Кібербезпека в державному секторі: ризики та захист

Богдан Демченко
Департамент інформаційно-аналітичної підтримки Національної поліції України

Віталій Носов
Харківський національний університет внутрішніх справ

Зміст

- Державний сектор і кібербезпека
- Актуальні типи кіберзагроз та захист від них
- Шкідливе програмне забезпечення
- Безпека мобільних пристроїв

Державний сектор

- Органи державної влади
- Бюджетні установи
- Державні підприємства
- Фонди та банки

Кіберпростір

- середовище для здійснення комунікацій

- утворене системами і мережами передачі даних

Що загрожує?

- агресія рф проти України у кіберпросторі
- кіберзлочинність
- кібершпигунство
- кібертероризм

Кібератаки на державні органи України: Основні загрози

- **APT28 (Fancy Bear)** - спеціалізуються на кібершпигунстві та складних атаках, спрямованих на урядові, військові та оборонні структури, ГРУ рф
- **Gamaredon (Armageddon)** - є одним з найактивніших угруповань, що діють проти України, асоційовані з ФСБ рф
- **UAC-0056** - часто використовують скомпрометовані облікові записи державних службовців для розсилки шкідливих листів
- **Sandworm** - відомі своїми руйнівними кібероперaціями, спрямованими на критичну інфраструктуру, асоційовані з ГРУ рф.

Кібербезпека

- захищеність під час використання кіберпростору забезпечуються через:
  - сталий розвиток інформаційного суспільства
  - виявлення, запобігання і нейтралізація загроз у кіберпросторі

