Конспект уроку:

«Інтернет без пасток»

(для 6-7 класів)

Учитель: Боєчко О.Р.

-2026 -

Тема: «Інтернет без пасток» (6-7 кл.)

Тип уроку: урок формування компетентностей із застосуванням кейс-методу, інтерактивних технологій та розвитку критичного мислення.

Форма уроку: урок-дослідження з елементами групової роботи.

Мета уроку:

***навчальна*:** сформувати в учнів уявлення про основні загрози в Інтернеті; навчити розпізнавати фішинг, кібербулінг, онлайн-шахрайство; сформувати алгоритм безпечної поведінки онлайн.

***розвивальна*:** розвивати критичне мислення; формувати вміння аналізувати ситуації та приймати рішення; розвивати навички аргументованого висловлювання.

виховна: виховувати відповідальність за власну цифрову репутацію; формувати культуру безпечного онлайн-спілкування.

Обладнання: роздруковані картки з кейсами (ситуаціями); маркери, аркуші для груп; інтерактивна вправа Genially з кейс-ситуаціямиЖкартки “Заряд знань” та магніти (для рефлексії)

Компетентності, що формуються: інформаційно-цифрова**,** соціальна та громадянська**,** уміння вчитися**,** ініціативність та підприємливість**,** критичне мислення

ХІД УРОКУ

І. Організаційний момент (2 хв)

Привітання, перевірка готовності учнів до уроку.

Слова вчителя:

Інтернет — це величезний світ можливостей. Але чи завжди він безпечний? Сьогодні ми спробуємо стати експертами з цифрової безпеки.

ІІ. Мотивація навчальної діяльності (5 хв)

Метод «Провокаційні твердження»

На екрані з’являються твердження:

1. Якщо профіль закритий — я повністю в безпеці.
2. Якщо повідомлення від знайомого — можна довіряти.
3. Безкоштовні подарунки в Інтернеті — це завжди вигідно.

Учні висловлюють позицію та аргументують.

Проблемне запитання:

Чому люди стають жертвами інтернет-пасток?

Оголошення теми і мети уроку.

III. Актуалізація знань (5 хв)

Слова вчителя:

Сьогодні ви не просто учні. Ви — експерти з цифрової безпеки. Але кожен експерт повинен знати професійні терміни. Перевіримо, чи готові ви?

Запускаємо колесо wheelofnames (https://wheelofnames.com/zkw-cyy).

Учні почергово прокручують колесо на екрані інтерактивної панелі. Отримавши термін:

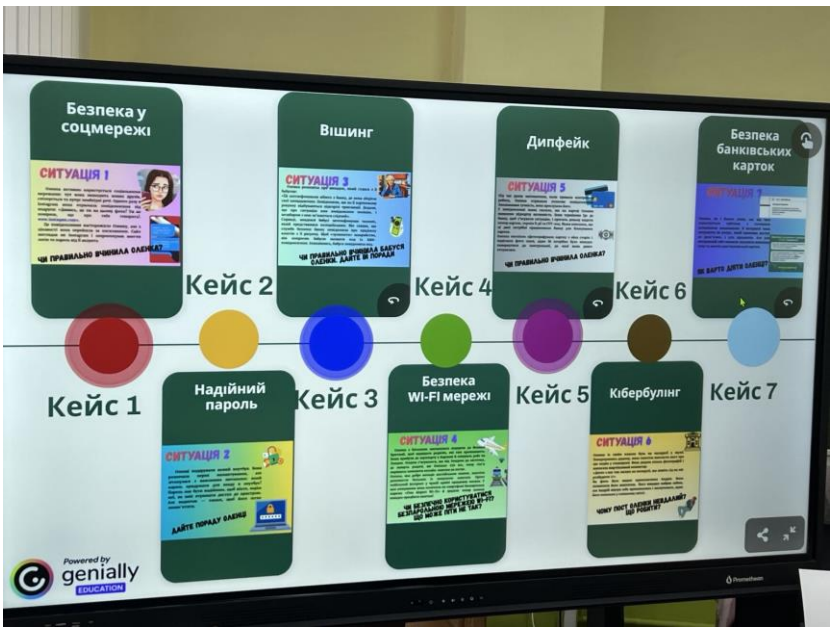
1. Пояснює його своїми словами.
2. Наводить приклад із життя.
3. Каже, чим це може бути небезпечно (якщо доречно).

Клас може доповнювати.

