Google | iKeepSafe™

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Обачність
Пильність
Захист
Ввічливість
Сміливість

Посібник із цифрового громадянства й безпеки

Комісією з інформатизації закладів освіти Науково-методичної ради з питань освіти Міністерства освіти і науки України розглянуто навчальний посібник з цифрового громадянства й безпеки «Обачність. Пильність. Захист. Ввічливість. Сміливість» та надано висновок «Схвалено для використання в загальноосвітніх навчальних закладах» (протокол № 5 від 09.08.2018 року)

Рецензенти:

ЛИТВИНОВА С.Г. - доктор педагогічних наук, с.н.с.
БУКАЧ А.В. - Google for Education Certified Trainer

Представляємо вашій увазі навчальний посібник із цифрового громадянства й безпеки, розроблений Google у співробітництві з Альянсом із захисту безпеки користувачів в Інтернеті (Internet Keep Safe Coalition, iKeepSafe.org).

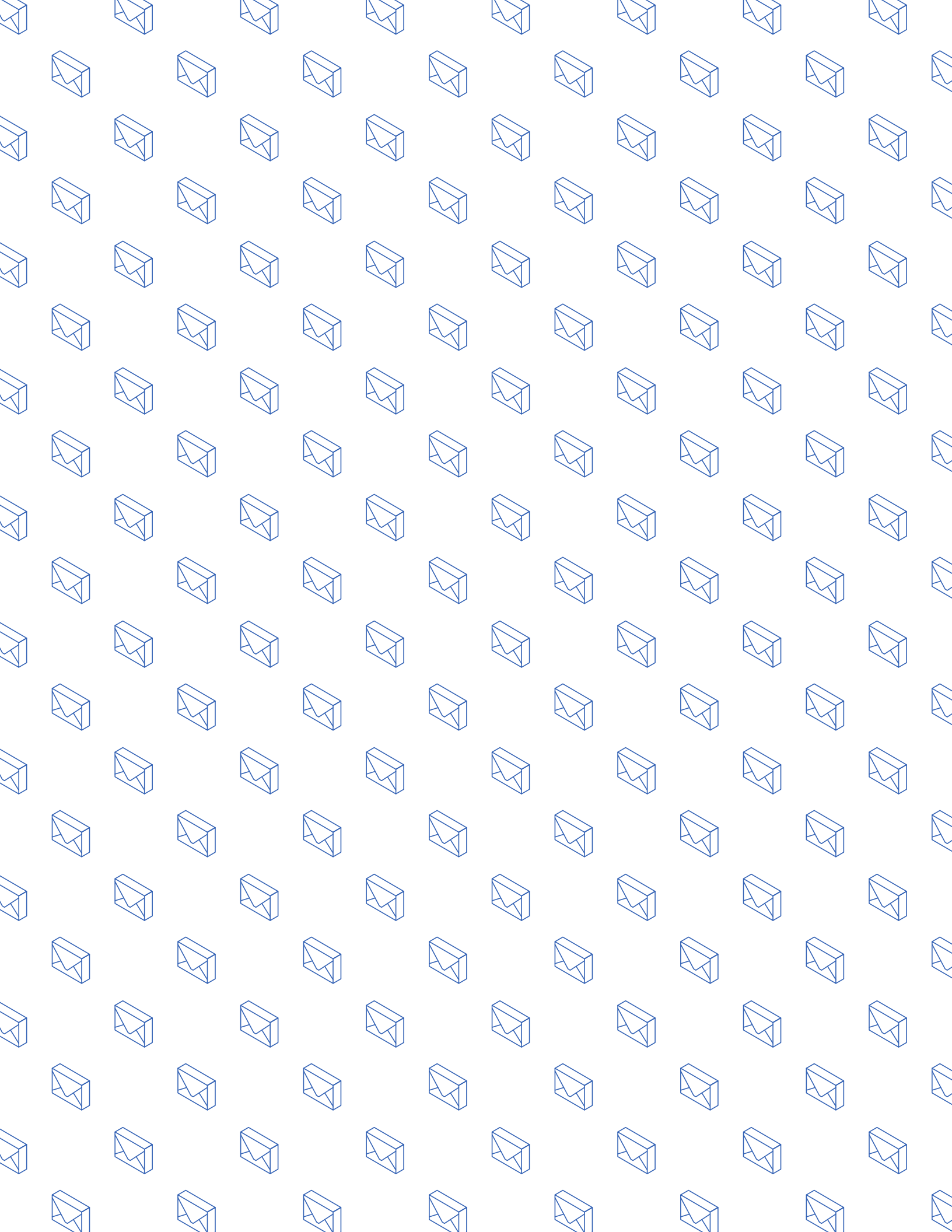
Цей посібник містить матеріали та методики, необхідні для викладання основ безпеки в Інтернеті. Плани уроків призначені для учнів початкової школи та зосереджені на ключових принципах мережевого етикету й безпеки. Вони допоможуть учителям виховати в дітях обережність і відповідальність під час роботи в Інтернеті.

Посібник охоплює п'ять засадничих тем:

- **Діліться з обачністю (обачність в Інтернеті)**
- **Не піддавайтеся обману (пильність в Інтернеті)**
- **Бережіть свої таємниці (захист в Інтернеті)**
- **Круто бути доброзичливим! (доброзичливість в Інтернеті)**
- **Сумніваєтеся? Спитайте! (сміливість в Інтернеті)**

Міжнародна спілка з використання технічних засобів у сфері освіти (International Society for Technology in Education, ISTE) визнала публікацію "Посібник із мережевого етикету й безпеки" ресурсом, що допомагає підготувати учнів на рівні Стандартів ISTE 2016, і відзначила її грифом для матеріалів підготовчого рівня (Seal of Alignment for Readiness).

Зміст



Урок 1. Обачність в Інтернеті

Діліться з обачністю

Захист своєї репутації в мережі

Огляд уроку

Заняття 1. **Чи вмієте ви зберігати таємницю?**
Заняття 2. **Гра: складання профілю**
Заняття 3. **Як інші нас бачать?**
Заняття 4. **Конфіденційність на практиці**

Теми

Учителі й батьки знають, як необачне поводження дитини в мережі може вплинути на її репутацію в майбутньому. Однак десятирічним дітям важко пояснити, що нібито цілком невинний пост колись можуть побачити та неправильно зрозуміти люди, для яких він не призначався.

Запропоновані заняття допоможуть на практичних прикладах навчити школярів захищати свою особисту інформацію й конфіденційність даних, щоб підтримувати позитивну репутацію в мережі.

Цілі

- ✓ **Навчити** дітей створювати та підтримувати позитивну репутацію в мережі.
- ✓ **Пояснити**, чому потрібно поважати конфіденційність і межі приватного життя інших.
- ✓ **Розповісти** про можливі наслідки необачних дій у мережі.
- ✓ **Переконати**, що в делікатних ситуаціях слід звертатися по допомогу до дорослих.

Застосовні стандарти

Стандарти ISTE для вчителів: 1a, 1b, 1d, 2a, 2c, 3b, 3d, 4a, 4b, 4c, 4d, 5b. **Стандарти ISTE для учнів (2016):** 1d, 2a, 2b, 2d. **Навчальні стандарти AASL:** 1.1.1, 1.1.2, 1.1.8, 1.3.3, 1.3.5, 2.1.3, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4.

Діліться з обачністю
Словник

Цифровий слід
Цифровий слід – це всі дії людини в Інтернеті, з яких складається її електронний портрет. Коли вона публікує фотографії, аудіозаписи, відео, текстові повідомлення, дописи в блозі чи пише на сторінках друзів, то залишає в мережі так званий слід.

Особиста інформація
Інформація про конкретну особу. Вона може бути загальнодоступною, призначеною лише для деяких людей або цілковито приватною, залежно від того, наскільки конфіденційною вона є.