Забезпечення кібербезпеки

- використання кіберпростору →
- загрози → ризики →

процес зниження ризиків

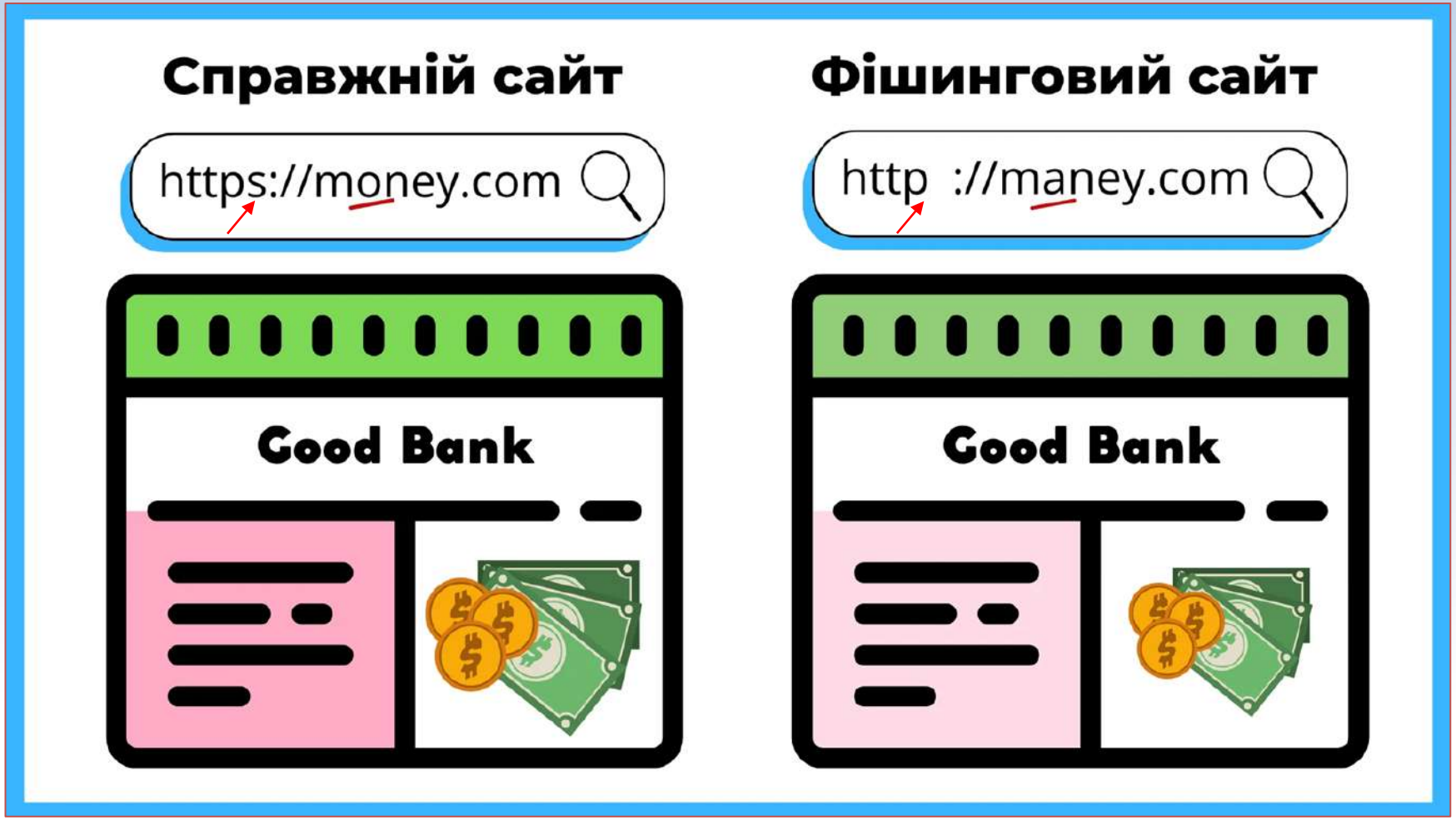
Соціальна інженерія

- спонукання користувача
  - повідомити зловмиснику певну інформацію,
  - щось зробити,
- що дозволить зловмиснику далі отримати доступ до інформаційних ресурсів

Фішинг

https://www.valimail.com/resources/guides/guide-to-phishing/

Фішинг



https://cityhost.ua/uk/blog/fishing-kak-ne-popastsya-na-ulovki-moshennikov-i-raspoznat-poddelnyy-sayt.html

Що можуть пропонувати?

- безкоштовні програми
- обхід захисту платних програм
- завантаження ДУЖЕ потрібного файлу
- «підтвердити» дані облікового запису або номеру платіжної карти
- продаж ДУЖЕ дешево дорогих товарів
- роботу
- ….

Ознаки фішингового листа

Адреса відправника не збігається з офіційною

Створення відчуття терміновості та погрози

Загальні та безособові звертання

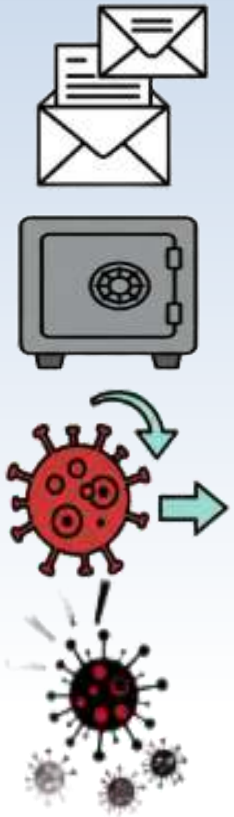
Граматичні помилки, одруківки та дивний стиль

Підозрілі посилання, що ведуть на підроблені сайти

Найпоширеніший вид атаки на державні органи України

Атака відбувається не напряму, а через ланцюжок дій, де головна мета — змусити співробітника **самостійно** завантажити та запустити шкідливий файл

Схема доставки вірусу:



