НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

Кібергігієна

Безпека в Інтернеті

Зміст

Основи кібергігієни

Ключові поняття та базові принципи захисту інформації в державних органах

- Вступ
- Визначення
- Загальні заходи кібергігієни

Технічні заходи захисту

Впровадження інструментів та налаштувань для забезпечення безпеки інформаційних систем

- Захист інформаційної системи
- Встановлення патчів та оновлень
- Протидія шкідливому ПЗ
- Міжмережеві екрани (Firewalls)
- Wi-Fi мережі
- Налаштування веб-браузера
- Мобільні пристрої
- Віддалений доступ

Зміст (продовження)

Застосування належних практик доступом

Стратегії контролю доступу для захисту конфіденційної інформації.

- Паролі
- Облікові записи
- Доступ співробітників
- Журнали (логування)

Підсумок та висновки

Узагальнення ключових принципів та системний підхід до кібербезпеки

- Регулярні тренінги
- Підсумок
- Висновок

Підвищення обізнаності з кібербезпеки та навчання та поширені кіберзагрози

Ознайомлення з основними загрозами та навчання персоналу.

- Атаки соціальної інженерії
- Фішинг
- Drive-by завантаження
- Атаки «людина посередині» (MITM)
- USB drop атаки
- Шкідливе ПЗ (Malware)

ВСТУП

Ця презентація є оглядом **мінімальних стандартів** для впровадження систем кібергігієни у **державних органах влади.** Вона містить перелік **базових заходів**, які кожна організація має впровадити, аби забезпечити **належний рівень інформаційної безпеки** своїх цифрових систем, зокрема тих, що обробляють, зберігають або передають **службову чи конфіденційну інформацію.**

Метою є пояснення **важливості кібергігієни в державному секторі** та надання **практичних кроків** для **зменшення ризиків**, пов'язаних із **кібератаками, витоками даних чи технологічними збоями**, які можуть вплинути на **стабільність роботи державної інфраструктури та якість надання послуг громадянам.**

> Безпека в кіберпросторі багато в чому схожа на базову гігієну. У 1850 році угорський лікар **Ігнац Земмельвайс** започаткував революцію в медицині, закликавши до **регулярного миття рук.** Його відкриття, хоча спершу й ігнорували, згодом стало фундаментом профілактики інфекцій. Так само й кібергігієна — це **щоденні практики, які значно зменшують ризик зараження шкідливим програмним забезпеченням, несанкціонованого доступу до систем або втрати критичних даних.**

У контексті **державного управління**, де від сталості та безпеки IT-систем залежить **національна безпека, довіра громадян та ефективність адміністративних процесів**, системна кібергігієна є **не розкішшю, а обов'язковою умовою стабільної роботи.**

Кожен державний орган має впроваджувати **внутрішні політики інформаційної безпеки**, налаштовувати відповідні **технічні засоби захисту**, а також забезпечувати **регулярне навчання персоналу** для формування **стійкої культури безпеки.**

Визначення

Існує багато різних визначень кібергігієни, і всі вони є точними:

> **Digital Guardian** визначає кібергігієну як «практики та кроки, які користувачі комп'ютерів та інших пристроїв здійснюють для підтримки здоров'я системи та покращення онлайн-безпеки».
>
> **Security Magazine** описує кібергігієну як «забезпечення роботи базових засобів безпеки та їх послідовного застосування у вашому середовищі».
>
> **CyberSecurity Forum** зазначає, що кібергігієна «є розмовним терміном, який стосується найкращих практик та інших дій, які адміністратори систем і користувачі можуть здійснювати для покращення кібербезпеки під час звичайної онлайндіяльності, такої як веб-серфінг, електронна пошта, обмін повідомленнями тощо».
>
> **Endpoint Blog** характеризує кібергігієну як «набір звичних практик для забезпечення безпечного оброблення критичних даних та захисту мереж. Це схоже на особисту гігієну, коли ви розробляєте рутину маленьких, чітких дій для запобігання або пом'якшення проблем зі здоров'ям».

Іншими словами, кібергігієна — це набір базових практик безпеки, які можуть здійснювати всі співробітники для захисту себе, а також здоров'я апаратного та програмного забезпечення у комп'ютерних системах організації.

Загальні заходи кібергігієни

Для забезпечення надійного кіберзахисту організація має впровадити низку **системних заходів**, які складають фундамент «гігієни» в кіберпросторі:

Визначення політик безпеки

Створення чітких правил роботи з даними, паролями, пристроями та доступом.

Стандартизовані процедури

Шаблони дій для регулярних процесів (оновлення, резервне копіювання, інцидент-менеджмент).

Навчання персоналу

Регулярне підвищення обізнаності співробітників щодо нових типів загроз та методів їх розпізнавання.

Регулярне оновлення програмного забезпечення

Усунення вразливостей у системах.