Налаштування
Розділ на сайті, у додатку тощо, де можна вказати, яку інформацію про себе користувач хоче показувати іншим і як служба оброблятиме дані його облікового запису.

Межі
Кордони або точки переходу між двома різними зонами; неписані правила поведінки. З одного боку меж певні дії можуть бути прийнятні, а з іншого – неприпустимі.

Чи вмієте ви зберігати таємницю?

Учні розбиваються на пари та порівнюють вигадані таємниці, щоб отримати уявлення про рівні конфіденційності.

Цілі

- ✓ **Зрозуміти**, яку особисту інформацію слід зберігати в таємниці.
- ✓ **Запам'ятати**, що кожен має право на збереження своїх таємниць.
- ✓ **З'ясувати**, які ще види особистої інформації можна знайти в мережі.

Обговорення

Чому конфіденційність має таке велике значення?

Цифровий слід – це всі дії людини в Інтернеті, з яких складається її електронний портрет. Коли вона публікує фотографії, аудіозаписи, відео, текстові повідомлення чи пише на сторінках друзів, то залишає в мережі так званий слід. Якщо правильно представити себе в Інтернеті, з віком від цього можна отримати різноманітні переваги. В Інтернеті зручно спілкуватися з рідними, друзями, однодумцями, надсилати повідомлення та зображення, брати участь в обговореннях у соціальних мережах – і часом ми навіть не замислюємося, перш ніж опублікувати щось онлайн.

Але принада й небезпека всесвітньої мережі в тому, що з неї ніщо не зникає безслідно. Сьогодні ви можете поділитися смішним дописом або картинкою, які видаються вам цілковито невинними, а завтра їх можуть побачити не ті люди та зробити неправильні висновки. Тож пам'ятайте:

- ваш цифровий слід (як і будь-який інший вміст у мережі) може побачити хто завгодно;
- вміст, опублікований у мережі, важко або навіть неможливо видалити з неї назавжди.

Ось чому так важливо піклуватися про свою конфіденційність. Щоб захистити її, публікуйте лише вміст, який ви вважаєте цілковито безпечним для себе та своєї репутації (інакше кажучи, ретельно стежте за своїм іміджем в Інтернеті). Як то кажуть, мовчання – золото, й іноді вчасно промовчати означає захистити власну конфіденційність і приватне життя інших людей.

Продовження на наступній сторінці →

Діліться з обачністю. Заняття 1 (продовження)

Практичне завдання

1. Вигадайте таємницю

Виберіть якусь таємницю (не ваш справжній секрет, а щось вигадане).

2. Розкажіть таємницю своєму партнеру

Розбийтеся по парах, обміняйтеся таємницями й обговоріть наведені далі два питання.

- Чи поділилися б ви з кимось цією таємницею?
- Якщо так, то з ким і чому?

3. Розкажіть класу

Розкажіть класу, яка ваша вигадана таємниця, з ким ви нею поділилися б і чому.

Висновки

Таємниці – один із багатьох різновидів особистої інформації, якою варто ділитися лише з найближчими рідними та друзями або взагалі ні з ким. Яку ще інформацію слід захищати від чужих?

- Домашня адреса й номер телефону
- Пароль від електронної пошти й інших облікових записів у мережі
- Імена користувача
- Домашні завдання й інші роботи
- Фотографії, відео, музика й інший вміст

Гра: складання профілю

Учні аналізують особисту інформацію про вигаданих осіб і намагаються скласти про них уявлення.

Цілі

- ✓ **Визначити**, якими способами можна знайти в мережі інформацію про людей.
- ✓ **З'ясувати**, що можна дізнатися про людину на основі її особистих даних.
- ✓ **Усвідомити**, що здогади на підставі таких даних не завжди правдиві.

Обговорення

Що ми знаємо про знайомих у мережі (або думаємо, що знаємо)

В Інтернеті можна знайти багато особистих даних, і часом на їх підставі ми робимо не зовсім правдиві припущення. Тож поговорімо про наведені далі питання.

- Що можна дізнатися про людину на основі її особистої інформації?
- Які припущення можна зробити на підставі особистої інформації, навіть якщо ми в них невпевнені?
- Чи завжди відомо, як отримано цю особисту інформацію?

Практичне завдання

Необхідні матеріали:

– Роздруківки з різноманітними вигаданими особистими даними. Ви можете скористатися матеріалами на наступній сторінці або розробити фіктивні профілі самостійно. Вони мають включати:

- дописи й коментарі із соціальних мереж (якщо дозволяє вік персонажа);
- надрукована історія з веб-переглядачів;
- перелік місць, де персонаж "відмічався" (кафе, кав'ярні, точки доступу Wi-Fi).
- зошити чи пристрої для виконання короткого письмового завдання.

1. Вивчіть людину

Кожен із вас отримає профіль вигаданого персонажа з його цифровим слідом. Ознайомтеся з ним.

2. Опишіть людину

Потім клас розіб'ється на групи, і кожна група повинна буде коротко описати персонажа: його характер, захоплення тощо.

3. З'ясуйте правду

Хто ж наші персонажі насправді?

- **Женя** – випускниця. Наступного року вона планує вступити в університет на економічний факультет, а в майбутньому мріє започаткувати власний модний бренд. Її головні інтереси – це родина, волонтерство, поп-культура та мода.
- **Дмитро** – центральний гравець у шкільній баскетбольній команді. Йому 16 років, і він живе в Івано-Франківську. У нього є восьмирічна сестричка. Його головні інтереси – це баскетбол, мистецтво, гра на гітарі та спілкування з друзями.
- **Лілі** 17 років. Вона має двох котів і нещодавно приєдналася до шкільної футбольної команди. У Лілі чудові інженерні здібності, і у вихідні вона любить збирати роботів. Її головні інтереси – це техніка й футбол, а ще тварини та захист їхніх прав.

Про що ми здогадалися правильно, а про що ні?

Продовження на наступній сторінці →

Висновки

Часом наші припущення про інших людей бувають помилковими. Не знаючи цього, часто ми судимо людину за власними неправильними висновками. Тож не варто занадто довіряти своїм припущенням – завжди перевіряйте, чи відповідають вони дійсності! Завжди намагайтеся переконатися, що ви дійсно знайте про людину те, що ви думаєте, що ви про неї знаєте!

Прочитайте опис дій кожного персонажа в мережі. Після кожного прикладу напишіть, які висновки з нього можна зробити про цю людину: що вона любить або не любить, що її цікавить?

Женя

- Наклацала трохи фото зі шкільної дискотеки. Народ, ви всі красунчики!
- 5 секретних засобів, які назавжди позбавлять тебе від прищів
- Мій менший брат Сашко ТААК мене дратує. Може він прибулець?
- Київська лазертаг-арена
- Міжнародна конференція молодих дизайнерів
- НАРЕШТІ ПОДИВИЛАСЯ НОВИЙ ФІЛЬМ "ВІЙНИ ШПИГУНІВ". Це просто щось неймовірне!

Дмитро

- Ми виграли! Ще один матч – і ми в національному турнірі. Треба ще трохи попрацювати над блокшотами.
- Ненавиджу шкільні дискотеки. #бойкот
- Київський університет імені Бориса Грінченка
- 10 ознак того, що батьки намагаються зруйнувати тобі життя
- Цієї суботи їдемо з татом рибалити на ставок! Буде круто
- Фудкорт La La Luna, "Сіті-центр"

Ліля

- Царство бургерів
- Пропустила переможний гол, хай би йому грець. Добре хоч, що ми витягнули нічию.
- 25 неймовірно милих фото цуценят
- Новорічна дискотека загальноосвітньої школи № 22
- Зацініть сайт моєї подруги! Це я його розробила.
- Новий рекорд!!! Оце я молодець. Обожнюю Gem Jam!!!

Як інші нас бачать?

Учні обговорюють, яке уявлення про персонажів із попереднього заняття склалося б у різних людей: батьків, роботодавців, друзів, поліцейських.