Слова вчителя: “Ви чудово знаєте терміни. А тепер перевіримо, чи зможете ви застосувати ці знання на практиці”

IV. Основна частина (20 хв)

Інтерактивна вправа Genially«Експерти цифрової безпеки»



Учні об’єднуються у 3 групи (по 4 учні). Кожна група почергово методом випадкового вибору обирає кейс-ситуацію, наперед не знаючи її змісту (використовуємо інтерактивну стрічку Genially, яку виводимо на екран інтерактивної панелі:

https://view.genially.com/69690f9f49dd7ea39705583f/interactive-content-internet-bez-pastok).

Для кожної групи передбачено дві кейс-ситуації. Після вибору кожна група отримує роздрукований аркуш з кейс-ситуацією для опрацювання.

Завдання для групи учнів отримати відповіді на запитання:

- Що зроблено неправильно?
- Які можливі наслідки?
- Як потрібно було діяти?

Презентація результатів

Кожна група по черзі презентує свої висновки дослідження конкретних ситуацій. Учитель організовує безпечне обговорення, ставить уточнювальні запитання та допомагає учням глибше проаналізувати ситуацію. Також він узагальнює висновки й формулює чіткі правила цифрової безпеки, пов'язуючи їх із реальним життям.

Кейс 1: «Безпека у соцмережі»

Що зроблено неправильно?

Учні, зверніть увагу:

- Оленка перейшла за підозрілим посиланням.
- Вона не перевірила адресу сайту (instaqam.com — це не офіційний сайт).
- Ввела свій логін і пароль на сторонньому ресурсі.
- Діяла під впливом емоції — цікавості та хвилювання.

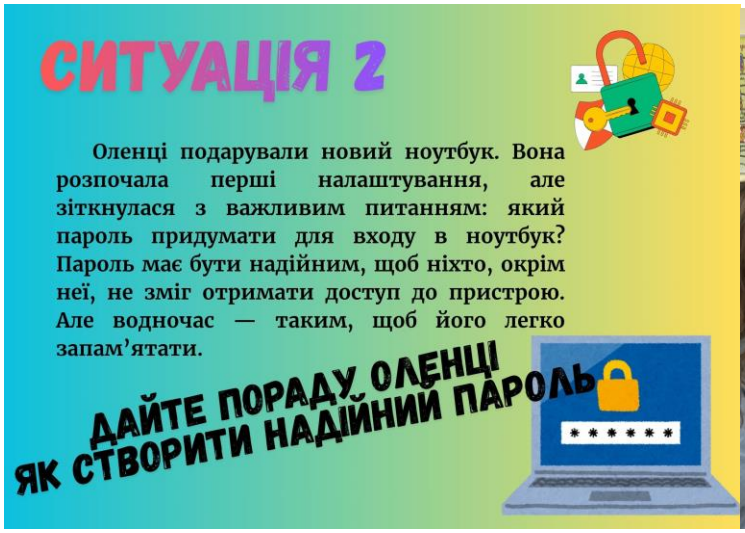
Це приклад ***фішингу*** — коли шахраї створюють підроблені сайти, щоб викрасти ваші дані.

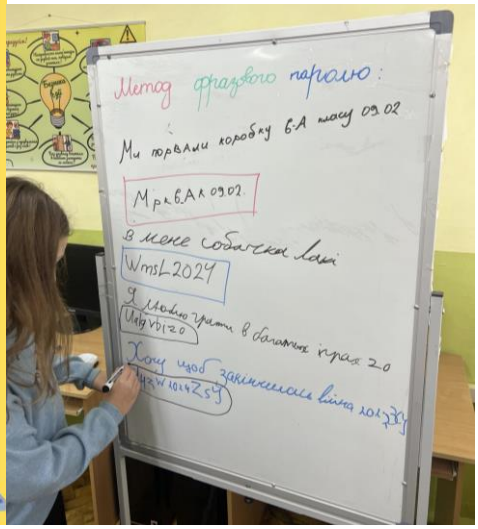
Як наслідок зловмисники можуть отримати доступ до її акаунта, можуть розсилати повідомлення від її імені, вимагати гроші в друзів, можуть змінити пароль і заблокувати власницю акаунта, особисті фото та переписки можуть стати доступними стороннім людям.

Як потрібно було діяти?

- не переходити за підозрілими посиланнями;
- перевірити адресу сайту (офіційний сайт має правильне написання);
- написати подрузі в особисті повідомлення: «Ти це надсилала?»;
- якщо вже перейшла — НЕ вводити логін і пароль;
- повідомити дорослих або змінити пароль, якщо є підозра на злам.

