Курс із мережевого етикету й безпеки

Джерело: g.co/DigitalCitizenshipCourse

ВСТУП. НАВІЩО НАВЧАТИСЯ МЕРЕЖЕВОГО ЕТИКЕТУ ТА ПРАВИЛ БЕЗПЕКИ?

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку

- Усвідомити, чому важливо розвивати в учнів навички безпеки в мережі.
- Дізнатися, як допомогти учням опанувати мережевий етикет.

Вступ
Вітаємо вас в онлайн-курсі з мережевого етикету й безпеки. Цей курс призначений для вчителів та учнів, які прагнуть навчитися безпечно та комфортно працювати в Інтернеті. Він містить текстові матеріали, відеоролики та завдання, які допоможуть вам інтегрувати вивчення мережевого етикету та правил безпеки в навчальну програму.

Як викладачі, ми добре розуміємо важливість уміння правильно себе поводити в аудиторії та навчальному закладі. Однак зараз люди дедалі більше часу проводять у мережі, тому важливо прищепити учням навички безпечного користування Інтернетом. Для цього молодь повинна вміти критично мислити, захищати конфіденційність своєї інформації та знати правила безпечного поводження в Інтернеті.

Уміння правильно користуватися сучасними технологіями допомагає в навчанні як учневі, так і навчальному закладу в цілому. Ми переконані, що ця програма стане важливим кроком у вихованні високої культури онлайн-етикету в студентів і допоможе їм комфортно й ефективно користуватись Інтернетом.

Курс

Орієнтовна тривалість уроку: 5 хвилин

Навчання мережевого етикету та правил безпеки
Мережева безпека й конфіденційність даних – це дві частини мережевого етикету, які можуть бути складними для розуміння. Тому важливо почати з основ. Перш за все слід пояснити учням, що особисту інформацію треба цінувати та захищати так само, як особисті речі.

Тема мережевої безпеки й конфіденційності є непростою для вивчення, зокрема, тому, що в ній немає "правильних" і "неправильних" відповідей. До безпеки в Інтернеті не існує універсального підходу. Тому важливо озброїти учнів інформацією, адекватною для їхнього віку, і навчити їх мислити самостійно, щоб вони могли доходити до власних висновків і встановлювати комфортні для себе межі.

Вчителі не завжди здатні захистити учнів від усіх небезпек, але вони спроможні навчити їх самостійно виходити зі складних ситуацій у мережі. Ви можете заохочувати учнів до відкритого та чесного діалогу, а також навчити їх, як отримувати допомогу й підтримку в разі потреби.

Рекомендуємо використовувати в навчанні конкретні приклади, завдання та рольові ігри. Ваше завдання – донести до учнів важливість дотримання мережевого етикету, захисту своєї особистої інформації й поваги до конфіденційності даних інших людей.

Курс із мережевого етикету й безпеки для викладачів
Масовий відкритий онлайн-тренінг "Курс із мережевого етикету й безпеки для викладачів" складається з п’яти аудіовізуальних модулів із короткими тестами наприкінці кожного модуля.

Пройшовши курс, ви зможете завантажити пакет навчальних ресурсів із мережевого етикету й безпеки, який допоможе зацікавити учнів і наочно пояснити матеріал. Якщо ви успішно складете всі п’ять тестів, ви отримаєте значок просвітянина з питань мережевого етикету й безпеки. Почніть навчання просто зараз!

РОЗДІЛ 1. НАВЧАННЯ ПРАВИЛ БЕЗПЕКИ Й КОНФІДЕНЦІЙНОСТІ В ІНТЕРНЕТІ

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку

- Ознайомитися з критеріями надійності паролів і порадами щодо створення надійних і легких для запам’ятовування паролів.
- Дізнатися, що таке двоетапна перевірка та як вона захищає облікові записи в мережі.
- Опанувати концепції, інструменти й налаштування, які допоможуть учням захистити свої облікові записи в мережі від хакерів та інших загроз.

Вступ
Усі ми змалечку навчаємося правил безпечної поведінки вдома, у навчальному закладі, а найголовніше – на вулиці. Ми знаємо, як важливо бути пильними та стежити за своїми речами. Ті самі принципи діють і в мережі, але замість особистих речей ми повинні пильнувати нашу особисту інформацію та доступ до своїх облікових записів у мережі.

