ПРАКТИЧНА РОБОТА. Загрози при роботі в Інтернеті і їх уникнення
МЕТА: навчитися розпізнавати типові загрози в мережі (фішинг, шкідливе ПЗ, соціальну інженерію), відпрацювати навички створення надійних паролів та освоїти базові алгоритми захисту персональних даних для мінімізації ризиків у цифровому середовищі.

!Усі завдання виконати в Google документі

ЗАВДАННЯ 1. «Кейс-стаді»

Ситуація: *«Ваш знайомий у месенджері просить терміново скинути йому 2000 грн на картку, бо він потрапив у біду. Які ваші дії?»*

Написати алгоритм із 3-х кроків, як перевірити автентичність прохання та не стати жертвою шахраїв.

ЗАВДАННЯ 2. «Налаштування приватності»

Зайдіть в налаштування безпеки свого (або навчального) облікового запису Google або будь-якої соцмережі.

Перевірити список активних сеансів (де ще виконано вхід).

Перевірити, які сторонні додатки мають доступ до даних.

Крок 1. Вхід у центр керування

1. Відкрийте браузер і перейдіть за посиланням: myaccount.google.com.
2. Переконайтеся, що ви увійшли у свій навчальний або власний акаунт.
3. У меню зліва (або зверху на мобільних пристроях) оберіть вкладку **«Безпека»** (Security).

Крок 2. Ревізія активних сеансів (Ваші пристрої)

1. Прокрутіть сторінку вниз до розділу **«Ваші пристрої»**.
2. Натисніть **«Керувати всіма пристроями»**.
3. Проаналізуйте список:
    - Чи є у списку пристрої, якими ви вже не користуєтеся?
    - Чи є там незнайомі вам гаджети або входи з інших міст?
4. **Дія:** Якщо ви знайшли підозрілий або старий пристрій, натисніть на нього та оберіть **«Вийти»**.
5. *Зафіксуйте у звіті:* Скільки пристроїв мали доступ до вашого акаунта до очищення?

Крок 3. Перевірка доступу сторонніх додатків

1. Поверніться у розділ «Безпека» і знайдіть блок **«Зв’язки зі сторонніми додатками й сервісами»**.

2. Натисніть **«Переглянути всі зв’язки»**.
3. Перегляньте список ігор, сайтів чи тестів, яким ви колись надали доступ до свого імені, пошти чи Google Диску.
4. **Дія:** Виберіть додаток, яким ви більше не користуєтеся, натисніть на нього та оберіть **«Видалити всі зв’язки»**.
5. *Зафіксуйте у звіті:* Назву одного додатка, доступ якому ви скасували.

Крок 4. Перевірка двофакторної автентифікації (2FA)

1. У розділі «Безпека» знайдіть підрозділ **«Як ви входите в обліковий запис Google»**.
2. Знайдіть пункт **«Двоступенева перевірка»**.
3. **Дія:**
    - Якщо вона «Вимкнена» — натисніть на неї та подивіться, які способи підтвердження пропонує система (SMS, додаток Authenticator, електронний ключ).
    - Якщо вона «Увімкнена» — перевірте, чи актуальний там номер телефону.
4. *Зафіксуйте у звіті:* Який основний спосіб підтвердження входу ви б обрали як найнадійніший і чому?

Крок 5. Перевірка безпечних технологій

1. Знайдіть пункт **«Безпечний перегляд із покращеним захистом»**.
2. Переконайтеся, що цей перемикач **увімкнено**. Це дозволяє браузеру активніше попереджати вас про небезпечні сайти та завантаження.

Зробіть скриншоти

1. **Скріншот** сторінки «Ваші пристрої» після видалення зайвих сеансів.
2. **Скриншот** розділу «Двоступенева перевірка» (як доказ того, що учень знає, де вона знаходиться).
3. **Короткий висновок (1-2 речення):** «Під час аудиту я виявив(ла) [кількість] зайвих пристроїв та [кількість] додатків з доступом до моїх даних. Тепер мій акаунт захищений краще».