Колективна робота

1) Змініть надпис “Учень №” на своє прізвище та ім’я

2) Працюйте тільки в своєму рядку - відповідайте на запитання

№	Запитання	Які основні загрози для безпеки твоєї особистої інформації в інтернеті?	Які заходи ти приймаєш для того, щоб захистити свій пароль від несанкціонованого доступу?	Які правила ти використовуєш для того, щоб визначити, чи можна довіряти веб-сайтові чи онлайн-ресурсу ?	Як ти ставишся до ідентифікації і надання особистих даних в інтернеті?	Як ти реагуєш на надходження небажаних повідомлень чи електронних листів?
1	Бойко Влад	***Основними загрозами для безпеки особистої інформації в інтернеті є шкідливе програмне забезпечення (віруси), фішинг та шахрайство, крадіжка особистих даних, несанкціонований доступ, кібербулінг та небажаний контент. Також існують випадкові загрози, як-от збої в роботі обладнання***	***Використовуйте надійні паролі. ... Не використовуйте один пароль для кількох облікових записів. ... Регулярно змінюйте та оновлюйте паролі. ... Використовуйте менеджер паролів. ... Увімкніть двофакторну автентифікацію. ... Будьте пильними щодо фішингових атак.***	***Щоб перевірити достовірність даних з інтернету, шукайте підтвердження в кількох авторитетних джерелах, перевіряйте авторство та посилання на першоджерела, аналізуйте дату публікації, використовуйте фактчекінгові сайти***	***Надання особистих даних в інтернеті має як переваги, так і ризики, тому слід ставитися до цього обережно та відповідально. Ідентифікація потрібна для багатьох сервісів, але важливо знати, як захистити свої дані.***	***Щоб реагувати на небажані повідомлення чи електронні листи, слід позначати їх як спам, блокувативідправника або скасовувати підписку. Важливо також не клікати підозрілі посилання та не завантажувати вкладення, аби уникнути вірусів чи шкідливого програмного забезпечення.***

2	Поліщук Тимофій	Шкідливе програмне забезпечення, шахраї та віруси.	Використовувати надійний пароль в якому є багато символів англійської мови та цифри.	Читати відгуки про сайт, порівнюю критерії та роблю аналіз точності.	Я нікому не даю дані про себе в інтернеті й ставлюсь до цього погано.	Я додаю повідомлення в корзину, або до відділу спам.
3	Чернов Богдан	**Витік даних**. Це несанкціоноване поширення, зміна або видалення конфіденційних даних. Часто витоки відбуваються через злам великих компаній або вебсайтів, де ви зареєстровані, і ваша інформація може потрапити в руки зловмисників.	Використовуйте надійні паролі. ... Не використовуйте один **пароль** для кількох облікових записів. ... Регулярно змінюйте та оновлюйте паролі. ... Використовуйте менеджер паролів. ... Увімкніть двофакторну автентифікацію. ... Будьте пильними щодо фішингових атак.	Для оцінки надійності вебсайту чи онлайн-ресурсу я використовую набір критеріїв, схожий на ті, що застосовують фактчекери та дослідники. Ці критерії охоплюють аналіз авторитетності, точності, об'єктивності, актуальності та безпеки.	Надання особистих даних в інтернеті — це компроміс між зручністю і ризиком. Як мовна модель, я не маю власних почуттів чи ставлення, але можу представити збалансований погляд на цю тему, зважаючи на існуючі ризики та переваги.	Як мовна модель, я не маю власної поштової скриньки, емоцій чи суб'єктивної реакції на небажані повідомлення. Проте я можу описати, як системи штучного інтелекту (ШІ) реагують на спам і чому це важливо для моєї роботи:

4	Єгор Остапенко	Основними загрозами для безпеки особистої інформації в інтернеті є шкідливе програмне	Використовуйте надійні паролі. Ваші паролі мають бути довжиною щонайменше 12 символів. Вони мають містити комбінацію великих і малих літер, цифр і символів. Уникайте використання особистих даних, таких як ваше ім'я, дата народження чи адреса.	При перевірці домену (крок 2) можна дізнатись й про власника сайту. Не виключено, що це буде підставна особа. В будь-якому разі ви знатимете, наскільки прозора політика даного ЗМІ і що від нього очікувати.	Надання особистих даних в інтернеті має як переваги, так і ризики, тому слід ставитися до цього обережно та відповідально. Ідентифікація потрібна для багатьох сервісів, але важливо знати, як захистити свої дані.	добре але якщо це від людей яких я знаю
5	Таранков Данил	1)віруси та розголошення своєї особистої інформації	2)роблю його складним і нікому не говорю 3)перевіряю наскільки сайт популярний і дивлюсь обзори	4)ігнорую чи видаляю.		
6	Аліксійчук Валерія	Несанкціонований доступ. Така загроза може призвести до поширення, зміни або видалення важливих конфіденційних даних.	● **Віруси та трояни.** Це програми, які можуть викрадати ваші дані, пошкоджувати файли, а також надавати зловмисникам	зверніть увагу на декілька ключових ознак. Вони допоможуть відрізнити надійні сайти від шахрайських або неякісних.	Намагайтеся ділитися лише необхідною інформацією. Якщо вам незручно надавати певні дані, спробуйте знайти альтернативний спосіб отримати послугу або інший ресурс.	

			віддалений доступ до вашого пристрою.			
7	Рижа Софія	віруси фішинг та шахрайство				
8	Рябченко Олександер	віруси				
9	максим	віруси плохо	ше			
10	Семенко юля					
11	корнійчук дмитро	1)можуть розказати не тим людя	2)можу зробити його складним	3))перевіряю наскільки сайт популярний і дивлюсь обзори		
12	Учень №12					
13	Учень №13					
14	Учень №14					
15						

Несанкціонований доступ. Така загрза може призвести до поширення, зміни або видалення важливих конфіденційних даних.ю як