Моніторинг і аудит

Постійне спостереження за активністю у мережі для виявлення підозрілої поведінки.

Резервне копіювання

Створення копій важливих даних, які можуть бути відновлені у разі інциденту.

Усі ці заходи мають впроваджуватись **на рівні організаційної культури**, а не залишатись виключно відповідальністю IT-відділу.

У наступних розділах буде розглянуто детальніше, які **кіберзагрози** найчастіше трапляються в державному секторі та які **практики** варто реалізувати для їх запобігання.

Захист інформаційної системи

Оновлюйте операційну систему та програмне забезпечення

Підтримка системи та додатків у **актуальному стані** може здаватися клопіткою, але це надзвичайно важливо з кількох причин:

1

Безпека

Оновлення допомагають **захистити** комп'ютер від атак. Коли виявляються нові загрози, виявляються прогалини, які кіберзлочинці використовують для компрометації системи та додатків. Ці прогалини усуваються через оновлення.

2

Нові функції

Microsoft, Apple, Android та інші пропонують додаткові функції в оновленнях, а деякі програми інших виробників можуть не працювати без попереднього оновлення цих систем.

3

Виправлення

Не всі проблеми викликані вірусами. Деякі збої виникають у системах і програмному забезпеченні і потребують просто **виправлення**. Багато збоїв, які впливають на кінцевих користувачів, усуваються через оновлення.

Саме тому доцільно використовувати **автоматичне оновлення** систем і додатків. Це забезпечує автоматичне завантаження необхідних виправлень безпеки, які усувають вразливості системи.

Пам'ятайте: коли з'являється повідомлення про оновлення, це може бути корисно, але все одно важливо не натискати бездумно.

Протидія шкідливому ПЗ

Впровадження антивірусного програмного забезпечення

Шкідливе програмне забезпечення (malware) – це будь-яка програма, створена для виконання небажаних або шкідливих дій, що впливають на комп’ютери, сервери та мережі. Антивірусне програмне забезпечення є необхідною частиною комплексу заходів з кібербезпеки.

Раніше компанії з кібербезпеки намагалися створити універсальний антивірус, який би задовольняв усі потреби в одному продукті. Однак зараз це вже не ефективно, оскільки кіберзлочинці розвинулися. Загрози стають усе більш складними, що змушує компанії розробляти спеціалізовані антивірусні програми.

Важливо розуміти, що всі віруси є шкідливим ПЗ, але не все шкідливе ПЗ є вірусом. Комп’ютерний вірус поширюється від користувача до користувача шляхом самовідтворення, а антивірусні програми визначають відомі загрози за унікальними сигнатурами. Сучасні антивірусні сканери використовують евристичне виявлення, що дозволяє проактивно шукати шкідливий код.

Додаткові можливості антивірусного ПЗ

Захист у реальному часі

Постійний моніторинг системи та файлів для миттєвого блокування загроз.

Захист від спаму та крадіжки особистих даних

Фільтрація небажаних електронних листів, фішингових атак та запобігання крадіжці особистих даних.

Сканування під час завантаження системи

Перевірка завантажуваних файлів та програм перед їх виконанням.