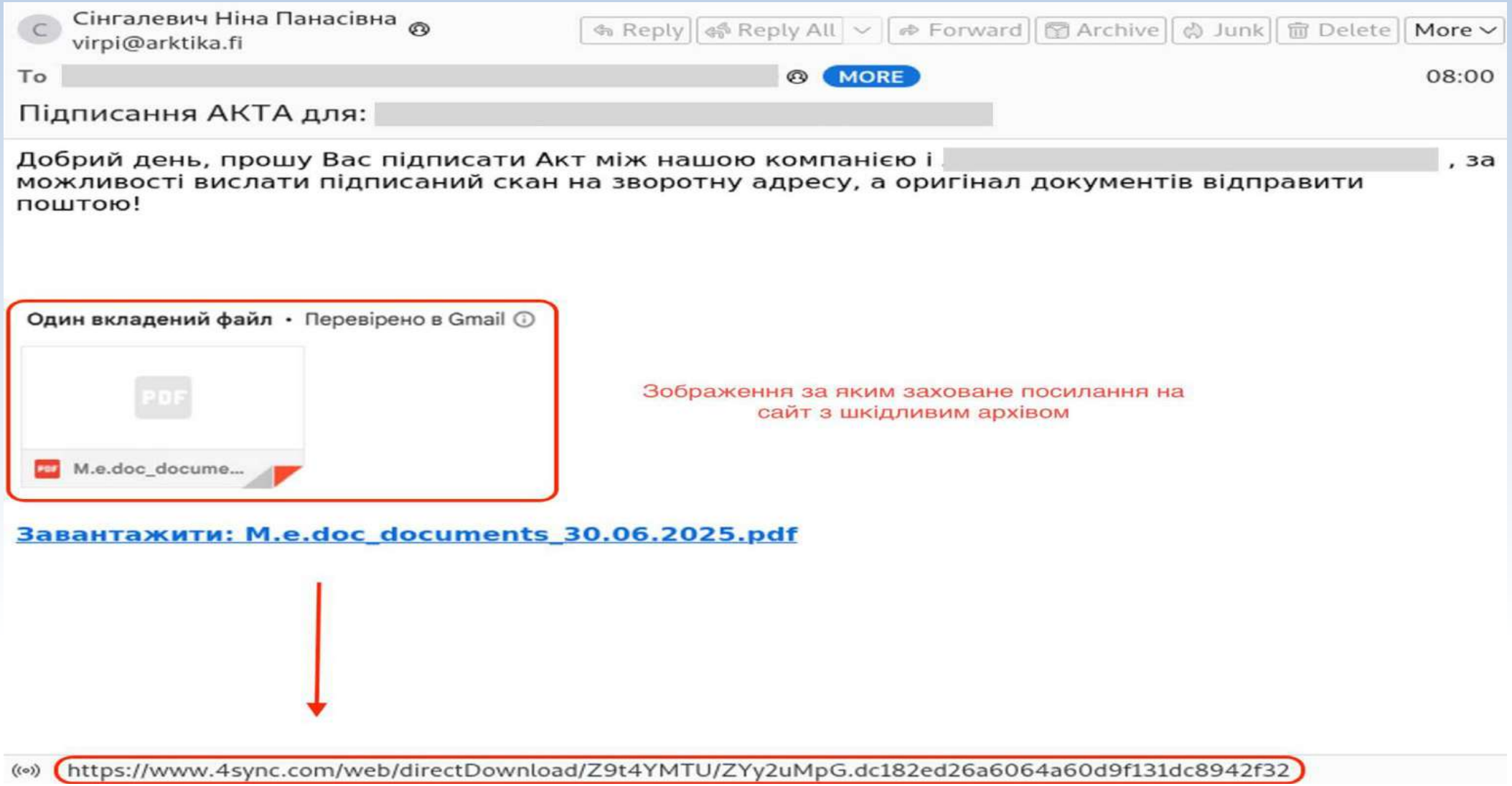
Приманка: Легітимний лист

"Контейнер": Безпечний на перший погляд

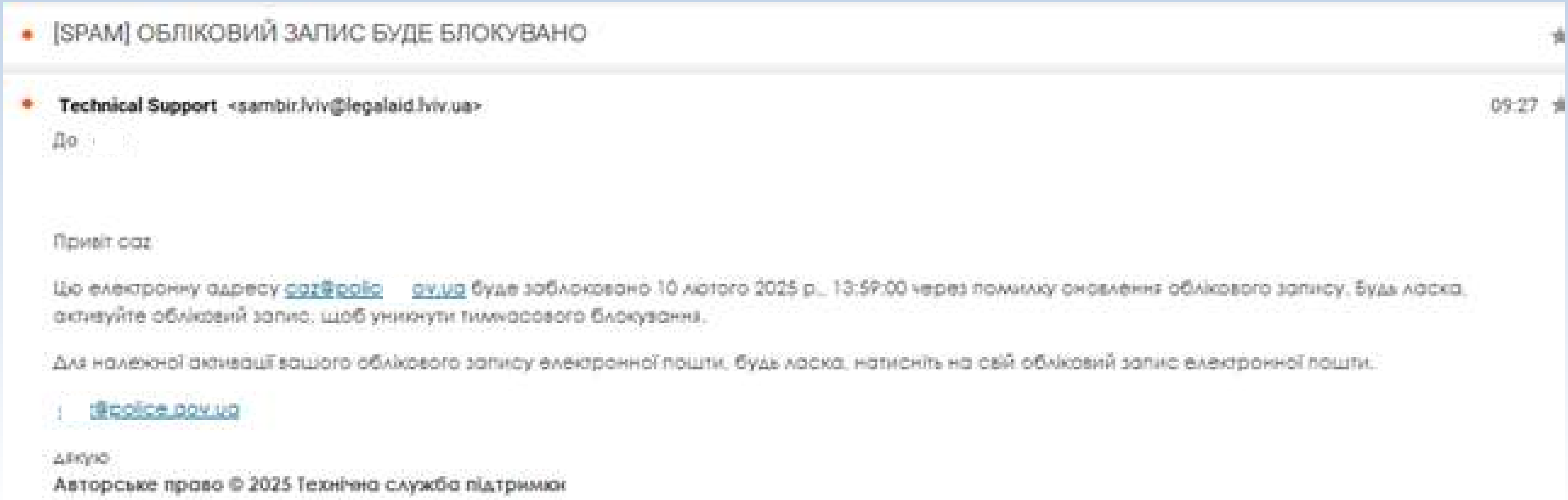
Ключовий момент: Перенаправлення

Зараження: Фінальний крок

Найпоширеніший вид атаки на державні органи України



Найпоширеніший вид атаки на державні органи України



[SPAM] ОБЛІКОВИЙ ЗАПИС БУДЕ БЛОКУВАНО

Technical Support <sambir.lviv@legalaid.lviv.ua> 09:27

До

Привіт cat

Що електронну адресу cat@police gov.ua буде заблоковано 10 лютого 2025 р., 13:59:00 через помилку оновлення облікового запису. Будь ласка, активуйте обліковий запис, щоб уникнути тимчасового блокування.

