення інформації

Віддалене приховане керування

Стеження

Знищення інформації

Сторонні додатки

Захисти себе сам

не встановлюй невідомих додатків

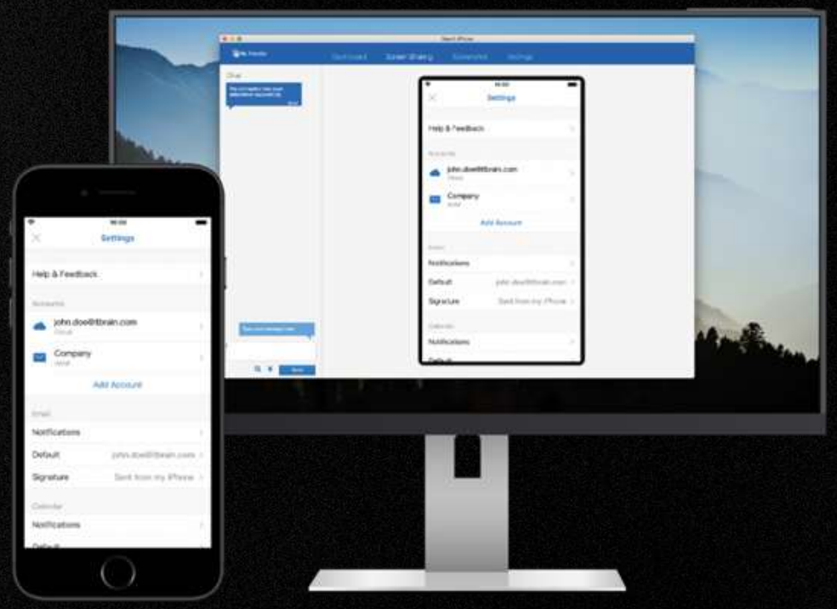
не дозволяй додатку мати доступ до «ВСІЄЇ» інформації

перевіряй свої додатки

дій негайно, якщо «Глючить»

Функціонал додатку може змінитися будь–якої миті – злочинці чекають на твою недбалість

Повний доступ



Можливості «Хакера» при повному доступі:

Перегляд та копіювання інформації з пристрою

Віддалене керування сервісами (розумний дім, відеонагляд, охоронна сигналізація, тощо)

Викрадення паролів від сервісів, електронних скриньок, сторінок соціальних мереж, тощо

Керування банківськими рахунками через відповідні додатки

Стеження за користувачем

Створення «копій» месенджерів на своїх пристроях

Видалення чи видозміна інформації

Повний доступ

Дії користувача на мінімізацію ризику стороннього доступу до мобільного пристрою:

Періодичний перегляд налаштувань месенджерів щодо сторонніх «прив’язаних» пристроїв

Постійне (за умови наявності) оновлення операційної системи

Постійний контроль транзакцій по банківських рахунках

По можливості періодично створювати копію пам’яті пристрою (Backup)

Періодична зміна паролів

Періодична «чистка» сторонніх додатків

Фізичні загрози

Викрадення

«Підглядання»