Кейс 2: «Надійний пароль»





Що може бути зроблено неправильно?

Найчастіші помилки при створенні пароля:

- використовувати дату народження;
- писати своє ім'я або ім'я домашнього улюбленця;
- ставити прості комбінації типу 123456 або qwerty;
- використовувати один і той самий пароль для всіх сайтів.

Такі паролі зламуються за кілька секунд спеціальними програмами.

Як наслідок: сторонні можуть отримати доступ до ноутбука, викрасти особисті фото або документ, увійти в пошту, соцмережі, банківські сервіси, можливе шахрайство від вашого імені. Пароль — це ключ до вашого цифрового життя.

Основні правила створення надійного пароля:

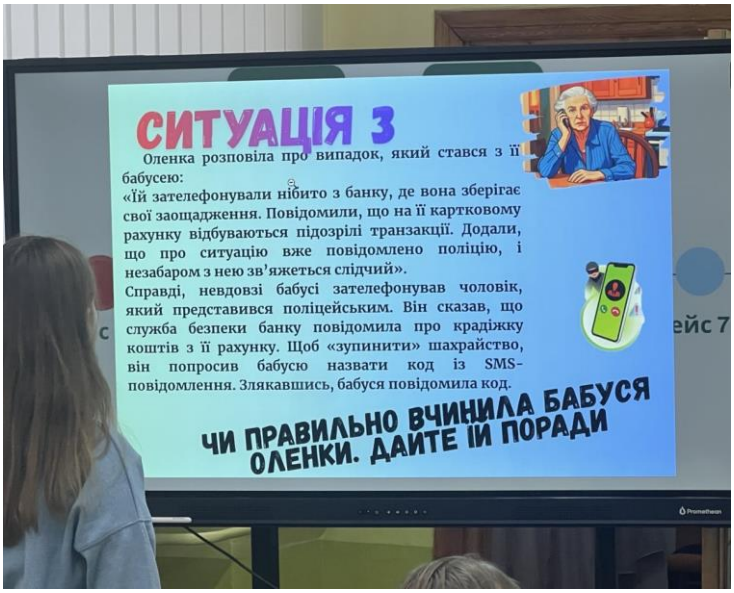
- не менше 8–12 символів;
- великі й малі літери;
- цифри;
- спеціальні символи (!, #, @ тощо);
- не використовувати особисті дані.

Використай ***методику фразового пароля***: згадай фразу, думку, або речення (з улюбленого твору, вірша, пісні чи щось особисте). Наприклад: “Мій кіт Мурчик любить грітися на сонці!”. Візьми перші літери кожного слова і подай їх англійськими літерами; додай інші символи та цифри (наприклад рік появи у вас домашнього улюбленця)

MkMlgns!2019

Такий пароль: довгий, складний для зламу, зрозумілий тільки вам.

Кейс 3: «Вішинг»



Що зроблено неправильно?

Учні, зверніть увагу:

- бабуся повірила незнайомим людям по телефону;
- вона не перевірила інформацію через офіційний номер банку;
- вона повідомила SMS-код сторонній особі;
- діяла під впливом страху та терміновості;

Це приклад ***вішингу*** — виду шахрайства, коли зловмисники телефонують і видають себе за працівників банку, поліції чи інших служб.