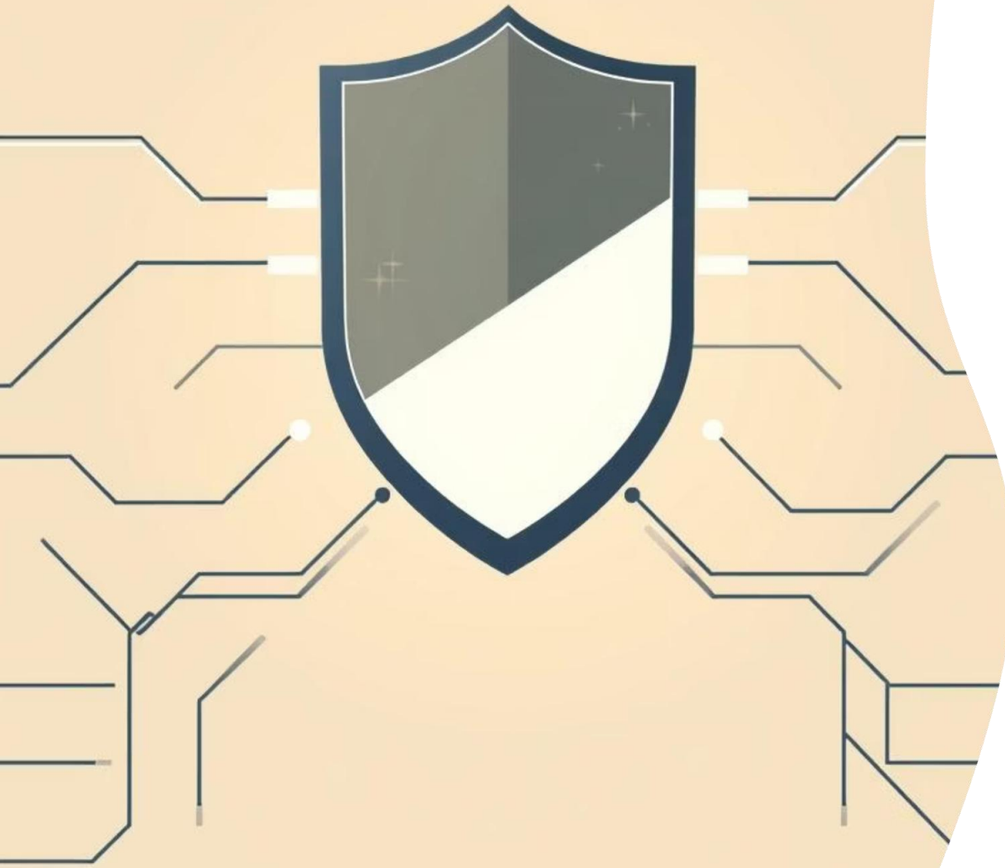
Сканування зовнішніх пристроїв

Автоматичне сканування USB-накопичувачів, зовнішніх дисків та інших підключених пристроїв.

Захист чутливої інформації

Запобігання витоку персональних даних та конфіденційної інформації.

Антивірусні рішення блокують більшість шкідливих і потенційно небажаних програм, а також сканують вхідні дані, щоб запобігти виконанню шкідливого ПЗ на пристрої, зміні налаштувань або завантаженню додаткового компрометованого програмного забезпечення. Вони також блокують доступ користувачів до вебсайтів, відомих розповсюдженням шкідливого коду (фішинг і атаки програм-вимагачів).



Мережеві екрани (Firewalls)

Захист мереж та пристроїв

Мережеві екрани забезпечують захист від кібератак, допомагаючи охороняти комп’ютери та мережі. Мережеві екрани можуть бути програмними або апаратними, встановленими на пристрої або в мережі, але всі вони працюють однаково: перевіряють трафік і блокують небажані пакети.

Мережеві екран значно знижує ризики для окремих користувачів і організацій. Організації, які не використовують мережеві екрани , полегшують роботу кіберзлочинців, дозволяючи їм потенційно отримати доступ до систем і файлів, а також поширювати шкідливий контент. Тому правильно налаштований, підтримуваний і контрольований фаєрвол є ключем до захисту даних, мережі та пристроїв.

Мережеві екрани захищають від широкого спектра загроз, зокрема:

- Віддалений вхід
- Перехоплення пошти
- Уразливості
- DoS атаки
- Електронні бомби
- Шкідливі макроси

WI-FI мережі

Захист WI-FI мереж

Для забезпечення безпеки ваших бездротових мереж, дотримуйтесь наступних ключових рекомендацій. Правильно налаштовані WI-FI мережі повинні бути захищеними, зашифрованими та прихованими, щоб уникнути несанкціонованого доступу та потенційних кібератак.

Шифрування мережі

Увімкніть шифрування бездротової мережі (WPA2 або WPA3) для конфіденційності даних. Замініть маршрутизатор, якщо він не підтримує актуальні протоколи шифрування.

Актуальне ПЗ

Регулярно встановлюйте всі оновлення та патчі безпеки для вашого маршрутизатора, щоб захиститися від відомих вразливостей.

Розташування маршрутизатора

Розміщуйте маршрутизатор у центрі офісу/будинку, подалі від вікон та дверей, щоб мінімізувати перехоплення сигналу ззовні.

Фільтрація MAC-адрес

Увімкніть фільтрацію MAC-адрес, щоб контролювати, які пристрої можуть підключатися до вашої мережі.

Відключення віддаленого адміністрування

Вимкніть функцію віддаленого адміністрування, якщо вона не потрібна, щоб запобігти зовнішньому доступу до налаштувань вашого маршрутизатора.

Налаштування веб-браузера

Конфігурування безпеки веб-браузера

Веб-браузери використовуються майже на всіх пристроях. Оскільки вони є невід'ємною частиною щоденного використання, важливо налаштувати їх безпечно, особливо враховуючи, що вони зазвичай використовуються з налаштуваннями за замовчуванням.

Веб-браузери є значною ціллю для кіберзлочинців, а ненадійний браузер може залишити користувачів або організації відкритими для встановлення шкідливого контенту без їх відома. У деяких випадках це може призвести до втрати контролю над пристроєм, використання інформації користувача або навіть використання пристрою для атак на інших.