Знищення

Фізичний доступ

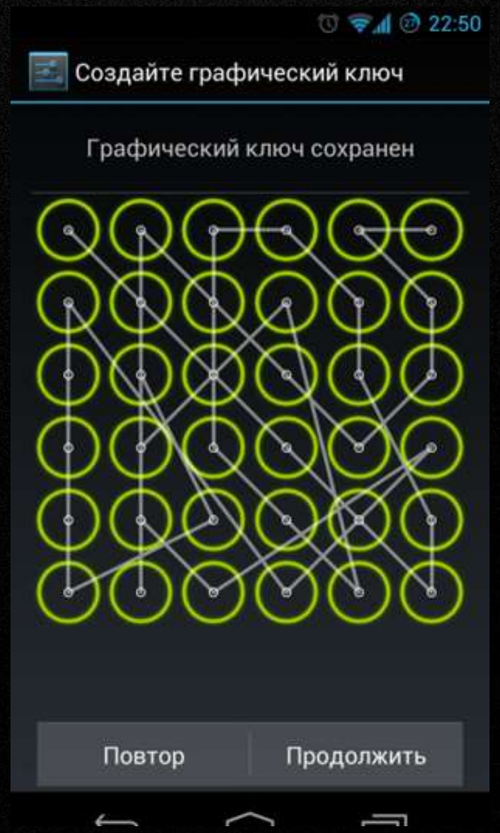
Підбір паролю

Халатність

Фізичні загрози

Поляризаційне скло

Складні паролі



Не залишайте без нагляду

Бездротові мережі Wi–Fi

Ризики бездротових мереж **Wi–Fi**

Перехоплення трафіку

Втрата даних

Встановлення «стороннього» програмного забезпечення

Доступ до пам’яті мобільного пристрою

Знищення інформації

Керування пристроєм (увімкнення камери, мікрофону)

Бездротові мережі Wi–Fi

БАЗОВІ ЗАСТЕРЕЖЕННЯ

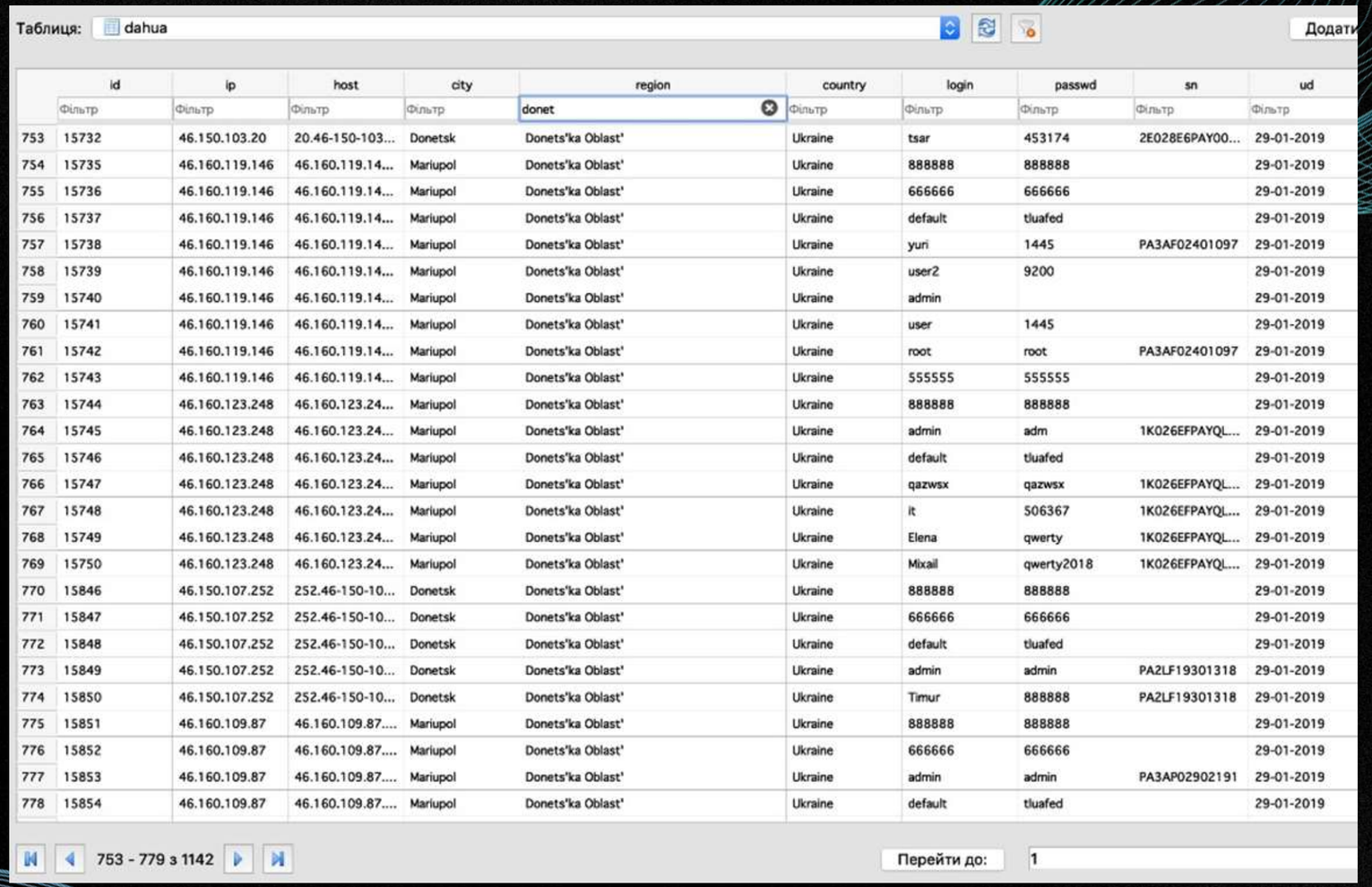
НЕ РЕКОМЕНДУЄТЬСЯ під’єднуватися до публічних (відкритих) мереж Wi–Fi