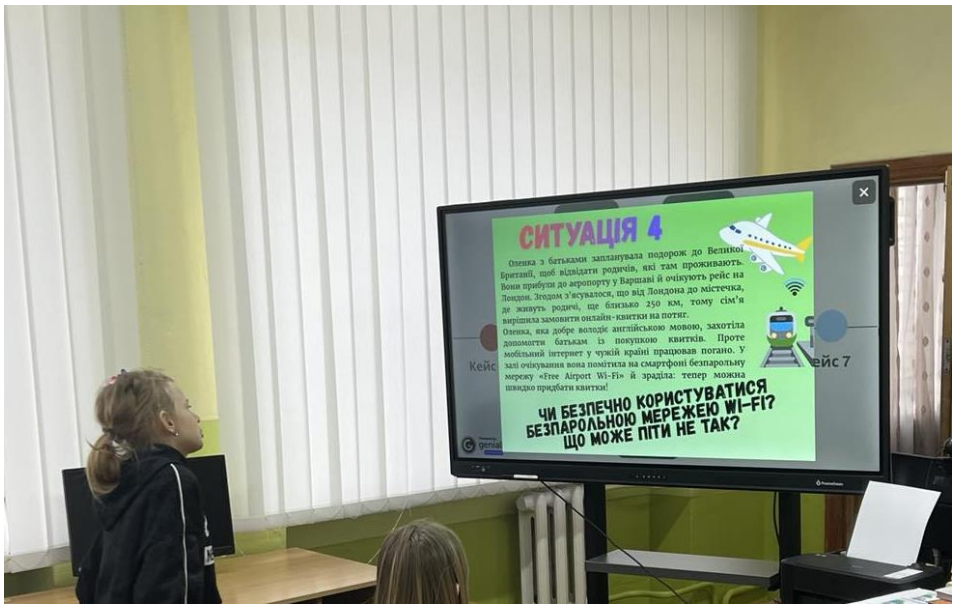
Як наслідок зловмисники можуть отримати доступ до банківського рахунку та списати всі кошти, можуть оформити кредити. SMS-код — це підтвердження операції. Передаючи його, людина фактично дозволяє доступ до рахунку.

Як потрібно було діяти?

Правильний алгоритм:

- ніколи не повідомляти SMS-коди;
- не довіряти дзвінкам, навіть якщо співрозмовник представляється банком чи поліцією;
- покласти слухавку;
- самостійно зателефонувати на офіційний номер банку (вказаний на картці);
- повідомити рідних.

Кейс 4: «Безпека WI-FI мережі»



Що зроблено неправильно?

Учні, зверніть увагу:

- Оленка підключилася до відкритої (безпарольної) мережі дані у якій не шифруються;
- вона планувала вводити особисті та банківські дані;
- не перевірила, чи це справжня мережа аеропорту;

Відкрита мережа — це мережа, до якої може підключитися будь-хто. Іноді шахраї створюють фейкові точки доступу з назвами типу «Free Wi-Fi», щоб перехоплювати дані.

Як наслідок можливе перехоплення логінів і паролів, викрадення банківських даних, встановлення шкідливого програмного забезпечення, втрата коштів.

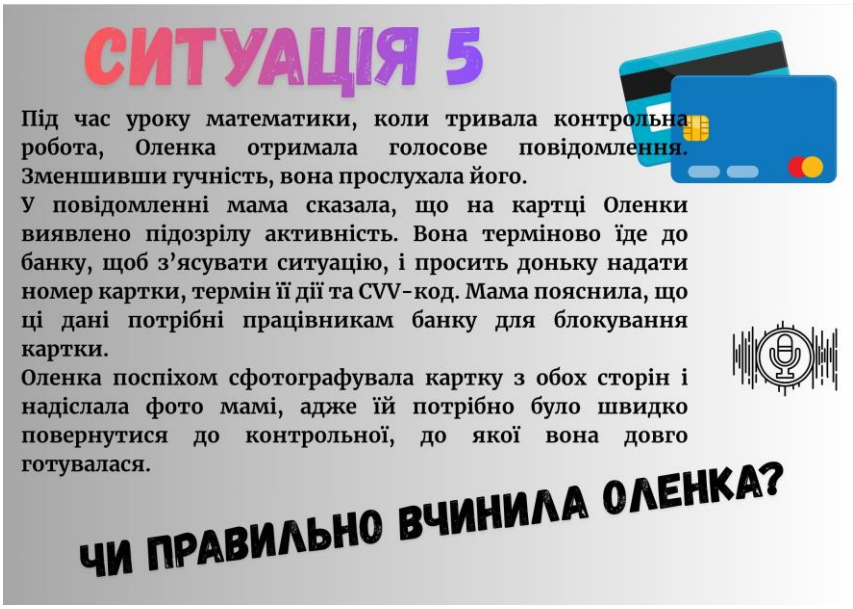
Як потрібно було діяти?

Правильний алгоритм:

- уточнити у працівників аеропорту офіційну назву мережі;
- не вводити банківські дані через відкритий Wi-Fi;
- використати мобільний інтернет (або мобільну тлчку доступу батьків);
- використовуй VPN-сервіси (краще перевірені та платні);
- вимикати автоматичне підключення до невідомих мереж;

Відкритий Wi-Fi — це як розмова в переповненій кімнаті: усі можуть «почути», що ви передаєте.

Кейс 5: «Дипфейк»



Ні, це було небезпечно.