Будь-який веб-браузер (Firefox, Chrome, DuckDuckGo, Brave тощо) повинен бути захищеним. Для цього необхідно:

- Увімкнути автоматичні оновлення
- Блокувати спливаючі вікна, плагіни та фішингові сайти
- Не зберігати паролі у браузері
- Вимкнути сторонні кукі (third-party cookies)
- Видалити невикористовувані розширення браузера
- Регулярно оновлювати використовувані розширення
- Відвідувати сайти через HTTPS замість HTTP

Мобільні пристрої та віддалений доступ

Захист мобільних пристроїв

Мобільні пристрої є значним викликом для безпеки, особливо якщо вони містять конфіденційну інформацію або мають доступ до корпоративної мережі. Для їх безпечного використання необхідно:

- Захищати пристрої паролем;
- Шифрувати всі дані;
- Використовувати програми безпеки для захисту в публічних мережах.

Віддалений доступ

Для безпечного, зашифрованого та прихованого віддаленого доступу необхідно:

- Регулярно оновлювати програмне забезпечення;
- Обмежити доступ з підозрілих локацій;
- Використовувати складні паролі;
- Включати багатофакторну аутентифікацію (MFA);
- Моніторинг та сповіщення про підозрілу активність.

Застосування належних практик – Паролі

Кожна організація повинна мати політику паролів, яка забезпечує використання складних та унікальних паролів, що регулярно змінюються. Паролі є першою лінією захисту від несанкціонованого доступу.

Найпоширеніші вразливості паролів:

- Звичка зберігати паролі в нотатках;
- Збереження паролів у браузерах;
- Використання паролів з особистою інформацією;
- Використання одного пароля для кількох облікових записів;
- Обмін паролями.

Найпростіший спосіб покращити поведінку користувачів щодо паролів — це використання менеджера паролів. Він дозволяє створювати, шифрувати та зберігати складні та унікальні паролі для різних облікових записів, вимагаючи від користувача пам’ятати лише один головний пароль.

Поради щодо створення політики паролів

Довші паролі кращі

Мінімум 12 символів.

Складність має значення

Використовуйте символи, великі/малі літери та цифри.

Уникайте передбачуваності

Використовуйте "абракадабру", без слів зі словників.

Унікальність паролів

Один запис – один пароль.

Пам'ятайте: важливо змінювати стандартні паролі перед тим, як передавати пристрої співробітникам, щоб уникнути ризику їхнього використання зловмисниками або інших серйозних порушень.

Управління обліковими записами

Використовуйте обмежені облікові записи для щоденної роботи

Існують два типи облікових записів: **Стандартний користувач (Standard User)** та **Адміністратор (Administrator)**.

1

Стандартний користувач

Обліковий запис стандартного користувача надає базові права, необхідні для виконання повсякденних завдань, такі як перегляд веб-сторінок, використання програм Microsoft Office, перевірка електронної пошти та інші офісні завдання. Цей тип облікового запису не дозволяє користувачам встановлювати програмне забезпечення або змінювати системні налаштування.

Переваги безпеки від використання облікового запису стандартного користувача:

- Захист від шкідливих програм: Запобігає встановленню небажаного або зловмисного програмного забезпечення.
- Обмеження доступу: Обмежує доступ до критично важливих системних файлів і налаштувань.
- Зниження ризику: Знижує загальний ризик компрометації системи у випадку успішної атаки.

2

Адміністратор

Обліковий запис адміністратора надає повний контроль над системою, дозволяючи встановлювати програмне забезпечення, змінювати системні налаштування, керувати іншими обліковими записами та виконувати інші адміністративні завдання. Цей тип облікового запису слід використовувати лише тоді, коли це абсолютно необхідно, і з максимальною обережністю.

Важливо, щоб адміністративні облікові записи використовувалися лише для виконання завдань, які вимагають підвищених привілеїв, а для повсякденної роботи використовувався стандартний обліковий запис, щоб мінімізувати ризики безпеки.

Ведення журналів (логування)

Ведення журналів є надзвичайно важливим для забезпечення безпеки системи. Логи надають детальну інформацію про всі дії, що відбуваються в системі, дозволяючи відстежувати події та виявляти потенційні загрози. Це критичний елемент для:

Налагодження (debugging)

Допомагає розробникам і системним адміністраторам знаходити та виправляти помилки у програмному забезпеченні та системах.

Відстеження помилок

Дозволяє ідентифікувати причини збоїв та аномалій, що виникають у системі.

Усунення проблем із продуктивністю

Надає дані для аналізу вузьких місць і оптимізації роботи системи.

Бухгалтерський облік

Фіксує транзакції та дії користувачів для фінансового моніторингу та звітності.

Аудит

Забезпечує докази відповідності нормативним вимогам та внутрішнім політикам безпеки.

Забезпечення безпеки

Виявляє підозрілу активність, спроби несанкціонованого доступу та кібератаки.