Речі, цінні для ваших учнів (наприклад, доступ до облікових записів електронної пошти чи соціальних мереж), можуть зацікавити і зловмисників, тому треба захищати їх надійними паролями.

Як же навчити учнів захищати свої облікові записи? Ознайомтеся з подальшими розділами, а потім перевірте свої знання, пройшовши тест. Бали за його складання враховуються в загальній оцінці.

Урок

Орієнтовна тривалість уроку: 8 хвилин

Поміркуйте…
Подумайте, як сучасні технології впливають на повсякденне життя та спілкування людей. Як часто вони вимагають використання облікових записів із паролем? Нижче наведено кілька запитань, які скерують вас у правильному напрямку.

Запитання

- Скільки разів на день ваші учні виходять в Інтернет?
- Як часто ваші учні спілкуються з друзями за допомогою електронної пошти, чатів і соціальних мереж?
- Скільки облікових записів має середньостатистичний користувач Інтернету? Чи знають ваші учні, як захистити свої облікові записи?
- Як ваші учні почуватимуться, якщо раптом втратять доступ до якогось зі своїх облікових записів?

Навчання правил безпеки й конфіденційності в Інтернеті
Отже, ви обдумали роль сучасних технологій у нашому житті й оцінили, скільки інформації про себе ми власноруч розміщуємо в мережі. Тепер ви готові дізнатися поради, які допоможуть вашим учням захистити особисту інформацію.

[ВБУДОВАНЕ ВІДЕО "Навчання правил безпеки й конфіденційності в Інтернеті"]

Тест

Запитання № 1. Яким правилом слід керуватися, вибираючи надійний пароль?

- Використовувати дуже довгу складну послідовність цифр
- **Використовувати комбінацію з 8–9 букв, спеціальних символів і цифр**
- Використовувати довільні букви та цифри
- Використовувати складні слова зі словника

Запитання № 2. Який із наведених паролів найнадійніший?

- Football123
- **ImA@SF#11**
- uhuo$
- 25041990

Запитання № 3. Надійні паролі важко запам’ятовуються. Що ви порадите своїм учням, щоб зробити їх легшими для запам’ятовування? (Виберіть усі правильні варіанти.)

- **Використовувати менеджер паролів**
- Записати всі паролі на папірці та сховати в безпечному місці

- Переслати собі електронного листа з іменем користувача та паролем
- **Створити парольну фразу**

Запитання № 4. Що ви порадите учневі, який вибирає новий пароль?
- Просто додати до старого пароля цифру чи спеціальний символ
- Вибрати щось пам’ятне – свою дату народження чи кличку домашнього улюбленця
- Вибрати наступне число після свого старого пароля
- **Придумати зовсім нову парольну фразу, яку буде легко запам’ятати**

Запитання № 5. Що таке двоетапна перевірка? (Виберіть усі правильні варіанти.)
- **Додатковий рівень захисту облікового запису**
- **Метод захисту, який передбачає двоетапну процедуру входу в обліковий запис**
- Метод шифрування
- Служба безпечного збереження паролів і доступу до них

РОЗДІЛ 2. БЕЗПЕКА КОРИСТУВАННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку
- Дізнатися, як блокування мобільного пристрою допомагає захистити особисту інформацію.
- Дізнатися, як розпізнавати потенційно шкідливі завантажувані файли.
- Дізнатися, як оновлення системи захищають мобільні пристрої.
- Навчитися пояснювати учням різницю між приватними та загальнодоступними мережами Wi-Fi, а також правила безпечного користування останніми.

Вступ
Мобільні пристрої викликали революцію в користуванні інтернет-службами. Зараз батьки дарують малим дітям смартфони, а студенти ведуть конспекти на планшетах замість зошитів.

Мобільні пристрої – дуже особистий і багатофункціональний аксесуар. Ми використовуємо їх і для спілкування в соціальних мережах, і для інтернет-банкінгу, і для багатьох інших цілей, які вимагають уважного ставлення до безпеки даних.

Як же навчити учнів безпечно користуватися мобільними пристроями? Ознайомтеся з подальшими розділами, а потім перевірте свої знання, пройшовши тест. Бали за його складання враховуються в загальній оцінці.

