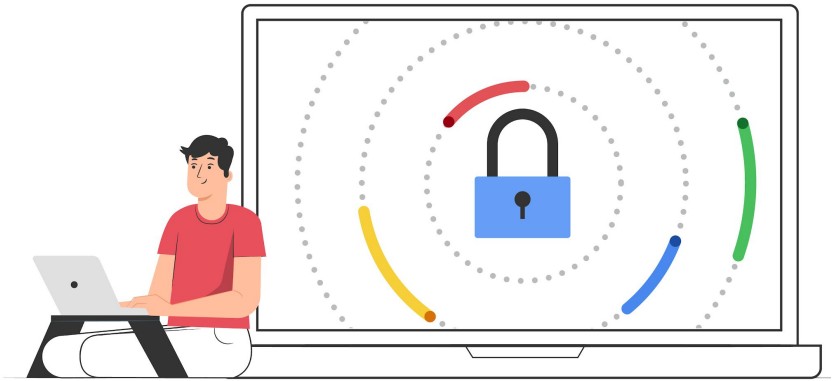
Безпечніше з Google

Google | ISSP

Онлайн-курс

Основи кібербезпеки для бізнесу

Що таке кібербезпека та кібергігієна та чому це важливо для Вашого бізнесу?



Роман Сологуб

- Генеральний директор ISSP
- Співзасновник CyberInnov8, Cyber Academy, GuardYoo

Досвід:

- 18+ років досвіду в захисті інформаційних систем та кібербезпеці

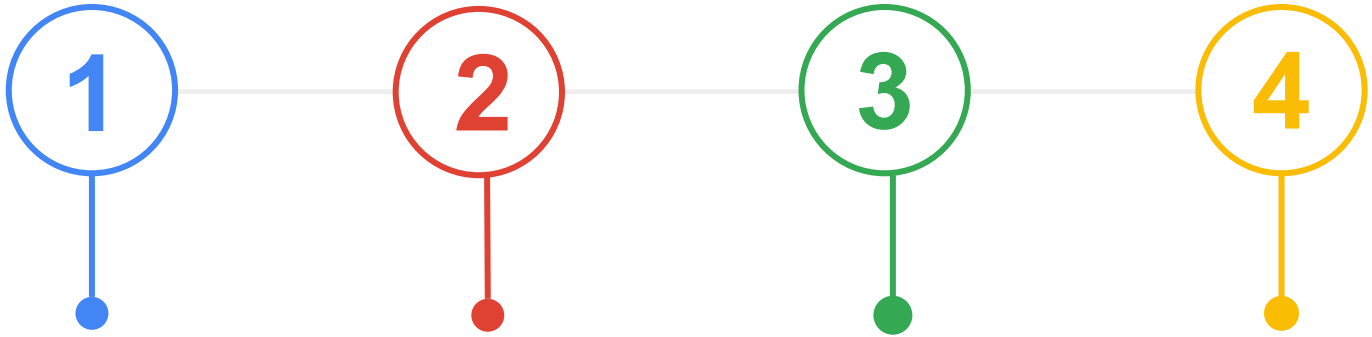
Експертиза:

- загальний стратегічний та операційний менеджмент
- маркетингове позиціонування та стратегія
- проєкти з розвитку та розбудови
- кібербезпека, IT та цифрова трансформація

Email: rsologub@issp.com
Київ

Про що курс?

На курсі Ви дізнаєтесь як



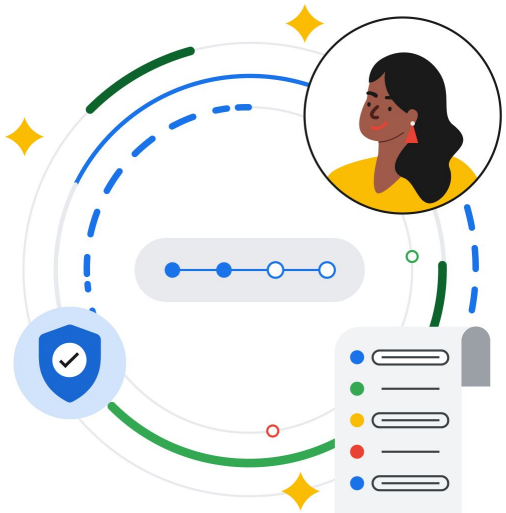
1. Захистити свій бізнес від кіберзагроз
2. Навчити співробітників дотримуватись кібергігієни
3. Використовувати AI для зміцнення кіберзахисту свого бізнесу
4. Розробити стратегію й тактику підвищення безпеки бізнесу

На Вас очікують

- **5 експертів** з кібербезпеки
- **4 тренінги** із практичною частиною
- **1 кейс-стаді** про подолання наслідків кібератак від компанії українським бізнесом
- можливість отримати індивідуальну **експертну консультацію**
- **розіграші з подарунками** наприкінці кожного тренінгу

Експертна консультація це

1. **Одна безкоштовна 30-хвилинна сесія** з експертом із кібербезпеки ISSP
2. **Безпечне** та **конфіденційне середовище** для запитань стосовно кіберзахисту свого бізнесу
3. Можливість отримати **персоналізовану пораду** на свій запит
4. **Кількість консультацій обмежена**, відбір учасників на основі заповненої форми запиту
5. **Рівень попередніх знань не є критерієм відбору**



Програма

1. Кібербезпека та кібератака
2. Спрямовані кібератаки і APT*
3. Кібератаки і малий та середній бізнес
4. Кібергігієна та кіберстійкість
5. Безпека даних
6. Виманювання інформації – фішинг

***APT** (англ. Advanced Persistent Threat) – розвинена стала загроза

1 Кібербезпека та кібератака

Кібербезпека та кіберзагроза

Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи та мережу від кібератак

→ захист від кіберзагроз

Кіберзагроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації та/або завдання збитків автоматизованій системі

→ те, що чинить шкоду через вплив на технології

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі

Кіберзагроза — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам держави у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів

Джерело: Закон України

Інформаційна безпека ≠ кібербезпека

Інформаційна безпека – забезпечує стан КЦД* даних чи інформації

Область дії

Кібербезпека – забезпечує захист автоматизованих систем від кіберзагроз

Область дії

***КЦД** – конфіденційність, цілісність, доступність інформації

48%

МСБ* по світу стикалися з кібербезпековим інцидентом у 2023 році

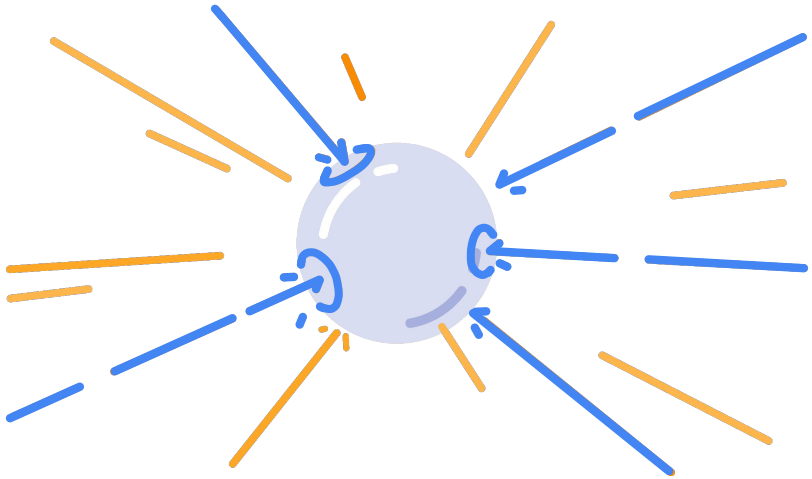
Джерело: stationX
***МСБ** – малі та середні бізнеси; група підприємств, які не перевищують визначені показники (наприклад: <250 співробітників)

Кібератака

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій

Характеристики:

- виконується людьми (частіше – організованою групою людей)
- не має відбуватись виключно через взаємодію з технологіями
- може експлуатувати усі наявні типи ресурсів організації



Джерела кібератак (за мотивацією)

Держави & терористи

Групи організованих злочинців & промисловий шпіонаж

Хакери & хактивісти

Основні кібератаки проти України

Травень 18
- Центральна виборча комісія

Грудень 23
- Чернівціобленерго
- Прикарпаттяобленерго
- Київобленерго

Грудень 15-17
- Укрзалізниця
- Міністерство інфраструктури
- Укренерго

Травень 12-18
- Комп'ютерний вірус WannaCry
- Програма-вимагач X-data

2014 | 2015 | 2016 | 2017

Жовтень 24
- Старлайт
- ТРК Україна

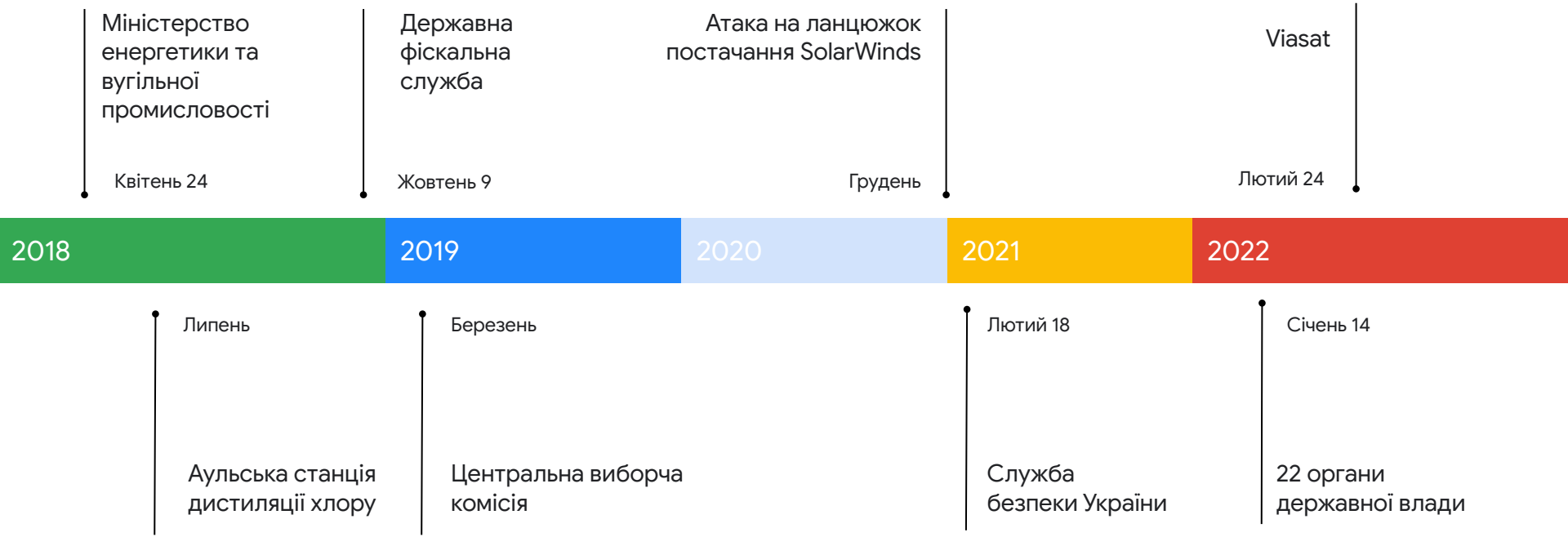
Січень 17, 20
- Аеропорт “Бориспіль”
- Укренерго

