Основи цифрової грамотності

ОСВІТНІ РЕСУРСИ

Зміст

УРОК 1

Загальна інформація про конфіденційність

МЕТА УРОКУ

Учні дослідять власне ставлення до конфіденційності та його вплив на життя. Вони розглянуть категорії інформації, які хотіли б залишити приватними, і ситуації, у яких поширюватимуть або ж не будуть поширювати певну інформацію.

ОСНОВНІ ЗАПИТАННЯ	Що для вас означає конфіденційність у контексті цифрового середовища?
ВІК	10–18
МАТЕРІАЛИ	Роздатковий матеріал для гри «Конфіденційність»
ПІДГОТОВКА	Роздрукуйте матеріали для всіх учнів
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПИЛЬНІСТЬ: Я несу відповідальність за свої дії в мережі та знаю, як захистити себе й інших ІНКЛЮЗИВНІСТЬ: Я готовий (готова) вислухати інших людей, визнаю право кожної людини на власну думку та виявляю повагу і співчуття під час спілкування з іншими людьми в Інтернеті.

ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

Що для вас означає «конфіденційність»?

Гра «Конфіденційність»

РОБОТА В КЛАСІ

Роздайте матеріал для гри «Конфіденційність».

СЛОВО ПЕДАГОГА

Щодня ви приймаєте рішення, пов'язані з вашою конфіденційністю, особливо коли перебуваєте в мережі та використовуєте свої мобільні або інші цифрові пристрої. Часто ви недовго думаєте над цими рішеннями. Але всі вони сумуються та формують ваше унікальне уявлення про конфіденційність.

Конфіденційність – це можливість керувати інформацією, яку інші люди знають про вас. Це можна робити, повідомляючи певні речі про себе (наприклад, повідомити іншій людині свою адресу чи розказати, як вам подобається проводити вільний час) або роблячи певні речі серед інших людей (наприклад, піти до магазину з друзями та вибрати те, що вам найбільше подобається). Конфіденційність однаково важлива, коли інші люди перебувають із вами в одній кімнаті та коли ви спілкуєтеся з ними в мережі.

Конфіденційність залежить від ваших власних рішень. Уявлення про конфіденційність у вас і вашої родини може значно відрізнятися від того, яке мають інші люди в цій групі та їхні родини. Що краще ми усвідомлюємо, яку інформацію ми вважаємо конфіденційною, і як наша поведінка в мережі впливає на нашу конфіденційність, то кращі рішення ми можемо приймати щодо рівня нашої конфіденційності.

Давайте зіграємо у швидку гру про конфіденційність (див. форму для гри «Конфіденційність»), яка допоможе вам визначитися з вашими уявленнями та ставленням до конфіденційності. Кожен із вас заповнить свою форму, пройде по класу та представиться іншому учневі. Потім ви з іншим учнем поставите один одному запитання щодо інформації у формі. Не показуйте форму іншим учням! Після гри форма залишиться у вас, і ви можете забрати її додому або викинути.

У кожній розмові кожен учень має відповісти принаймні на три запитання, які поставив співрозмовник. Учні можуть на власний вибір відповісти також більше, ніж на три запитання. Учні також можуть вибрати, на які три (чи більше) запитання вони хочуть відповісти. Скільки інформації повідомить кожен учень? Яку інформацію повідомить кожен учень? Походімо й поговорімо!

РОБОТА В КЛАСІ

Попросіть учнів заповнити анкети. Після цього вони матимуть 15 хвилин на обговорення з іншими учнями. Продовжіть гру загальним обговоренням питань, що наведені нижче. Не збирайте анкети — нехай учні заберуть їх із собою або викинуть.

Обговорення

ЗАПИТАЙТЕ В УЧНІВ

- Чи є факти, про які ви нікому не розповіли? Які саме?
- Чому? Про які факти ви розповіли? Чому?
- Чи всі учні приймали однакові рішення щодо інформації, якою вони діляться? Чому так і чому ні?
- Чому ви розповідаєте менше чи більше цієї інформації різним людям? Коли б ви поділилися нею?
- Чи розповідали ви під час цієї гри щось, чого не стали б розповідати всім, кого знаєте? Чому ні?
- Це публічна інформація? Чи приватна? Чому? Чи вона однакова для всіх?

СЛОВО ПЕДАГОГА

Як ви щойно почули, люди по-різному вирішують, що розповідати і що не розповідати. Їхні рішення також базуються на різних мотивах.

Зараз ми просто грали. Але ми приймаємо такі самі рішення щодня в реальному житті. Ми вирішуємо, публікувати чи не публікувати певні світлини в соціальних мережах. Ми вирішуємо, чи надавати загальний доступ в обліковому записі соціальної мережі до певної контактної інформації, як-от адреса електронної пошти. Наші рішення можуть відрізнятися від рішень нашого найкращого друга або від наших рішень, які ми прийняли місяць тому.

Навіть якщо ми приймаємо однакові рішення в різні моменти часу, наші мотиви можуть бути різними.

Ці різні рішення та мотиви являють собою наше особисте розуміння конфіденційності.

Простіше кажучи, конфіденційність – це спосіб, який ми вибираємо для обробки інформації про нас. Ця інформація може включати частини нашої особистості, діяльності, уподобань, звичок та інших аспектів нашого життя. У сучасному цифровому світі ми маємо більше можливостей, ніж будь-коли раніше, надавати іншим доступ до інформації про себе. Тому важливо, щоб ми усвідомлювали своє власне розуміння конфіденційності та подумали, чи воно нас задовольняє.

ЗАПИТАЙТЕ В УЧНІВ

- Як би ви визначили конфіденційність на підставі своєї поведінки у грі «Конфіденційність», а також поведінки в повсякденному житті? Чому?
- Чи вся приватна інформація є таємницею?
    - Можлива відповідь: необов'язково. Наприклад, дата вашого народження не може бути такою ж таємницею, як ваші записи в щоденнику. Багато людей знають або мають знати дату вашого народження, наприклад ваші батьки чи опікуни, ваш лікар. Але якщо інформація не є таємницею, ви все одно можете сприймати її як приватну. Більшість із нас не хотіли б, щоб усі знали наш день народження, тому що ми вважаємо, що ця інформація має бути доступна тільки близьким людям або людям, які мають певну причину її знати. Подібні рішення щодо того, хто й що має знати про нас, а також коли та чому, є ключем до конфіденційності.

ЗАПИТАЙТЕ В УЧНІВ

- Чи є якась інформація, яка необов'язково є таємницею, але доступ до якої ви не хотіли би надавати людям, яких ви не знаєте добре або з якими ви щойно познайомилися?
    - Приклади.
      Номери телефонів, адреси електронної пошти, світлини, відео тощо.
- Чи є якась інформація, якою ви не ділитеся з батьками/опікунами чи друзями? А із вчителями або вихователями?
    - Приклади.
      Оцінки у школі, обліковий запис Instagram, щоденник.
- Чи здивувало вас щось у власному розумінні конфіденційності?

СЛОВО ПЕДАГОГА

Коли ми закінчимо, ви можете взяти гру «Конфіденційність» із собою. Тепер, коли ви більше замислюєтеся про конфіденційність, ви бачитимете щодня безліч варіантів, які допоможуть вам втілити в життя своє власне розуміння конфіденційності.

Завдання

СЛОВО ПЕДАГОГА

Зараз ми дізнаємося трохи більше про ваше особисте розуміння конфіденційності.

1. Знайдіть у мережі три приклади контенту, який хтось опублікував, але який би ви залишили приватним. Це може бути контент, який опублікували чи яким поділилися зірки, політики, відомі бізнесмени. Ви також можете шукати випадкові приклади за хештегом або за допомогою стандартного пошуку в мережі. Постарайтеся знайти різні ресурси (наприклад,світлини, відео, тексти, як-от коментарі в соціальній мережі або на сайті новин) на різні теми.
2. Для кожного прикладу напишіть коротке пояснення, чому би ви залишили цю інформацію приватною. У цьому поясненні також укажіть, чи ваша думка щодо поширення цієї інформації змінюється, залежно від контексту (наприклад, людина, з якою ви спілкуєтеся, кількість людей, з якими ви спілкуєтеся, ціль спілкування, середовище (у школі чи поза школою)) і як вона змінюється.

ЗАВДАННЯ

Це завдання можна виконати в класі або вдома.

РОЗДАТКОВИЙ МАТЕРІАЛ

Гра «Конфіденційність»

Заповніть анкету. Якщо не хочете відповідати на якесь із питань, напишіть «Ні»,

Ім'я: **Прізвище:**

Вік: **Місце навчання/роботи:**

Домашня адреса:

Улюблений фільм: **Найкращий друг:**

Найбільший страх:

Вчинок, за який найбільше соромно:

Результат останнього тесту/роботи на уроці: **Дата народження:**

Електронна пошта: **Номер мобільного телефону:**

Профілі в соціальних мережах:

Остання світлина:

Додатково: *Якщо маєте із собою мобільний пристрій, можете вибрати й показати останню світлину та/або відео, які зробили*.

УРОК 2

Конфіденційність персональної інформації

МЕТА УРОКУ

Учні дізнаються, які типи інформації мають залишатися приватними, як налаштувати параметри конфіденційності в соціальних мережах і як пояснювати свій вибір щодо того чи іншого налаштування (наприклад, чому певний контент відображається лише для друзів, а інший є загальнодоступним).

ОСНОВНІ ЗАПИТАННЯ	Як визначити, якою інформацією можна (або не можна) ділитися в мережі та з ким? Як це пов'язано з обраною вами соціальною мережею?
ВІК	13–15
МАТЕРІАЛИ	Роздатковий матеріал для вікторини
ПІДГОТОВКА	Роздрукуйте матеріали для всіх учнів
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПИЛЬНІСТЬ: Я несу відповідальність за свої дії в мережі та знаю, як захистити себе й інших ІНКЛЮЗИВНІСТЬ: Я готовий (готова) вислухати інших людей, визнаю право кожної людини на власну думку та виявляю повагу і співчуття під час спілкування з іншими людьми в Інтернеті.

ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

Вікторина

Частина 1

РОБОТА В КЛАСІ

Роздайте матеріали для гри на вікторини та попросіть кожного учня заповнити їх. Попросіть учнів надати чотири факти про себе та попередьте, що розкажете ці факти всій групі. Попросіть їх лишити в себе другий аркуш.

Для цього завдання учням необхідно виділити 10 хвилин. Потім зберіть їх.

СЛОВО ПЕДАГОГА

Зараз я прочитаю деякі з фактів на кожному аркуші. У розділі «Здогадки» напишіть, про кого з учнів наведено факти на кожному аркуші.

РОБОТА В КЛАСІ

Переглянувши всі аркуші, проведіть колективне обговорення.

ЗАПИТАЙТЕ В УЧНІВ

- Чи є відомості, про які ви нікому не розповіли? Які саме? Чому?
- Чи всі учасники приймали однакові рішення щодо інформації, якою вони діляться? Чому так і чому ні?
- Чому ви розповідаєте менше чи більше цієї інформації різним людям? Коли б ви поділилися нею?
- Чи легко було вгадати людей за наданими фактами?
- Чи були випадки, коли хтось ненавмисно розкрив про себе більше інформації, ніж потребувала відповідь на запитання (наприклад, коли дізнавшись інформацію про улюблену страву, можна зробити висновок про культуру, до якої належить людина)?
- До яких припущень про вас могли б вдатись інші люди, якби ви поширили факти про себе з цієї гри в реальному житті?

Частина 2

СЛОВО ПЕДАГОГА

Конфіденційність – це можливість керувати інформацією, яку інші люди знають про вас. Це можна робити, повідомляючи певні речі про себе (наприклад, повідомити іншій людині свою адресу чи розказати, як вам подобається проводити вільний час) або роблячи певні речі серед інших людей (наприклад, піти до магазину з друзями та вибрати те, що вам найбільше подобається). Конфіденційність однаково важлива, коли інші люди перебувають із вами в одній кімнаті та коли ви спілкуєтеся з ними в мережі.

Конфіденційність залежить від ваших особистих рішень. Уявлення про конфіденційність у вас і вашої родини може значно відрізнятися від того, яке мають інші люди в цій групі та їхні родини. Що краще ми усвідомлюємо, яку інформацію ми вважаємо конфіденційною, і як наша поведінка в мережі впливає на нашу конфіденційність, то кращі рішення ми можемо приймати щодо рівня нашої конфіденційності. Конфіденційність також залежить від типу інформації, якою ділиться людина, і від того, з ким вона ділиться.

ЗАПИТАЙТЕ В УЧНІВ

Наприклад, чи назвали б ви свою домашню адресу таким людям:

- Батькам/опікунам або іншим важливим для вас дорослим членам сім'ї?
- Своїм друзям?
- Своєму вчителю?
- Незнайомій або малознайомій особі?
- Другу друга?
- Певній організації чи компанії?

Підсумок

СЛОВО ПЕДАГОГА

Коли ви ділитесь інформацією в мережі, важливо брати до уваги, хто бачитиме цю інформацію та чи буде вас (або особу, інформація про яку поширюється) влаштовувати поширення такої інформації певним аудиторіям.