НЕ РЕКОМЕНДУЄТЬСЯ завантажувати та встановлювати додатки, що пропонує Wi–Fi мережа

Бездротовий зв’язок ідентичний дротовому, тому Ви повністю не захищені від втрати даних

Засоби відеоспостереження

Стежимо за собою



	id	ip	host	city	region	country	login	passwd	sn	ud
	Фільтр	Фільтр	Фільтр	Фільтр	donet	Фільтр	Фільтр	Фільтр	Фільтр	Фільтр
753	15732	46.150.103.20	20.46-150-103...	Donetsk	Donets'ka Oblast'	Ukraine	tsar	453174	2E028E6PAY00...	29-01-2019
754	15735	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	888888	888888		29-01-2019
755	15736	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	666666	666666		29-01-2019
756	15737	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	default	tluafed		29-01-2019
757	15738	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	yuri	1445	PA3AF02401097	29-01-2019
758	15739	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	user2	9200		29-01-2019
759	15740	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	admin			29-01-2019
760	15741	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	user	1445		29-01-2019
761	15742	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	root	root	PA3AF02401097	29-01-2019
762	15743	46.160.119.146	46.160.119.14...	Mariupol	Donets'ka Oblast'	Ukraine	555555	555555		29-01-2019
763	15744	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	888888	888888		29-01-2019
764	15745	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	admin	adm	1K026EFPAYQL...	29-01-2019
765	15746	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	default	tluafed		29-01-2019
766	15747	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	qazwsx	qazwsx	1K026EFPAYQL...	29-01-2019
767	15748	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	it	506367	1K026EFPAYQL...	29-01-2019
768	15749	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	Elena	qwerty	1K026EFPAYQL...	29-01-2019
769	15750	46.160.123.248	46.160.123.24...	Mariupol	Donets'ka Oblast'	Ukraine	Mixail	qwerty2018	1K026EFPAYQL...	29-01-2019
770	15846	46.150.107.252	252.46-150-10...	Donetsk	Donets'ka Oblast'	Ukraine	888888	888888		29-01-2019
771	15847	46.150.107.252	252.46-150-10...	Donetsk	Donets'ka Oblast'	Ukraine	666666	666666		29-01-2019
772	15848	46.150.107.252	252.46-150-10...	Donetsk	Donets'ka Oblast'	Ukraine	default	tluafed		29-01-2019
773	15849	46.150.107.252	252.46-150-10...	Donetsk	Donets'ka Oblast'	Ukraine	admin	admin	PA2LF19301318	29-01-2019
774	15850	46.150.107.252	252.46-150-10...	Donetsk	Donets'ka Oblast'	Ukraine	Timur	888888	PA2LF19301318	29-01-2019
775	15851	46.160.109.87	46.160.109.87....	Mariupol	Donets'ka Oblast'	Ukraine	888888	888888		29-01-2019
776	15852	46.160.109.87	46.160.109.87....	Mariupol	Donets'ka Oblast'	Ukraine	666666	666666		29-01-2019
777	15853	46.160.109.87	46.160.109.87....	Mariupol	Donets'ka Oblast'	Ukraine	admin	admin	PA3AP02902191	29-01-2019
778	15854	46.160.109.87	46.160.109.87....	Mariupol	Donets'ka Oblast'	Ukraine	default	tluafed		29-01-2019

CyberLab
Комп'ютерна криміналістика

ОСНОВНІ ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лабораторія комп’ютерної криміналістики