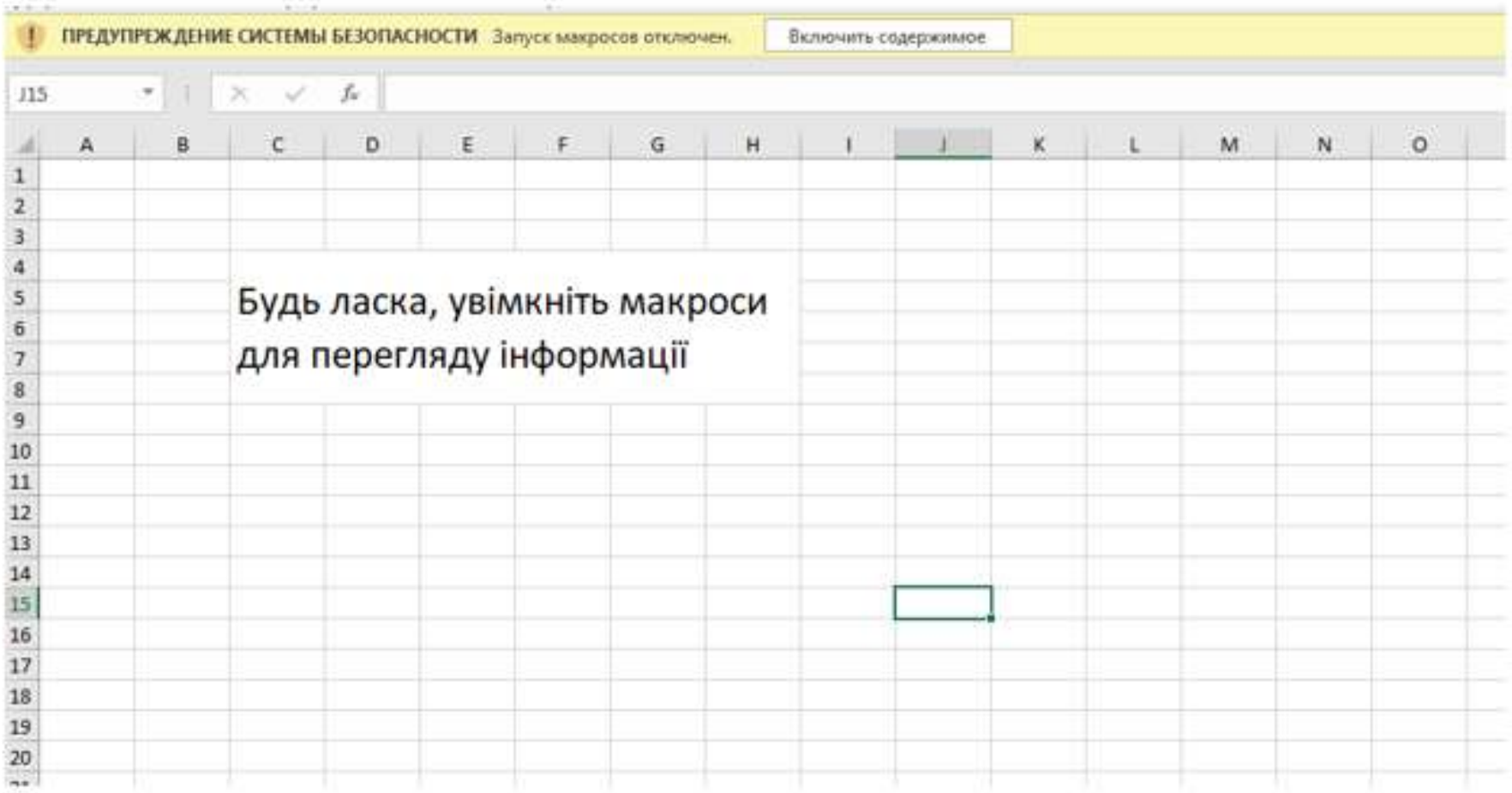
Для належної активації вашого облікового запису електронної пошти, будь ласка, натисніть на свій обліковий запис електронної пошти.

: @police.gov.ua

дякую

Авторське право © 2025 Технічна служба підтримки

Найпоширеніший вид атаки на державні органи України



Що робити при отриманні фішингового листа

Не взаємодіяти. Не переходити за посиланнями, не відкривати файли та не відповідати на лист.

Позначити як «Спам/Фішинг». Використовувати відповідну кнопку у вашому поштовому сервісі.

Повідомляти. Якщо лист прийшов на робочу пошту, обов'язково повідомляти вашу IT-службу або відділ безпеки.

Видаляти. Повністю видаляти лист з поштової скриньки.