Грудень 6
- Пенсійний фонд
- Держказначейство
- Міністерство фінансів

Червень, липень
- Програма-вимагач NotPetya
- Кібератака Crystal Intrusion

Джерело: ISSP

Основні кібератаки проти України



Джерело: ISSP

Основні кібератаки проти України

Вінницяобленерго

Квітень

Кількість кібератак проти критичної інфраструктури зросла у **5 разів**

Дата-центр “Парковий”

Січень 25

2022 | 2023 | 2024

Березень 26

Укртелеком

Увесь рік

Кількість кібератак на українські інформаційні системи ↗

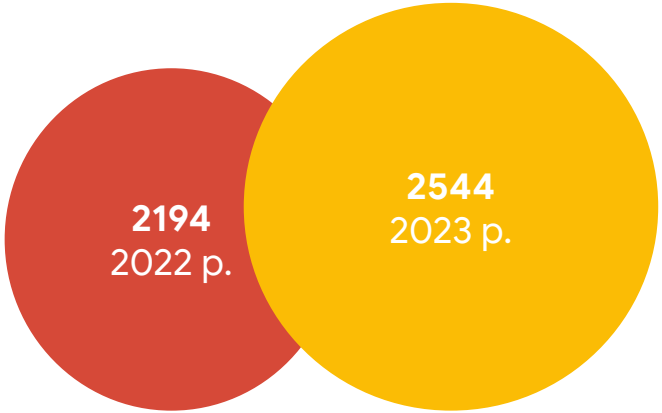
Грудень 23

Київстар

Джерело: ISSP

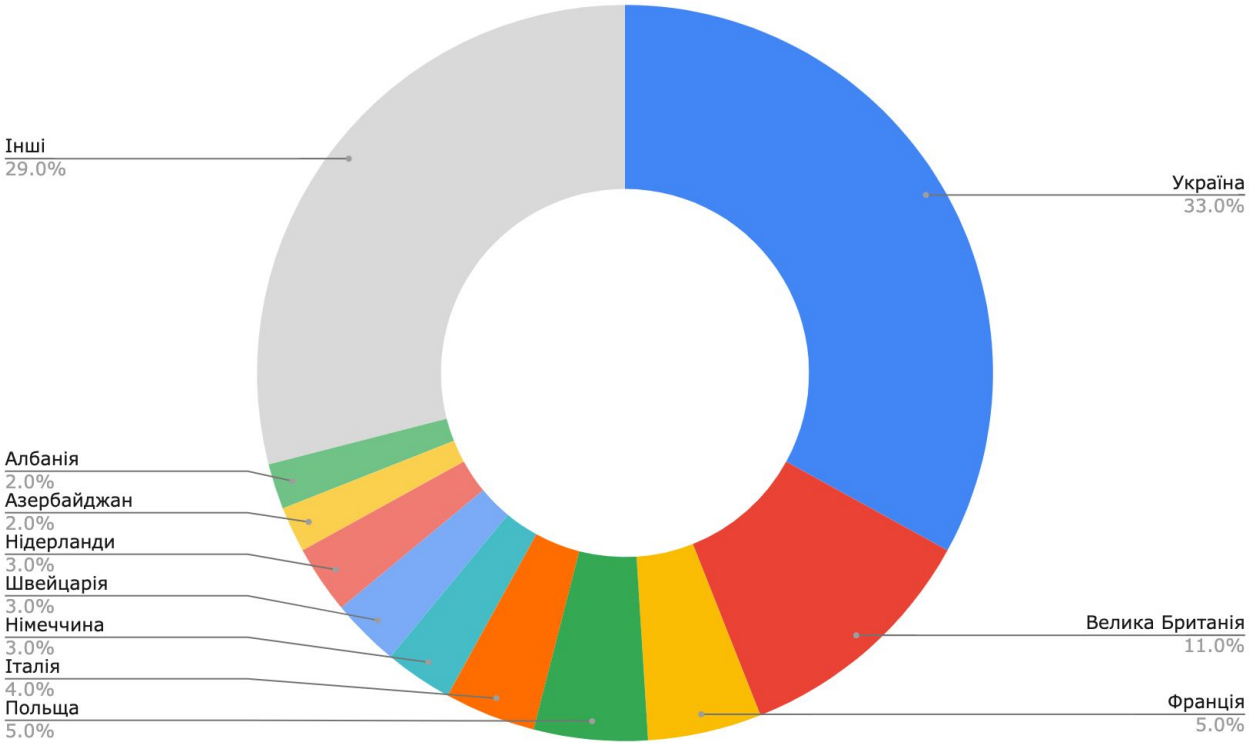
Україна у 2023 році

- Було зафіксовано 2554 інциденти, з яких лише 367 були критичними
- Порівнюючи з 2022, на 65% вдалось зменшити кількість кіберінцидентів критичного та високого значення



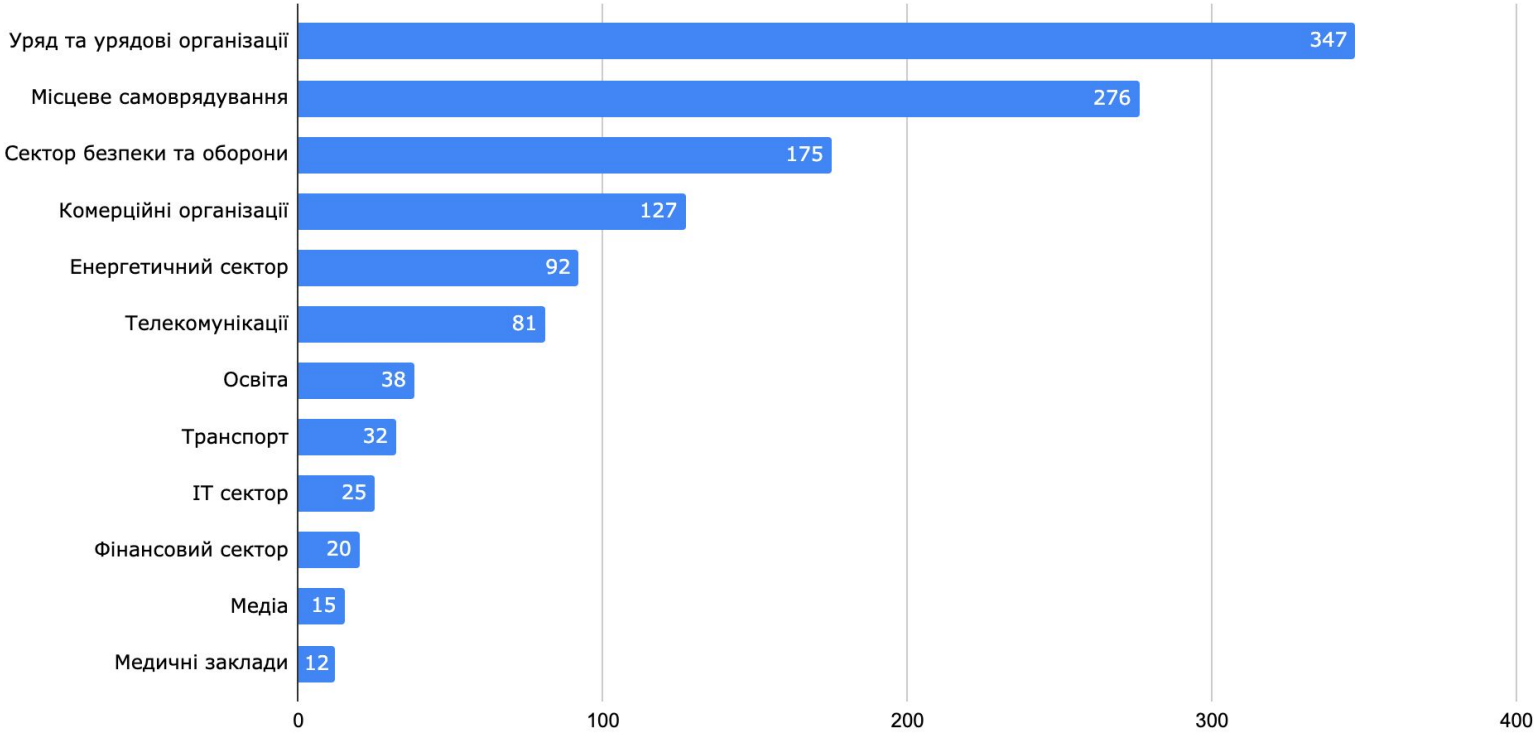
Джерело: Держспецзв'язку

Найбільш таргетовані регіони Європи у 2023 році



Джерело: Cyberpeace Institute

Галузі, які у 2023 році зазнали найбільшої кількості атак 🇺🇦



Джерело: 3SCIP

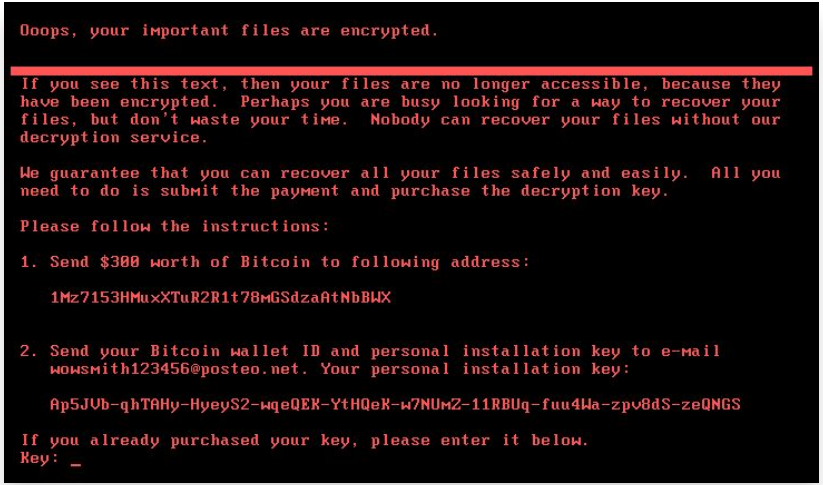
2 Спрямовані кібератаки та розвинена стала загроза (APT*)

***APT** (англ. Advanced Persistent Threat)

Ефект кібератаки очима користувачів

Очевидний, відкритий результат деструктивного впливу зловмисників, який може мати повідомлення для жертви, і / або виражається у:

- повній або частковій відмові роботи системи
- втраті даних
- інших видимих наслідках для користувача системи



Повідомлення “NotPetya”*, 27 червня 2017 р.