Цілі

- ✓ **Навчитися** дивитися на свої слова та дії в Інтернеті з точки зору інших людей.
- ✓ **Обміркувати** можливі наслідки оприлюднення особистої інформації та її вплив на свою репутацію (часто незворотний).

Обговорення

Нова точка зору

Цифровий слід може розказати про людину набагато більше, ніж вона сама того хотіла і наслідки цього часом бувають дуже серйозними.

Спробуймо поглянути на профілі наших персонажів із їхньої точки зору.

- Як ви думаєте, чи хотіли б вони, щоб інші люди знали всю цю особисту інформацію?
- Як сторонні можуть використати цю інформацію?

Різні обставини вимагають різних рівнів конфіденційності. Щоб зрозуміти, яких саме, треба поглянути на ситуацію з іншої точки зору.

Практичне завдання

Необхідні матеріали:

- примірник вигаданих профілів із заняття 2 для кожного учня.

1. Розгляньте профілі з іншої точки зору

Зараз ми розіб'ємося на групи, і кожна група обговорить персонажів із точки зору одного з указаних людей:

- Батько чи мати
- Тренер
- Роботодавець
- Друг
- Поліцейський
- Рекламодавець
- Ви самі через 10 років

На що звертатиме увагу ця людина? Яких висновків вона дійде на підставі інформації про нашого персонажа? Викресліть дані, які він не хотів би розкривати цій людині, і відомості, якими йому не варто було ділитися.

2. Представте свої висновки

Тепер кожна група має презентувати свою точку зору й обґрунтувати, чому вони викреслили ту чи іншу інформацію.

Висновки

Різні люди роблять із тієї самої інформації різні висновки.
Тож ваш інтернет-імідж в очах інших людей, найімовірніше, не збігатиметься з тим, як ви самі бачите себе.

Конфіденційність на практиці

Клас розглядає три випадки й обговорює, як забезпечити конфіденційність інформації в кожному з них.

Цілі

- ✓ **Навчитися** дивитися на питання конфіденційності з точки зору інших людей.
- ✓ **З'ясувати**, чому різні випадки вимагають різних рівнів конфіденційності.

Обговорення

Практичні приклади: що робити?

Приклад 1. Вашого однокласника вкусила комаха, і тепер у нього на животі бридкий різнокольоровий висип. Ваш товариш не хоче, щоб хтось про це знав.
- Чи мають інші люди право знати про це?
- Чи маєте ви їм про це розповісти?

Приклад 2. Ваша подруга веде щоденник. Хтось опублікував уривки з нього в мережі.
- Чи мала ця людина право публікувати записи з чужого щоденника?
- Як би ви почувалися, якби це був ваш щоденник?

Приклад 3. Подруга вашої тітки написала на її сторінці в соціальній мережі: "Гарного відпочинку!".
- Чи дійдуть інші люди висновку, що ваша тітка незабаром кудись їде?
- Чи можна було побажати гарного відпочинку більш конфіденційним способом (наприклад, приватним повідомленням або SMS)?

Практичне завдання

Розгляньмо три практичні приклади й поговорімо про те, якого рівня конфіденційності вимагає кожен із них.

Висновки

Різні обставини вимагають різної реакції. Але завжди слід поважати бажання інших людей щодо конфіденційності їхньої особистої інформації, навіть якщо ви на місці цих людей учинили б інакше.

Урок 2. Пильність в Інтернеті

Не піддавайтеся обману

Захист від фішингу та шахрайства

Огляд уроку

Заняття 1. **Як не потрапити на гачок фішингу?**
Заняття 2. **Хто це насправді?**

Теми

Важливо, щоб діти розуміли, що контенту в мережі не завжди можна довіряти та що часом його публікують зловмисники з метою викрадення чужої інформації. Зокрема, фішинг та інші види інтернет-шахрайства націлені на те, щоб змусити користувачів (незалежно від їхнього віку) відреагувати на пропозицію від невідомої людини чи переконати їх, що вони спілкуються зі знайомими.

Цілі

- ✓ **Пояснити**, що не можна довіряти будь-якій інформації в мережі.
- ✓ **Розповісти**, як працює фішинг і чим він небезпечний.
- ✓ **Навчити** дітей розпізнавати оманливі акції, призи й інші шахрайські пропозиції.

Застосовні стандарти

Стандарти ISTE для вчителів: 1a, 1b, 2a, 3d, 4a, 4b, 4c, 4d. **Стандарти ISTE для учнів (2016):** 1d, 2a, 2b, 2c, 2d, 3a, 3b. **Навчальні стандарти AASL:** 1.1.1, 1.1.5, 1.1.6, 1.1.8, 1.2.4, 1.2.6, 1.3.3, 1.3.5, 2.1.1, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 4.1.7, 4.3.2, 4.3.4, 4.4.4. **C3:** II:A, II:B, II:C, III:A, III:B,III:C, III:D.

Не піддавайтеся обману
Словник

Фішинг
Спроба виманити особисту інформацію в користувача Інтернету. Зазвичай для фішингу застосовуються електронні листи, оголошення та фіктивні сайти, за дизайном дуже подібні до тих, які часто відвідує користувач.

Цільовий фішинг
Фішингова атака, спрямована на конкретного користувача із застосуванням його особистої інформації.

Шахрайство
Спроба обманним способом отримати гроші або інші цінності.

Довірений
Надійний; той, що працює правильно чи виконує необхідні функції.

Справжній
Реальний, правдивий; не фіктивний і не скопійований.

Перевірка
Процедура, яка показує, чи справжній певний обліковий запис, сайт тощо.

Оманливий
Створений з метою створення у користувачів хибного враження.

Шахрайський
Створений, щоб ошукувати людей із метою отримання цінностей.

Брандмауер
Програма, яка захищає комп'ютер від більшості видів шахрайства.

Як не потрапити на гачок фішингу?

Учні в ігровій формі аналізують різні електронні листи й повідомлення, намагаючись визначити, які з них справжні, а які фішингові.

Цілі

- ✓ **Дізнатися**, які способи використовуються для крадіжки особистих даних.
- ✓ **Навчитися** захищати свої особисті дані від крадіжки.
- ✓ **Зрозуміти**, що в разі підозри крадіжки особистих даних важливо звернутися по допомогу до дорослого, якому довіряєте.
- ✓ **З'ясувати**, за якими ознаками можна виявити фішинг.
- ✓ **Усвідомити**, чому ділитись особистою інформацією слід дуже обачно.

Обговорення

Що таке фішинг?

Фішинг – це спроба викрасти ім'я користувача, облікові дані людини тощо, переконавши її, що вона спілкується з кимось, кому довіряє. Зазвичай для фішингу застосовуються текстові повідомлення, електронні листи й інші види онлайн-комунікацій. Фішингові листи та вкладені в них файли (а також сайти й завантажувані файли, посилання на які містять такі листи) можуть заражати комп'ютери користувачів вірусами, які отримують доступ до списку контактів і розсилають людям у ньому нові фішингові повідомлення. Інші шахрайські повідомлення можуть містити сповіщення про те, що пристрій заражено вірусами тощо й користувач повинен негайно завантажити "антивірусне" програмне забезпечення (насправді воно, звісно ж, зловмисне). Тож пам'ятайте: жоден сайт або оголошення не здатні визначити, чи правильно працює ваш комп'ютер!

Часом фішингові атаки легко розпізнати, але часто вони бувають складними й дуже переконливими. Наприклад, деякі зловмисники використовують у листах особисту інформацію користувачів. Це так званий цільовий фішинг, персоналізований для одного адресата, і він буває дуже дієвим.

Тож важливо вміти помічати в листах і повідомленнях дивні та незвичні риси: це вбереже вас від того, щоб ввести свій пароль на небезпечному сайті чи перейти за сумнівним посиланням.