Якщо певна інформація потрапить не в ті руки, це може завдати проблем у майбутньому. Якщо незнайомець чи малознайома вам особа отримає інформацію про вашу адресу, вона може прийти до вас додому, що може бути небезпечно. Хоча в різних частинах світу вірогідність такої ситуації різна, ризик (і потенційна шкода) може перевищити низьку вірогідність того, що це трапиться. Щоб правильно вибрати рівень конфіденційності, що гарантує вашу безпеку, важливо розуміти наслідки поширення інформації.

Непорозуміння

Обговорення

СЛОВО ПЕДАГОГА

Поговорімо про те, що ми пишемо в текстових повідомленнях, як ми висловлюємось, і чим письмове спілкування відрізняється від особистого.

ЗАПИТАЙТЕ В УЧНІВ

- Чим може відрізнятися письмове спілкування від особистого?
    - Можлива відповідь. Якщо ви не бачите реакцію людини, ви можете не знати, як вона сприйняла ваші слова. Ви можете образити когось, навіть не здогадавшись про це.

СЛОВО ПЕДАГОГА

Коли ви спілкуєтеся з кимось особисто, ви можете бачити реакцію цієї особи на ваші слова, включно з мовою тіла та тоном. Під час спілкування онлайн частина цього контексту втрачається.

Однак у мережі можуть бути доступні інші типи контекстної інформації, що можуть допомогти під час спілкування (наприклад, у соціальних мережах можуть бути певні норми спілкування, які допоможуть краще тлумачити інформацію).

ЗАПИТАЙТЕ В УЧНІВ

- Якщо під час спілкування бракує контексту (наприклад, ви не бачите чи не чуєте співрозмовника), як це може призвести до непорозуміння (наприклад, співрозмовник може неправильно витлумачити жарт і образитись)?
- Якщо під час особистої розмови виникає непорозуміння, як можна його вирішити (наприклад, попросити вибачення або пояснити, що ви насправді мали на увазі)? Чим може відрізнятися вирішення непорозуміння під час спілкування в мережі (наприклад, це буде простіше чи складніше зробити)?

Хто належить до вашої аудиторії?

Частина 1

СЛОВО ПЕДАГОГА

Хоча працюючи, спілкуючись і розважаючись у мережі, ми всі лишаємо по собі слід із даних, є кілька способів, що допоможуть керувати конфіденційністю та своєю репутацією онлайн. У соціальних мережах часто є вбудовані в платформу налаштування, що дають змогу вибирати, хто може бачити наші дописи. Хоча ці налаштування не обмежують використання даних з аналітичними цілями (зокрема для аналізу метаданих), наприклад третіми сторонами (рекламодавцями, дослідниками чи компаніями) або самими платформами, вони можуть обмежити те, яку інформацію бачать інші користувачі соціальної мережі, а також до яких даних матимуть доступ компанії чи рекламодавці.

Якщо вам цікаво, метадані – це фактично дані про дані. Метадані можуть, серед іншого, включати час входу користувача в соціальну мережу, його місцеположення під час входу та інформацію про з'єднання з Інтернетом.

Налаштування конфіденційності можуть виглядати по-різному в різних соціальних мережах, але вони допомагають нам визначити нашу аудиторію. Наприклад, можна зробити свої дописи повністю загальнодоступними, видимими лише друзям друзів, лише друзям певної особи чи взагалі лише кільком обраним друзям. Ці налаштування також можуть впливати на дані про місцеположення та дозволи на поширення. У більшості служб можна вимкнути файли cookie, таргетовану рекламу та пошукові рекомендації, змінивши відповідні налаштування та параметри. Для додаткового захисту конфіденційності під час перегляду сайтів є також розширення браузерів та інші служби (наприклад, розширення Privacy Badger «Do Not Track» від Electronic Frontier Foundation).

Частина 2

РОБОТА В КЛАСІ

Попросіть учнів розділитись на пари.

ЗАПИТАЙТЕ В УЧНІВ

Згадайте, у яких соціальних мережах ви маєте обліковий запис.

- Чи знаєте ви свої поточні налаштування конфіденційності для кожної з цих соціальних мереж?

Робота у групі

СЛОВО ПЕДАГОГА

Давайте розглянемо можливості, які надають ці налаштування, і з'ясуємо, які з них є найвідповіднішими, у яких ситуаціях і на яких платформах.

Самостійно перейдіть у свій обліковий запис соціальної мережі й перегляньте свої поточні налаштування конфіденційності. Зазвичай налаштування конфіденційності можна знайти в налаштуваннях облікового запису, а на деяких платформах навіть є спеціальні функції для перевірки конфіденційності.

Переглянувши свої налаштування конфіденційності, обговоріть їх зі своїм партнером. Чому в кожного з вас саме такі налаштування конфіденційності? Чи бувають налаштування конфіденційності контекстними (тобто доречними в одній ситуації та непотрібними в іншій)? Чи змінювали ви колись свої налаштування? Як часто ви змінюєте їх і чому?

Переконайтеся, що ви переглянули обидва типи налаштувань конфіденційності: як для показу інформації іншим користувачам соціальної мережі, так і для надання

даних платформі соціальної мережі та пов'язаним третім сторонам (як-от рекламодавцям). Усе це важливі аспекти керування вашою цифровою конфіденційністю: для незнайомих чи малознайомих людей, друзів, родичів і компаній.

РОБОТА В КЛАСІ

Дайте учням 5 хвилин, щоб обговорити це в парах, а потім залучіть до дискусії всю групу, використовуючи наведені нижче запитання.

Обговорення

ЗАПИТАЙТЕ В УЧНІВ

- Яке налаштування конфіденційності встановлено для всього вашого облікового запису: загальнодоступний, приватний чи щось інше? Чому ви вирішили встановити саме це налаштування?
- Чи відповідають ваші поточні налаштування конфіденційності вашим вимогам?
- Коли варто надавати до інформації загальний доступ, а коли краще зробити контент приватним?
- Чи почуваєтеся ви впевнено, надаючи доступ до своєї інформації соціальній мережі чи компаніям, що рекламують свої товари та послуги в цій мережі? Чому так або чому ні?
- Чи допомогла вам ця розмова змінити думку про свої налаштування конфіденційності? Чому так або чому ні?

Завдання

СЛОВО ПЕДАГОГА

Тепер, коли ми поговорили про конфіденційність, про те, що люди можуть дізнатися про вас із контенту, яким ви ділитесь, про те, як різні люди можуть по-різному розуміти одні й ті самі повідомлення, а також про те, як налаштування можуть допомогти визначити, яким контентом ділитися з певною аудиторією, застосуємо отримані знання на практиці.

Впродовж наступних 30 хвилин самостійно обдумайте три наведені ситуації і запропонуйте рішення.

1. Марійці тринадцять років, і вона нещодавно почала займатися співами. Вона розуміє, що поки що в неї виходить не дуже, але хоче поділитися своїм новим захопленням із друзями та дізнатися їхню думку. Вона хоче додати кілька відео, на яких вона співає свою улюблену пісню, в одну із соціальних мереж. Який тип платформи ви порекомендуєте? Які, на вашу думку, налаштування конфіденційності найкраще підійдуть для цієї мережі? Поясніть чому.
2. Миколі шістнадцять, і він дуже любить готувати та вигадувати нові рецепти. Він створив кілька цікавих рецептів страв із курки й хоче поділитися ними із друзями й іншими любителями кулінарії. Який тип платформи ви порекомендуєте? Які, на вашу думку, налаштування конфіденційності найкраще підійдуть для цієї мережі? Поясніть чому.
3. Аліні вісімнадцять, і вона хоче почати шукати роботу наступного місяця. Вона знає, що роботодавцям потрібне резюме, але не впевнена, як краще написати його. Вона хоче працювати в галузі IT, але не знає, на які посади її можуть взяти та чи має вона достатньо досвіду для цих посад. Вона б хотіла отримати поради чи рекомендації від інших людей, що мають такі самі інтереси, але ніхто в її колі спілкування не працює в галузі IT. Який тип платформи ви порекомендуєте Аліні? Які, на вашу думку, налаштування конфіденційності найкраще підійдуть для цієї мережі? Поясніть чому.

ЗАВДАННЯ

На наступній зустрічі, за можливості, поділіть учнів на ті ж самі пари й попросіть обговорити наведені ситуації.

Дайте учням 30 хвилин на виконання цього завдання. Це завдання можна виконати в класі або вдома.

РОЗДАТКОВИЙ МАТЕРІАЛ

Вікторина

Виберіть чотири пункти із наведених нижче та заповніть пропуски. Цю інформацію отримають інші учасники вікторини. Вкажіть своє ім'я на анкеті.

(Інформація лише для педагога) **Ім'я:**

Перша літера вашого імені:

Місяць народження:

Назва вашої вулиці:

Ім'я одного з батьків/опікунів чи іншої дорослої особи, яка відіграє важливу роль у вашому житті:

Ваш улюблений фільм:

Ваша улюблена страва:

Ваш найбільший страх:

РОЗДАТКОВИЙ МАТЕРІАЛ

Вікторина

Зберігайте цей аркуш навіть після того, як інструктор збере перші частини. Інструктор зачитуватиме відповіді з роздаткових матеріалів, а ви маєте вгадати, кому із групи вони належать.

1.	**11.**
2.	**12.**
3.	**13.**
4.	**14.**
5.	**15.**
6.	**16.**
7.	**17.**
8.	**18.**
9.	**19.**
10.	**20.**

УРОК 3

Паролі

МЕТА УРОКУ

Учні дізнаються, як захистити свою інформацію в Інтернеті, використовуючи та зберігаючи надійні паролі. Вони зрозуміють принципи створення надійних паролів та ознайомляться із потенційними ризиками, які можуть виникнути у разі, якщо пароль дізнається стороння людина. Учні навчаться принципів захисту паролів та запобіганню несанкціонованого доступу до облікових записів.

ОСНОВНІ ЗАПИТАННЯ	Наскільки надійно паролі захищають вашу інформацію в мережі?
ВІК	11–18
МАТЕРІАЛИ	Роздатковий матеріал для уроку про паролі
ПІДГОТОВКА	Роздрукуйте матеріали для всіх учнів
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПИЛЬНІСТЬ: Я несу відповідальність за свої дії в мережі та знаю, як захистити себе й інших





ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

Основні правила використання паролів

Частина 1

СЛОВО ПЕДАГОГА

Зазвичай ми не замислюємося про паролі, які ми використовуємо для сайтів, додатків і служб. Проте від надійності пароля залежить захист вашої інформації.

РОБОТА В КЛАСІ

Ініціюйте у класі обговорення наведених нижче питань. Нагадайте учням, що вони не повинні вказувати свої справжні паролі під час цієї або будь-якої іншої вправи.

ЗАПИТАЙТЕ В УЧНІВ

- Скільки у вас паролів?
- Ви використовуєте різні паролі для кожного облікового запису електронної пошти чи соціальної мережі?
- Вони різні чи це варіації того самого пароля?
- Якщо у вас кілька паролів, як ви запам'ятовуєте, який із них якому обліковому запису належить?

ЗАПИТАЙТЕ В УЧНІВ

- Як часто ви забували важливий пароль?
- Що ви робили, коли забули свій пароль?
- Що ви робите, щоб паролі було легко запам'ятати?
- У вас є пароль, який ви використовуєте кожного дня?
- Що би сталося (наскільки вам відомо), якби хтось дізнався ваш пароль?
- Чи залежить розвиток подій від того, що це за особа?
- Яку інформацію про вас може дізнатись інша особа, якщо вона отримає доступ до вашого облікового запису за допомогою пароля?

Частина 2

РОБОТА В КЛАСІ

Попросіть учнів розділитись на пари.

СЛОВО ПЕДАГОГА

Разом із партнером обговоріть таку ситуацію: що може статися, якщо людина, яка бажає вам зла, дізналася пароль до вашої улюбленої платформи соціальної мережі?

РОБОТА В КЛАСІ

Надайте учням 5 хвилин на обговорення. Попросіть групи поділитися міркуваннями.

СЛОВО ПЕДАГОГА

Тепер обговоріть із партнером таку ситуацію: що може статися, якщо хакер дізнається пароль до банківського рахунку ваших батьків або опікунів?

РОБОТА В КЛАСІ

Через 5 хвилин обговорення у групах попросіть учнів поділитися міркуваннями у класі.

Частина 3

СЛОВО ПЕДАГОГА

Вам може бути цікаво, як хакер може дізнатися персональний пароль. Є кілька способів. Один із них називається соціальна інженерія – це спроби обманом змусити когось надати свій пароль. Хакер може це зробити, надіславши електронного листа, яке виглядає як справжнє повідомлення з платформи чи сайту, на якому користувач має обліковий запис. В електронному листі можна попросити перейти за посиланням і ввести ім'я користувача та пароль. Коли особа вводить ці дані, вони стають доступні хакерам.

Хакери іноді намагаються вгадати паролі, використовуючи загальні фрази як-от password123, test або ім'я чи прізвище.