Що робити при отриманні фішингового листа

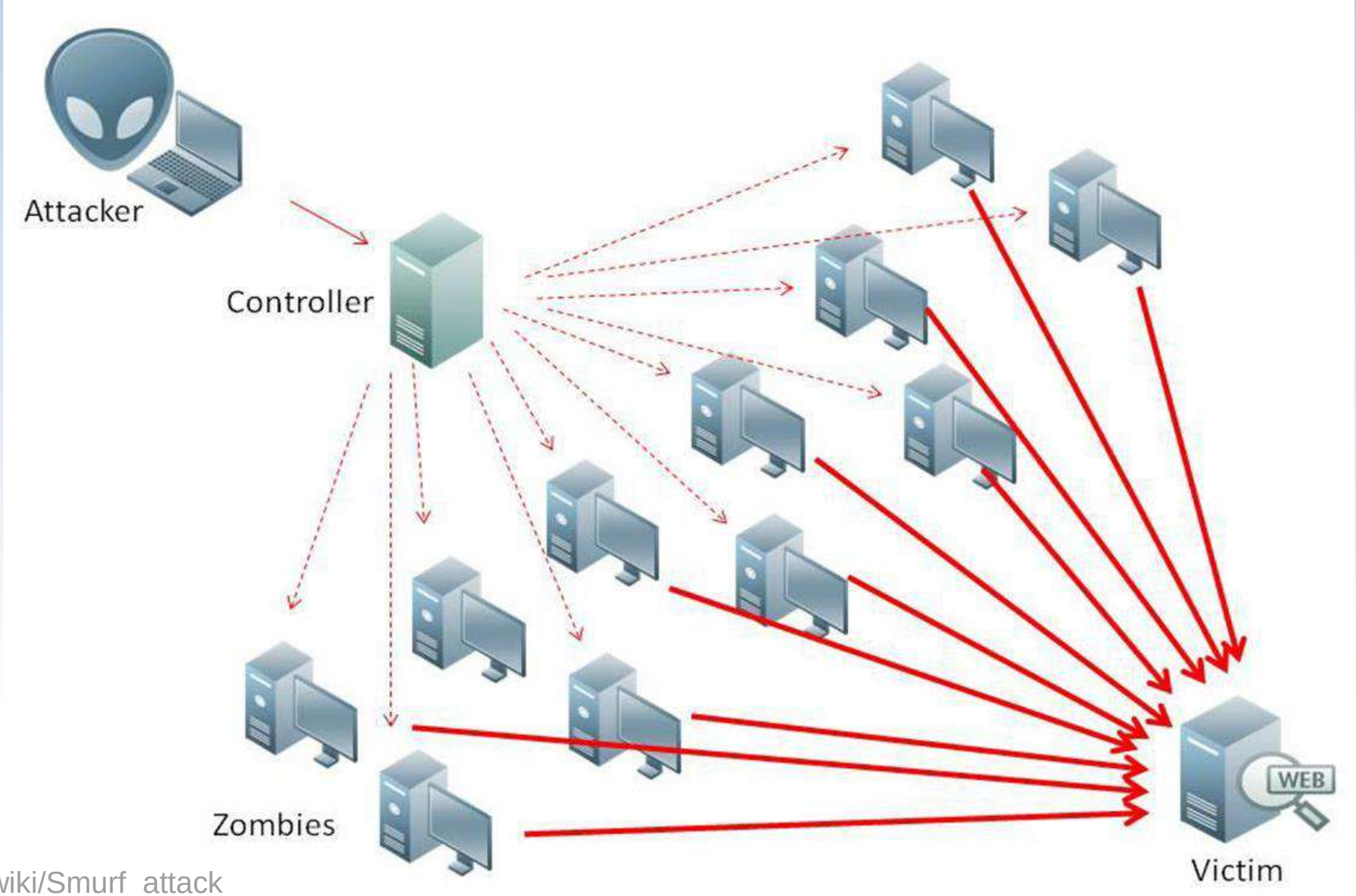
Проявляйте "здорову" підозрілість

Перевіряйте, не натискаючи

Увага до завантажених файлів

Підтверджуйте інформацію альтернативним шляхом

DDoS-атака (Distributed Denial of Service)



https://en.wikipedia.org/wiki/Smurf_attack

Захист від DDoS-атак

- на рівні TCP/UDP з’єднань
  - Rate Limiting
  - Geo-blocking
  - IP Reputation
  - Anycast Routing
- на рівні застосунку
  - WAF (Web Application Firewall)
  - CAPTCHA
  - Behavioral Analysis
- зовнішні сервіси: Reverse Proxy, хмара

Витоки даних (data breach)

- Паролі та логіни
- Ім’я, адреса, номер телефону
- Номери банківських карт
- Медична інформація
- Фото, листування
- Дані з біометричних систем (відбитки, зображення облич)
- …

Наслідки для користувача

- Фінансові втрати
- Фішинг
- Крадіжка особистості
- Підрив репутації
- Шантаж / вимагання

Стілери — тихі мисливці за вашими даними

01 Стілери викрадають дані з комп'ютера.

02 Будьте обережні з невідомими програмами.

03 Вони збирають логіни та паролі.