Урок

Орієнтовна тривалість уроку: 8 хвилин

Поміркуйте…
Подумайте, як смартфони й інші мобільні пристрої впливають на життя ваших учнів. Як молодь використовує ці пристрої? Які небезпеки через це на неї чатують? Нижче наведено кілька запитань, які допоможуть стимулювати обговорення в класі.

Запитання

- Скільки разів на день середньостатистичний учень перевіряє свій смартфон?
- Для чого учні найчастіше застосовують смартфони (наприклад, для користування соціальними мережами, спілкування з рідними та друзями, фотографування, покупок в інтернет-магазинах тощо), і яке значення ці заняття мають у повсякденному житті молоді?
- Як він почуватиметься, якщо хтось інший переглядатиме вміст його телефона? Яку інформацію може отримати стороння особа, якщо в її руки потрапить телефон когось зі учнів?
- Як ви вважаєте, чи серйозно ваші учні ставляться до безпеки користування мобільними пристроями?

Безпека користування мобільними пристроями
Отже, ви обміркували, наскільки важливими та особистими є для нас наші мобільні пристрої. Тепер ви готові ознайомитися з порадами щодо безпечного користування ними.

[ВБУДОВАНЕ ВІДЕО "Безпека користування мобільними пристроями"]

Тест

Запитання № 1. Що потрібно робити учням, щоб захистити свої мобільні пристрої? (Виберіть усі правильні варіанти.)

- **Блокувати екран за допомогою надійного PIN-коду чи ключа**
- **Установлювати оновлення системи відразу після їх виходу**
- Виконувати інструкції на сайтах, які повідомляють, що телефон інфіковано
- Ніколи не підключатися до жодних мереж Wi-Fi, крім домашньої

Запитання № 2. Як ви порадите учням убезпечити себе від небажаних або потенційно небезпечних завантажуваних файлів? (Виберіть усі правильні варіанти.)

- **Завантажувати файли тільки з авторитетних джерел (наприклад, офіційних магазинів додатків)**
- Завжди перевіряти розмір завантажуваного файлу
- **Читати відгуки та коментарі інших користувачів, перш ніж завантажувати додатки**
- **Не натискати на оголошення й не виконувати інструкції на сайтах, які повідомляють, що телефон інфіковано**

Запитання № 3. Що ви порадите учням не робити в загальнодоступних мережах Wi-Fi?

- Вводити імена користувачів і паролі від облікових записів (наприклад, електронної пошти чи соціальних мереж)
- Користуватись інтернет-банкінгом
- Вводити реквізити кредитних карток
- **Усе вищенаведене**

Запитання № 4. Чи безпечно вводити й надсилати особисту інформацію, коли пристрій підключено до невідомої чи недовіреної мережі?

- Так, безпечно
- **Ні, зловмисники можуть перехопити особисту інформацію**

Запитання № 5. У яких випадках необхідно виходити з облікових записів?

- **Після користування загальнодоступним бібліотечним комп’ютером**
- **Після користування позиченим пристроєм (наприклад, планшетом друга)**
- Після користування загальнодоступною мережею Wi-Fi
- В усіх вищенаведених випадках

РОЗДІЛ 3. ПРАВИЛА БЕЗПЕЧНОГО ПОШУКУ ІНФОРМАЦІЇ

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку

- Навчити учнів розрізняти авторитетні й сумнівні джерела інформації.
- Отримати практичні поради, які допоможуть учням критично оцінювати онлайн-джерела інформації.
- Навчитися пояснювати учням, що не всім матеріалам в Інтернеті можна довіряти.

Вступ

Інтернет уже став незамінним освітнім ресурсом. Уявіть собі, що ви запропонувати учням написати реферат, не користуючись Інтернетом. Напевно, вони б і не знали, з якого боку підступитися.

Пошук інформації не обмежується навчальними цілями. Ми шукаємо в Інтернеті інформацію про здоров'я, про світові новини, про те, як зіграла улюблена команда... У всіх випадках важливо застосовувати критичне мислення, щоб вибирати інформацію, яка є корисною та надійною..

Отже, поговорімо про те, як навчити учнів розрізняти авторитетні й сумнівні джерела інформації. Ознайомтеся з подальшими розділами, а потім перевірте свої знання, пройшовши тест. Бали за його складання враховуються в загальній оцінці.

Урок

Орієнтовна тривалість уроку: 8 хвилин

Поміркуйте…
Подумайте, наскільки легко шукати інформацію в мережі та чому важливо завжди порівнювати відомості з кількох джерел. Нижче наведено кілька запитань, які скерують вас у правильному напрямку.