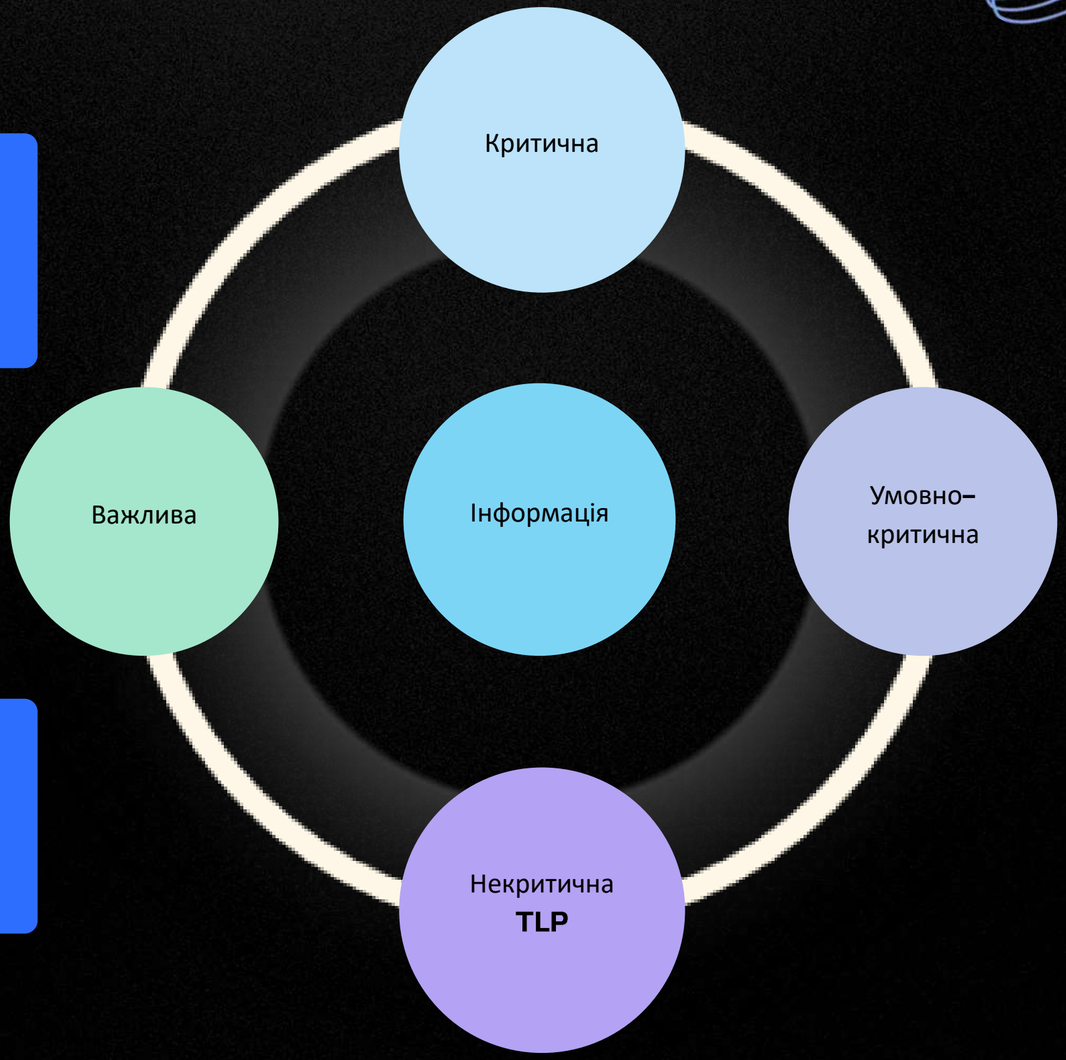
F-7.5-1-

TLP:AMBER

Інформація

Не для поширення
Призначена для обмеженого кола користувачів

Поширюється між організацією і потенційними партнерами/клієнтами



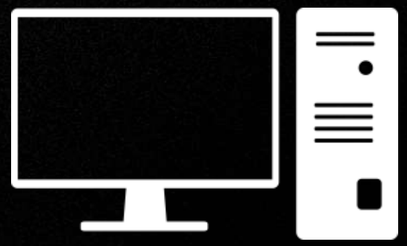
Поширюється тільки в середині організації