Інший спосіб дізнатися особистий пароль – це так званий «метод грубої сили». Атака методом грубої сили відбувається, коли хакер намагається ввійти в обліковий запис, багаторазово намагаючись підібрати пароль. Хоча хакери можуть проводити атаку методом грубої сили вручну, часто вони запускають комп'ютерну програму, яка швидко й автоматично перебирає всі можливі комбінації паролів. Наприклад, це може бути список можливих паролів або набір паролів, що складаються з комбінацій різних букв і цифр. Ці паролі вводяться, доки не знайдеться відповідний пароль.

Звісно, атаки методом грубої сили можуть бути й досконалішими. Якщо ваш пароль входить до списку ймовірних паролів, наприклад fido123 або password, деякі програми можуть швидше вгадати його, перебираючи ці варіанти, перш ніж перейти до менш імовірних або випадкових. Пароль можна розгадати набагато швидше, якщо хакер щось знає про вас. Наприклад, якщо йому відомо, що вашого кота звати Тобі, він може спробувати використати цю кличку з різними наборами цифр у кінці (наприклад, Toby629 або Toby3020).

Принципи створення паролів

ЗАПИТАЙТЕ В УЧНІВ

- Хто знає, що таке «надійний» або «надійніший» пароль?
- Чому це потрібно?

СЛОВО ПЕДАГОГА

Надійний пароль допомагає захищати інформацію. Хоча надійний пароль не гарантує, що обліковий запис не зламають, ненадійний пароль значно спростить іншим особам доступ до вашої інформації.

Вправа з паролями

ЗАПИТАЙТЕ В УЧНІВ

- Наведіть приклади ненадійних паролів.
  - Приклади. Password, 12345, Hello!, дата народження, прізвисько.
- Чому ви вважаєте, що це ненадійні паролі?
  - Відповідь. Їх може легко вгадати особа або комп'ютер, що використовує атаку методом грубої сили.
- Як зробити пароль надійнішим?
  - Приклади. Додавайте цифри, великі та малі букви, спеціальні символи, створюйте довші паролі, уникайте загальних фраз і слів.

РОБОТА В КЛАСІ

Після того як учні наведуть свої приклади паролів, напишіть на дошці такі інструкції:

1. Додайте принаймні одну цифру.
2. Додайте принаймні один спеціальний символ.
3. Додайте принаймні одну велику та малу букви.
4. Паролі мають складатися як мінімум із 7 символів.
5. Паролі мають бути легкими для запам'ятовування, якщо ви не використовуєте диспетчер паролів.
6. Диспетчер паролів – це сайт чи додаток, який допомагає користувачам зберігати та впорядковувати паролі.
7. Пароль не може бути загальновживаним словом або містити особисту інформацію (дата народження, ім'я одного з батьків тощо).
8. Не використовуйте один пароль на кількох сайтах.

СЛОВО ПЕДАГОГА

Є два способи створення надійних паролів. Перший – дотримуватися рекомендацій, як-от тих, що записані на дошці. Відповідно до цих інструкцій, слід додати в пароль складні для вгадування текстові й цифрові елементи, що зробить пароль надійнішим. Недоліком цього підходу є те, що такі паролі складніше запам'ятати.

Надійні паролі

СЛОВО ПЕДАГОГА

Інший спосіб створити надійний пароль – зробити його довшим. Оскільки надійність пароля пов'язана з його довжиною, пароль у вигляді рядка з чотирьох або більше незв'язаних слів набагато складніше підібрати методом «грубої сили». Цей метод має додаткову перевагу, оскільки його простіше запам'ятати, ніж пароль, створений за «рецептом».

Крім того, можна використовувати комбінацію цих двох методів – створити рядок із чотирьох або більше незв'язаних слів і додати символи та цифри.

Мета застосування цих різних методів та сама – створити унікальні паролі, які буде складно вгадати іншим людям.

РОБОТА В КЛАСІ

Попросіть учнів розділитись на пари.

СЛОВО ПЕДАГОГА

У парах спробуйте створити надійний пароль, дотримуючись інструкцій, написаних на дошці раніше. Пам'ятайте, що пароль, який складно випадково вгадати комп'ютеру, може легко вгадати людина або комп'ютер зі списком поширених довгих паролів. Аркуші з паролями не будуть збиратися в кінці уроку. Не слід використовувати цей пароль для свого реального облікового запису, оскільки ви його вже розголосили групі.

РОБОТА В КЛАСІ

Надайте учням 5 хвилин для виконання цього завдання. Потім пройдіться по кімнаті та попросіть учнів надати приклади найнадійніших паролів. Запитайте учнів, чи вони можуть згадати паролі, які вони створили, не дивлячись на аркуші, де їх записано.

СЛОВО ПЕДАГОГА

Деякі сайти вимагатимуть, щоб паролі відповідали частині цих умов (або всім умовам), інші сайти не мають таких обмежень. Ви також можете створювати паролі у вигляді послідовності випадкових загальновживаних слів.

РОБОТА В КЛАСІ

Залишаючись у тих самих парах, нехай учні створять нові паролі у вигляді послідовності слів. Скажіть їм, що пароль має містити принаймні чотири слова, щоб бути надійним і легким для запам'ятовування. Надайте учням 5 хвилин для виконання цього завдання. Потім обійдіть клас і попросіть учнів надати їхні приклади паролів. Знову ж таки, нагадайте учням, що аркуші паперу не збиратимуться наприкінці завдання і що їм не слід використовувати ці паролі для своїх фактичних облікових записів.

СЛОВО ПЕДАГОГА

Деякі сайти використовують систему, яка називається багатофакторною (або двофакторною) автентифікацією для перевірки особи. Ці сайти часто надсилають одноразовий код, який потрібно ввести після пароля, за допомогою текстового повідомлення, додатка або електронної пошти.

Цей метод надійніше захищає облікові записи і забезпечує додатковий рівень захисту, який набагато складніше зламати. Наприклад, щоб увійти до вашого облікового запису, зловмисник повинен мати пароль і доступ до додатка, пристрою або адреси електронної пошти, пов'язаної з обліковим записом.

Безпека паролів

СЛОВО ПЕДАГОГА

Навіть якщо ви створите пароль, який справді складно зламати комп'ютеру або людині, він може бути ненадійним з інших причин.

ЗАПИТАЙТЕ В УЧНІВ

- Чому пароль може бути ненадійним?
  - Деякі приклади: один пароль для кількох облікових записів, пароль, що містить особисту інформацію, використання одного пароля протягом кількох років, забутий пароль.
- Як часто, на вашу думку, потрібно змінювати пароль?

СЛОВО ПЕДАГОГА

Навіть надійні паролі можна зламати або вкрасти, але ви можете захистити себе, вживши певних заходів. Якщо на сайті, де ви створили обліковий запис, виявлено витік інформації, обов'язково змініть пароль цього облікового запису, а також інших облікових записів, де ви використовуєте подібні паролі.

Запам'ятати багато довгих і складних паролів досить важко.

ЗАПИТАЙТЕ В УЧНІВ

- Як ви вважаєте, чи варто записувати паролі на аркуші паперу або у файлі на комп'ютері? Чому так або чому ні?

РОБОТА В КЛАСІ

Наведіть приклади можливих варіантів розвитку подій, якщо хтось знайде цей аркуш паперу або побачить файл на комп'ютері. Поясніть, що одним із варіантів є використання диспетчера паролів – додатка, який допомагає зберігати та впорядковувати паролі.

СЛОВО ПЕДАГОГА

Кожного дня ми використовуємо безліч облікових записів на різних сайтах. Щоразу заходити на сайт і виходити з нього незручно.

ЗАПИТАЙТЕ В УЧНІВ

- Ви колись використовували функцію запам'ятовування паролю в браузері, щоб зберегти його для певного сайту? Чому так або чому ні?
- Ви розумієте, як сайт вас запам'ятовує?
  - Попросіть пояснити.
  - Потім поясніть, що сайти запам'ятовують вхід, зберігаючи файли cookie. Файли cookie – це маленькі файли, що зберігаються на комп'ютері та допомагають сайтам запам'ятовувати користувача та його комп'ютер, щоб йому не доводилося кожного разу вводити облікові дані. Проте за допомогою файлів cookie також можна відстежувати, як ви переходите між сайтами. Завдяки цій технології відображається реклама, призначена саме для вас.
- Чи варто зберігати пароль на своєму комп'ютері?

ЗАПИТАЙТЕ В УЧНІВ

- Чи потрібно вводити пароль для входу на ваш комп'ютер? Що станеться, якщо ви надасте доступ до комп'ютера іншим користувачам?

СЛОВО ПЕДАГОГА

У цьому випадку, навіть якщо пароль у полі вводу приховано за допомогою чорних точок або зірочок, інші користувачі, які використовують ваш комп'ютер, потенційно можуть викрити його. Якщо ви не бачите пароль на екрані, це не означає, що він десь не зберігається.

ЗАПИТАЙТЕ В УЧНІВ

- Чи існують ситуації, коли можна передати комусь свій пароль? Коли? Чому?
  - Наприклад, батьки можуть попросити у вас пароль або хочуть приєднатися до спільного облікового запису Netflix.
- Ви передаєте паролі іншим людям? Якщо так, то кому та чому?
- Якщо близький друг скаже «якщо я тобі небайдужий», це буде для вас приводом дати йому свій пароль? Чому так або чому ні?

СЛОВО ПЕДАГОГА

Ви можете поділитися паролем з близькою людиною, але врахуйте, що довірливі стосунки не передбачають доступ до усіх ваших облікових записів.

Добре подумайте про свої стосунки з цією конкретною людиною, перш ніж надавати їй пароль. Зокрема подумайте про те, що ці стосунки можуть змінитися з часом. Наприклад, надати свій пароль комусь із батьків чи опікунів, це зовсім інша справа, ніж надати його найкращому другові.

ЗАПИТАЙТЕ В УЧНІВ

- Що може статися, якщо ви надасте комусь пароль?
  - Приклади. Хтось може зламати ваш банківський рахунок, видавати себе за вас у мережі або дізнатися деякі ваші секрети.
- Якщо ви надали пароль до облікового запису, чи будете ви використовувати цей обліковий запис інакше?

ЗАПИТАЙТЕ В УЧНІВ

- Чи є речі, які ви не дивитиметесь на Netflix або не писатимете в електронному листі, якщо хтось інший зможе побачити, що ви робите?

РОБОТА В КЛАСІ

Учні мають поміркувати над своєю поведінкою під час використання спільного облікового запису. Вони мають враховувати, що їхні дії в мережі бачать інші користувачі.

ЗАПИТАЙТЕ В УЧНІВ

- Якщо обліковий запис, наприклад профіль у соціальній мережі, репрезентує вас у віртуальній реальності, чи варто дозволяти іншим людям використовувати його?

РОБОТА В КЛАСІ

Обговоріть можливу ситуацію, коли інша людина видає себе за вас і надсилає повідомлення вашим друзям.

ЗАПИТАЙТЕ В УЧНІВ

- Чи ви дозволяєте пристроям, які використовуєте, зберігати паролі? Чому так або чому ні? Чи означає це, що зберігати паролі на телефоні чи комп'ютері безпечно? Що станеться, якщо ви позичите свій телефон чи комп'ютер другу?
- Ви використовуєте пристрої спільно з іншими користувачами, наприклад із рідними або друзями? Ви використовуєте спільний обліковий запис на цьому пристрої, чи кожний користувач має свій обліковий запис?
- Ви використовуєте загальнодоступні пристрої, наприклад у бібліотеці, у школі тощо? Під час використання цього пристрою ви поводитеся так само, як і на будь-якому іншому пристрої?

РОБОТА В КЛАСІ

Попросіть учнів розділитись на пари.

СЛОВО ПЕДАГОГА

Обговоріть у парах таку ситуацію. Ви входите на загальнодоступний комп'ютер у школі, бібліотеці або іншому публічному місці та бачите, що хтось не вийшов зі свого облікового запису в соціальній мережі або електронній пошті. Попросіть учасників подумати, розглядали би вони контент облікового запису чи виконували інші дії.

РОБОТА В КЛАСІ

Дайте учням 5 хвилин на обговорення питання несанкціонованого доступу до облікових записів, а потім обговоріть цю тему в групі.

Несанкціонований доступ до облікового запису

Частина 1

Зауваження. Частина матеріалу цієї вправи входить до вправи № 1: «Основні правила використання паролів». Ви можете ще раз пройти цей матеріал або пропустити його.

СЛОВО ПЕДАГОГА

Інші люди можуть отримати доступ до вашого облікового запису, навіть якщо вони не знають пароль і не вгадали його випадково. Якщо комусь відомо достатньо особистої інформації про вас, ця особа може мати уявлення про ваш пароль або може переконати когось у компанії передати вашу персональну інформацію. Оскільки в такому випадку для втручання в обліковий запис не використовуються технології, це втручання називається соціальним зламуванням або соціальною інженерією.