Навіть якщо голос був схожий на мамин, це могло бути шахрайство або дипфейк**.**

Дипфейк — це технологія, яка за допомогою штучного інтелекту може:

- підробляти голос людини;
- створювати фейкові відео;
- імітувати манеру говорити.

Сьогодні шахраї можуть:

- записати кілька фраз людини із соцмереж;

- створити штучну копію голосу;
- подзвонити родичам і вимагати гроші або дані.

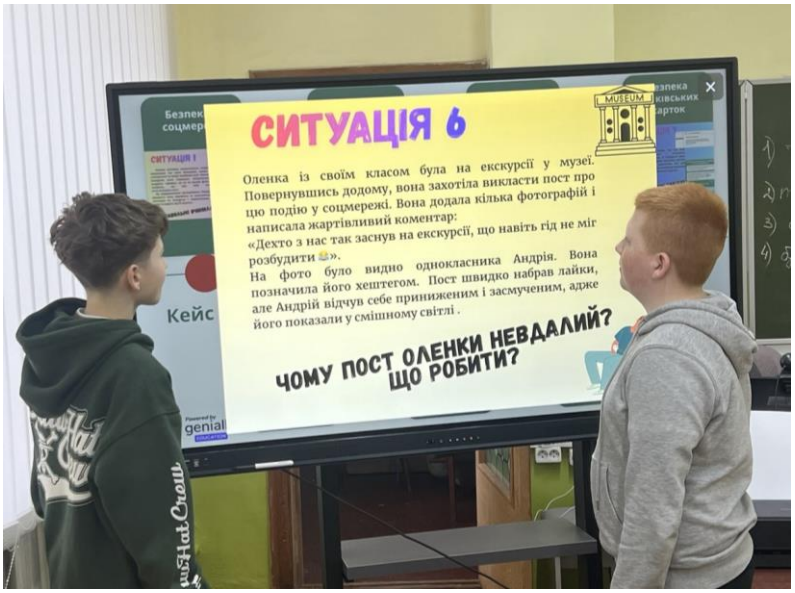
Голос може звучати дуже переконливо. Під впливом терміновості і паніки ми можемо шахраям надати конфіденційні дані картки. Якщо хтось отримує: номер картки, термін дії, CVV-код він може розраховуватися в інтернеті, зняти кошти,

Оленка мала:

1. Не надсилати фото картки.
2. Передзвонити мамі на звичайний номер і уточнити ситуацію

3. Пам’ятати правило:банківські дані — це таємниця. Їх не передають навіть родичам у месенджерах.

Кейс 6: «Кібербулінг»



На перший погляд — це просто жарт. Але важливо розуміти: те, що смішно одному, може бути боляче іншому. Якщо людину висміюють публічно, публікують її фото без згоди, принижують у соцмережах, це може бути формою кібербулінгу**.**

Кібербулінг — це приниження, образи або висміювання людини через інтернет (соцмережі, месенджери, ігри).

Навіть «жартівливий» допис може знизити самооцінку, викликати сором, стати причиною насмішок у класі.

Які помилки зробила Оленка?

- виклала фото без згоди Андрія.
- підписала його у принизливому контексті.

- не подумала про його почуття.
- публічно зробила його об’єктом насмішок.

Кібербулінг може призвести до тривожності, замкнутості, конфліктів у класі, втрати довіри між однокласниками. Пам’ятайте: лайки не означають, що вчинок правильний.

Як потрібно було діяти?

- перед публікацією запитати дозволу.
- подумати: «А якби це фото виклали про мене?»
- якщо хтось образився — видалити пост і вибачитися.

Пам’ятайте про правило “***великого білборда***”: уявіть, що все, що ви публікуєте в інтернеті, розміщується на величезному білборді в центрі міста, біля школи так, щоб це бачили всі: однокласники, батьки, вчителі. Запитайте себе:

- *Чи хотів(ла) б я, щоб це фото або допис висів на великому білборді?*
- *Чи не буде людині соромно або боляче?*

Якщо відповідь «ні» — публікувати цього не варто.

Фізкультхвилинка «Цифрова розминка»

«Антена Wi-Fi»

Підняти руки вгору, потягнутися, стати «антеною». Повторити 3 рази.

«Блокування шахрая»

Руки вперед — «стоп» (напружити), потім розслабити. Повторити 3 рази

«Перезавантаження»

Колові рухи плечима вперед і назад. Повторити 3 рази.

«Нахили безпечного користувача»

Повільні нахили голови вправо–вліво, вперед–назад (без різких рухів).