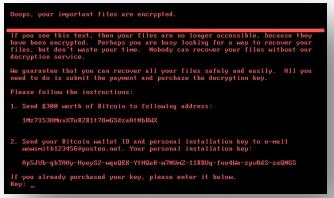
***NotPetya** - шкідливий вірус, який шифрує дані на комп'ютерах та розповсюджується шляхом використання вразливостей у мережах

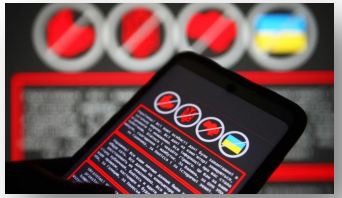
Складна кібератака

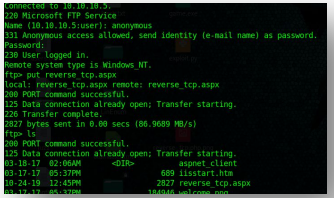
Розвинена стала загроза (англ. Advanced persistent threat - APT) — різновид складних кібератак з **метою отримання несанкційованого доступу** до інформаційних систем жертви та **встановлення прихованого доступу до неї** з метою використання або контролю в майбутньому

Складна кібератака

- Ефекти та наслідки (досвід користувача)







Складна кібератака

- Ефект, який бачить користувач
- Інтерактивні стадії поза нашою увагою:
  - кульмінація
  - захоплення
  - проникнення
  - підготовка

Складна кібератака = прихована частина айсберга

Кібератака на Київстар 12 грудня 2024 року

Досвід CEO*

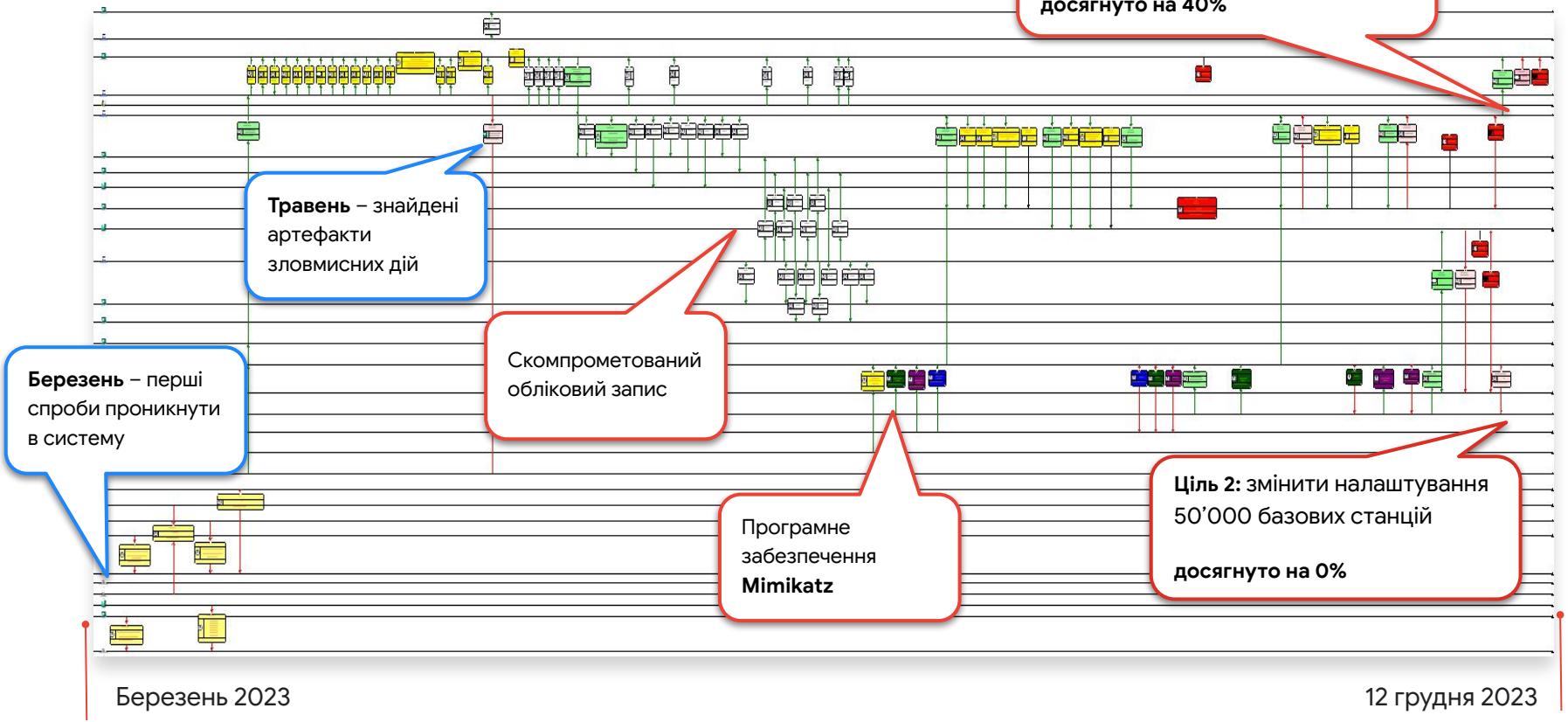
- **06:00** “Йшлося про нетипову поведінку мережі, хоча в мене все ще працювало”
- **09:00** “У соцмережах з’явилися фото з офісу компанії, де перебувало кілька десятків силовиків. Перша гіпотеза – «Київстар» націоналізовують”

Досвід абонента

- Приблизно “**24 млн абонентів** одномоментно занурилися в телеком-блекаут”.

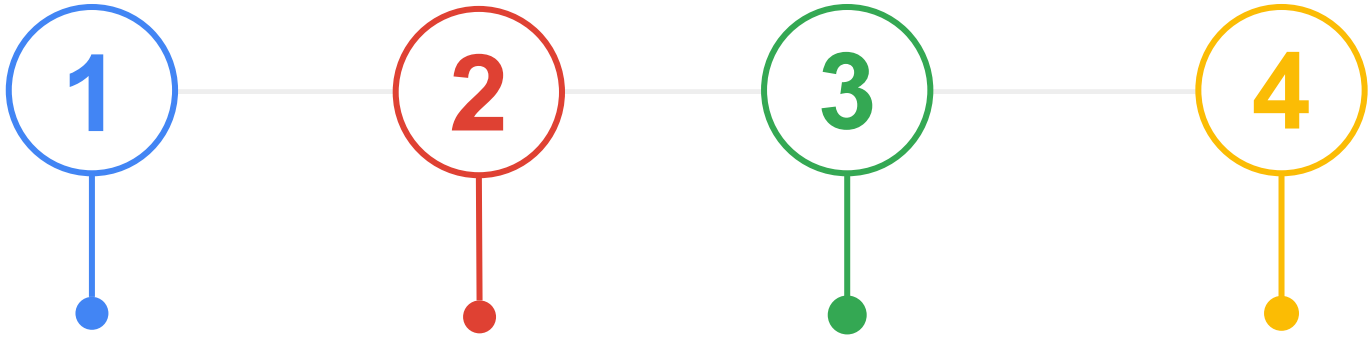
*Згідно матеріалів: Forbes Україна “*Телеком-Чорнобиль*”

Кібератака на Київстар 12 грудня 2023 року



Джерело: Forbes Україна “*Телеком-Чорнобиль*” (таймлайн кібератаки - довільний малюнок)

Основні етапи спрямованої атаки*

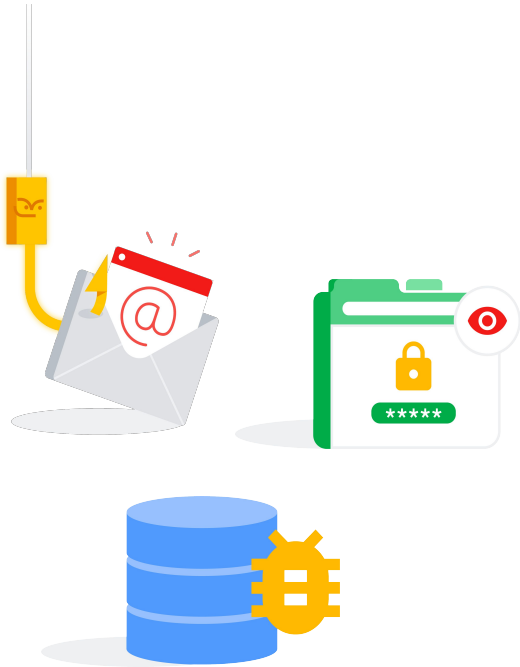


1. Збір інформації про ціль
2. Підготовка сценарію дій та засобів атаки
3. Встановлення зв’язків
4. Досягнення мети: проникнення і первинна компрометація

***Спрямована атака** – атака, для якої проведено прискіпливу розвідку і виявлено детальний контекст для подальших маніпуляцій.