ЗАПИТАЙТЕ В УЧНІВ

- Підніміть руку, якщо ви колись забували пароль до якогось сайту. Що відбувається, коли ви вибираєте варіант «Я не пам'ятаю пароль»?
  - Приклади. Сайт зазвичай запитує відповіді на контрольні запитання або намагається зв'язатися з вами за номером телефону чи через електронну пошту.
- Що це за контрольні запитання?
  - Поясніть, як друзі або знайомі можуть дати відповіді на ці запитання чи вгадати їх. Як правило це такі дані: ім'я домашньої тварини, місто народження, дівоче прізвище мами, ім'я улюбленого вчителя, ім'я найкращого друга, улюблена спортивна команда.
- Хто ще може знати відповіді на ці запитання?
  - Як сайт зв'язується з вами, якщо ви забули пароль? Хто ще має доступ до цих засобів зв'язку?

ЗАПИТАЙТЕ В УЧНІВ

- Як незнайомець може дізнатися особисту інформацію, пов'язану з вашими відповідями на секретні запитання?
    - Приклади. Можна почитати дописи в соціальних мережах, пошукати загальнодоступну інформацію в мережі, кілька разів спробувати вгадати, зв'язатися з вашими друзями тощо.
- Наведіть кілька прикладів дописів у соціальних мережах, які можуть містити особисту інформацію.
    - Наприклад, світлина вашого кота в Instagram з його кличкою в заголовку, світлина з позначкою розташування або загальнодоступні дописи про день народження.
- Як за допомогою Google можна більше дізнатися про іншу людину та зламати її пароль?
    - Приклади. Якщо в пошуковій системі знайти світлину дев'ятого класу зі шкільної онлайн-газети, на якій зображено певну особу, можна з'ясувати ім'я вчителя цього класу.

Частина 2

СЛОВО ПЕДАГОГА

Публікувати інформацію, яка містить відповіді на секретні запитання, може бути дуже небезпечно. Обирайте секретні запитання, відповіді на які знаєте тільки ви.

Ви також можете вигадати відповіді на секретні запитання та зберегти їх у диспетчері паролів, або ці відповіді мають бути легкі для запам'ятовування.

Сайти можуть зв'язуватися з користувачами за допомогою номера телефону або адреси електронної пошти, пов'язаної з обліковим записом користувача. Якщо користувач забуває свій пароль, сайти часто надають тимчасовий пароль або гіперпосилання, за допомогою якого можна скинути пароль.

ЗАПИТАЙТЕ В УЧНІВ

- Як переконатися у тому, що людина, котра запитує новий пароль, не є зловмисником?
- Що станеться, якщо ви надасте комусь доступ до адреси електронної пошти, пов'язаної з паролем?
    - Приклади. У більшості випадків використання посилання для скидання пароля є безпечним, але якщо ви надаєте доступ до облікового запису або пароль іншій особі, це наражає вас на ризик.

СЛОВО ПЕДАГОГА

Соціальне зламування можуть здійснювати люди, які безпосередньо контактують із вами і намагаються виманити у вас вашу особисту інформацію. Наприклад, людина може надіслати вам електронне повідомлення, у якому вона видає себе за когось іншого (друга, члена сім'ї чи працівника банку), і попросити надати важливу інформацію (наприклад, дату народження), щоб підтвердити вашу особу. Це також можна зробити більш непомітно. Наприклад, зловмисник зламав обліковий запис у соціальній мережі вашого друга та просить вас (і, можливо, багатьох інших) назвати свій день народження або рідне місто. Якщо ви отримуєте повідомлення від друга, яке вам здається дивним, спочатку зв'яжіться із другом (за межами платформи соціальних мереж), щоб з'ясувати, чи це справді друг надіслав це повідомлення.

Атаки, у яких використовуються схожі на справжні адреси електронної пошти або сайти, називаються фішингом і можуть призвести до крадіжки персональних даних. Наприклад, злодій, що вкрав персональні дані, може відкрити кредитні картки на ваше ім'я та використовувати їх. Це може ускладнити для вас отримання кредитної картки в майбутньому.

Використовуючи фішинг, злодій може видавати себе за вас і отримати доступ до додаткової інформації, яка дасть йому змогу переглядати вашу електронну пошту, спілкуватися із друзями, видаючи себе за вас, або викрасти гроші. Використовуючи цю технологію, злодій також може заблокувати вам доступ до облікового запису, створивши новий пароль, який ви не знаєте.

Завдання

Попросіть учнів відповісти на наведені нижче запитання та додайте їхні відповіді у вигляді тексту або візуальних елементів до роздаткового матеріалу для уроку про паролі.

9. Які три принципи, які ви дізналися під час цього тренінгу, ви застосуєте наступного разу, коли створюватимете пароль?
10. Наведіть один приклад, коли ви вважаєте припустимим надати свій пароль іншій людині.
11. За допомогою яких трьох стратегій можна безпечно надати свій пароль іншій особі?
12. Наведіть три приклади розвитку подій, коли ваш пароль потрапляє до зловмисників.

РОЗДАТКОВИЙ МАТЕРІАЛ

Паролі

1. **Назвіть 3 принципи, про які ви дізналися під час цього уроку, котрі врахуєте під час створення паролів у майбутньому.**

2. **Наведіть 1 приклад ситуації, коли, на вашу думку, можна поділитися паролем з іншою людиною.**

3. **За допомогою яких 3 стратегій можна безпечно надати свій пароль іншій особі?**

4. **Наведіть три приклади розвитку подій, коли ваш пароль потрапляє до зловмисників.**

УРОК 4

Загальнодоступні мережі Wi-Fi

МЕТА УРОКУ

Учні дізнаються про переваги й ризики використання незахищених мереж Wi-Fi. Вони навчаться розпізнавати незахищені доступні мережі Wi-Fi, дізнаються про негативні сторони користування ними та навчаться приймати обґрунтовані рішення щодо того, коли підключатися до незахищеної мережі Wi-Fi і використовувати її.

ОСНОВНІ ЗАПИТАННЯ	▸ Наскільки надійно захищена ваша інформація в загальнодоступній мережі Wi-Fi? ▸ Що необхідно зробити, щоб уникнути можливих ризиків під час підключення до такої мережі?	
ВІК	▸ 15–18	
МАТЕРІАЛИ	▸ Роздатковий матеріал щодо безпеки підключення ▸ Примірник роздаткового матеріалу щодо безпеки підключення для педагога ▸ Зображення бездротового модема	
ПІДГОТОВКА	▸ Роздрукуйте матеріали для всіх учнів	
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	▸ ПИЛЬНІСТЬ: Я несу відповідальність за свої дії в мережі та знаю, як захистити себе й інших	

ДОПОМІЖНІ МАТЕРІАЛИ

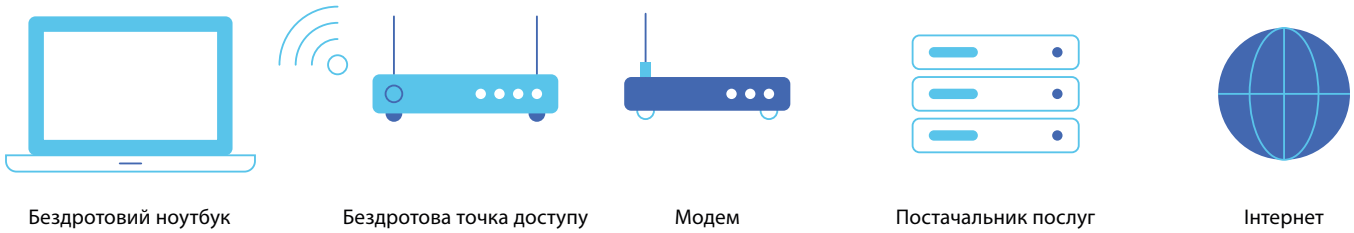
Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

Що таке Wi-Fi?

Частина 1

ЗАПИТАЙТЕ В УЧНІВ

- Які пристрої ви використовуєте для доступу до Інтернету?
- Як ці пристрої підключаються до Інтернету?



Бездротовий ноутбук | Бездротова точка доступу – маршрутизатор | Модем | Постачальник послуг Інтернету | Інтернет

РОБОТА В КЛАСІ З ЗОБРАЖЕННЯМ

Wi-Fi – це поширений спосіб підключення пристроїв до Інтернету. Wi-Fi використовує радіосигнали для підключення пристроїв без фізичного або дротового з'єднання.

Уявіть, що у вас вдома є три ноутбуки, які ви хочете підключити до Інтернету. Щоб підключитися до Інтернету через Wi-Fi, вам потрібні такі елементи:

1. **Точка доступу.** Точка доступу – це пристрій, який передає сигнал Wi-Fi і забезпечує доступ до Інтернету. Для підключення до Інтернету пристроям потрібно прийняти ці сигнали. Іноді може знадобитися спеціальний дозвіл (наприклад, ім'я користувача й пароль), щоб увійти в мережу та використовувати сигнал бездротового зв'язку, який передає точка доступу.
2. **Маршрутизатор.** Маршрутизатор – це пристрій, який створює мережу між усіма пристроями (наприклад, комп'ютерами, планшетами, мобільними телефонами) у певному розташуванні (наприклад, у школі, бібліотеці або у вас удома). Зазвичай точку доступу вбудовано в маршрутизатор (див. схему нижче).
   - Маршрутизатори мають обмежений (зазвичай короткий) радіус дії. Тому якщо пристрій розташовано далеко від маршрутизатора, він отримає слабкий сигнал Wi-Fi або не отримає його взагалі. Крім того, якщо між пристроєм і маршрутизатором є перешкода (наприклад, будівля або цегляна стіна), вона зменшить силу сигналу.
   - Хоча підключення до маршрутизатора забезпечує доступ до мережі, це ще не доступ до Інтернету. Щоб кілька пристроїв у мережі могли підключатися до Інтернету, маршрутизатор має бути під'єднано до модема.
3. **Модем.** Модем – це пристрій, який створює та підтримує підключення до інтернет-провайдера, щоб надати вам доступ до Інтернету. Він перетворює сигнали, що надходять ззовні, на сигнали, які можуть зчитуватися комп'ютером або іншими цифровими пристроями.
   - У типовому налаштуванні точка доступу й маршрутизатор – це єдиний пристрій, фізично під'єднаний до модема за допомогою кабелю Ethernet. Таке підключення мається на увазі, коли йдеться про «дротове» підключення до Інтернету. Мобільні пристрої також можуть використовувати стільниковий зв'язок для підключення до Інтернету, особливо поза школою, бібліотекою чи домом. Стільниковий зв'язок – це вид бездротового радіосигналу, який має набагато більшу зону покриття, ніж маршрутизатор. Для підключення мобільного пристрою до Інтернету за допомогою стільникового зв'язку використовуються спеціальні приймачі-передавачі, які називаються базовими станціями.

Частина 2

ЗАПИТАЙТЕ В УЧНІВ

- Які переваги має Wi-Fi?
- Які недоліки має Wi-Fi?
- Які проблеми з безпекою можуть виникнути під час використання Wi-Fi порівняно з дротовим інтернет-підключенням?
- Чому ви втрачаєте доступ до Wi-Fi на телефоні, коли залишаєте будинок?

Вибір мережі Wi-Fi

ЗАПИТАЙТЕ В УЧНІВ

- Чи всі мережі Wi-Fi безпечні? Чому так і чому ні?

СЛОВО ПЕДАГОГА

Іноді ви можете вибрати мережу Wi-Fi, яку хочете використовувати. Важливо пам'ятати, що ви наражаєтеся на серйозні ризики, якщо підключитеся не до тієї мережі. Наприклад, незахищені мережі Wi-Fi не вимагають пароль під час входу. Якщо ви перебуваєте в незахищеній мережі, інші користувачі в тій самій мережі можуть переглядати вашу інформацію. Вони можуть викрасти інформацію, яку ви надсилаєте через мережу, або стежити за тим, що ви робите.

Натомість захищені та надійні мережі Wi-Fi – це мережі, які вимагають пароль і підтримують шифрування даних, а також мережі, щодо яких ви впевнені, що їх назва представляє саме ту мережу, у яку ви входите. Наприклад, коли ви входите в мережу, яка називається іменем школи (але не є мережею школи), це може призвести до розкриття інформації про обліковий запис. Саме безпечні та надійні мережі пропонують найбільший захист.

Слід враховувати контекст або розташування мережі Wi-Fi. Наприклад, якщо ви перебуваєте в кінотеатрі й бачите на телефоні назву мережі своєї школи, коли шукаєте підключення до Wi-Fi, можете вважати, що ця мережа намагається імітувати або «підробляти» мережу школи, щоб збирати паролі з довірливих учнів.

Під час налаштування захищеної паролем мережі Wi-Fi її власник повинен увімкнути протокол шифрування маршрутизатора. Загальні протоколи шифрування – це Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) або WPA2. За допомогою цих протоколів інформація, яка надсилається бездротовою мережею, шифрується.

Шифрування було створено для того, щоб хакери не могли побачити, що ви надсилаєте. Проте всі ці протоколи (WEP, WPA і WPA2) виявилися вразливими до хакерства. Тому важливо покладатися на безпечні веб-підключення для передачі інформації в мережі.

HTTPS – це стандарт, який використовують сайти для шифрування даних, переданих через Інтернет. Шифрування може завадити третій стороні легко переглядати дані з вашого підключення. Воно гарантує додатковий рівень безпеки. Цей стандарт можна використовувати в будь-якому веб-браузері, додаючи «https: //» перед URL-адресою, яку ви використовуєте (наприклад, https://www.mysite.com). Проте не всі сайти підтримують протокол HTTPS.