Підвищення обізнаності з кібербезпеки

Кібератака — це зловмисна і свідома спроба фізичної або юридичної особи порушити інформаційну систему іншої особи або організації. Зазвичай зловмисник прагне отримати певну вигоду від порушення роботи мережі цілі. Організації стикаються з безліччю кіберзагроз, а атакуючі використовують різні стратегії для спроб або здійснення атак.

Атаки соціальної інженерії

Атаки соціальної інженерії вводять жертву в оману та маніпулюють нею, щоб отримати інформацію або доступ до їхніх комп’ютерів. Цей тип атаки покладається на взаємодію з людиною та зазвичай включає маніпуляції користувачем, щоб він порушив процедури безпеки та найкращі практики, надаючи несанкціонований доступ до систем або розкриваючи конфіденційну інформацію.

У атаках соціальної інженерії кіберзлочинці приховують свою справжню особу та мотиви, видаючи себе за надійних осіб. Атака виконується шляхом обману користувачів, щоб вони натиснули на шкідливі посилання, або через фізичний доступ до комп’ютера.

Фішинг

Більшість кібератак починаються з фішингового електронного листа. Фішинг — це тип атаки соціальної інженерії, коли кіберзлочинці обманом змушують жертву передати конфіденційну інформацію або встановити шкідливе ПЗ.

Навіть при постійному покращенні технічних заходів безпеки, фішинг залишається одним із найпростіших і найдешевших способів для кіберзлочинців отримати доступ до конфіденційної та персональної інформації. Користувачу достатньо лише натиснути на посилання, щоб його безпека була під загрозою, і він міг стати жертвою крадіжки особистих даних.

Як працює фішинг?

Більшість фішингових кампаній використовують один із двох основних методів:

1. **Шкідливі вкладення** в електронних листах, які зазвичай мають тривожні теми, наприклад «INVOICE» (рахунок-фактура). При відкритті такі вкладення встановлюють шкідливе ПЗ на комп'ютері користувача.
2. **Посилання на шкідливі вебсайти**, які часто є клонами легітимних сайтів. Перехід на сайт може призвести до завантаження шкідливого ПЗ або сторінка входу на сайт може містити скрипти для збору облікових даних.

Поширені кіберзагрози

Spear Phishing: Цільова Атака

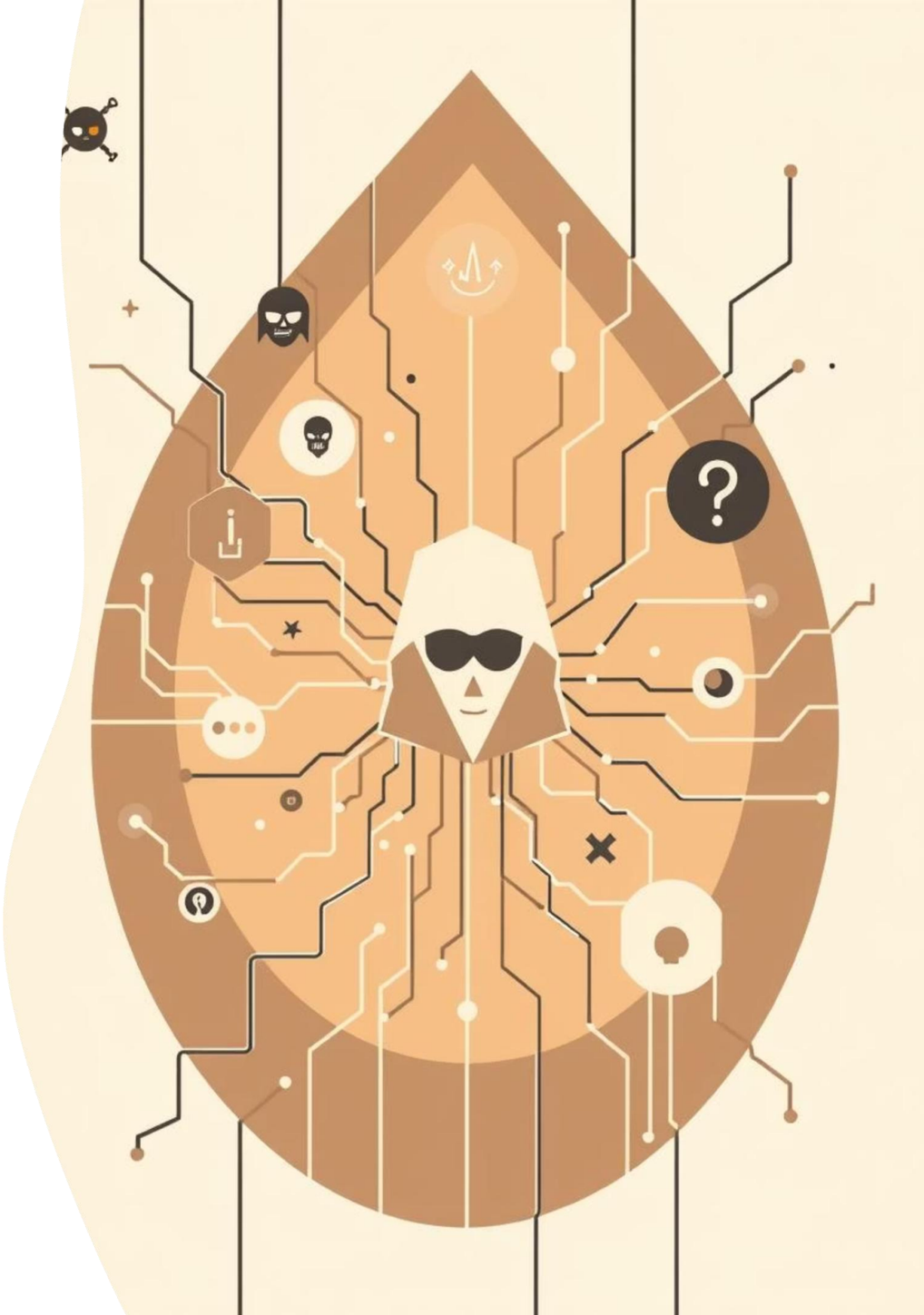
Spear phishing — це шкідлива атака з підробкою електронної пошти, спрямована на конкретну організацію або особу з метою несанкціонованого доступу до конфіденційної інформації. Такі атаки зазвичай проводять не випадкові хакери, а кіберзлочинці, що прагнуть фінансової вигоди або отримання цінної інформації.