Первинна взаємодія. Глобальна перспектива 🌍

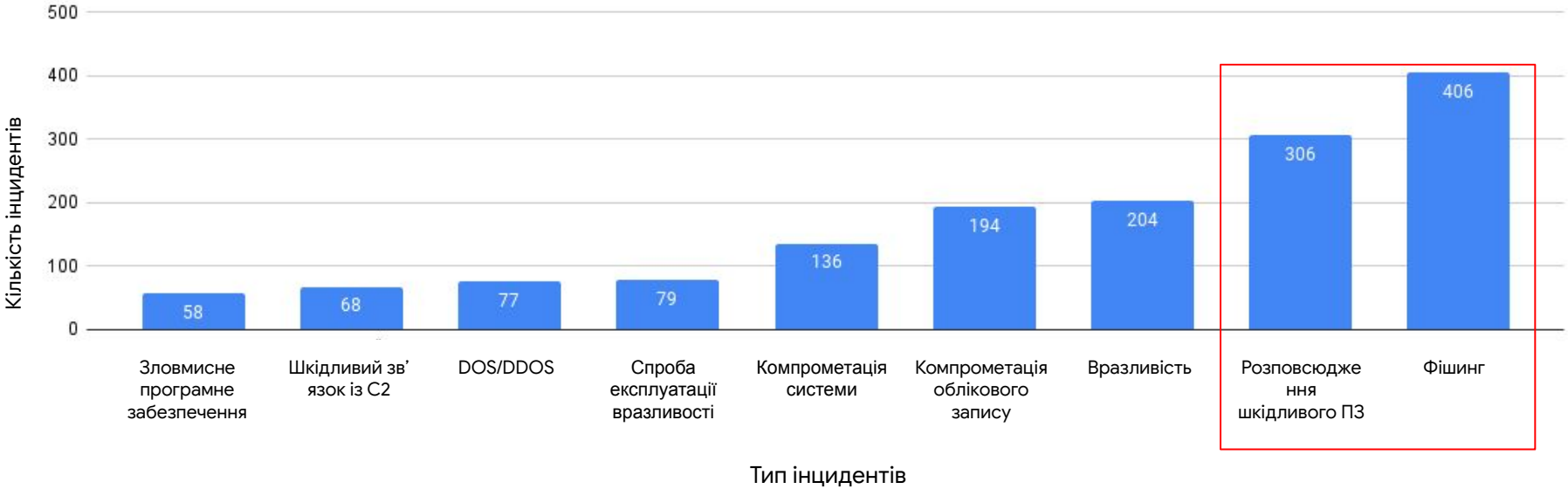
- експлуатація вразливості – 31.8%
- фішинг – 22.1%
- вкрадені облікові записи – 13.8%
- повернення – 12.1%
- компрометація веб – 6.8%
- через підрядника – 3.8%
- підбір грубою силою – 3.8%



Джерело : cip.gov.ua

Первинна взаємодія. Українська перспектива 🇺🇦

Кількість інцидентів vs Тип інцидентів



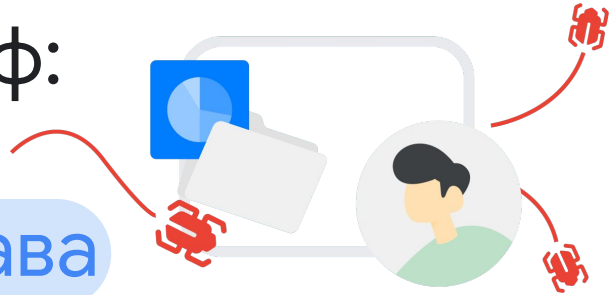
Джерело : cip.gov.ua

3 Кібератаки і малий та середній бізнес

Кібератаки і МСБ*

Розповсюджений міф:

“Моя компанія не цікава кіберзловмисникам”



***МСБ** – малі та середні бізнеси; група підприємств, які не перевищують визначені показники (наприклад: <250 співробітників)

МСБ сектор і кібератаки, тренди 🌍

За день, МСБ у середньому стикався з:

- **2019 р. – 6300 атак**
- **2020 р. – 17 500 атак**
- **2022 р. – 31 000 атак**

67% організацій до 1,000 співробітників зазнали кібератаки, а 58% фіксували втручання у роботу інформаційних систем.

1. 46% усіх кібератак стосуються підприємств із кількістю співробітників менше 1000 осіб.
2. У 2021 році 61% малих і середніх підприємств були об'єктами кібератак.
3. Зловмисне програмне забезпечення (18%) є найпоширенішим типом кібератак, спрямованих на малий бізнес.
4. 82% атак програм-вимагачів у 2021 році були спрямовані проти компаній із кількістю співробітників менше 1000 осіб.
5. 37% компаній, постраждалих від програм-вимагачів, мали менше 100 співробітників.
6. Малі підприємства отримують найвищий відсоток цільових шкідливих електронних листів.
7. Працівники малого бізнесу зазнають на 350% більше атак соціальної інженерії, ніж працівники великих підприємств.
8. 87% малих підприємств мають дані клієнтів, які можуть бути скомпрометовані під час атаки.
9. 27% малих підприємств, які взагалі не мають спроможностей кіберзахисту, збирають інформацію про кредитні картки клієнтів.

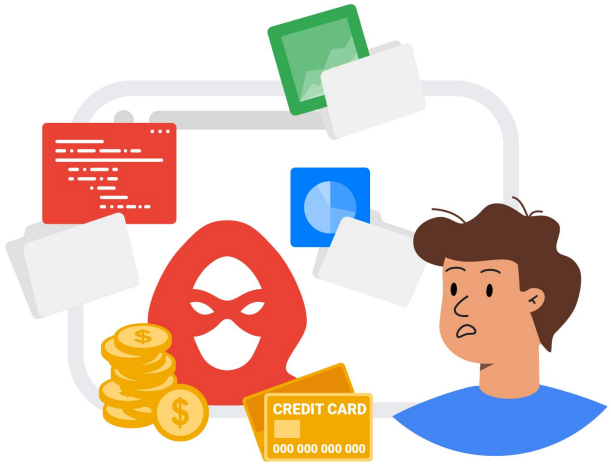
Джерело : StrongDM, TechRepublic, StationX
Малюнок: ключові тренди кібератак на МСБ

Найпоширеніші наслідки кібератак на малий бізнес

- Тимчасова зупинка діяльності бізнесу та зниження продуктивності – 30%
- Втрата доходу – 28%

- Втрата довіри клієнтів – 16%
- Безповоротна втрата критично важливих для бізнесу даних – 16%
- Втрата майбутніх бізнес-можливостей/продажів – 16%

- Гонорари, сплачені адвокатам – 14%
- Судові позови, подані проти бізнесу – 14%
- Втрата ділової репутації – 13%



Джерело : StationX.net

Методи й мотивація кібератак на МСБ. Глобальна перспектива 🌍

82%

всіх атак з використанням програм-вимагачів спрямовані на МСБ

92%

всіх порушень припадає на вторгнення в систему, соціальну інженерію та базові атаки на вебдодатки

350%

більше атак соціальної інженерії зазнає працівник МСБ (<100 людей) ніж працівник великого підприємства

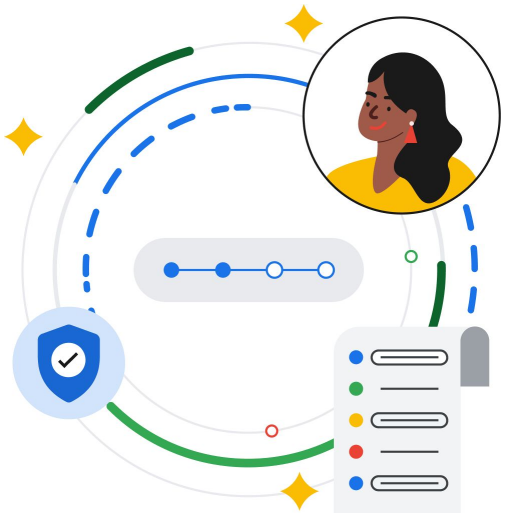
Джерело : StationX

Готовність МСБ до кіберінциденту 🌍

- **46%** МСБ **не** використовують **брандмауери***
- **42%** МСБ **не** створюють резервні копії **критично важливих даних**

- **57%** МСБ стежать за **безпекою віддаленої роботи**
- Лише **28%** власників малого бізнесу в США повідомили, що мають **кіберстрахування**

- **56%** власників малого бізнесу проводять **тренінги з кібербезпеки** для своїх співробітників раз на рік, порівняно з 94% середнього бізнесу
- **24%** власників малого бізнесу надсилають працівникам **тестові фішингові листи**, порівняно з 65% власників середнього бізнесу



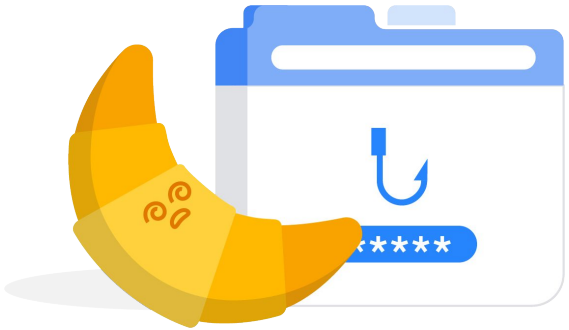
Джерело : StationX
***Брандмауер** (фаєрвол) - це програма або пристрій, який захищає ваш комп'ютер або мережу від несанкціонованого доступу

4 Кібергігієна та кіберстійкість

Кібергігієна та кіберстійкість

Кібергігієна – уміння, навички користування інформаційними технологіями, спрямовані на своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних кіберзагроз

Кіберстійкість – це спроможність організації протистояти та відновлюватись після інцидентів кібербезпеки



З чого потрібно починати?

Людський фактор лишається найвразливішим місцем у кіберзахисті

2022 Internet Crime Report* зафіксував **21 832 скарг компрометації корпоративної пошти** (BEC)* що призвело до втрат у 2.7 мільярда доларів США