1. Вводьте конфіденційну інформацію (наприклад, пароль, інформацію кредитної картки) тільки на веб-сторінках із префіксом HTTPS://.
2. Більшість стандартних браузерів мають індикатори безпеки у вигляді замка біля адресного рядка. Вони вказують на HTTPS-підключення.
3. На жаль, HTTPS не гарантує повну безпеку, оскільки деякі шкідливі сайти можуть також підтримувати HTTPS. Стандарт HTTPS захищає підключення, але не гарантує, що сайт є надійним.

СЛОВО ПЕДАГОГА

Безпеку стандарту HTTPS гарантує технологія Secure Sockets Layer (SSL)/Transport Layer Security (TLS). SSL/TLS використовує цифрові ключі шифрування, які працюють, як справжні ключі. Якщо ви написали якусь таємницю на аркуші паперу для друга, той, хто знайде цей папірець, зможе її побачити. А тепер уявіть, що ви особисто дали другові копію ключа та надіслали таємницю в закритій скриньці. Якщо хтось перехопить скриньку, йому буде важко побачити таємницю без ключа. Якщо хтось спробує підмінити скриньку подібною, ви помітите, що ключ не працює. Протокол SSL/TLS функціонує так само, але із сайтом.

Індикатори безпеки браузера також повідомлятимуть інформацію про сертифікат розширеної перевірки (EV). Сертифікати EV видаються сайтам, що підтвердили свою ідентифікацію в органі сертифікації. Іноді в браузерах індикатор EV відображається біля рядка адреси як назва сайту або органу реєстрації. Якщо вміст певного сайту здається підозрілим, ви можете перевірити, чи збігається URL-адреса в сертифікаті з URL-адресою у веб-браузері. Для цього скористайтеся функцією «Переглянути сертифікат». (Варто на екрані проектора показати учасникам, як знайти функцію «Переглянути сертифікат»). Навігація до цієї функції залежить від браузера. Наприклад, у Chrome потрібно відкрити меню «Вид», вибрати «Розробник», а потім – «Інструменти розробника». У меню «Інструменти розробника» виберіть вкладку «Безпека», потім – «Переглянути сертифікат».

ЗАПИТАЙТЕ В УЧНІВ

- Про що варто подумати під час підключення до нової мережі?
  - Можливі відповіді: розташування (тобто кому належить мережа), доступ (хто ще може підключитися до мережі) і дія (що ви збираєтеся робити в мережі).
- Кому належить мережа Wi-Fi у вас удома? А в школі? А в кав'ярні?
  - Домашня мережа Wi-Fi належить батькам чи опікунам, шкільна мережа – адміністраторам чи дирекції школи, а мережа в кав'ярні – власнику кав'ярні.
- Ви знаєте цих людей особисто? Ви довіряєте цим людям?
  - Залучіть учнів до обговорення про різні рівні довіри до цих людей.

СЛОВО ПЕДАГОГА

Ви маєте знати власника мережі Wi-Fi і довіряти йому. Іноді можна визначити власника мережі за ідентифікатором SSID.

Ідентифікатор SSID – це ім'я мережі Wi-Fi, яке ви бачите, коли намагаєтеся підключитися. Цей ідентифікатор часто повідомляє, кому належить мережа, а також містить відомості по неї. Будьте обережні, тому що майже всі люди (які знають, як це робиться) можуть створити SSID. Наприклад, хтось може створити SSID, що збігається з ідентифікатором, який ви використовуєте в школі. Це приклад видавання мережі за відому та довірену мережу для потенційного збору імен користувачів і паролів.

Якщо ви знаєте, кому належить мережа, ви можете визначити, чи вона безпечна. Якщо вона належить особі або організації, яким ви довіряєте, ви, скоріше за все, можете спокійно підключитися до неї. Проте, якщо мережа невідома, не варто з'єднуватися з нею, оскільки ви не знаєте, кому належить маршрутизатор, до якого ви підключаєтеся.

Оскільки весь трафік мережі проходить через маршрутизатор, власник може відстежувати та записувати його повністю.

Коли ви з'єднуєтеся з мережею Wi-Fi, пристрій підключається до локальної мережі пристроїв, яка зв'язана з Інтернетом. Оскільки ваш пристрій обмінюється інформацією через цю мережу, важливо, щоб ви довіряли іншим пристроям, до яких ви підключені, тобто кожному пристрою в мережі. Так само, як під час групової роботи в школі, ви повинні довіряти кожному учаснику, з яким ви працюєте.

Використання пароля для мережі обмежує коло людей, які можуть до неї підключитися. Це означає, що ви краще знатимете, хто перебуває в цій мережі (сім'я, друзі або інші клієнти кав'ярні), ніж у випадку з відкритою мережею.

Рішення щодо приєднання до мережі, яка виглядає підозрілою, має базуватися на компромісах, на які ви готові піти в плані безпеки в мережі. Вам потрібно подумати, чи готові ви ризикнути зламом свого облікового запису, щоб підключитися до доступної мережі?

ЗАПИТАЙТЕ В УЧНІВ

- Чи варто читати новини або блог у мережі, використовуючи мережу Wi-Fi удома? А в школі? А в кав'ярні?
  - Поясніть, що контент сайту зазвичай не містить конфіденційної інформації. Ви можете робите це в будь-якій мережі.
- Чи варто надсилати номер кредитної картки, використовуючи домашню мережу Wi-Fi? А в школі? А в кав'ярні? Чому?
  - Організуйте дискусію навколо питання, чому найбільш безпечно робити це через домашню мережу Wi-Fi і чому небезпечно через мережу в кав'ярні. Також обговоріть таку тему: хоча мережа школи, ймовірно, є надійною, не варто ризикувати, тому що саме ця інформація є надзвичайно конфіденційною.
- Чи варто перевіряти електронну пошту, використовуючи домашню мережу Wi-Fi? А в школі? А в кав'ярні?
  - Обговоріть, що найбезпечніше це робити через домашню мережу, залежно від контенту облікового запису електронної пошти. Наприклад, деякі люди мають кілька облікових записів електронної пошти, які вони використовують для різних цілей (наприклад, електронні листи з маркетингом і рекламою вони отримують в одному обліковому записі, а інший обліковий запис використовують для листування із друзями та родичами).

СЛОВО ПЕДАГОГА

Конфіденційні дані, зокрема паролі та банківську інформацію, краще передавати та переглядати у приватній і захищеній мережі, на сайтах, що використовують протокол SSL/TLS, а не у спільній загальнодоступній мережі. Ця приватна інформація буде під загрозою, якщо ви надішлете її або отримаєте доступ до неї у спільній мережі, яку використовують люди, яких ви не знаєте та яким не довіряєте.

Не завжди ясно, чи є інформація конфіденційною, оскільки рішення про конфіденційність ви приймаєте самостійно. Важливо розглядати кожну ситуацію окремо, щоб вирішити, чи варто підключатися до мережі. Перш ніж приймати рішення щодо підключення, запитайте себе, чи довіряєте ви власнику мережі й іншим людям, пов'язаним із нею, які дії ви виконуєте в мережі та якою інформацією ви ділитесь.

Захищені та незахищені мережі

Частина 1

Зауваження. Частина матеріалу цієї вправи входить до вправи № 2: «Вибір мережі Wi-Fi». Ви можете ще раз пройти цей матеріал або пропустити його.

СЛОВО ПЕДАГОГА

Як говорилося раніше, незахищені мережі Wi-Fi не вимагають пароль під час входу. Якщо ви використовуєте незахищені мережі, ви наражаєте на ризик дані, які передаєте й отримуєте через мережу.

Захищені мережі Wi-Fi вимагають пароль під час входу та підтримують шифрування даних. Особа, яка налаштовувала мережу, вирішує, вмикати шифрування

чи ні. Шифрування кодує інформацію, яку ви надсилаєте й отримуєте через мережу, тому хакерам у тій самій мережі Wi-Fi набагато важче побачити, що ви надсилаєте чи отримуєте.

Те, що мережа є захищеною, не означає, що дані в безпеці. Звісно, використовувати цю мережу безпечніше, ніж незахищену. Проте вмілий хакер все одно може знайти спосіб отримати доступ до персональної інформації.

Є три стандартні протоколи шифрування Wi-Fi-мереж. Це Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) або WPA2. WEP і WPA застарілі, тому мережі, які їх використовують, слід вважати незахищеними.

Крім того, протокол WPA2 також виявився вразливим до хакерства.

Щоб бути впевненими, що ваша інформація повністю захищена, переконайтеся, що сайти, які ви використовуєте, зашифровані за допомогою технології SSL/TLS.

ЗАПИТАЙТЕ В УЧНІВ

- Наведіть приклади захищених мереж, які ви раніше використовували.
  - Деякі приклади включають домашні мережі Wi-Fi, шкільні мережі, а також загальнодоступні мережі, наприклад, у кав'ярнях.
- Наведіть приклади незахищених мереж, які ви раніше використовували. А приклади захищених?

СЛОВО ПЕДАГОГА

Щоб перевірити, чи мережа Wi-Fi зашифрована, перегляньте налаштування мережі чи налаштування бездротового з'єднання на своєму пристрої.

Частина 2

РОБОТА В КЛАСІ

Для підготовки до цього уроку пошукайте в мережі інформацію про те, як перевірити типи шифрування мережі Wi-Fi в різних операційних системах. Потім продемонструйте, як дізнатись, який тип шифрування використовує мережа. Наприклад, у MacOS виберіть «Параметри системи» -> «Мережа» -> «Вибрати Wi-Fi». Потім виберіть ім'я відповідної мережі. У вкладці Wi-Fi ви побачите список відомих мереж і стовпець, що містить дані про шифрування, яке використовується в мережі.

СЛОВО ПЕДАГОГА

Не всі підключення однакові. До незахищеної мережі може підключитися будь-хто, і невідомо, хто її контролює. Приєднуючись до незахищеної мережі, ви стаєте вразливими, оскільки інформація, яку ви надсилаєте й отримуєте, а також увесь веб-трафік (сторінки, паролі тощо) може переглянути будь-хто в мережі, якщо ви не використовуєте SSL/TLS-підключення.

РОБОТА В КЛАСІ

Залежно від технічної обізнаності учнів, ви можете обговорити використання віртуальних приватних мереж як додаткового рівня безпеки під час використання Wi-Fi.

Безпечне підключення до Інтернету

РОБОТА В КЛАСІ

Розділіть учнів на групи по 2-3 особи. Роздайте учням матеріал щодо безпеки підключення та призначте ситуацію кожній групі. Дайте учням 5 хвилин на обговорення ситуацій. Потім попросіть групи повідомити відповіді.

Завдання

1. Намалюйте часову шкалу звичайного дня, позначаючи мережі Wi-Fi, до яких ви підключаєтесь.
2. З вибраних мереж, зображених на часовій шкалі, учні мають обрати дві та коротко описати їх. Хто ще підключається до цих мереж? Наскільки вони безпечні?
3. Крім того, для двох обраних мереж учні мають описати, які можливості надають ці підключення, і які ризики з ними пов'язані.

РОЗДАТКОВИЙ МАТЕРІАЛ

Безпечне підключення до Інтернету

Для кожної ситуації враховуйте місце, рівень доступу та свої дії в мережі. Потім визначте рівень ризику (низький, середній чи високий) і поясніть, чому ви визначили саме такий рівень.

РОЗТАШУВАННЯ	ДОСТУП	ДІЇ	РИЗИК
Будинок друга	**Сім'я друга**	**Онлайн-гра**	
Кав'ярня	**Тільки для клієнтів**	**Соціальна мережа**	
Бібліотека	**Тільки для відвідувачів**	**Фінансова транзакція**	
Аеропорт	**Загальний доступ**	**Електронна пошта**	

РОЗДАТКОВИЙ МАТЕРІАЛ

Безпечне підключення до Інтернету

ПРИМІРНИК ДЛЯ ПЕДАГОГА

Для кожної ситуації враховуйте місце, рівень доступу та свої дії в мережі. Потім визначте рівень ризику (низький, середній чи високий) і поясніть, чому ви визначили саме такий рівень.

РОЗТАШУВАННЯ	ДОСТУП	ДІЇ	РИЗИК
Будинок друга	**Сім'я друга**	**Онлайн-гра**	**НИЗЬКИЙ** У мережі небагато людей, і ви їм довіряєте. Дії не передбачають передачу конфіденційної інформації.
Кав'ярня	**Тільки для клієнтів**	**Соціальна мережа**	**СЕРЕДНІЙ** Соціальна мережа не обов'язково містить конфіденційну інформацію, але кожен, хто раніше був у кав'ярні, матиме доступ до мережі та може вкрасти ваші паролі.
Бібліотека	**Тільки для відвідувачів**	**Фінансова транзакція**	**ВИСОКИЙ** Банківська інформація є надзвичайно конфіденційною. Хоча доступ до бібліотеки дещо обмежений, ви не знаєте, хто може зі злими намірами отримати доступ до вашої інформації.
Аеропорт	**Загальний доступ**	**Електронна пошта**	**ВИСОКИЙ** Навіть якщо ваша електронна пошта не містить конфіденційних даних, використання загальнодоступної мережі не є безпечним.