Запитання

- Наскільки важливим є вміння знаходити достовірну інформацію для вас як для викладача? А наскільки важливим є це вміння для ваших учнів, коли вони виконують домашні завдання?
- Звідки учні зазвичай дізнаються про світові новини?
- Чому учні довіряють статтям на інтернет-сайтах?
- Чи вміють ваші учні шукати в мережі надійну інформацію?

Правила безпечного пошуку інформації
Отже, ви поміркували про те, скільки інформації доступно користувачам Інтернету й чому важливо навчити учнів критично оцінювати прочитані матеріали. Розглянемо тепер деякі рекомендації, які допоможуть вашим учням оцінювати авторитетність інтернет-джерел.

[ВБУДОВАНЕ ВІДЕО "Правила безпечного пошуку інформації"]

Тест

Запитання № 1. Які ознаки вказують, що стаття на певному веб-сайті є надійним джерелом інформації?

- Наявність імені та прізвища автора
- Наявність дати публікації
- Наявність відомостей про автора (освіта, кваліфікація тощо)
- **Усе вищенаведене**

Запитання № 2. Важливо навчити учнів порівнювати відомості принаймні з трьох онлайн-джерел під час пошуку інформації на такі теми:

- Сьогоднішні новини й останні події у світі
- Історичні події
- Здоров’я
- **Усі можливі теми**

Запитання № 3. Виберіть твердження, що найточніше пояснює, як виявляти сумнівні джерела інформації.

- Сумнівну інформацію зазвичай розміщено на сайтах, які виглядають підозріло
- Якщо в матеріалі вказано ім’я та прізвище автора, то інформація має бути надійною
- **Слід порівняти інформацію принаймні з трьох джерел за такими ключовими запитаннями: "Хто? Що? Де? Коли?"**
- Слід завжди звертати увагу на дату публікації та довіряти лише найновішій інформації

Запитання № 4. Якщо ваш учень захоче процитувати у своїй роботі анонімну статтю з Інтернету, що ви йому порадите?

- **Зіставити інформацію в анонімній статті та роботах інших кваліфікованих авторів і, якщо вона виявиться правдивою, використати відповідні цитати з авторських робіт**
- Процитувати анонімну статтю, не звіряючи її з іншими джерелами, але при цьому вказати в роботі, що автор "анонімний" або "невідомий"
- Негайно відкинути анонімну статтю як сумнівне джерело інформації

Запитання № 5. Ви помітили, що ваші учні постійно покладаються на те саме джерело інформації. Як можна заохотити їх мислити критично?

- Заборонити використовувати це джерело інформації
- **Запропонувати учням завжди порівнювати інформацію принаймні з трьох джерел (включно з тими, що представляють протилежну точку зору)**
- Перевірити, чи авторитетне це джерело інформації

РОЗДІЛ 4. САМОЗАХИСТ ВІД ФІШИНГУ ТА ШАХРАЙСТВА

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку

- Навчитися розпізнавати потенційно шахрайські сайти та електронні листи й уникати їх.
- Розібратися, що таке шифрування та як перевірити, чи зашифровано веб-сторінку.
- Дізнатися, як діяти, зіштовхнувшись із інтернет-шахрайством.

Вступ
У більшості людей слово "інтернет-шахрай" відразу асоціюється з хакером, озброєним надзвичайно складними технологіями. Однак насправді більшість інтернет-шахраїв застосовують досить прості методи. Щоб ошукати пересічного користувача Інтернету, достатньо вміло зіграти на його емоціях. Якщо зловмисник переконає людину, що їй треба терміного діяти, йому буде значно легше видурити в неї гроші чи особисту інформацію.

Щодня ваші учні відвідують найрізноманітніші сайти й отримують безліч електронних листів і повідомлень. Тому дуже важливо, щоб вони вміли виявляти потенційних інтернет-шахраїв, які полюють на особисту інформацію.

Важливо пояснити учням, що постійна пильність не означає, нібито їм потрібно всього боятися. Отже, поговорімо про те, як допомогти вашим учням не стати жертвами інтернет-шахраїв. Ознайомтеся з подальшими розділами, а потім перевірте свої знання, пройшовши тест. Бали за його складання враховуються в загальній оцінці.