Отримавши певне повідомлення чи відкривши сайт, завжди перевіряйте, чи вони справжні. Зокрема, завжди ставте собі наведені запитання:

- Чи є в сайту якісь ознаки, які свідчать про його надійність (значки тощо)?
- Чи відповідає URL-адреса сайту його назві та заголовку?
- Чи є на сайті спливаючі вікна? (Такі вікна часто використовуються на шахрайських ресурсах).
- Чи починається URL-адреса сторінки з префікса https://, перед яким відображається значок зеленого замка? (Це вказує, що з'єднання безпечне та зашифроване).
- Що написано дрібним шрифтом? (Усякі хитрі нюанси та невигідні умови часто пишуть саме так).

Продовження на наступній сторінці →

Але що робити, якщо ви попалися на гачок? Перш за все не панікуйте!

- Негайно повідомте батьків, учителя чи іншого дорослого, якому довіряєте. Що довше ви зволікаєте, то гіршими будуть наслідки.
- Змініть паролі своїх облікових записів.
- Повідомте всіх друзів, яких ви могли підставити під удар.
- Якщо можливо, то позначте фішингове повідомлення як спам.

Практичне завдання

Необхідні матеріали:

– роздруківки з прикладами фішингу.

Ключ до роздруківок із прикладами фішингу:

1. **Справжнє.** У повідомленні просять користувача ввійти в обліковий запис самостійно, а не за наданим у листі посиланням, яке може бути небезпечним.
2. **Шахрайське.** URL-адреса підозріла й незахищена.
3. **Справжнє.** У URL-адресі є префікс https://.
4. **Шахрайське.** Підозріла пропозиція в обмін на введення банківських реквізитів.
5. **Шахрайське.** URL-адреса підозріла й незахищена.

1. Аналіз прикладів (у групах)

Зараз ми розіб'ємося на групи та проаналізуємо ці приклади повідомлень і веб-сайтів.

2. Перевірка справжності (індивідуально)

Учні мають самостійно вирішити, чи справжнє повідомлення або веб-сайт, чи ні, і записати свої аргументи.

3. Обговорення думок учнів (у групах)

Які повідомлення та сайти вам видалися надійними, а які підозрілими? Чи здивували вас якісь відповіді?

4. Подальше обговорення

Ось іще кілька запитань, які допоможуть вам оцінити справжність онлайн-повідомлень і сайтів:

• Чи не виглядає це повідомлення сумнівно?

Що вам підказує інстинкт? Чи не помітили ви чогось підозрілого?

• Чи пропонується в листі щось безкоштовне?

Безкоштовний сир буває лише в мишоловці.

• Чи просять вас указати особисту інформацію?

Деякі сайти вимагають надати її, щоб надсилати вам нові шахрайські повідомлення. Наприклад, усілякі тести можуть насправді збирати про вас факти, які допоможуть угадати ваш пароль тощо. А от справжні компанії зазвичай не просять особистої інформації, окрім електронної пошти.

• Це ланцюговий лист або публікація в соціальній мережі?

Якщо в листі чи публікації вимагається переслати їх, наприклад, "10 друзям", це дуже ризиковано. Робіть це тільки тоді, коли точно знаєте, від кого цей лист і що він безпечний.

• Чи є в листі або повідомленні текст дрібним шрифтом?

Унизу повідомлень часто вказується додаткова інформація дуже дрібним шрифтом. Зазвичай її ніхто не читає – на те вона й розрахована. Наприклад, у заголовку листа може бути вказано, що ви виграли телефон, а дрібним шрифтом унизу уточнюватиметься, що за приз доведеться щомісячно доплачувати по 200 грн.

Примітка

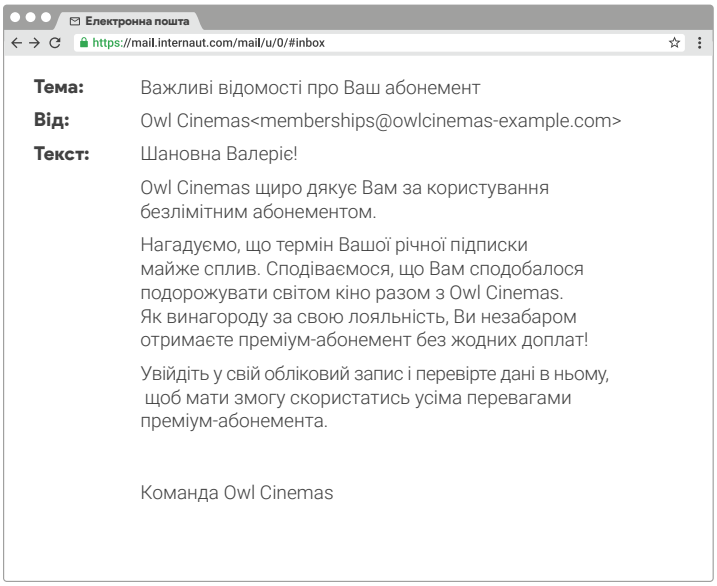
Internaut Mail – вигадана компанія, але уявімо, що це справжня поштова служба.

Висновки

Користуючись Інтернетом, завжди будьте насторожі: пам'ятайте про загрозу фішингових листів, повідомлень і публікацій. А якщо ви все ж потрапили на гачок, негайно повідомте людей, яким довіряєте.

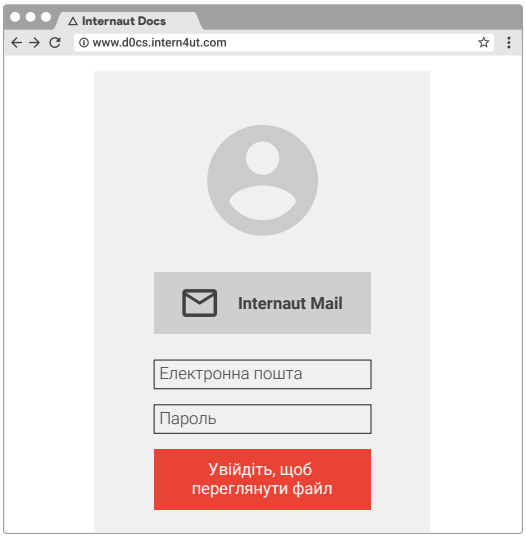
Аркуш із вправами. Заняття 1

Приклади фішингу



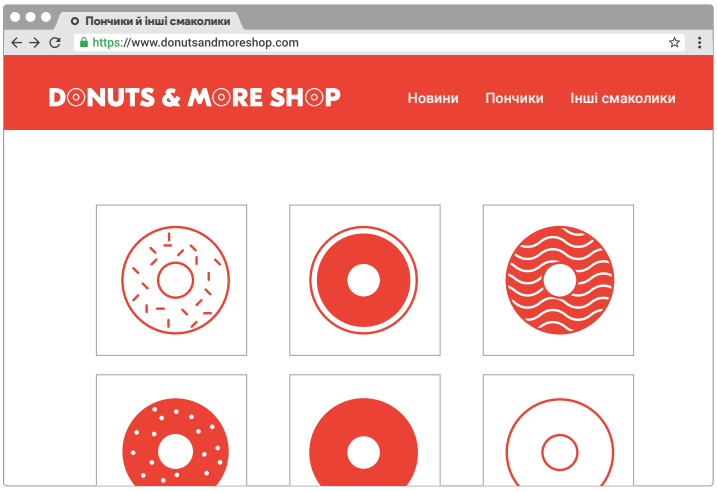
1. Цей веб-сайт справжній чи шахрайський?

Справжній _____ Шахрайський _____



2. Цей веб-сайт справжній чи шахрайський?