УРОК 5

Кібербезпека, фішинг і спам

МЕТА УРОКУ

Учні дізнаються про зловмисників у мережі, які можуть намагатися використати слабкі місця системи безпеки для збору інформації про користувачів. Учні зможуть описати ризики перебування в мережі, розробити стратегії для безпечнішої поведінки, визначити спам-повідомлення та пояснити, хто має право запитувати їхній пароль.

ОСНОВНІ ЗАПИТАННЯ	Як дізнатися, чи захищені ваша інформація, пристрої та ресурси (наприклад, паролі) під час використання цифрових технологій?
ВІК	15–18
МАТЕРІАЛИ	Роздатковий матеріал щодо спаму Примірник роздаткового матеріалу щодо спаму для педагога
ПІДГОТОВКА	Роздрукуйте матеріали для всіх учнів
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПИЛЬНІСТЬ: Я несу відповідальність за свої дії в мережі та знаю, як захистити себе й інших

ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

Ризики в Інтернеті

СЛОВО ПЕДАГОГА

Коли ви користуєтеся Інтернетом, ви можете наражатися на ризик, просто відкриваючи веб-сторінки, спілкуючись у мережі або завантажуючи дані. Іноді сайти, які ви відкриваєте, люди у вашій мережі або навіть треті сторони можуть визначити ваше місцезнаходження чи іншу інформацію про вас.

ЗАПИТАЙТЕ В УЧНІВ

- Хто може скористатися слабкими місцями в онлайн-безпеці, щоб побачити особисту інформацію?
  - Можливі відповіді: кіберзлочинці, державні служби нагляду тощо.

СЛОВО ПЕДАГОГА

Коли ви переглядаєте веб-сторінки, кіберзлочинці можуть збирати дані про вас так само, як це роблять інтернет-провайдери. Щоб зменшити такий ризик, для доступу до сайтів необхідно використовувати безпечне підключення. Незалежно від типу підключення багато сайтів намагаються відстежувати характер використання вами мережі на різних платформах. Вони можуть визначити ваш браузер, місцезнаходження й інші особливості використання, щоб більше про вас дізнатися.

ЗАПИТАЙТЕ В УЧНІВ

- Чому кіберзлочинці намагаються отримати доступ до інформації про користувача в мережі?
- Яку інформацію шукають ці люди?
- Чому сайт, на якому ви не зареєстровані, хоче дізнатися, хто ви?
- Приклади: будь-яка інформація, яка ідентифікує особу, та будь-яка інформація, яку можна продати або використати для отримання грошової вигоди.
- Хтось знає, що таке шкідливі програми? Що вони можуть робити?

СЛОВО ПЕДАГОГА

Шкідлива програма – це шкідливий програмний код, який непомітно виконується на комп'ютері. Деякі шкідливі програми можуть збирати дані з будь-якої частини локального комп'ютера – від жорсткого диска до даних веб-браузера. Вони також дають хакерам змогу взяти ваш комп'ютер під контроль і використовувати його на свій розсуд. Більшість шкідливих програм досить прості, наприклад сайти, які імітують захищені портали (такі як сайти банку), або розширення, які розміщують рекламу у браузері, щоб заробляти гроші.

ЗАПИТАЙТЕ В УЧНІВ

- Що можна зробити, щоб захистити себе від шкідливих програм, шпигунства та відстеження?

СЛОВО ПЕДАГОГА

Будьте обережні, натискаючи посилання, рекламні оголошення або дописи в соціальних мережах. Чи збігається URL-адреса з тією, яку ви очікуєте? Чи потрапляєте ви на ту саму сторінку, коли вводите її знову самостійно або шукаєте сайт? Візьміть за правило захищати за допомогою протоколів SSL/TLS сторінки входу у всі важливі облікові записи (наприклад, Google, Facebook, Twitter або банківські рахунки). Протоколи SSL/TLS дуже ускладнюють хакеру в мережі надсилання підроблених сайтів, якщо ви вводите правильну URL-адресу, яка може бути дуже простою.

Деякі сайти можуть запускати код для доступу до вашої особистої інформації або облікових записів у мережі, якщо на платформах виникає помилка кодування. Вони потім можуть надсилати з ваших облікових записів спам іншим користувачам.

Завантажуйте й інсталюйте програмне забезпечення тільки з надійних джерел і будьте уважні, коли завантажуєте виконувані файли (з розширенням .exe, .pkg, .sh, .dll або .dmg). Виконувані файли – це файли, які виконують дію. Іноді ці дії можуть бути зловмисними. Наприклад, зловмисник може написати виконуваний код, щоб стерти чийсь жорсткий диск або інсталювати підробний браузер. Саме тому ви повинні інсталювати додатки тільки з надійних джерел.

За допомогою антивірусного програмного забезпечення можна запобігти запуску шкідливих програм. Деякі антивірусні програми постачаються разом із комп'ютером (наприклад, Microsoft Security Essentials для Windows); а деякі операційні системи, як-от на комп'ютерах Apple, мають налаштування безпеки, які блокують програмне забезпечення з ненадійних джерел. Добре подумайте, перш ніж змінювати ці налаштування.

Ви також можете установити розширення браузера, які, наприклад, блокують плагіни. Завдяки цьому сайтам буде складніше з'ясувати, хто ви, або стежити за вами. Однак такий плагін може блокувати функції сайтів, зокрема можливість перегляду відео.

Рішення щодо інсталяції розширення для веб-браузера має базуватися на ваших побажаннях і компромісах, на які ви готові піти щодо безпеки в мережі. Ви можете поміркувати над такими питаннями: Наскільки незручно для мене те, що мої дії відстежуються? Чого варта моя конфіденційність? Наскільки мені хочеться переглянути цей контент (наприклад, коли розширення браузера блокує плагін, який відтворює відео)?

Інструменти безпеки

Зауваження. Частина матеріалу цієї вправи входить до вправи № 1: «Ризики в мережі». Ви можете ще раз пройти цей матеріал, якщо ви вже розглянули його від час виконання вправи № 1, або пропустити його.

ЗАПИТАЙТЕ В УЧНІВ

- Ви впевнені у своїй безпеці, коли використовуєте Інтернет?

СЛОВО ПЕДАГОГА

Не вживаючи належних запобіжних заходів, дуже важко (а часом навіть неможливо) успішно захистити себе від цих ризиків у мережі (описаних у попередньому розділі).

Окрім того, постійно виникають нові онлайн-ризики, тому дуже важливо бути уважними.

ЗАПИТАЙТЕ В УЧНІВ

- Що може зробити особа, яка переконає вас, що її сайт насправді є важливим?
- Ось інструменти, які допоможуть вам уникнути ризиків або знизити їх. Хто з вас знає ці інструменти?

СЛОВО ПЕДАГОГА

HTTPS – це стандарт, який використовують сайти для шифрування даних, переданих через Інтернет. Шифрування може завадити третій стороні легко переглядати дані з вашого підключення. Воно гарантує додатковий рівень безпеки. Цей стандарт можна використовувати в будь-якому веб-браузері, додаючи «https: //» перед URL-адресою, яку ви використовуєте (наприклад, https://www.mysite.com). Проте не всі сайти підтримують протокол HTTPS.

1. Вводьте конфіденційну інформацію (наприклад, пароль, інформацію кредитної картки) тільки на веб-сторінках із префіксом HTTPS://.
2. Ви можете використовувати програмні інструменти, які гарантуватимуть, що ви завжди використовуватимете протокол HTTPS, коли це можливо.
3. Більшість стандартних браузерів мають індикатори безпеки у вигляді замка біля адресного рядка. Вони вказують на HTTPS-підключення.
4. На жаль, HTTPS не гарантує повну безпеку, оскільки деякі шкідливі сайти можуть також підтримувати HTTPS. Стандарт HTTPS захищає підключення, але не гарантує, що сайт є надійним.

Безпеку стандарту HTTPS гарантує технологія Secure Sockets Layer (SSL)/Transport Layer Security (TLS). SSL/TLS використовує цифрові ключі шифрування, які працюють, як справжні ключі. Якщо ви написали якусь таємницю на аркуші паперу для друга, той, хто знайде цей папірець, зможе її побачити. А тепер уявіть, що ви особисто дали другові копію ключа та надіслали таємницю в закритій скриньці. Якщо хтось перехопить скриньку, йому буде важко побачити таємницю без ключа. Якщо хтось спробує підмінити скриньку подібною, ви помітите, що ключ не працює. Протокол SSL/TLS функціонує так само, але із сайтом.

Індикатори безпеки браузера також повідомлятимуть інформацію про сертифікат розширеної перевірки (EV). Сертифікати EV видаються сайтам, що підтвердили свою ідентифікацію в органі сертифікації. Іноді в браузерах індикатор EV відображається біля рядка адреси як назва сайту або органу реєстрації. Якщо вміст певного веб-сайту здається підозрілим, ви можете перевірити, чи збігається URL-адреса в сертифікаті з URL-адресою у веб-браузері. Для цього скористайтеся функцією «Переглянути сертифікат». Можливо, буде корисно показати на екрані проектора, як знайти функцію «Переглянути сертифікат». Навігація до цієї функції залежить від браузера. Наприклад, у Chrome потрібно відкрити меню «Вид», вибрати «Розробник», а потім – «Інструменти розробника». У меню «Інструменти розробника» виберіть вкладку «Безпека», потім – «Переглянути сертифікат».

Не запускайте програмне забезпечення з ненадійних джерел, використовуйте антивірусне програмне забезпечення, яке може запобігти відвідуванню ненадійних сторінок і завантаженню шкідливих програм.

Акт «фішингу» починається з електронного листа від спамера, який видає себе за легітимну сторону. Потім у вас запитують пароль. Спамер сподівається, що ви надішлете пароль електронною поштою або введете його на підробленому сайті. Фільтри спаму можуть запобігти відображенню деяких із цих листів у папці «Вхідні». Щоб покращити роботу фільтрів спаму, обов'язково позначайте всі підозрілі електронні листи, які потрапляють до поштової скриньки, як спам.

ЗАПИТАЙТЕ В УЧНІВ

- Що б ви могли зробити, щоб запобігти випадковому завантаженню файлів, шкідливих для комп'ютера?

СЛОВО ПЕДАГОГА

Завжди переконуйтеся, що ви завантажуєте файли з надійних сайтів. Будьте особливо обережні, відкриваючи вкладені файли електронної пошти, які ви не впізнаєте, і натискаючи спливні вікна та повідомлення про помилки. Ви також можете інсталювати на комп'ютер перевірені програми захисту від шкідливого програмного забезпечення.

Передавання паролів

ЗАПИТАЙТЕ В УЧНІВ

- Як ви вважаєте, коли припустимо передавати комусь свій пароль?
  - Можлива відповідь: спільні облікові записи (наприклад, Netflix).
- Які ризики можуть бути пов'язані з передаванням пароля?
  - Якщо пароль отримають зловмисники, вони можуть зламати ваш обліковий запис. Передавання пароля збільшує ймовірність того, що хтось отримає доступ до облікового запису. Якщо ви

використовуєте один і той самий пароль на інших сайтах, зловмисники можуть також можуть отримати доступ до них.

СЛОВО ПЕДАГОГА

Ви не повинні передавати паролі нікому, використовуйте їх тільки для додатка, який вимагає пароль для входу. Це має бути стандартною практикою. Як описано раніше, фішинг – це спроба обманом змусити когось повідомити свій пароль.

Однак у вас можуть явно попросити пароль, щоб отримати доступ до облікових записів, стверджуючи, що вони в небезпеці. Незважаючи на те, що деякі з цих людей можуть мати добрі наміри, (наприклад, друг, який хоче допомогти з'ясувати щось у вашому обліковому записі, що вас непокоїть), не варто передавати свій пароль, особливо якщо ви використовуєте його для кількох облікових записів. Якщо ви плануєте передати пароль, переконайтеся, що він більше ніде не використовується, а для надання доступу використовуйте диспетчер паролів.

Іноді пароль можуть запитувати дорослі люди, яких ви знаєте та яким ви довіряєте, наприклад, батьки, вчителі чи роботодавці. Незважаючи на те, що ви знаєте цих людей і довіряєте їм, буде корисно для всіх (і для вас, і для них) поговорити про те, навіщо їм потрібен ваш пароль, і що вони збираються з ним робити. Якщо питає дорослий, який не є членом вашої родини, варто запитати його прямо, чи є якийсь закон або інше правило, що вимагає від вас надати пароль.

Особливо важливо ставити ввічливі й чіткі запитання про закони та правила, якщо запит на пароль надходить від дорослого, який не є членом вашої родини та якого ви не знаєте особисто. Наприклад, якщо це працівник правоохоронних органів. Якщо працівники поліції чи інші державні службовці запитують у вас паролі до соціальних мереж, поводьтеся спокійно та ввічливо. Поцікавтеся, чому вони питають про паролі і які закони або правила дають їм, на їхню думку, право отримати цю інформацію від вас.