Урок

Орієнтовна тривалість уроку: 8 хвилин

Поміркуйте…
Подумайте, з якими видами шахрайства учні можуть зіткнутися в Інтернеті та на яку інформацію зазвичай полюють зловмисники. Нижче наведено кілька запитань, які скерують вас у правильному напрямку.

Запитання

- У мережі часто можна побачити оголошення про знижки, подарунки тощо. На яку реакцію користувачів вони розраховані? На який ризик можна наразитися, якщо відповісти на шахрайське оголошення?
- Чи відповідали колись ваші учні на електронні листи від незнайомих відправників? Чи містили такі листи якісь прохання чи вказівки? Яку інформацію можна мимоволі розкрити стороннім особам, відповідаючи на такі листи?
- Чи знають ваші учні, як перевірити, чи безпечно вказувати реквізити кредитної картки під час покупки в інтернет-магазині?
- Що може зробити кіберзлочинець, якщо в руки йому потрапить чиєсь ім’я користувача та пароль?

Самозахист від фішингу та шахрайства
Отже, ви поміркували про види шахрайства, з якими можна зіткнутись у мережі. А тепер поговорімо про те, які тактики використовують кіберзлочинці для ошукування користувачів і як допомогти вашим учням захистити себе.

[ВБУДОВАНЕ ВІДЕО "Самозахист від фішингу та шахрайства"]

Тест

Запитання № 1. Що таке соціальна інженерія?

- **Методи, якими зловмисник змушує людину повідомити йому особисту інформацію (наприклад, пароль або номер кредитної картки)**
- Правильне використання соціальних мереж

Запитання № 2. Які тактики шахраї найчастіше використовують для крадіжки особистої інформації?

- Створити в людини враження, що їй потрібно негайно діяти, інакше вона впустить вигідну пропозицію або станеться щось погане
- Створити сайт, дуже схожий на той, яким людина зазвичай користується
- Указати в електронному листі адресу відправника, схожу на адресу когось із контактів жертви
- **Усе вищенаведене**

Запитання № 3. На що вказує літера "s" у префіксі "https"?

- **На те, що з'єднання безпечне і зашифроване**
- На те, що з'єднання не є безпечним

Запитання № 4. Чи може сайт або оголошення визначити, що комп'ютер інфіковано?

- Так
- **Ні**

Запитання № 5. Що ви порадите учневі, який отримав підозрілого електронного листа від постачальника послуг електронної пошти чи якоїсь іншої компанії?

- Написати на листа відповідь із проханням надати докладніші відомості
- **Відкрити нове вікно веб-переглядача, перейти на офіційний сайт відповідної компанії чи електронної поштової служби та знайти її контактну електронну адресу**
- Переслати листа людині, якій ви довіряєте, і попросити поради

Запитання № 6. Що потрібно перевірити, перш ніж вводити на веб-сторінці особисту інформацію?

- Чи стоїть на початку URL-адреси сторінки префікс "https"
- Чи відображається перед URL-адресою сторінки значок зеленого замка
- Чи правильна URL-адреса сторінки
- **Усе вищенаведене**

РОЗДІЛ 5. ТУРБОТА ПРО СВОЮ РЕПУТАЦІЮ В МЕРЕЖІ

Вступ

Орієнтовна тривалість уроку: 5 хвилин

Цілі уроку

- Допомогти учням усвідомити значення конфіденційності та зрозуміти, яку інформацію про себе вони публікують у мережі.
- Навчити учнів розпізнавати неприйнятну поведінку інших людей і скаржитися на неї.
- Навчити учнів, як поводити себе в мережі, навіть у складних ситуаціях.

Вступ
Сучасні технології та соціальні мережі радикально змінили те, як ми спілкуємось один з одним і взаємодіємо зі світом. Зараз існує безліч соціальних онлайн-платформ, тож важливо навчити учнів свідомо ставитися до інформації, яку вони поширюють про себе, та контролювати, що і кому вони повідомляють.

Мережевий етикет – делікатна тема, яку не завжди легко обговорювати в аудиторії. Тому дуже важливо налагодити з групою відкритий діалог, щоб учні почувалися комфортно і безпечно, розмовляючи з дорослими про свій досвід спілкування в Інтернеті.