04 Стілери можуть отримати доступ до ваших файлів.

Небезпека збереження паролів у доступних місцях

- Уникайте збереження паролів у браузері
- Не зберігайте паролі у текстових файлах
- Використовуйте менеджери паролів для безпеки
- Запам'ятовуйте складні паролі самостійно

Перевірка

факту компрометації облікового запису та паролю:

- https://haveibeenpwned.com/

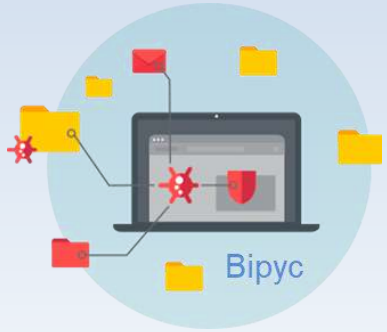
Have I Been Pwned

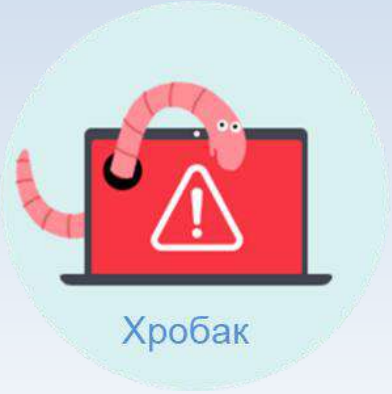
Як захиститися

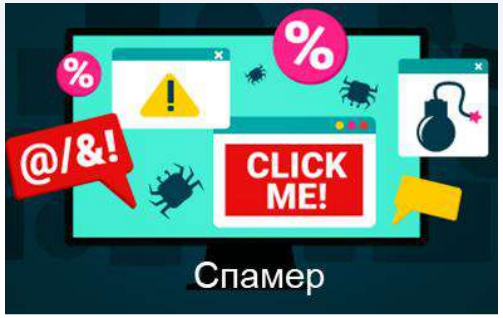
- паролі
- 2FA
- оновлення ПЗ
- обізнаність
- перевірка

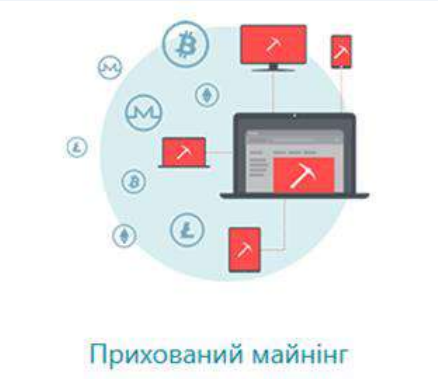
Що таке ШПЗ?

- програма (код), що виконує зловмисний намір її автора чи оператора









Категорії ШПЗ за функціями

Виконавці	Розповсюджувачі	Помічники
Шифрувальник	Троян	Логічна бомба
Локер	Хробак	Руткіт
Стіллер	RAT	Буткіт
Спамер	Установник	Ініціалізатор
Ботнет	Вірус	

Можливості шкідливої програми

Користувач

Windows 10

Керування

З'єднання

Зловмисник

Kali Linux

Backdoor.exe

Backdoor.exe

youtu.be/HftcPEa7RLI

Захист

- налаштування захисту у браузері
- налаштування вбудованої системи захисту від вірусів і загроз операційних систем
- онлайн перевірка файлів і ресурсів на наявність ШПЗ
- встановлення сторонніх антивірусних систем

Безпека мобільних пристроїв

- несанкціонований фізичний доступ:
  - PIN код на SIM
  - блокування екрану
  - шифрування
  - функція пошуку
  - backup

Безпека мобільних пристроїв

- несанкціонований віддалений доступ:
  - VPN
  - Bluetooth
  - антивірус
  - оновлення
  - офіційні репозиторії
  - 2FA
  - passkeys
  - обмеження додатків

Підсумки

Ознайомились із:

- поняттям кібербезпеки
- актуальними кіберзагрозами
- основними методами захисту
- видами ШПЗ
- безпекою мобільних пристроїв

SCAN ME