Залежно від обставин запиту від батьків чи опікунів, вчителів, роботодавців, працівників правоохоронних органів, державних службовців або інших дорослих, вам можливо доведеться надати їм свої паролі. Підставою для надання паролів може бути закон або правило, яке вимагає від вас цього. Або ж ви можете надати пароль, якщо вважаєте, що користь, яку ви отримаєте від їхньої допомоги, перевищує ризики надання паролів.

Якщо доросла особа питає вас про паролі і через це ви почуваєтеся незручно, зверніться негайно до батьків/опікунів або інших дорослих, яким довіряєте. Найкраще буде звернутися до них, перш ніж відповідати на запит.

ЗАПИТАЙТЕ В УЧНІВ

- За яких обставин вам слід надавати свій пароль у мережі?

- Приклади. Тільки коли потрібно ввести пароль для входу на сайт. Ніколи нікому не надавайте свій пароль, зокрема через електронну пошту, що, як правило, використовує незашифроване та ненадійне з'єднання.

Завдання

Частина 1

РОЗДАТКОВИЙ МАТЕРІАЛ

Розділіть учнів на групи по 2-3 особи. Роздайте роздатковий матеріал щодо спаму. Потім попросіть, щоб кожен учень побудував блок-схему, щоб показати іншим, як можна виявити спам і чи слід надавати певну інформацію окремим особам або групам людей.

СЛОВО ПЕДАГОГА

Прочитайте опис кожної ситуації та обговоріть кожне повідомлення: чи є воно спамом і чи слід надавати інформацію особі або групі людей у такій ситуації.

РОБОТА В КЛАСІ

Надайте учням 10 хвилин для виконання цього завдання. Потім попросіть групи повідомити відповіді.

ЗАПИТАЙТЕ В УЧНІВ

- Коли слід передавати свій пароль електронною поштою?

СЛОВО ПЕДАГОГА

Сайти та компанії ніколи не просять надати їм пароль електронною поштою. Це стандартна практика. Ніколи нікому не передавайте пароль по такому каналу, навіть якщо той, хто його запитує, видається справжнім. Електронна пошта майже ніколи не буває захищеною.

Частина 2

Попросіть учнів залишити групи, оскільки наступну вправу вони мають виконувати самостійно.

Дайте учням 15 хвилин на створення блок-схем.

СЛОВО ПЕДАГОГА

Тепер на аркуші паперу намалюйте блок-схему, щоб показати всім, як можна ідентифікувати спам і чи слід надавати певну інформацію в мережі іншим людям. Учні можуть застосувати конкретну ситуацію, на якій буде засновано їхню блок-схему. Це може бути будь-яка з ситуацій, представлених у роздатковому матеріалі (у такому разі над блок-схемою слід зазначити її номер), або абсолютно нова. Якщо ви вирішите придумати власну ситуацію, опишіть її коротко над своєю блок-схемою.

Дайте учням 15 хвилин на створення блок-схем.

РОЗДАТКОВИЙ МАТЕРІАЛ

Спам

У кожній ситуації визначте, чи повідомлення є спамом і чи слід надати інформацію цій людині. Напишіть відповідь на кожне запитання у відповідному полі.

СИТУАЦІЯ 1. Ви отримуєте електронного листа від адвоката, у якому повідомляють, що далекий родич залишив вам гроші. У повідомленні сказано: «Щоб отримати гроші, надішліть мені номер свого банківського рахунку та номер маршрутизації, щоб ми могли переказати Вам гроші».

СИТУАЦІЯ 2. Друг надсилає вам повідомлення про те, що він намагається знайти світлину, яку ви показали йому раніше, але в нього немає дозволу на її перегляд. У вас немає доступу до комп'ютера, щоб надіслати зараз світлину. Друг відповідає: «Я можу ввійти у твій обліковий запис, щоб завантажити світлину. Який у тебе пароль?»

СИТУАЦІЯ 3. Ви отримуєте електронного листа зі свого навчального закладу. У ньому повідомляється, що багато облікових записів учнів зламано. Текст повідомлення: «Нещодавно ми виявили, що багато облікових записів студентів було зламано. Просимо вибачення за незручності. Ми працюємо над вирішенням цієї проблеми. Щоб скинути обліковий запис, повідомте у відповіді на цей електронний лист своє ім'я користувача та пароль».

СИТУАЦІЯ 4. Ви отримуєте електронного листа з банку, у якому маєте дійсний рахунок. В електронному листі повідомляється, що систему банку зламано, і що ви повинні змінити пароль свого облікового запису. Також слід змінити паролі всіх облікових записів, для яких ви використовуєте такий самий пароль.

РОЗДАТКОВИЙ МАТЕРІАЛ

Спам

ПРИМІРНИК ДЛЯ ПЕДАГОГА

У кожній ситуації визначте, чи повідомлення є спамом і чи слід надати інформацію цій людині. Напишіть відповідь на кожне запитання у відповідному полі.

СИТУАЦІЯ 1

Ви отримуєте електронного листа від адвоката, у якому повідомляють, що далекий родич залишив вам гроші. У повідомленні сказано: «Щоб отримати гроші, надішліть мені номер свого банківського рахунку та номер маршрутизації, щоб ми могли переказати Вам гроші».

- Найімовірніше це спам. Навіть якщо в цьому листі міститься правильне ім'я вашого родича, скоріше за все відправник не той, за кого себе видає. Відправник міг отримати інформацію про родича іншим способом. Надаючи реквізити банківського рахунку, ви ризикуєте, тому це треба робити обережно. Ніколи не надсилайте свою інформацію людині, з якою ви самі спочатку не зв'язались. І навіть у таких випадках будьте обережні. Наприклад, не варто надсилати свою інформацію електронною поштою в незашифрованому повідомленні. Саме тому більшість лікарень, юристів і банків мають спеціальні сайти для спілкування з клієнтами.

СИТУАЦІЯ 2

Друг надсилає вам повідомлення про те, що він намагається знайти світлину, яку ви показали йому раніше, але в нього немає дозволу на її перегляд. У вас немає доступу до комп'ютера, щоб надіслати зараз світлину. Друг відповідає: «Я можу ввійти у твій обліковий запис, щоб завантажити світлину. Який у тебе пароль?»

- Хоча це не спам, не варто надавати свої паролі іншим людям. Після отримання паролю вони можуть заблокувати вам доступ до вашого облікового запису або отримати доступ до інших облікових записів із таким самим паролем. Крім того, якщо стороння особа, хакер або випадковий свідок побачить це повідомлення, більше людей зможуть отримати доступ до облікового запису без вашого відома.

СИТУАЦІЯ 3

Ви отримуєте електронного листа зі свого навчального закладу. У ньому повідомляється, що багато облікових записів студентів зламано. Текст повідомлення: «Нещодавно ми виявили, що багато облікових записів студентів було зламано. Просимо вибачення за незручності. Ми працюємо над вирішенням цієї проблеми. Щоб скинути обліковий запис, повідомте у відповіді на цей електронний лист своє ім'я користувача та пароль».

- Як правило, у користувачів не запитують таку інформацію. Навіть якщо відправник виглядає справжнім, ви повинні припускати, що будь-який електронний лист, який запитує пароль, є спамом.

СИТУАЦІЯ 4

Ви отримуєте електронного листа з банку, у якому маєте дійсний рахунок. В електронному листі повідомляється, що систему банку зламано, і що ви повинні змінити пароль свого облікового запису. Також слід змінити паролі всіх облікових записів, для яких ви використовуєте такий самий пароль.

- Правильно буде відкрити нове вікно веб-браузера та ввійти на сайт, як ви завжди це зробите. Повідомлення такого типу (про злам облікових записів), як правило, розміщуються на порталі для клієнтів компанії або банку. Інструкції на порталі мають бути такими, щоб їх можна було безпечно виконати. Як і в ситуації 3, жоден законний представник організації не буде вимагати від вас надіслати облікові дані в електронному листі.

УРОК 6

Пошук та оцінка онлайн-ресурсів

МЕТА УРОКУ

- **На цьому уроці учні зрозуміють, що популярність і надійність – це два основні фактори, які слід брати до уваги під час пошуку й вибору онлайн-ресурсів**
- **Вони також складуть контрольні списки для оцінювання результатів пошуку, які потім зможуть використовувати в повсякденному житті.**

ОСНОВНІ ЗАПИТАННЯ	Як вибрати надійне джерело інформації серед великої кількості результатів пошуку?
ВІК	11–14
МАТЕРІАЛИ	Папір Ручки або олівці Примірники роздаткового матеріалу «Приклад пошукового запиту в Google»
ПІДГОТОВКА	Роздрукуйте матеріали для всіх учнів
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПОІНФОРМОВАНІСТЬ: Я отримую інформацію з точних, достовірних і об'єктивних цифрових інформаційних ресурсів і дописів у соціальних мережах.

ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте ***facebook.com/fbgetdigital***, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

ОГЛЯД УРОКУ

Мета цього уроку – в епоху Google та інших пошукових систем допомогти учням зорієнтуватися у способах отримання інформації за допомогою інструментів онлайн-пошуку. Вони оцінять результати пошуку в Google і дізнаються, що популярні сайти не завжди надійні. Під час проведення власного дослідження вони створять інструмент для незалежного визначення найбільш відповідних і актуальних джерел у формі контрольних списків.

ПЛАН РОБОТИ

1. Розділіть учнів на невеликі групи й роздайте їм матеріали «Приклад пошукового запиту в Google». Попросіть учнів розташувати результати пошуку в порядку від більш надійних до менш надійних. Запишіть на дошці визначення терміну «надійність».
2. Попросіть учнів поділитися результатами вправи та пояснити, чому вони розмістили джерела саме в такому порядку.
3. Створіть на дошці таблицю із двома стовпцями – «Надійні джерела» й «Ненадійні джерела». На основі створеного учнями рейтингу розмістіть кожне джерело із прикладів пошуку у відповідному стовпці. Також запишіть, чому, на думку учнів, цим джерелам можна (або не можна) довіряти.
4. Поясніть учням, що в пошукових системах, як і у ваших роздаткових матеріалах, результати пошуку сортуються не за надійністю, а за популярністю, місцем розташування та історією пошукових запитів.
5. Попросіть учнів розділитися на пари та вдвох скласти контрольний список для оцінювання результатів пошуку.
6. Потім запропонуйте їм поділитися цим списком з усім класом і складіть загальний контрольний список. Слід розрізняти обов'язкові й необов'язкові пункти (наприклад, адреса сайту може мати розширення .edu або заголовок сайту не повинен бути вираженням якоїсь думки).
7. Контрольні списки можуть, серед іншого, містити такі критерії:
   - До якої категорії належить сайт або сторінка? (Як правило, особисті блоги, форуми й колонки порад не є надійними джерелами.)
   - Чи пов'язаний сайт із навчальним закладом чи організацією?
   - Чи належить сайт авторитетному джерелу новин, яке здійснює перевірку фактів, наприклад Associated Press або Washington Post?
   - Яке розширення має URL-адреса сайту – .edu, .com, .org, .net або інше? Про що це свідчить?
   - Чи схожий заголовок сайту на «клікбейт» або містить надмірно емоційні чи «сенсаційні» заяви?
   - Чи вказано на сторінці або сайті ім'я авторитетного автора?
   - Чи вказано джерела інформації?
   - Чи виражено точку зору авторів у заголовку або назві?
   - Коли створено сайт або опубліковано статтю?
8. Якщо учні забудуть згадати які-небудь важливі критерії, запропонуйте їх і поясніть, чому вони важливі.
9. Попросіть учнів записати в зошитах відповіді на такі запитання: Чому, на вашу думку, результати пошуку не сортуються виключно за надійністю? Чому важливо мати контрольний список для перевірки надійності? Як змінилося ваше ставлення до результатів пошуку в мережі після цієї вправи?

СЛОВНИК

алгоритм (іменник) – процес або набір правил, яких потрібно дотримуватися під час розрахунків або інших операцій для розв'язання задачі, особливо за допомогою комп'ютера

алгоритм пошуку (іменник) – математичний процес, за допомогою якого пошукова система виконує запити користувачів

надійність (іменник) – характеристика того, хто заслуговує на довіру

популярність (іменник) – інтерес, захоплення або підтримка з боку багатьох людей

Джерела:
Google Dictionary
merriam-webster.com
en.oxforddictionaries.com

tolerance.org/classroom-resources/tolerance-lessons/understanding-and-evaluating-online-searches

РОЗДАТКОВИЙ МАТЕРІАЛ

Приклад пошукового запиту в Google

Нижче ви бачите результати пошуку в Google за ключовими словами «мобільні телефони впливають на підлітків». Працюючи в команді, впорядкуйте ці результати від більш надійних до менш надійних. Підготуйтеся, щоб пояснити хід своїх думок.

Негативний вплив мобільних телефонів на здоров'я підлітків...

livestrong.com **› Батьки й діти**
13 серпня 2015 року – Мобільні телефони викликають залежність у підлітків. Вони становлять небезпеку для здоров'я підлітків – від порушень сну до написання текстових повідомлень за кермом...

7 прикладів негативного впливу мобільних телефонів на підлітків | MomJunction

momjunction.com **› Від 13 до 15 років › Безпека**
6 січня 2017 року – Як мобільні телефони впливають на здоров'я дітей? Чи небезпечні вони для підлітків? Читайте далі, щоб дізнатися...