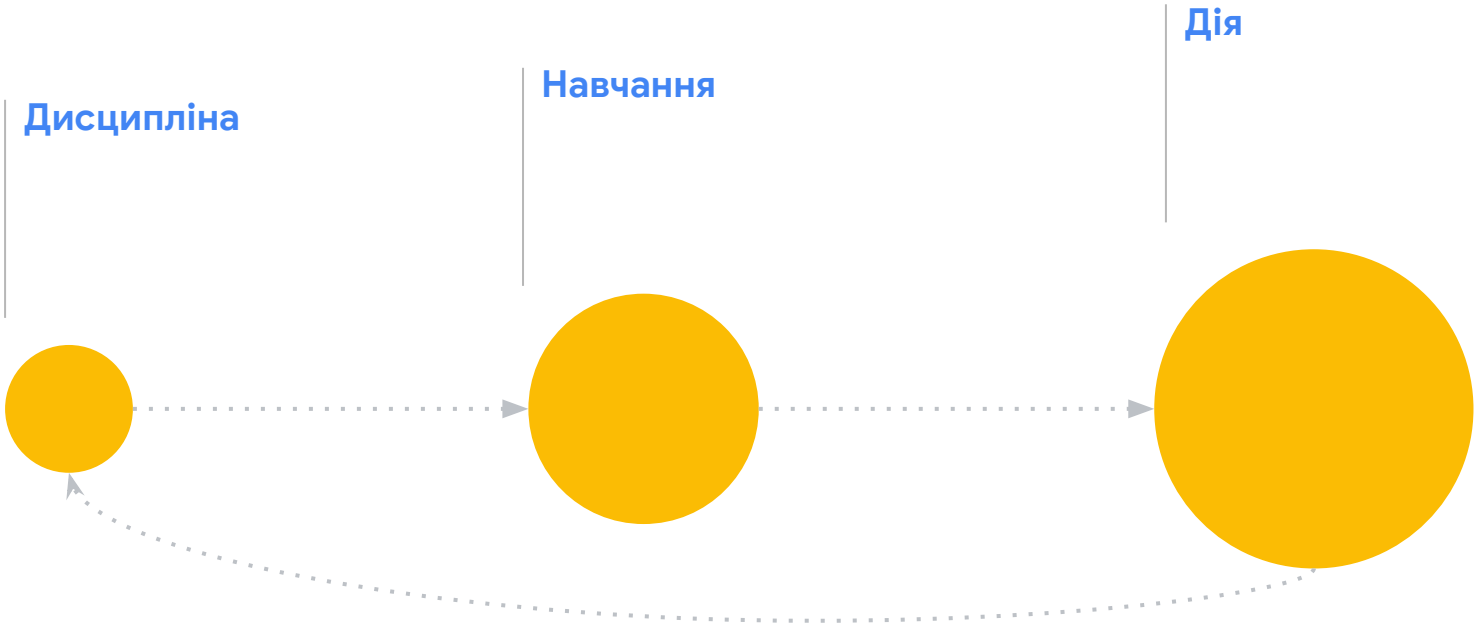
*BEC (англ. Business Email Compromise) – компрометація корпоративної пошти, різновид фішингових атак, націлених на організації

Управлінський підхід до кібербезпеки

Корпоративна культура – це **система цінностей, символів, переконань, зразків поведінки,** які розділяються всіма співробітниками організації.

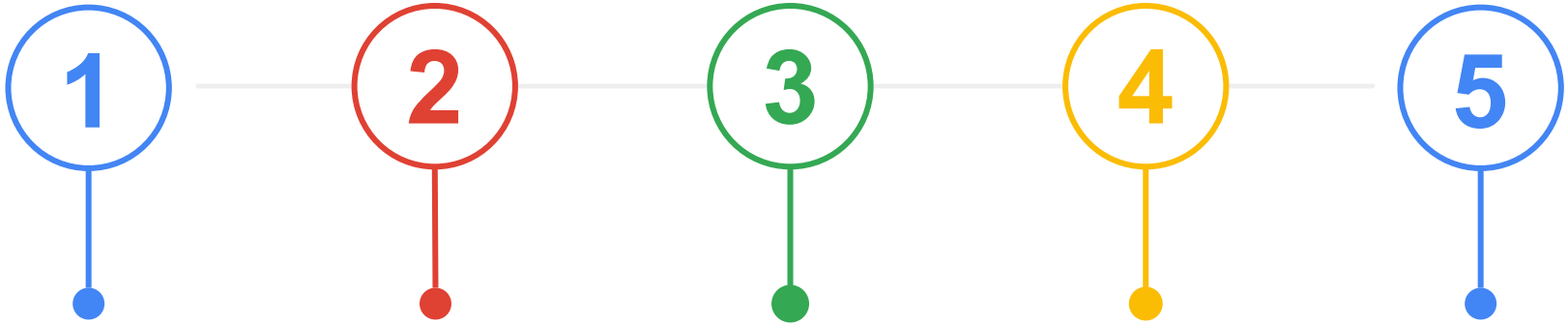
«Культура з'їдає стратегію на сніданок»
– Пітер Друкер

Маховик культури



Джим Колінс - автор бестселлера “від Хорошого до Величного”, досліджується ефект маховика

Корпоративні процеси для запровадження кібербезпеки



Агітація кібербезпеки

настільні матеріали для співробітників

Формалізація кібербезпеки

створення політики інформаційної безпеки

Перегляд процесів та інструментів

налаштування корпоративних інструментів

Впровадження тренінгів та симуляцій

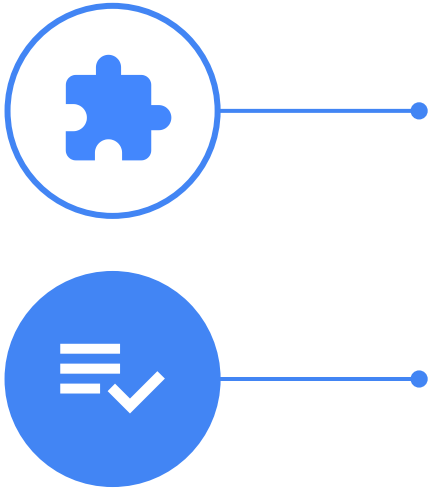
фішингові симуляції, тренінги зі сценаріями

Наймання радника / консультанта

Запровадження ризик-комітету

5 Безпека даних

Дані та інформація



Дані – це фактичні спостереження, вимірювання або факти, які можна зібрати, записати та зберегти.

Дані можуть бути у числовій, текстовій або іншій формі.

Інформація – це оброблені та організовані дані, які набули сенсу та цінності в певному контексті.

Інформація може бути представлена у формі звітів, таблиць, графіків, діаграм та інших способів візуалізації даних

Приклади даних та інформації

Дані

Приклади даних: числа, текстові рядки, зображення, звукові записи тощо.

- example@email.com
- IP-адреса: 192.168.0.1
- широта 37.7749° N, довгота -122.4194° E
- транзакційні дані на банківському рахунку: $5000

Інформація

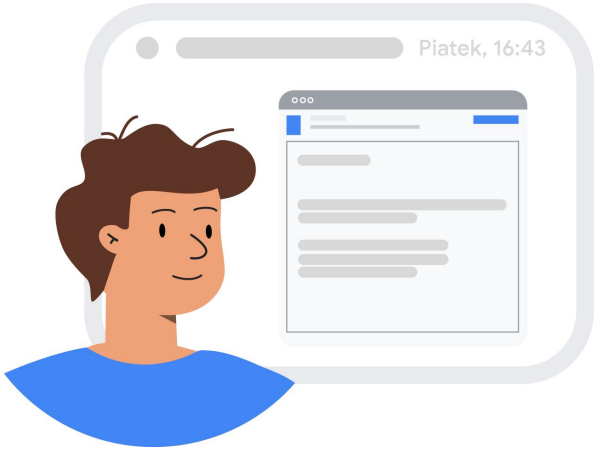
Приклади інформації:

- контакт власника та можливість зв’язатись за даними електронної пошти example@email.com
- IP-адреса 192.168.0.1 дає інформацію, що це локальна IP-адреса мережі
- широта та довгота дає визначити місце розташування
- транзакційні дані показують доступну суму коштів на рахунку

Дані можуть бути неважливими для користувача, але дуже корисними для зловмисників для подальшого впливу на цифрові активи цього користувача

Особисті цифрові дані

- Ім’я та прізвище
- Номер телефону
- Адреса
- Електрона пошта
- Платіжні дані
- Медичні дані
- Соціальні мережі та профілі



Важливість особистих даних

Приватність

Особисті дані включають інформацію про особисте життя, таку як ім'я, адреса, номери телефонів, електронні адреси, фінансові дані та багато іншого.

Збереження приватності особистих даних є **важливим для забезпечення безпеки та захисту особистості.**

Безпека

Особисті дані можуть бути цінною метою для зловмисників, які можуть використовувати ці дані для шахрайства, крадіжки ідентичності, фішингу* та інших злочинів.

Збереження та захист особистих даних є **важливим для запобігання несанкціонованому використанню та зловживанню.**

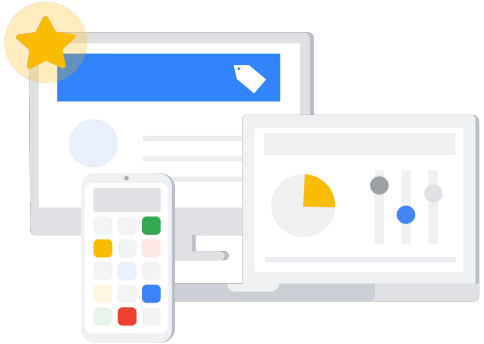
*__фішинг__ – вид атаки, під час якої зловмисник намагається ввести в оману користувача з метою видобування конфіденційної інформації або інфікування користувацької системи

Безпека даних

Безпека даних – це процес захисту конфіденційності, цілісності та доступності даних від несанкціонованого доступу, втрати, пошкодження або розкриття.

4 засоби, які у комплексі дають найкращі результати:

1. шифрування даних
2. встановлення багаторівневої системи доступу до даних
3. резервне копіювання
4. встановлення антивірусного програмного забезпечення



№1 Шифрування даних

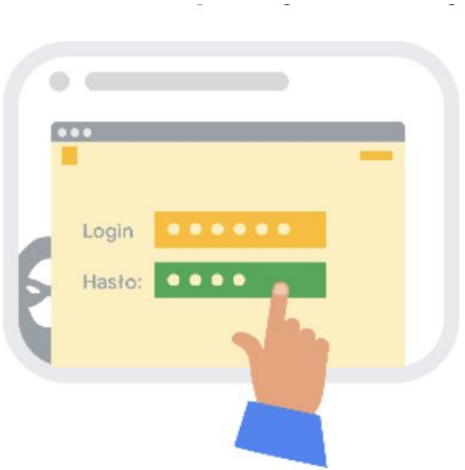
Шифрування даних **використовується для захисту** конфіденційності даних шляхом **перетворення їх у незрозумілу форму** для несанкціонованих осіб.

Наприклад: шифрування електронної пошти або зберігання файлів у зашифрованому вигляді на пристроях забезпечує захист від несанкціонованого доступу до цих даних.

№2 Багаторівнева система доступу

Встановлення багаторівневої системи доступу до даних **дозволяє обмежити права доступу до інформації** лише необхідним користувачам

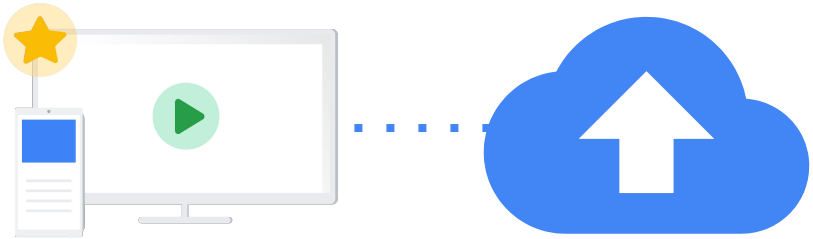
Наприклад: адміністратор мережі має повний доступ до всіх систем, тоді як звичайні користувачі мають обмежений доступ лише до необхідних даних.