Справжній _____ Шахрайський _____

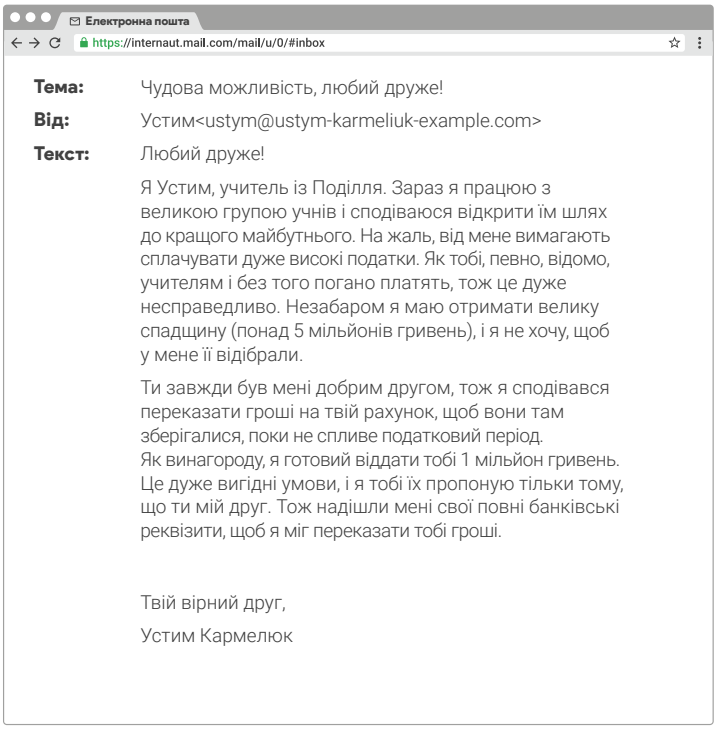


3. Цей веб-сайт справжній чи шахрайський?

Справжній _____ Шахрайський _____

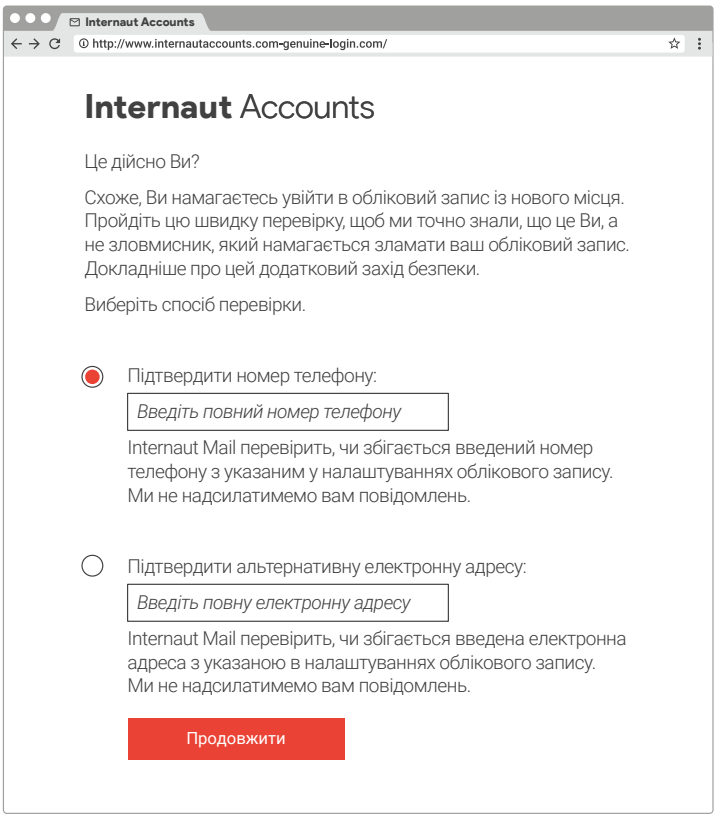
Продовження на наступній сторінці →

Аркуш із вправами. Заняття 1 (продовження)



4. Цей веб-сайт справжній чи шахрайський?

Справжній _____ Шахрайський _____



5. Цей веб-сайт справжній чи шахрайський?

Справжній _____ Шахрайський _____

Хто це насправді?

Учні відпрацьовують навички розпізнавання фішингу, розігруючи сценарії з підозрілими онлайн-повідомленнями, дописами, зображеннями, електронними листами й обговорюючи можливу реакцію на них.

Цілі

- ✓ **Зрозуміти**, що мережева аудиторія людини може бути набагато більшою, ніж їй здається.
- ✓ **Запам'ятати**, що необхідно завжди перевіряти особи людей, з якими спілкуєшся в мережі.
- ✓ **Усвідомити**, що потрібно спершу думати, а вже потім додавати людину в друзі чи починати з нею спілкуватися.
- ✓ **Навчитись** уважно вибирати, кому надавати особисту інформацію та яку саме.
- ✓ **Зрозуміти**, що в підозрілих ситуаціях завжди потрібно звертатися до дорослих, яким довіряєте, якім довіряєте.
- ✓ **Запам'ятати**, що треба повідомляти дорослих, коли хтось у мережі заводить розмову на некомфортні для учня теми.
- ✓ **Усвідомити**, що під час спілкування в мережі завжди потрібно поводитися чесно.

Обговорення

Ви певні, що це дійсно та людина?

Коли ви розмовляєте з другом по телефону, звідки ви знаєте, що це саме він, адже ви його не бачите? Іноді люди видають себе в мережі за когось іншого, щоб пожартувати з нього, а іноді – щоб украсти його особисту інформацію. Часом незнайомці в Інтернеті можуть писати вам і намагатися додати вас у друзі. У таких випадках ваше завдання – вирішити, що їм відповісти та чи хочете ви взагалі з ними спілкуватися.

На щастя, є кілька способів перевірити особу іншої людини та визначити, чи це не шахрай. Ось для початку кілька ідей.

• Чи не виглядає зображення профілю підозріло?

Якщо воно розмите або обличчя людини важко розгледіти, це тривожний дзвіночок. Ще шахраї часто крадуть справжні фото в інших людей і використовують як зображення власного фіктивного профілю.

• Чи збігається відображуване ім'я людини з її іменем користувача?

Наприклад, URL-адреса профілю в соціальній мережі має відповідати імені, указаному в цьому профілі. Якщо людину звуть Іван Іваненко, то його адреса має виглядати приблизно так: SocialMedia.com/ivan.ivanenko.

• Чи заповнено в профілі розділ біографії?

Якщо так, чи схоже, що його дійсно писала людина, якій нібито належить профіль? У фіктивних облікових записах розділ "Про мене" часто порожній чи заповнений абиякою інформацією.

• Як довго обліковий запис був активним?

Якщо профіль зовсім новий або в ньому багато аномальної активності, це тривожний дзвіночок. У фіктивних облікових записах часто мало чи зовсім немає дописів і взаємодій з іншими людьми.

Продовження на наступній сторінці →

Не піддавайтеся обману. Заняття 2 (продовження)

Практичне завдання

Необхідні матеріали:

- аркуш із вправами "Хто це насправді?", порізаний на смужки (по одному сценарію на кожній смужці);
- миска чи інша ємність, з якої учні всліпу витягуватимуть смужки;
- аркуші з відповідями (стор. 23–24).

1. Групи аналізують сценарії

Добре, а тепер розбиймося на групи. Кожна група витягне по сценарію й обговорить, як варто реагувати в описаній ситуації.

2. Групи розігрують сценарії

Тепер кожна група розіграє свій сценарій. Один учень зачитає текст, інший озвучить повідомлення, третій продемонструє правильну реакцію, а четвертий може її аргументувати.

3. Клас обговорює реакцію груп

Клас аналізує реакцію кожної групи та порівнює її з правильними відповідями.

Висновки

Уважно стежте за колом свого спілкування в мережі. Обов'язково перевіряйте, чи дійсно ваші Інтернет-знайомі – ті, за кого себе видають.

Аркуш із вправами. Заняття 2

Хто це насправді?