Мобільні телефони: вплив на здоров'я підлітків | Як стати щасливим...

openlab.citytech.cuny.edu/the-composition-of-happiness-f2014/2014/11/24/cell-phones-physical-effects-on-teenagers
24 листопада 2014 року – Вчені неодноразово досліджували вплив мобільних телефонів на здоров'я підлітків... У підлітків, які часто користуються мобільними телефонами, підвищується рівень тривожності та порушується сон. Крім того, їм важко зосередитися, і вони швидше втомлюються. Цитата зі статті: «Люди не можуть обходитися без мобільних телефонів».

Вплив мобільних телефонів на дітей і підлітків | HuffPost

huffpost.com/entry/examining-the-effects-of-mobile-phones-on-kids-and-teens_b_8633658
27 листопада 2015 року – Порівняно нещодавно вчені почали досліджувати вплив радіочастотного електромагнітного поля, створюваного мобільними телефонами, на сон, роботу мозку й когнітивні функції дітей у віці від 10 до 18 років. Раніше досліджувався вплив радіовипромінювання від мобільних телефонів та інших пристроїв на дорослих, але не на дітей.

Як мобільний телефон впливає на мозок підлітка? | CBS News

cbsnews.com/news/what-do-mobile-phones-do-to-teenage-brains
20 травня 2014 року – У рамках наймасштабнішого дослідження на цю тему вчені проаналізують вплив мобільних телефонів на людський мозок, який розвивається: на пам'ять, увагу тощо.

РОЗДАТКОВИЙ МАТЕРІАЛ

Приклад пошукового запиту в Google

Підлітки й мобільні телефони: вплив, ризики та проблеми...

unitec.researchbank.ac.nz/handle/10652/1270

Автор: Ш. Равідчандран (S Ravidchandran) - 2009 - Кількість цитувань: 4 - Інші статті на цю тему. Стан проблеми. Сьогодні люди, а особливо підлітки, все рідше випускають із рук мобільні телефони. У літературі наведено надійні докази того, що...

Залежність від мобільних телефонів у підлітків | PsychGuides.com

psychguides.com/guides/teen-cell-phone-addiction

Ознаки, симптоми й наслідки залежності від мобільних телефонів у підлітків: як виявити проблему й допомогти підлітку впоратися з нею.

Підлітки й мобільні телефони: поради батькам | CHLA

chla.org/blog/rn-remedies/parents-guide-teens-and-cell-phones

Батьки нерідко хвилюються через те, що їхня дитина проводить дуже багато часу з мобільним телефоном... цькування в мережі має вкрай негативні наслідки й може навіть загрожувати життю підлітка.

5 фактів про вплив екрана телевізора, комп'ютера й мобільного телефона на підлітків...

fit.webmd.com/teen/recharge/article/teens-screen-time

Більшість підлітків проводить багато часу перед екраном телевізора, комп'ютера або мобільного телефона, що негативно впливає на їхні здоров'я, настрій і успішність. WebMD рекомендує...

УРОК 7

Оцінка надійності онлайн-ресурсів

МЕТА УРОКУ

- **Оцінити надійність джерел**
- **Використовувати різні засоби для перевірки джерел з точки зору точності й неупередженості**
- **Виявити та зрозуміти поширені помилки в оцінюванні достовірності**
- **Розробити спосіб або засіб оцінювання достовірності джерел**

ОСНОВНІ ЗАПИТАННЯ	Чому демократичне суспільство покладається на чесні й надійні засоби інформації? Чому одні засоби оцінювання достовірності, які можна застосувати до інтернет-джерел або новин, надійніші, ніж інші?
ВІК	15–19
МАТЕРІАЛИ	Відео «Fake News Stories Thriving on Social Media» *edition.cnn.com/2016/11/20/opinions/fake-news-stories-thrive-donath/index.html* Повний посібник з оцінювання інтернет-ресурсів *hostingfacts.com/evaluating-online-resources/#Checklist* Десять запитань для виявлення фейкових новин *courts.ca.gov/documents/BTB24-PreCon2G-3.pdf* Оцінювання джерел – використання тесту C.R.A.P.! *libraries.mercer.edu/research-tools-help/citation-tools-help/evaluating-sources* Вірити чи ні: розміщення питань споживача, стор. 17 і 18 Оцінювання інтернет-ресурсів: оманливі сайти *eduscapes.com/tap/topic32.htm* Роздатковий матеріал «Оцінювання надійності джерел»
ПІДГОТОВКА	Роздрукуйте по одній копії матеріалів для кожного учня або групи учнів.
КОМПЕТЕНЦІЯ ЗГІДНО З ISTE DIGCITCOMMIT	ПОІНФОРМОВАНІСТЬ: Я отримую інформацію з точних, достовірних і об'єктивних цифрових інформаційних ресурсів і дописів у соціальних мережах.

ДОПОМІЖНІ МАТЕРІАЛИ

Відвідайте *facebook.com/fbgetdigital*, щоб отримати доступ до ресурсів для батьків і дітей, які можуть доповнити сьогоднішній урок з основ цифрової грамотності.

ОГЛЯД УРОКУ

Демократичне суспільство прагне підтримувати вільне поширення інформації та забезпечувати доступ до надійної й достовірної інформації. На цьому уроці учні дізнаються, як вибрати надійні джерела інформації. Працюючи в невеликих групах, учні обговорять, як визначити надійність інтернет-ресурсів, а потім спробують самостійно оцінити низку сайтів і новинних публікацій.

ПЛАН РОБОТИ

1. На початку уроку запитайте учнів, де вони дізнаються новини. У соціальних мережах? У новинних додатках? З телевізора? З газет? Розкажіть учням, що до появи кабельного телебачення й Інтернету у США було всього чотири телевізійні мережі, а щоб прокоментувати новини в газеті, читачам доводилося надсилати листи до редакції. Запитайте їх, як, на їхню думку, змінилося суспільство й уявлення людей про світ, після того як людям стало набагато простіше дізнаватися новини, ділитися ними й залишати коментарі.
2. Покажіть їм відео з телеканалу CNN про фейкові новини в соціальних мережах. Обговоріть із класом такі запитання:
   - Як ви вважаєте, чому деякі люди публікують фейкові новини?
   - Чим небезпечні фейкові новини, і що буде, якщо їх не викривати?
   - Чому, на ваш погляд, у наш час люди менше довіряють ЗМІ?
3. Аналіз поведінки людей у мережі у 2016 році показав, що користувачі соціальних мереж частіше діляться фейковими новинами, ніж достовірними. Обговоріть із класом такі запитання:
   - Чому важливо, щоб фейкові новини не публікували частіше, ніж достовірні?
   - Чому небезпечно ділитися фейковою інформацією?
   - Чи зобов'язані Facebook, Twitter та інші соціальні мережі попереджати користувачів про те, що деякі публікації неправдиві?
   - Чи зобов'язані люди перевіряти достовірність інформації, якою вони діляться в соціальних мережах?
4. Розділіть учнів на групи для роботи за принципом «подумай, обговори в парі, поділися» та попросіть їх у цих групах відповісти на наведені нижче запитання. Попросіть кількох охочих поділитися відповідями й пояснити хід своїх думок.
   - Я з більшою ймовірністю прочитаю публікацію, яка викликає в мене емоційну реакцію. Так чи ні?
   - Я з більшою ймовірністю поділюсь публікацією, яка викликає в мене емоційну реакцію. Так чи ні?
   - Перш ніж поділитися публікацією, я думаю, чи вона правдива. Так чи ні?
5. Обговоріть результати опитування, а потім задайте учням ще кілька питань:
   - Чому демократичне суспільство покладається на чесні й надійні засоби інформації?
   - Чому людям необхідна точна й достовірна інформація (фактична й без помилок)?
   - Чому нам важливо відокремлювати суб'єктивну (нічим не обґрунтовану або засновану на упередженнях) інформацію в новинах від об'єктивної?
6. Розкажіть учням, що існує багато засобів для оцінювання точності й неупередженості інформації. Наприклад, джерело інформації (автор, видавець), мета й аудиторія публікації, об'єктивність і точність викладу, а також джерела, якими користувався автор.
7. Розділіть учнів на групи по чотири або п'ять осіб. Попросіть їх ознайомитися з роздатковими матеріалами до вправи «Оцінювання надійності джерел». Потім виділіть кожній групі один із сайтів зі списку «Оцінювання інтернет-ресурсів: оманливі сайти».
8. Зачекайте, доки учні заповнять роздатковий матеріал «Оцінювання надійності джерел».
9. Потім поставте їм наведені нижче питання та організуйте обговорення ефективності засобів оцінювання. Наголосіть на тому, наскільки важливо перевіряти достовірність інформації, перш ніж ділитися нею.
   - Які висновки ви зробили про цей сайт з урахуванням всієї отриманої інформації? Чи правильно ви визначили надійність сайту?
   - Чи допомогли запропоновані засоби визначити надійність сайту або достовірність новин?
   - Які аспекти засобу ви вважаєте найефективнішими?
   - Які аспекти засобу ви вважаєте найменш ефективними?
   - Що б ви зробили, щоб удосконалити цей засіб?
   - Порівняйте свій перший спосіб оцінювання сайтів із засобом, який ви використовували вдруге. Чим вони відрізняються один від одного? Який із них, на вашу думку, ефективніший, і чому?

Додаткове завдання

1. Попросіть учнів самостійно підготувати коротку презентацію за результатами попереднього завдання:
   - Назва сайту й публікації
   - Порівняння першого способу із

другим засобом оцінювання

- Головні переваги й недоліки засобу
- Перелік дій, необхідних для оцінювання достовірності джерел (на майбутнє)
- Чому вам та іншим людям потрібні ефективні способи оцінювання достовірності інформації

2. Попросіть учнів скласти список своїх критеріїв оцінювання достовірності новин і сайтів. Попросіть їх протягом кількох днів активно використовувати цей список, щоб потім розповісти класу про результати.

СЛОВНИК

фейкові новини (іменник) – хибна інформація або пропаганда, яка публікується під виглядом справжніх новин

соціальні мережі (іменник) – сайти й інші інтернет-ресурси, на яких великі групи людей діляться інформацією та спілкуються один з одним

засіб оцінювання (іменник) – процес або процедура оцінювання надійності будь-чого

достовірність (іменник) – правдивість або надійність будь-чого

суб'єктивність (іменник) – упередженість (усвідомлена чи неусвідомлена) щодо певної особи або точки зору.

точність (іменник) – правдивість, достовірність або повнота інформації, відсутність помилок

надійність (іменник) – здатність викликати довіру (у контексті точності, чесності або ефективності)

Джерела:
dictionary.com
freethesaurus.com

tolerance.org/classroom-resources/tolerance-lessons/evaluating-online-sources

РОЗДАТКОВИЙ МАТЕРІАЛ

Оцінювання надійності джерел

Під час цієї вправи група учнів повинна визначити надійність інтернет-джерел і ефективність різних засобів оцінювання.

ВКАЗІВКИ

1. Викладач призначить вам сайт, який потрібно оцінити.
2. На основі своїх знань і досвіду спробуйте самостійно визначити, наскільки можна довіряти цьому сайту. Приготуйтеся пояснити свій хід думок. Заповніть анкету нижче під назвою «Як я оцінюю сайти».
3. Ознайомтесь із викладеними нижче ресурсами щодо засобів оцінювання достовірності. Виберіть один із них і повторно проаналізуйте сайт.
   - «Повний посібник з оцінювання інтернет-ресурсів» ***hostingfacts.com/evaluating-online-resources/#Checklist***
   - «Десять запитань для виявлення фейкових новин» ***courts.ca.gov/documents/BTB24-PreCon2G-3.pdf***
   - «Оцінювання джерел – використання тесту C.R.A.P.!» ***libraries.mercer.edu/research-tools-help/citation-tools-help/evaluating-sources***
   - «Вірити чи ні: розміщення питань споживача», стор. 17 і 18 ***newseumed.org/tools/lesson-plan/believe-it-or-not-putting-consumers-questions-work***
4. Заповніть форму «Використання засобу оцінювання надійності сайтів» на основі власного досвіду.

РОЗДАТКОВИЙ МАТЕРІАЛ

Як я оцінюю сайти

Назва сайту

Джерело (посилання або назва публікації):

Перерахуйте способи, за допомогою яких ви оцінили надійність цього сайту, і висновки, які ви зробили на основі кожного з них.

1.

2.

3.

4.

5.

Підбийте підсумки оцінювання надійності цього сайту:

РОЗДАТКОВИЙ МАТЕРІАЛ

Використання засобу оцінювання надійності сайтів

Назва сайту

Назва засобу:

Джерело (посилання або назва публікації):

Перерахуйте способи, за допомогою яких ви оцінили надійність цього сайту, і висновки, які ви зробили на основі кожного з них.

1.

2.

3.

4.

5.

Підбийте підсумки оцінювання надійності цього сайту:

РОЗДАТКОВИЙ МАТЕРІАЛ

РОЗДАТКОВИЙ МАТЕРІАЛ

facebook.com/fbgetdigital