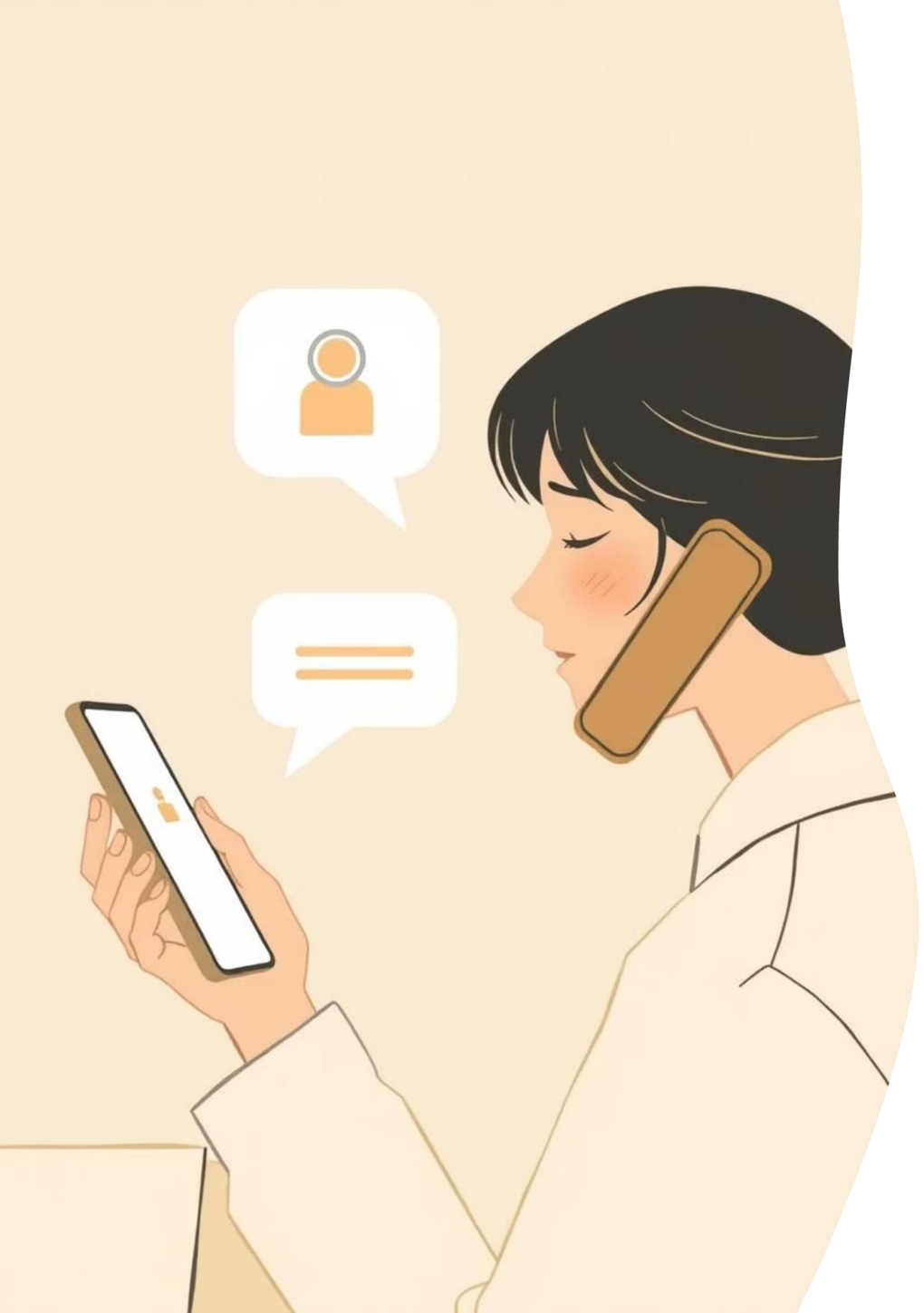
При spear phishing лист надсилається з надійного джерела, але веде на підроблений сайт із шкідливим ПЗ. Ці листи часто використовують креативні методи, щоб привернути увагу користувачів.