Сценарій 1	Якийсь незнайомець пише вам у соціальній мережі: "Привіт! Ти прикольний чувак, розважмося разом! Додаси мене до друзів? – Микола"
Сценарій 2	Ви отримуєте SMS із незнайомого номера: "Привіт, це Аня, ми познайомились улітку. Пам'ятаєш мене?"
Сценарій 3	Після уроку англійської мови з Тетяною Василівною на ваш телефон надходить повідомлення: "Привіт, це Марк. Ти зрозумів, що нам задала Тетяна Василівна?"
Сценарій 4	Людина, на яку ви не підписані, надсилає вам таке повідомлення: "Привіт! Я просто в захваті від твоїх дописів, ти такий дотепний!!! Напиши мені свій номер телефону, я хочу з тобою поспілкуватися!"
Сценарій 5	Якась незнайомка пише вам у чаті: "Я бачила тебе сьогодні на перерві. Ти дуже симпатичний!!! Де ти живеш? Я можу прийти до тебе в гості".
Сценарій 6	Хтось пише вам у соціальній мережі: "Привіт, я нещодавно бачилася з твоєю подругою Наталкою, і вона мені багато про тебе розповідала. Я хочу з тобою дружити! Де ти живеш?"

Аркуш із відповідями з теми фішинг. Заняття 2

Хто це насправді?

Сценарій 1

Якийсь незнайомець надсилає вам таке повідомлення: "Привіт! Ти прикольний чувак, розважмося разом! Додаси мене до друзів? – Микола"

- **Проігнорувати Миколу.** Якщо ви не знаєте цю людину, то можете просто нічого не відповідати.
- **"Привіт, Миколо. Ми знайомі?"** Якщо ви не впевнені, що знаєте цю людину, можна спитати в неї самої.
- **Заблокувати Миколу.** Якщо ви впевнені, що не знаєте цю людину, можна її заблокувати. Тоді ви більше не отримуватимете від неї повідомлень.
- **Додати Миколу до друзів.** Якщо ви не впевнені, хто він такий, краще цього не робити.
- **Переглянути профіль Миколи.** Якщо ви не бачите нічого підозрілого, то можна додати цю людину до друзів. Але будьте обережні, адже профіль можна легко підробити! Також зверніть увагу на список друзів цієї людини – він теж може вказувати, фіктивний профіль чи ні.
- **Написати Миколі щось про себе.** Чи варто відповісти йому щось на кшталт: "Авжеж, я тут новенький і ще мало кого знаю! Зустріньмося якось після школи (я вчусь у ліцеї на Шевченка)"? У жодному разі! Ніколи не варто надавати свою особисту інформацію людям, яких ви не знаєте, особливо в Інтернеті.

Сценарій 2

Ви отримуєте SMS із незнайомого номера: "Привіт, це Аня, ми познайомились улітку. Пам'ятаєш мене?"

- **Заблокувати Аню.** Якщо ви дійсно знайомі, то можете її образити. Блокуйте цю людину, тільки якщо цього літа ви точно не знайомилися ні з ким на ім'я Аня (або ж пам'ятаєте цю дівчинку, але просто не хочете з нею спілкуватися).
- **Проігнорувати Аню.** Як уже говорилося вище, якщо ви не знаєте цю людину, можна просто нічого їй не відповідати.
- **"Привіт, Аню. Нагадай, будь ласка, як ми зустрілися".** Це безпечний варіант, якщо ви не впевнені, що робити.
- **"Привіт! Як справи? Я дуже рада, що ти мені написала!"** Так можна відповідати, тільки якщо ви дійсно пам'ятаєте цю людину з літа.
- **"Ти ж та дівчинка з рудою косою?"** Якщо ви не впевнені, що знаєте цю людину, можна спробувати розпитати її – можливо, тоді ви її пригадаєте.
- **"Я тебе не пам'ятаю, але можемо зустрітися".** Це дуже погана ідея. Ніколи не варто пропонувати незнайомій людині зустрітися.

Сценарій 3

Після уроку англійської мови з Тетяною Василівною на ваш телефон надходить повідомлення: "Привіт, це Марк. Ти зрозумів, що нам задала Тетяна Василівна?"

- **Проігнорувати Марка.** Як завжди – якщо ви не знаєте цю людину, можна їй не відповідати.
- **Заблокувати Марка.** Якщо ви впевнені, що у вашому класі немає ніякого Марка, то варто зробити саме так.

Продовження на наступній сторінці →

Аркуш із відповідями з теми фішинг. Заняття 2 (продовження)

- **"Привіт, Марку. Ти ж той новенький із задньої парти?"** Якщо ви не впевнені, що знаєте цю людину, можна розпитати її детальніше.
- **"Звісно. Після школи поясню".** Так можна відповісти, тільки якщо ви впевнені, що знаєте цю людину.
- **"Я не в курсі, я з підгрупи Івана Павловича".** Якщо повідомлення цієї людини виглядає підозріло, краще просто проігнорувати його. І в жодному разі не слід повідомляти їй свою особисту інформацію, наприклад ім'я вашого вчителя англійської мови.
- **"Дзвони, поясню. Мій номер (012) 345-67-89".** Якщо ви не впевнені, що знаєте цю людину, повідомляти їй свою особисту інформацію – погана ідея.

Сценарій 4

Людина, на яку ви не підписані, надсилає вам таке повідомлення: "Привіт! Я просто в захваті від твоїх дописів, ти такий дотепний!!! Напиши мені свій номер телефону, я хочу з тобою поспілкуватися!"

- **Проігнорувати користувача @nastusik122.** Якщо ви не хочете відповідати цій людині, то можете просто промовчати.
- **Заблокувати користувача @nastusik122.** Якщо ця людина видається вам підозрілою, можна просто заблокувати її, і тоді вона вам більше не писатиме.
- **"Привіт, ми знайомі?"** Якщо ви не впевнені, що знаєте цю людину, розпитайте її, перш ніж надавати будь-які відомості про себе.
- **"Добре, ось мій номер..."** Так робити не можна! Навіть якщо ви впевнені, що вам пишуть не з фіктивного профілю, ніколи не варто надсилати свою особисту інформацію через соціальні мережі. Зв'яжіться іншим способом: через батьків, учителів або через того, кому довіряєте.

Сценарій 5

Якась незнайомка пише вам у чаті: "Я бачила тебе сьогодні на перерві. Ти дуже симпатичний!!!
Де ти живеш? Я можу прийти до тебе в гості".

- **Проігнорувати цю людину.** Це розумний вибір.
- **Заблокувати цю людину.** Якщо вона підозріла, блокуйте її без вагань.
- **"Ти хто?"** Так робити не варто. Якщо повідомлення виглядає підозріло, краще просто не відповідати на нього чи взагалі заблокувати відправника.
- **"Це ти, Оксано? Ти теж мені дуже подобаєшся!!! Я живу на Шевченка , буд. 2".** Це дуже погана ідея, навіть якщо ви вважаєте, що знаєте відправника. Перш ніж давати комусь свою адресу або іншу особисту інформацію, обов'язково ретельно перевірте, хто ця людина.

Сценарій 6

Хтось пише вам у соціальній мережі: "Привіт, я нещодавно бачилася з твоєю подругою Наталкою, і вона мені багато про тебе розповідала. Я хочу з тобою дружити! Де ти живеш?"

- **Проігнорувати цю людину.** Якщо ви не знаєте цю людину, але у вас дійсно є така подруга, найкраще спершу написати Наталці, а вже потім відповідати на це повідомлення.
- **Заблокувати цю людину.** Якщо ви не знаєте цю людину й не маєте подруги на ім'я Наталка, варто заблокувати відправника, щоб він більше нічого вам не писав.
- **"Ти хто?"** Це не найкраща ідея. Якщо ви не знаєте цю людину, варто просто проігнорувати її (принаймні поки ви не дізнаєтесь у Наталки, чи дійсно вона комусь про вас розповідала).