№3 Резервне копіювання

Резервне копіювання даних є важливою складовою безпеки даних і **дозволяє відновлювати втрачені або пошкоджені дані.**

Наприклад: у разі хакерської атаки чи випадкової втрати даних, регулярне створення резервних копій на зовнішніх носіях або в хмарному сховищі забезпечить можливість їх відновлення



№4 Антивірусне програмне забезпечення

Використання антивірусного програмного забезпечення допомагає виявляти і блокувати шкідливі програми, які можуть пошкодити дані або викрасти їх

Наприклад: антивірусна програма перевірить файли та документи на наявність вірусів, троянських програм та інших загроз, забезпечуючи безпеку від шкідливих програм

“Людський фаєрвол”

"Людський фаєрвол":

- ≠ термін в області кібербезпеки, а метафоричний вираз
- вказує на концепцію використання здатності людей, замість програмного забезпечення, для для захисту від небажаних впливів або відомостей.

Рекомендації для людського фаєрволу

1

Складні паролі

Паролі повинні:

- бути унікальними
- бути довгими
- складатися з комбінації букв, цифр і спеціальних символів

2

Розсудливе використання соцмереж

- Будьте обережні з інформацією, яку публікуєте в соціальних мережах
- Обмежуйте доступ до особистої інформації

3

Уважність до фішингу

Не відкривайте вкладення або не вводьте свої особисті дані на ненадійних вебсайтах

4

Уважність у мережі

Уникайте передачі чутливої інформації, такої як паролі або фінансові дані, через:

- ненадійні мережі
- громадські Wi-Fi мережі

Використовуйте віртуальні приватні мережі (VPN)

Рекомендації для людського фаєрволу

1

Складні паролі

Паролі повинні:

- бути унікальними
- бути довгими
- складатися з комбінації букв, цифр і спеціальних символів

2

2-етапна перевірка

Додатковою перевіркою може бути:

- код, надісланий на телефон користувача
- фізичний ключ безпеки
- додаток для підтвердження Вашої особи

3

Оновлення ПЗ*

Потрібно регулярно оновлювати:

- програмне забезпечення
- операційні системи

4

Уважність у мережі

Уникайте передачі чутливої інформації, такої як паролі або фінансові дані, через:

- ненадійні мережі
- громадські Wi-Fi мережі

Використовуйте віртуальні приватні мережі (VPN)

***ПЗ** – програмне забезпечення

Рекомендації для людського фаєрволу

5

Розсудливе використання соцмереж

- Будьте обережні з інформацією, яку публікуєте в соціальних мережах
- Обмежуйте доступ до особистої інформації

6

Резервне копіювання даних

Регулярно робіть резервні копії своїх важливих даних, таких як фотографії, документи й контакти

7

Уважність до фішингу

Не відкривайте вкладення або не вводьте свої особисті дані на ненадійних вебсайтах

*__фішинг__ – вид атаки, під час якої зловмисник намагається ввести в оману користувача з метою видобування конфіденційної інформації або інфікування користувацької системи

Політики “чистоти”

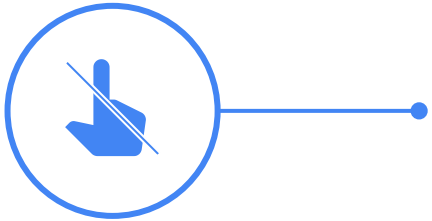
Політика чистого столу передбачає:

- Відсутність записів ключів та атрибутів доступу (паролів або підказок) на паперових носіях
- Не збереження цих записів поряд з об’єктами доступу

Політика чистого екрану передбачає:

- Закриття активних сесій по завершенню використання
- Блокування робочого столу, коли відходите від нього
- Зберігання файлів не на робочому столі

Використання корпоративної інформації

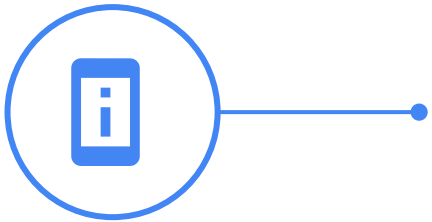


Обмеження доступу

співробітники повинні мати обмежений доступ до корпоративної інформації відповідно до своєї ролі та потреби доступу до цієї інформації

Захист даних

співробітники мають забезпечувати безпеку зберігання та передачі корпоративних даних



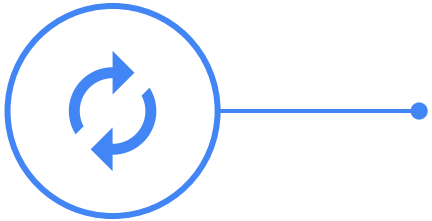
Заборона використання особистих облікових записів

співробітники не повинні використовувати особисті облікові записи або пристрої для доступу до корпоративної інформації

Використання корпоративної інформації

Заборона копіювання інформації

співробітники не повинні копіювати корпоративну інформацію на зовнішні носії даних або інші засоби зберігання без належного дозволу



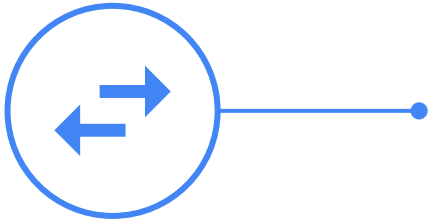
Дотримання політик безпеки

співробітники мають дотримуватися всіх політик і процедур безпеки, встановлених організацією, і регулярно оновлювати свої знання щодо цих політик

Захист від соціальної інженерії

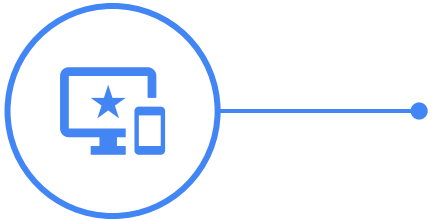
співробітники мають бути обережними щодо запитів на інформацію від невідомих осіб і завжди перевіряти, чи є ці запити легітимними

Використання корпоративної інформації



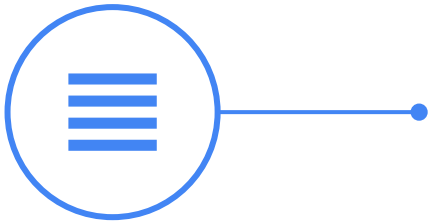
Реєстрація та аудит дій

організація може вести журнал реєстрації та аудиту дій співробітників, щоб відстежувати доступ до корпоративної інформації та виявляти можливі порушення безпеки



Видалення даних

при завершенні роботи над проєктами або при звільненні співробітники мають видаляти корпоративну інформацію зі своїх пристроїв і облікових записів

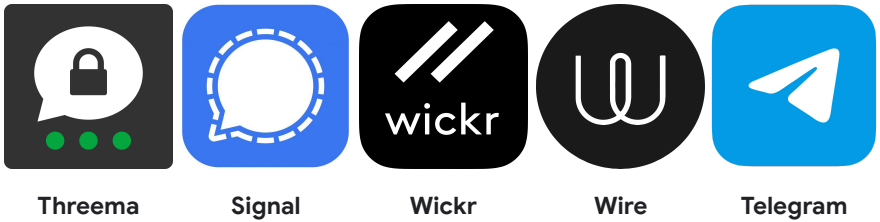


Інструкції щодо виявлення і реагування на інциденти

співробітники повинні знати, як виявляти інциденти безпеки й негайно повідомляти їх відділу безпеки організації

Які платформи використовувати в бізнесі?

особисті*



корпоративні

*Особисті платформи – месенджери відображені за рейтингом безпековості (від найбезпечніших до найнебезпечніших)
Джерело: Molfar

6 Виманювання інформації – фішинг

***фішинг** – вид атаки, під час якої зловмисник намагається ввести в оману користувача з метою видобування конфіденційної інформації або інфікування користувацької системи

Спам та фішинг

Спам

Спам – несанкціонована масова розсилка електронних листів, яка зазвичай містить рекламні матеріали або посилання на шкідливі вебсайти.

Мета спаму - заманити користувачів натиснути на посилання або завантажити файл, який може заразити їхні комп'ютери шкідливим програмним забезпеченням.

На **спам** припадає близько **54,6% від світового трафіку пошти**.

Фішинг

Фішинг – вид атаки, під час якої зловмисники використовують електронну пошту, щоб обманом змусити користувачів надати особисту інформацію або завантажити шкідливий код.

Мета фішингу – отримати конфіденційну інформацію або інфікувати користувацьку систему.

90% витоків даних виникають у результаті **фішингу**.

Небезпека фішингу та наслідки його успішної реалізації

Етап 1: Початок атаки

Працівник натискає на фішингове посилання в електронній пошті

Результат: незрозуміла або **невидима** реакція системи, працівник спокійний

Етап 2: 3+ тижні

Зловмисник встановлює інструменти для внутрішньої розвідки системи

Результат: працівник спокійний, зловмисник збирає внутрішню інформацію.

Етап 3: Наступні декілька тижнів

Якщо за цей час зловмисник ніяк себе не проявив, відбувається пошук цілі - як правило - адміністративного облікового запису.

Результат: зловмисник готує спроможності для захоплення контролю над інсрфаструктурою.

Небезпека фішингу та наслідки його успішної реалізації

Етап 4: Наступні декілька тижнів

Привілейований обліковий запис скомпрометовано, відбувається перехоплення та витік критичної інформації та/або підготовка до спричинення деструктивного ефекту.

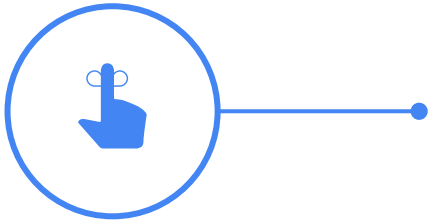
Результат: зловмисник, залишаючись непоміченим збирає внутрішню інформацію, захоплює контроль над інфраструктурою

Етап 5: Наступні декілька тижнів

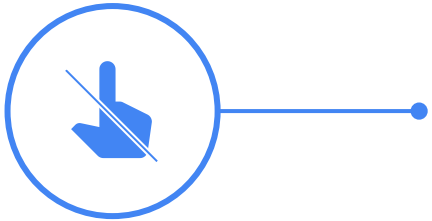
Проведено атаку на ціль: інфраструктура скомпрометована, дані скомпрометовані

Результат: компанія стала жертвою кіберзловмисників, її сервіси заблоковані, дані втрачено з вимогою викупу.