Spear phishing значно ефективніший за інші фішингові атаки, але вимагає від кіберзлочинців витрат часу та ресурсів на підготовче дослідження, оскільки шанси на успіх зростають, якщо вони заздалегідь дізнаються про свою ціль.

Whale Phishing (Whaling): Полювання на Велику Рибу

Whale phishing схожий на spear phishing, з кількома відмінностями. Якщо spear phishing зазвичай спрямований на членів групи, whale phishing фокусується на конкретній особі — зазвичай на «найважливішій особі» в організації.





Поширені кіберзагрози (продовження)

Vishing (голосовий фішинг)

Vishing або «голосовий фішинг» передбачає маніпуляції людьми через телефон. Зловмисники схиляють цільову особу до розкриття конфіденційної інформації, намагаючись використати ці дані для власної вигоди, зазвичай для фінансової.

Smishing (SMS-фішинг)

Термін smishing означає фішинг через SMS і передбачає отримання текстового повідомлення замість електронного листа. Цільові особи отримують оманливе повідомлення, яке змушує їх надати особисту або фінансову інформацію кіберзлочинцю, який видає себе за державну установу, банк або іншу легітимну компанію.

Атаки Smishing часто спрямовані на отримання персональної або банківської інформації, такої як облікові дані, номери кредитних карток та ідентифікаційні номери. Потім зловмисники використовують цю інформацію для проведення різних атак, включно з фінансовими шахрайствами, шахрайством із подарунковими картками або обслуговуванням клієнтів.

Як запобігти фішинговим атакам

У електронній пошті: уважно перевіряйте листи, особливо якщо вони містять вкладення або веб-посилання. Освіта щодо розпізнавання фішингових спроб і повідомлення про підозрілі листи надзвичайно важлива. Ось кілька ознак, що лист може бути шкідливим:

Навчання та обізнаність

Регулярно проводьте тренінги для співробітників, щоб навчити їх розпізнавати та повідомляти про фішингові спроби. Розвивайте культуру обережності.

Перевірка відправника

Завжди уважно перевіряйте повну адресу електронної пошти відправника на наявність підозрілих символів, розбіжностей або елементів спуфінгу.

Обережність з посиланнями

Перед натисканням наведіть курсор на посилання, щоб побачити справжню URL-адресу. Якщо вона виглядає підозріло або веде на невідомий домен, не відкривайте її.

Увага до вкладень

Будьте вкрай обережними з несподіваними вкладеннями, особливо якщо вони пропонують "термінову" інформацію або вимагають негайної дії. Не відкривайте їх без перевірки.

Двофакторна аутентифікація (MFA)

Увімкніть MFA для всіх облікових записів, де це можливо, щоб додати додатковий рівень безпеки та ускладнити доступ зловмисникам.

Ознаки фішингових листів, на які варто звернути увагу:

- **Орфографічні та граматичні помилки:** Непрофесійний текст, численні помилки, незвичні формулювання або дивний синтаксис є частою ознакою шахрайства. Легітимні організації зазвичай ретельно перевіряють свої повідомлення.
- **Підозрілі посилання:** URL-адреси, які не відповідають назві компанії (наприклад, "paypal.com.ua" замість "paypal.com"), містять дивні символи або є скороченими. Завжди наведіть курсор миші (або довго натисніть на мобільному) на посилання, щоб побачити справжню адресу перед переходом.
- **Підозрілі вкладення:** Неочікувані файли, особливо з розширеннями типу `.zip`, `.exe`, `.docm`, `.xlsm`, або файли з подвійними розширеннями (наприклад, `invoice.pdf.exe`). Перевіряйте легітимність відправника та зміст листа, перш ніж відкривати будь-які вкладення.
- **Примусові повідомлення:** Листи, що створюють відчуття паніки, терміновості або погрози ("ваш обліковий запис буде заблоковано", "негайні дії необхідні", "термін дії вашої картки закінчується"). Фішери використовують емоції для спонукання до необдуманих дій.
- **Спуфінг та невідповідності:** Адреса відправника може виглядати схожою на справжню (наприклад, `supp0rt@company.com` замість `support@company.com`) або бути повністю підробленою. Невідповідності між іменем відправника та фактичною адресою, а також нестандартні вітання (наприклад, "Шановний клієнте" замість вашого імені) також є червоними прапорцями.
- **Запити особистої інформації:** Жодна легітимна організація ніколи не запитуватиме конфіденційні дані (паролі, номери банківських карток, ПІН-коди або інші особисті дані) через електронну пошту або за посиланнями в листах.