Необмежене поширення включаючи ЗМІ, Інтернет чи соціальні мережі

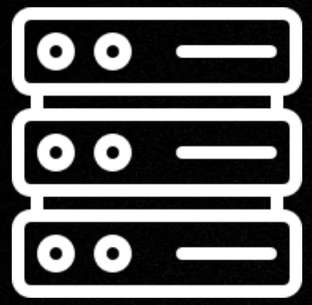
Встановлення критичності інформації невід’ємна частина інформаційної безпеки

Типова схема розміщення інформації

Домашній комп’ютер користувача



Робочий комп’ютер користувача



Сервер компанії

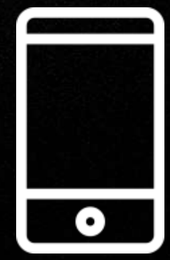
Інтернет

Хмарні сховища

Віддалені ресурси

Електронна пошта

Користувач



Мобільні пристрої

За збереження інформації відповідальність несе користувач

Організація безпеки

Документування системи управління інформаційної безпеки;

Безпека людських ресурсів;

Керування ресурсами;

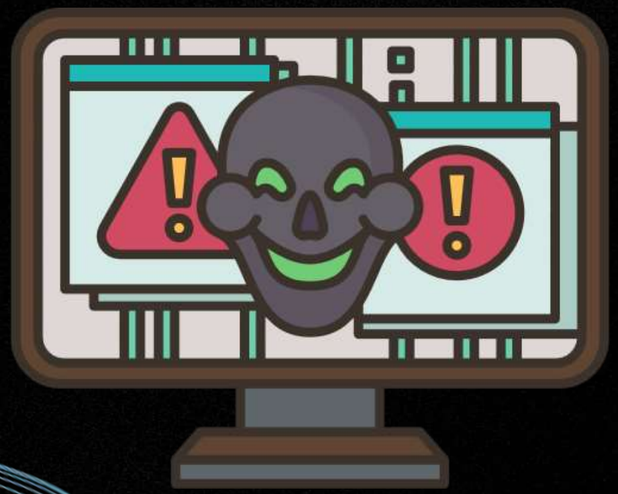
Організація доступу до інформації, включаючи і віддалену роботу;

Фізична безпека;

Правило «чистого столу»;

Політика паролів;

Навчання.



Основні рекомендації керуванням ризикми

Легалізація «цифрових» активів;

Створення резервних копій;

Розподілення обов’язків персоналу (включаючи відповідальність);

Встановлення правил «Цифрової гігієни».

Реагування на інцидент

Зупинку інциденту (якщо він продовжується);

Фіксація подій;

Аналіз критичності інциденту;

Збір доказів;

Підготовка доказів до передачі в правоохоронні органи.

У РАЗІ ВИЯВЛЕННЯ ІНЦИДЕНТУ – НЕГАЙНО ПОВІДОМЛЯЙТЕ ВІДПОВІДНІ ОРГАНИ

Нештатні ситуації

У РАЗІ ВИНИКНЕННЯ НЕШТАТНИХ СИТУАЦІЙ– НЕ ПАНІКУЙТЕ

ПЕРШОЧЕРГОВІ ДІЇ:

Вимкнути комп’ютерну техніку;

По–можливості, забрати з собою цінні речі (ноутбуки, мобільні пристрої) та залишити приміщення;

Повідомити вище керівництво;

Викликати захисника (адвоката);

Уважно прочитати документи, на основі яких завітали «небажані гості»;

Не давати необдуманих пояснень (посилаючись на ст. 63 Конституції України);

Фіксація дій «небажаних гостей».

ПРИСУТНІСТЬ АДВОКАТА – ВИМОГА ЗАКОНУ

Висновки

Всі користувачі мають займатися інформаційною безпекою на своєму рівні. Не повинно бути користувачів кого це не стосується.

Основа вимога – постійне навчання та перевірка знань користувачів. Нажаль найслабша ланка в системі інформаційної безпеки – це люди.

В інформаційній безпеці, немає неважливих питань

Питання?