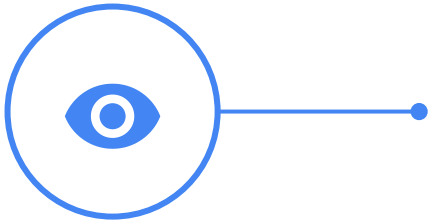
Захист від фішингу



Бути обережними, натискаючи на вкладення електронної пошти, завантажуючи файли чи відвідуючи нові URL-адреси



Перевіряти посилання та файли перш ніж їх відкривати



Перевіряти адреси електронної пошти та підписи **електронних листів підозрілих відправників**

Сервіси для перевірки файлів

Virustotal

перевірка антивірусами

IRIS-H

перевірка документів MS Office

Internxt

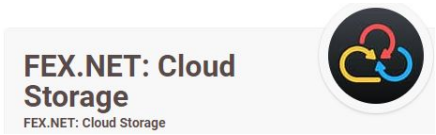
статистичний та динамічний аналіз файлів

URLScan

перевірка URL на шкідливий вміст

Інструменти для передачі файлів

особисті*



корпоративні

Практика.
Як розпізнати фішингові атаки?

Приклад №1

Від: PayPal <paypal@notice-access-273.com>

Від: PayPal <paypal@notice-access-273.com>
Кому: example@gmail.com
Тема: Ваш рахунок було обмежено (Case ID Number: PP-003-153-352-657)

PayPal

Шановний клієнт.

Нам потрібна Ваша допомога у розв'язанні проблеми з Вашим акаунтом. Щоб дати нам час для спільної роботи над цим, ми тимчасово обмежили можливості Вашого акаунта до розв'язання проблеми. Ми розуміємо, що відсутність повного доступу до акаунта PayPal може розчаровувати. Ми хочемо співпрацювати з Вами, щоб якомога швидше відновити нормальну роботу Вашого акаунта.

У чому проблема?
Ми помітили незвичну активність у Вашому акаунті PayPal.
З метою безпеки, щоб захистити Ваш акаунт, поки ми не отримаємо від Вас більш детальну інформацію, ми встановили обмеження для Вашого акаунта.

Як ви можете допомогти?
Зазвичай про такі речі досить легко подбати. Здебільшого нам просто потрібно трохи більше інформації про Ваш акаунт.
Щоб допомогти нам з цим і дізнатися, що Ви можете і що не можете робити зі своїм акаунтом, поки проблема не буде вирішена, увійдіть у свій обліковий запис і перейдіть до Центру вирішення проблем.

Увійти

Допомога | Контакти | Безпека
Цей лист було надіслано Вам, будь ласка, не відповідайте на нього. На жаль, ми не можемо відповісти на запити, надіслані на цю адресу. Щоб отримати негайну відповідь на Ваші запитання, просто відвідайте наш Центр допомоги, натиснувши кнопку "Допомога" внизу будь-якої сторінки PayPal.

Приклад №4

Шановний користувачу Paypal,

У зв'язку із занепокоєнням щодо безпеки та цілісності облікового запису PayPal, ми опублікували це попереджувальне повідомлення.
Нам стало відомо, що інформація про ваш обліковий запис потребує оновлення у зв'язку з неактивним користуванням, шахрайством та повідомленнями про підробку.
Якщо ви приділите 5-10 хвилин часу і оновите свої дані, у вас не виникне жодних проблем з онлайн-сервісом у майбутньому.
Однак, якщо ви не оновите свої записи, це призведе до призупинення дії вашого облікового запису
Термін дії цього повідомлення закінчується через 48 днів.

Після того, як ви оновите дані вашого облікового запису, обслуговування вашого PayPal рахунку не буде перервано і продовжуватиметься у звичайному режимі.

Будь ласка, перейдіть за посиланням нижче, увійдіть до свого облікового запису і поновіть дані свого облікового запису

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

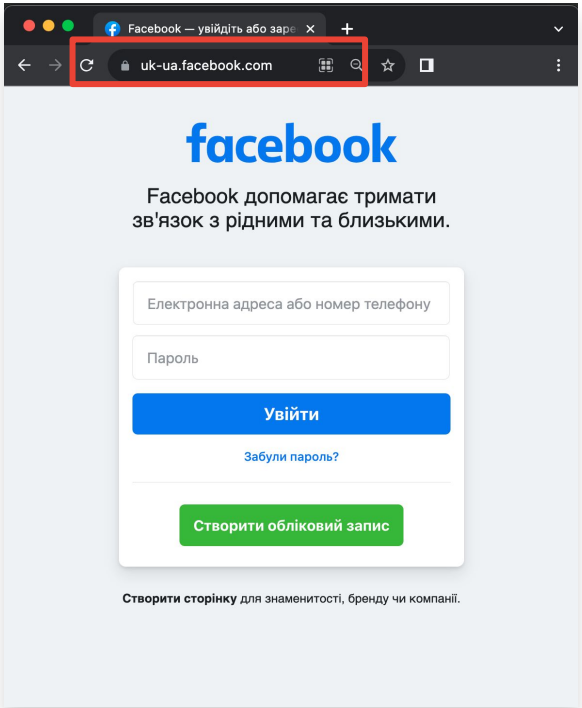
http:// evilphishingsite.tld /catalog/paypal/

Справжнє посилання не відповідає тексту.

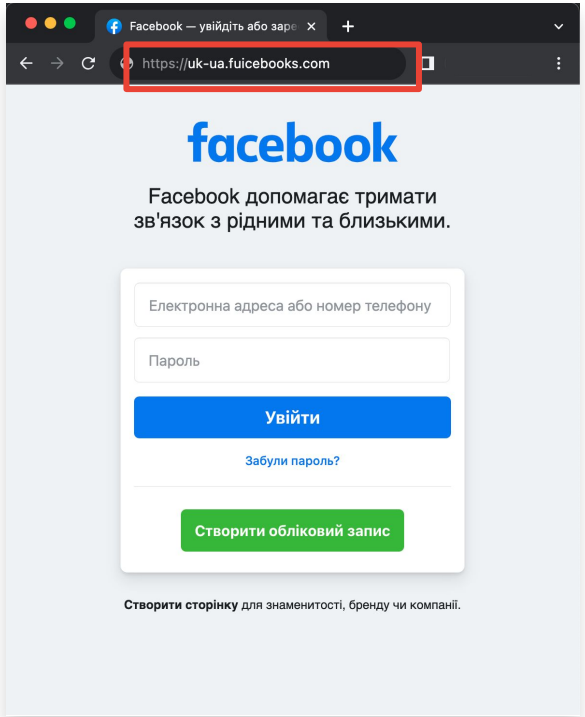
З повагою,
Відділ PayPal по роботі з клієнтами

Будь ласка, не відповідайте на цей електронний лист. На листи, надіслані на цю адресу, не можна відповідати. Для отримання допомоги увійдіть до свого облікового запису PayPal і виберіть посилання "Help" у нижньому колонтитулі будь-якої сторінки
Щоб отримувати сповіщення звичайним текстом замість HIML, змініть свої налаштування тут