Шкідливе ПЗ (Malware)

Malware — загальний термін для будь-якого файлу чи програми, призначеної для пошкодження або порушення роботи комп'ютера.

Ботнети

інфікують велику кількість пристроїв, підключених до Інтернету. Деякі ботнети складаються з багатьох пристроїв, кожен з яких використовує невелику кількість ресурсів процесора. Це ускладнює виявлення ботнету навіть під час його роботи.

Програмне забезпечення-вимагач (Ransomware)

шифрує інформацію користувача та вимагає викуп для отримання ключа розшифровки. Сплата викупу не гарантує відновлення даних.

Шпигунське ПЗ (Spyware)

нелегально відстежує активність користувача та збирає персональні дані.

Трояни

виглядають як легітимне ПЗ, але при виконанні здійснюють шкідливу діяльність.

Віруси та черв'яки

шкідливий код, який встановлюється без відома користувача. Віруси можуть самовідтворюватися, поширюючись на інші комп'ютери, прикріплюючись до файлів. Черв'яки також самовідтворюються, але не потребують прикріплення до іншої програми.

Інші поширені кіберзагрози

- **Drive-by** завантаження

  У разі атаки **drive-by download** шкідливі скрипти завантажуються на комп’ютер або інший пристрій без відома користувача, піддаючи його різним кіберзагрозам. Це може трапитися на будь-якому пристрої з будь-якою операційною системою, зазвичай під час перегляду скомпрометованого вебсайту.

- Атаки «людина посередині» (MITM)

  MITM-атака відбувається, коли кіберзлочинець таємно вставляє себе між пристроями або між пристроєм та незахищеною Wi-Fi мережею, щоб перехоплювати комунікації, які можуть бути прочитані або змінені. У такому випадку користувач може ненавмисно передати кіберзлочинцю облікові дані чи іншу інформацію.

- **USB drop** атаки

  USB drop атака передбачає підключення USB-пристрою із шкідливим кодом до комп’ютера. Як правило, загроза такої атаки полягає у зараженні шкідливим ПЗ або вірусом. Зараження через USB може бути як навмисним, так і випадковим, залежно від виду шкідливого ПЗ.

  Організаціям рекомендується припинити довіряти застарілій USB-технології та використовувати захищені цифрові мережі через хмарне сховище.

Регулярні тренінги

Щоб підвищити обізнаність щодо кіберзагроз та інформаційної безпеки, навчання з кібергігієни є одним із найважливіших елементів, які може впровадити будь-яка організація. Воно навчає співробітників уникати, розпізнавати та повідомляти про потенційні загрози.

Запис співробітників на комплексний курс з обізнаності у сфері безпеки — це проактивний захід, що допомагає запобігати кібератакам. Ігнорування людського фактору залишає «двері відкритими» для кіберзагроз.

Навчання з безпеки допомагає підвищити знання користувачів про потенціальні загрози, що:

- підвищує стійкість до кіберзагроз;
- забезпечує захист інформації;
- зменшує ризики порушення конфіденційності;
- підвищує готовність до інцидентів безпеки.

Підсумок

Більшість кібератак виникає через порушення базових принципів кібергігієни: відсутність оновлень, помилки в налаштуваннях, низьку обізнаність персоналу. Нехтування щоденними практиками безпеки створює загрозу зсередини самої установи.

Щоб покращити кібергігієну в організації:

1. Навчайте персонал основам кібербезпеки та розпізнаванню загроз.
2. Регулярно оновлюйте всі пристрої (сервери, ПК, мобільні телефони).
3. Запровадьте політики контролю доступу (MFA, складні паролі).
4. Контролюйте та забезпечте прозорість мережевих доступів.

Замість ускладнення систем, варто повертатись до основ — чітко прописаних правил, навчання та регулярного моніторингу.

Висновок

Низький рівень кібергігієни є основною причиною успішних атак. Тому організації мають формувати культуру відповідального ставлення до безпеки на всіх рівнях.

Рекомендовані у цій презентації заходи актуальні не лише в межах установи, а й у повсякденному цифровому житті. Коли співробітники дотримуються кібергігієни вдома — вони автоматично підвищують рівень безпеки і в робочому середовищі.

Культура кібергігієни повинна охоплювати обидва простори — **особистий і професійний**.