А тепер поговорімо про те, як навчити учнів відповідально ставитися до поширення інформації в Інтернеті та бути гідними членами онлайн-спільнот, у яких вони беруть участь. Ознайомтеся з подальшими розділами, а потім перевірте свої знання, пройшовши тест. Бали за його складання враховуються в загальній оцінці.

Урок

Орієнтовна тривалість уроку: 8 хвилин

Поміркуйте…
Нижче наведено кілька запитань, які допоможуть учням поміркувати про свою взаємодію з іншими людьми в Інтернеті.

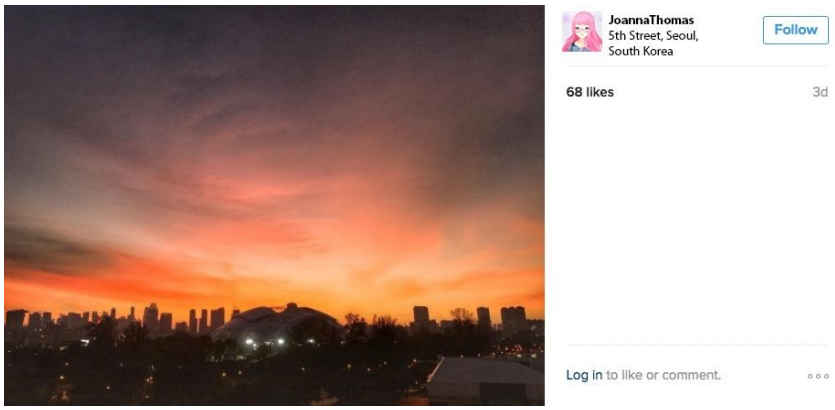
Запитання

- Чи публікують ваші учні в мережі якісь дописи, фото чи інші матеріали? Що ваші учні публікують найчастіше? Що інші можуть дізнатися про людину за її публікаціями?
- Якими соціальними мережами (сайтами, додатками тощо) ваші учні користуються найчастіше? Чи траплялися їм дописи або коментарі, які могли когось образити?
- Що робили ваші учні, коли бачили такі образливі коментарі? Чи вчинили б вони зараз інакше?

Турбота про свою репутацію в мережі

[ВБУДОВАНЕ ВІДЕО "Турбота про свою репутацію в мережі"]

Тест



Запитання № 1. Імовірно, вам уже траплялися публікації в соціальних мережах, подібні до наведеної вище. Що можна з неї дізнатися? (Виберіть усі правильні варіанти.)

A. Ім’я та прізвище автора
B. Вік автора
C. Де автор був три дні тому
D. Чи любить автор морозиво

Запитання № 2. Переглянувши всі фотографії за два роки в профілі певної людини в соціальній мережі, зловмисник помітив, що більшість знімків, зроблених на кухні, позначено тією самою адресою, а от в останні кілька днів ця людина публікує фото туристичних пам’яток з іншої країни. Які висновки з цього може зробити зловмисник? (Виберіть усі правильні варіанти.)

- Скільки в цієї людини братів і сестер
- **Де живе ця людина**
- **Що ця людина зараз у від’їзді, а її квартира порожня**
- Де народилася ця людина

Запитання № 3. Один із ваших учнів дізнався, що його товариші цькують новачка, який перевівся в клас на тому тижні. Як слід гідно вчинити в такій ситуації? (Виберіть усі правильні варіанти.)

A. Згуртувати інших учнів і разом виступити проти цькування, хоча вони самі від нього й не потерпають
B. Присоромити товаришів, сказавши, що своїми діями вони не тільки ображають новачка, а й принижують себе
C. За потреби повідомити вчителів і батьків новачка, щоб вони контролювали ситуацію та підтримували його
D. Зачекати пару тижнів і подивитися, чи не виправиться ситуація

Запитання № 4. Яких практичних заходів можна вжити, щоб допомогти учням захистити конфіденційність своїх даних під час спілкування у віртуальних спільнотах? (Виберіть усі правильні варіанти.)

A. Порадити їм уникати віртуальних спільнот
B. Порадити їм навчитися керувати налаштуваннями конфіденційності й відкривати доступ лише до інформації, якою вони готові ділитися
C. Порадити їм обмежувати доступ до своїх публікацій, щоб їх могли переглядати лише вибрані люди
D. Провести обговорення в класі, щоб допомогти учням визначити комфортні для себе межі: яка інформація занадто приватна й особиста, а якою можна ділитися (і з ким саме)