Приклад №2

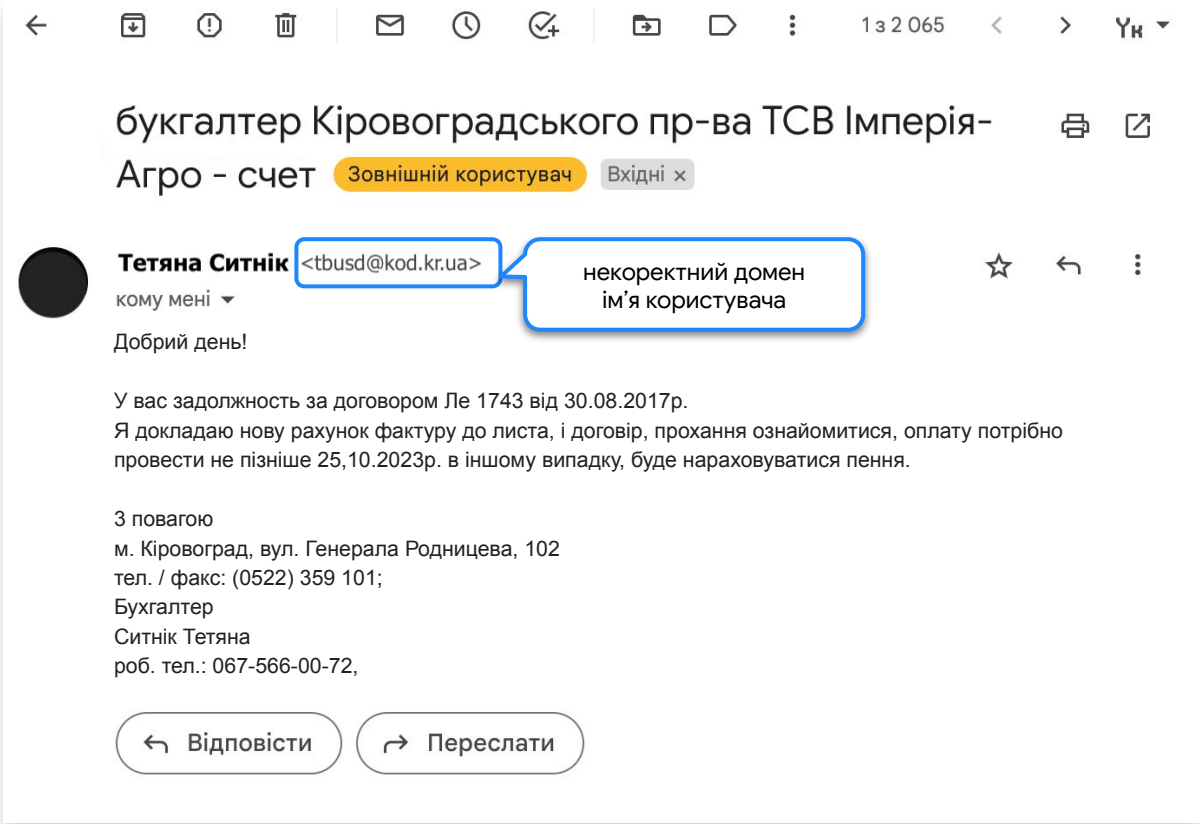


uk-ua.facebook.com



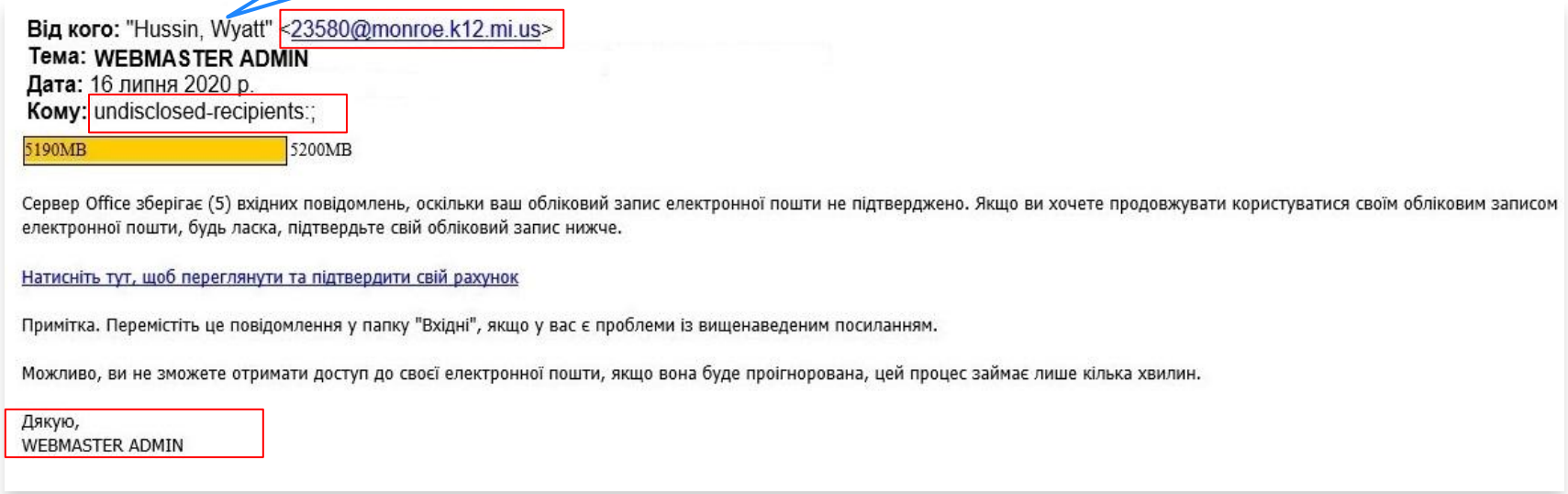
uk-ua.fuicebooks.com

Приклад №3


1 з 2 065
букгалтер Кіровоградського пр-ва ТСВ Імперія-Агро - счет
Зовнішній користувач
Вхідні ×
Тетяна Ситнік <tbusd@kod.kr.ua>
некоректний домен
ім'я користувача
кому мені
Добрий день!
У вас задолжность за договором Ле 1743 від 30.08.2017р.
Я докладаю нову рахунок фактуру до листа, і договір, прохання ознайомитися, оплату потрібно провести не пізніше 25,10.2023р. в іншому випадку, буде нараховуватися пення.
З повагою
м. Кіровоград, вул. Генерала Родницева, 102
тел. / факс: (0522) 359 101;
Бухгалтер
Ситнік Тетяна
роб. тел.: 067-566-00-72,
Відповісти
Переслати

Приклад №5

невідомий відправник



Від кого: "Hussin, Wyatt" <23580@monroe.k12.mi.us>
Тема: **WEBMASTER ADMIN**
Дата: 16 липня 2020 р.
Кому: undisclosed-recipients:;

5190MB 5200MB

Сервер Office зберігає (5) вхідних повідомлень, оскільки ваш обліковий запис електронної пошти не підтверджено. Якщо ви хочете продовжувати користуватися своїм обліковим записом електронної пошти, будь ласка, підтвердьте свій обліковий запис нижче.

Натисніть тут, щоб переглянути та підтвердити свій рахунок

Примітка. Перемістіть це повідомлення у папку "Вхідні", якщо у вас є проблеми із вищенаведеним посиланням.

Можливо, ви не зможете отримати доступ до своєї електронної пошти, якщо вона буде проігнорована, цей процес займає лише кілька хвилин.

Дякую,
WEBMASTER ADMIN

Кейс №1. Чи є це фішингом? Чому?

Ввідні дані:

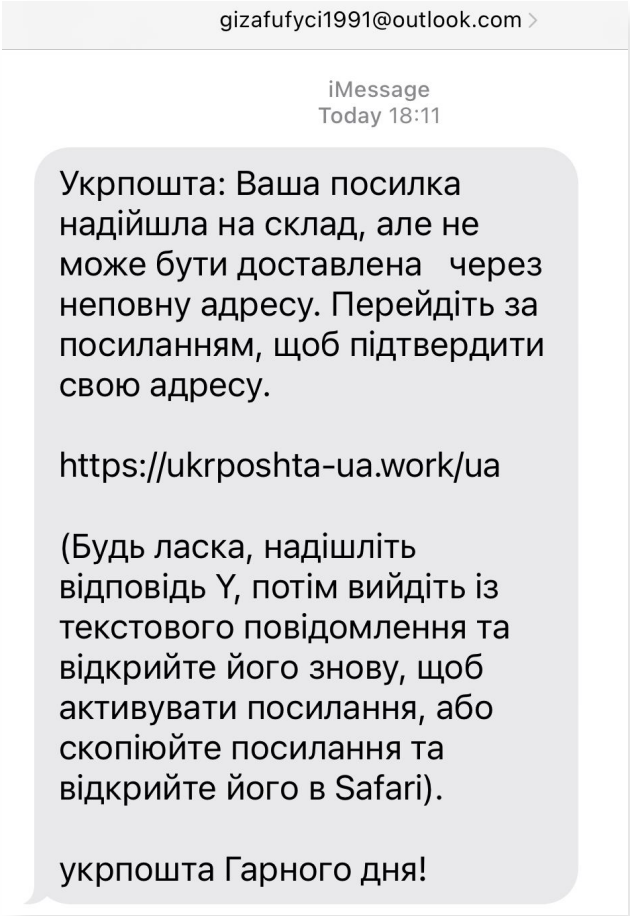
- Співробітниця - адміністраторка служби безпеки
- Вона підписана на різноманітні розсилки з робочої пошти
- Впродовж робочого дня, вона постійно переглядає вебсторінки
- Одного дня вона отримує такий e-mail від Ryanair

Кейс №2

Ввідні дані:

- Отримане повідомлення по iMessage від Укрпошти про неможливість доставлення посилки
- Заклик пройти за посиланням, щоб підтвердити адресу

Що має зробити співробітник? Чи є це фішингом?

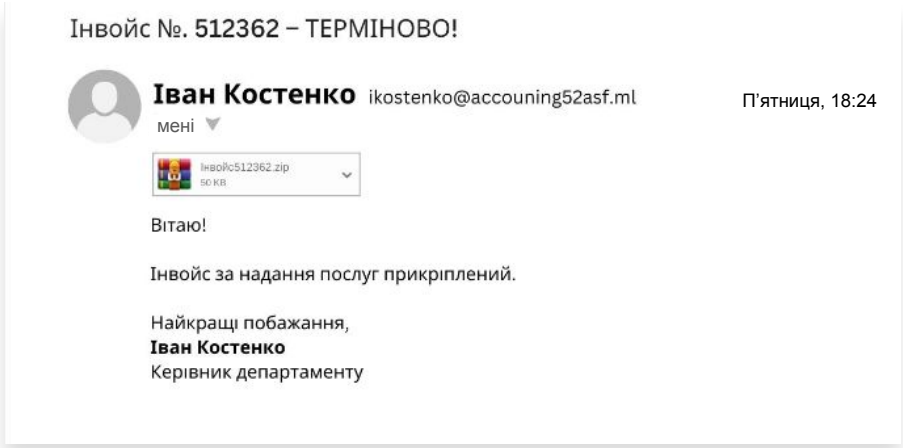


Кейс №3

Ввідні дані:

- Співробітник - бухгалтер
- Одного дня він отримує електронний лист від керівника департаменту Івана
- Лист має рахунок за надані послуги та прикріплений до листа як заархівований файл

Що має зробити співробітник? Чи є це фішингом?

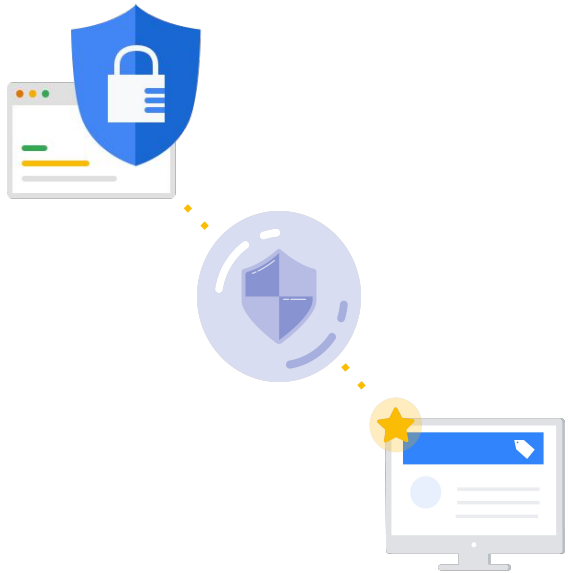


Висновки та поради

Найкращі практики забезпечення безперервності бізнесу

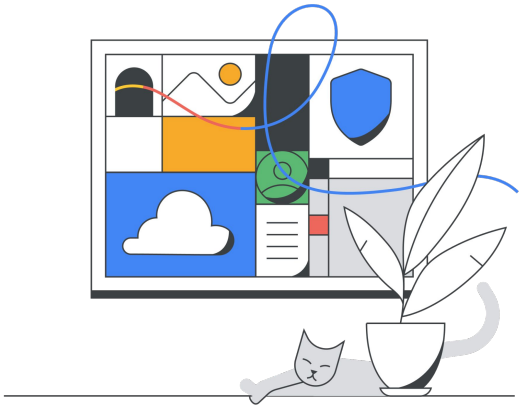
Погодьте план безперервності бізнесу:

1. Визначте критичні бізнес-процеси та активи, та захистіть саме їх в першу чергу
2. Розробіть плани швидкого відновлення систем
3. Перевіряйте та оновлюйте політики та плани регулярно



Наступні кроки у разі виявлення інцидентів безпеки

- Співробітник: повідомте про подію відповідальній особі
- Керівник: зверніться до політики кризових комунікацій у залежності від того, чи є інцидент внутрішнім або впливає на зовнішніх клієнтів
- Технічний персонал: розпочніть процес реагування на інцидент



Дякую за увагу!