«Глибокий вдих — видих»

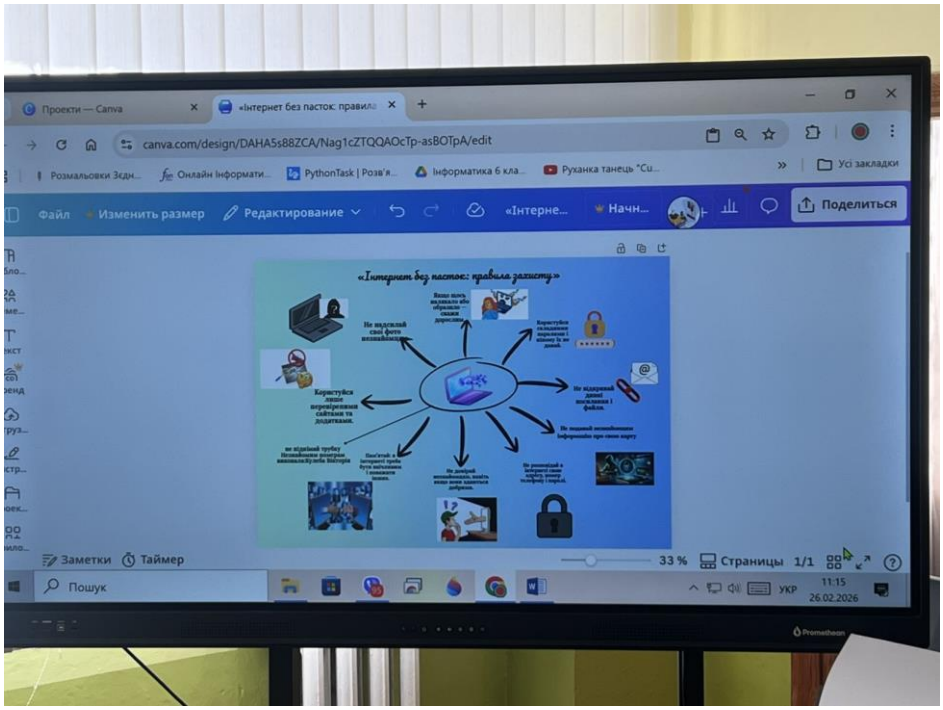
Вдих через ніс — руки вгору, видих через рот — руки вниз (3 рази).

V Практична робота за комп’ютером (10–15 хв.)

Створення спільного плаката «Інтернет без пасток: правила захисту» в Canva.

Учні працюють у спільному шаблоні Canva . Кожен обирає 1–2 правила цифрової безпеки (наприклад: не передавати банківські дані, перевіряти посилання, правило великого білборду, не користуватися відкритим Wi-Fi для оплат) та оформлює їх у вигляді короткого

чіткого формулювання + відповідної ілюстрації (іконка, символ, зображення) без повторів. Мета роботи — створити єдиний класний плакат, де кожне правило буде подано зрозуміло, візуально привабливо та лаконічно. Наприкінці роботи учитель виводить його на екран для спільного обговорення.



Валеохвилинка: виконати вправи за плакатом

VI Рефлексія

Використовуємо прийом “Заряд знань”: кожен учень, використовуючи зелений, жовтий або червоний колір магніту дає відповідь на запитання:

- Я впевнений(а), що зможу застосовувати ці знання.
- Мені ще потрібно краще розібратися.
- У мене залишилися запитання.

Відповідний магніт прикріплює на дошку.

VII Домашнє завдання

Поспілкуватися з батьками та з’ясувати: які правила цифрової безпеки вони використовують; чи знають вони про дипфейки, фішинг, правило великого білборду, метод фразового паролю. Якщо ні, поділися з ними знаннями. Оціни результат та запиши у зошит 3 висновки.

Матеріали до уроку:

1.Кейс-ситуації для друку:

https://drive.google.com/file/d/1yE8vH8Y0g2YX1JnrLrow-pZ0fljcYpHS/view?usp=drive_link

2. Інтерактивна вправа на повторення термінів:

https://wheelofnames.com/zkw-cyy

3. Інтерактивний аркуш Geniallyдля демонстрації:

https://view.genially.com/69690f9f49dd7ea39705583f/interactive-content-internet-bez-pastok

4. Шаблон спільного плакату ««Інтернет без пасток: правила захисту»»:

«Інтернет без пасток: правила захисту»