Бережіть свої таємниці

Серйозне ставлення до конфіденційності та безпеки

Огляд уроку

Заняття 1. **Як придумати надійний пароль**
Заняття 2. **Як керувати налаштуваннями конфіденційності**

Теми

У питань конфіденційності й безпеки в Інтернеті не завжди є чіткі правильні та неправильні відповіді. Щоб захистити свою особисту інформацію й імідж, потрібно вміти ставити правильні запитання та знаходити на них обґрунтовані відповіді.

Цілі

- ✓ **Пояснити**, чому важливо захищати конфіденційність своїх даних і як вона пов'язана з безпекою в Інтернеті.
- ✓ **Відпрацювати** навички створення надійних паролів.
- ✓ **Розглянути** інструменти й налаштування, які допоможуть захиститися від хакерів та інших загроз.

Застосовні стандарти

Стандарти ISTE для вчителів: 1a, 1b, 2a, 3b, 4a, 4b, 4c, 4d, 5a. **Стандарти ISTE для учнів (2016):** 1d, 2a, 2d. **Навчальні стандарти AASL:** 1.1.8, 1.3.5, 2.1.3, 2.3.1, 2.3.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4. **CSTA:** II:A, II:B, II:C, III:A, III:B.

Бережіть свої таємниці
Словник

Конфіденційність
Захист своєї й чужої особистої інформації.

Безпека
Правильні звички поводження з апаратним і програмним забезпеченням, які допомагають його захистити.

Двоетапна перевірка
Процедура безпечного входу в обліковий запис, яка відбувається у два етапи (наприклад, коли спершу потрібно ввести пароль, а потім код із SMS).

Маркер безпеки
Брелок або інший невеликий пристрій для отримання доступу до системи.

Пароль
Таємна комбінація символів для доступу до чогось.

Як придумати надійний пароль

Учні навчаються створювати надійні паролі та тримати їх у таємниці.

Цілі

- ✓ **Усвідомити**, чому свої паролі можна повідомляти лише батькам або опікунам.
- ✓ **Дізнатися**, як паролі захищають пристрої.
- ✓ **Навчитися** створювати паролі, які легко запам'ятати й важко відгадати.
- ✓ **Зрозуміти**, як вибрати рівень безпеки налаштувань входу та коли потрібно використовувати двофакторну перевірку.

Обговорення

Береженого Бог береже

Завдяки цифровим технологіям можна вільно спілкуватися з друзями, однокласниками, учителями тощо, використовуючи для цього найрізноманітніші способи: електронну пошту, SMS, чати; текстові повідомлення, зображення, відео; телефони, планшети та ноутбуки. (А як ви спілкуєтеся з друзями?)

Але ці засоби не тільки полегшують комунікацію, а й дають хакерам і шахраям широкі можливості для викрадення наших даних і використання їх на шкоду нашим пристроям, стосункам і репутації.

Щоб захистити ці дані, потрібно небагато: не забувати блокувати екрани пристроїв і намагатися не зберігати свою особисту інформацію на пристроях, які легко вкрасти чи загубити. А найголовніше – треба завжди використовувати надійні паролі.

- Хто здогадається, які два паролі найпопулярніші у світі? (Відповідь: "123456" і "password").
- А які ще паролі не варто використовувати? (Приклади: власне ім'я та прізвище, власний номер телефону, слово "shokolad").

Хто вважає, що це надійні паролі?

Продовження на наступній сторінці →

Бережіть свої таємниці. Заняття 1 (продовження)

Практичне завдання

Необхідні матеріали:

- пристрої з підключенням до Інтернету (по одному на кожного учня чи групу учнів);
- дошка чи проектор;
- роздруківки "Рекомендації щодо створення надійних паролів".

А тепер пограємо в гру зі створення паролів для закріплення набутих навичок.

1. Створіть паролі

Зараз ми розіб'ємося на команди по двоє. Кожна команда повинна буде придумати пароль за 60 секунд.

2. Порівняйте паролі

До дошки виходитимуть по дві команди за раз. Кожна команда повинна буде записати на дошці свій пароль.

3. Проголосуйте

Клас обговорить кожну пару паролів і проголосує за надійніший.

Висновки

Ось корисна порада зі створення дуже надійного пароля.

Придумайте чи згадайте цікаву фразу, яку буде легко запам'ятати. Це може бути рядок з улюбленої пісні, слова з фільму, назва книжки тощо.

- Візьміть першу букву (чи дві букви) кожного слова у фразі. Запишіть їх латиницею.
- Замініть деякі букви символами.
- Зробіть деякі літери великими, а деякі малими.

Рекомендації щодо створення надійних паролів

Ось іще кілька порад зі створення паролів.

Надійні паролі часто засновані на реченні, яке вам буде легко запам'ятати, а комусь іншому – важко вгадати.

Паролі середньої надійності важко підібрати за допомогою зловмисного програмного забезпечення, але досить легко вгадати, якщо шахрай добре вас знає.

Ненадійні паролі зазвичай засновані на особистій інформації, і їх легко підібрати за допомогою зловмисного програмного забезпечення (або й просто вгадати, якщо шахрай добре вас знає).

Що треба робити

- Використовуйте для важливих облікових записів унікальні паролі.
- Кожен пароль має містити принаймні вісім символів.
- Кожен пароль має складатися з комбінації букв (великих і малих), цифр і спеціальних символів.

Чого не треба робити

- Не можна використовувати як пароль особисту інформацію (ім'я та прізвище, домашню й електронну адресу, номер телефону, номер паспорта, дівоче прізвище матері, дату народження тощо) чи звичайні слова.
- Не можна використовувати паролі, які легко вгадати: власне прізвисько чи відображуване ім'я, назву школи, улюблену футбольну команду тощо.
- Не можна розкривати свої паролі нікому, крім батьків чи опікуна.

Як керувати налаштуваннями конфіденційності

Учитель показує на шкільному пристрої, як правильно налаштувати параметри конфіденційності та де їх шукати.

Цілі

- ✓ **Дізнатися**, як налаштовувати параметри конфіденційності в онлайн-службах, якими найчастіше користуються учні.
- ✓ **Навчитися** приймати рішення щодо публікування даних у цих службах.
- ✓ **Зрозуміти**, що таке двофакторна та двоетапна перевірка й коли їх використовувати.

Обговорення

Конфіденційність – це безпека

Безпека в Інтернеті неможлива без захисту конфіденційності. У більшості додатків і програм є функції для керування доступом до інформації користувача.

Зазвичай вони містяться в розділі, який може називатися "Мій обліковий запис", "Налаштування", "Параметри" тощо.
У ньому зібрано налаштування безпеки та конфіденційності, які визначають:
• яка інформація відображається у вашому профілі;
• хто бачить ваші дописи, фотографії, відео й інший вміст, яким ви ділитеся.

Якщо ви навчитеся використовувати ці налаштування для забезпечення конфіденційності своєї інформації й не забуватимете вчасно їх редагувати, то зможете надійно себе захистити.

Практичне завдання

Необхідні матеріали:

– один шкільний пристрій, підключений до проектора та призначений для показу демонстраційного (наприклад, тимчасового) облікового запису на сайті чи в поштовій службі.

1. Ознайомлення з налаштуваннями

Отже, мій шкільний пристрій підключено до проектора. Перейдімо на сторінку налаштувань цього додатка. Як бачимо, тут доступні такі можливості:
• змінення пароля;
• увімкнення сповіщень про спроби входу в обліковий запис із невідомого пристрою;
• обмеження доступу до профілю разом з усіма фотографіями й відео (наприклад, його можна зробити видимим лише для кіл "Сім'я" та "Друзі");
• увімкнення двофакторної чи двоетапної перевірки.

2. Додаткові налаштування перевірки

А зараз поговоримо про двофакторну та двоетапну перевірку.
• Двоетапна перевірка: процедура входу в обліковий запис складається з двох етапів (наприклад, спершу потрібно ввести пароль, а потім указати код із SMS, який діє 10 хвилин).
• Двофакторна перевірка: для входу потрібно надати два типи інформації (наприклад, пароль і відбиток пальця).

Продовження на наступній сторінці →

Бережіть свої таємниці. Заняття 2 (продовження)

Як вибрати правильні налаштування безпеки та конфіденційності? Це питання варто обговорити з вашими батьками чи опікуном. Але пам'ятайте: найнадійніший захист – це ваш здоровий глузд. Саме ви вирішуєте, якою особистою інформацією ділитися, коли та з ким саме.

Висновки

Перший крок до захисту важливих облікових записів – створення надійного унікального пароля для кожного з них. Але після того ще треба зуміти не забути ці паролі та не дати зловмисникам украсти їх.

Записувати паролі не забороняється, але аркуш із ними не можна зберігати на видному місці (тримати на столі, приклеювати на монітор тощо). Виберіть для аркуша з паролями надійну непомітну схованку.

Урок 4. Доброзичливість в Інтернеті

Круто бути доброзичливим!

Сила доброзичливості в Інтернеті

Огляд уроку

Заняття 1. **Не будьте байдужими**
Заняття 2. **Ввічливість в Інтернеті**
Заняття 3. **Тон має значення**
Заняття 4. **Батьки і діти**

Теми

У цифровому світі діти стикаються з рядом специфічних проблем. У мережі важче зчитувати соціальні сигнали, анонімність породжує вседозволеність, а онлайн-залякування часом набуває серйозних масштабів і залишає стійкий цифровий слід.

Але в Інтернеті легше виявляти не лише злість, а й доброзичливість. Щоб діти вміли будувати здорові стосунки з іншими й не почувались ізольованими (адже ізоляція – одна з поширених причин залякування, депресії, низької успішності й інших проблем), потрібно вчити їх виявляти доброту та співчуття, а також коректно реагувати на чужу агресію.

Дослідження показали, що недостатньо просто сказати дітям чемно поводитися в Інтернеті: справжній педагог мусить виявити причину агресії й усунути її. Так, можна від початку заохотити учнів до спілкування в позитивному ключі та навчити їх, як не стати жертвою агресії самим і захистити інших.

Цілі

- ✓ **З'ясувати**, якою має бути доброзичлива поведінка в Інтернеті.
- ✓ **З'ясувати**, що таке доброзичливість у реальному й віртуальному світі.
- ✓ **Навчити** дітей подавати іншим добрий приклад під час спілкування в мережі.

Застосовні стандарти

Стандарти ISTE для вчителів: 1b, 1d, 2a, 3b, 4a, 4b, 4c, 5a. **Стандарти ISTE для учнів (2016):** 2a, 2b. **Навчальні стандарти AASL:** 1.1.5, 1.3.3, 1.3.5, 2.1.3, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 2.4.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.2, 3.3.3, 3.3.6, 4.1.7, 4.2.3, 4.3.4, 4.4.4. **C3:** I:B, I:D, I:E, I:F, I:H, II:C.

Круто бути доброзичливим!
Словник

Залякування
Небажана агресивна поведінка, яка з часом повторюється чи може повторюватися.

Спостерігач
Людина, яка має змогу завадити певним неприпустимим діям або повідомити про них, але нічого не робить.

Небайдужий
Людина, яка виступає проти певних неприпустимих дій або повідомляє про них.

Переслідування
Поведінка, за якої людина ставить жертву переслідувань у дискомфортне становище за допомогою непроханих і небажаних висловлювань або фізичних дій.

Посилення
Збільшення гучності чи інтенсивності.

Блокування
Заблокувавши певну людину, можна заборонити їй переглядати ваш профіль, надсилати вам повідомлення тощо.

Не будьте байдужими

Учні вчаться визначати ролі учасників конфлікту, пов'язаного із залякуванням (агресор, жертва, спостерігач), і реагувати на агресію з позиції жертви та спостерігача.

Цілі

- ✓ **Зрозуміти**, що означає бути спостерігачем і якою має бути поведінка небайдужої людини.
- ✓ **Дізнатися**, що робити, якщо ви стали свідком залякування.
- ✓ **Навчитися** реагувати на переслідування.

Обговорення

Навіщо потрібно бути доброзичливими в мережі?

Часом варто нагадувати собі, що за іменами користувачів і аватарами ховаються живі люди зі справжніми почуттями, які потрібно поважати. Зазвичай учасники конфліктів, пов'язаних із залякуванням та іншими неприпустимими діями, діляться на три групи.

- **Агресор** (або агресори).
- **Ціль** (**жертва**) агресії.
- Часто в конфлікті також беруть участь так звані **спостерігачі.**

Спостерігач має змогу завадити агресивним діям або повідомити про них, але воліє не втручатися. А небайдужа людина робить усе, щоб не дати агресору ображати інших. Навіть найменший прояв доброзичливості в Інтернеті може дуже багато значити, і навпаки: невеличка шпилька чи образа може перерости в масштабне цькування.

Ось кілька способів завадити залякуванню й агресії в мережі:

• Подавати гарний приклад.

Навіть якщо ваші друзі не бачать в агресивних діях нічого поганого, ви можете відкрити їм очі, просто доброзичливо поводячись і захищаючи жертв залякування.

• Бути дружніми.

Ставтеся з повагою до однокласників як у віртуальному, так і в реальному світі. Так ви покажете товаришам, що вони не самотні. Це особливо цінно для тих, кого залякують або кому зараз просто гірко на душі.

• Не заохочувати агресорів схваленням чи увагою.

Не відповідайте на образливі коментарі та дописи, не ставте їм оцінки "подобається". Часто агресори ображають інших просто для того, щоб привернути до себе увагу. Якщо ви з друзями їх не заохочуватимете, вони зупиняться швидше.

• Не поширювати образливі повідомлення.

Натомість краще сказати автору такого повідомлення, що це неприпустимо й геть не смішно. Також буде добре, якщо ви висловите жертві підтримку та запропонуєте допомогу.

Продовження на наступній сторінці →

• **Повідомляти про залякування й неприпустиму поведінку.**
У мережі для цього передбачено спеціальні інструменти (кнопки "Поскаржитися" тощо). Ви також можете розповісти про такі дії батькам, учителю, другу, брату чи сестрі.

Практичне завдання

Робота в групах
Якщо ви раптом станете жертвою залякування чи агресії в Інтернеті, ось що можна зробити.

Жертва може...
• Не реагувати на образи
• Заблокувати агресора
• Повідомити про напади батькам, учителю, другу, брату чи сестрі

А що робити, якщо ви стали свідком агресії чи переслідування?

Свідок може...
• Виявити до жертви доброту та співчуття
• Заблокувати агресора
• Повідомити про напади батькам, учителю чи іншій людині, яка може щось зробити

Якщо ви стали свідком агресивних дій і зробили щось, аби їм завадити, це говорить про вашу небайдужість.

Висновки

Залежно від обставин можна стати на захист жертви переслідувань різними способами – наприклад, повідомити про образливі висловлювання чи навіть просто проігнорувати їх, щоб не допустити посилення. Усі ми несемо відповідальність за те, щоб зробити Інтернет гостинним місцем, де панує приязнь.

Круто бути доброзичливим! Заняття 2

Ввічливість в Інтернеті

Студенти разом учаться переформульовувати негативні коментарі й обертати агресію на доброзичливість.

Цілі

- ✓ **Навчитися** висловлювати свої почуття й думки в позитивному ключі.
- ✓ **Навчитися** реагувати на негативні висловлювання та дії ввічливо й конструктивно.

Обговорення

Переведення негативних висловлювань у позитивне русло

Діти вашого віку створюють і споживають найрізноманітніший контент, зокрема й негативні повідомлення, які сприяють поганій поведінці.

- Чи виявляв хтось у мережі доброзичливість до вас або ваших друзів просто так, без усякої причини? Як ви після цього почувалися?
- Чи доводилося вам або вашим друзям бути свідками негативних дій чи висловлювань у мережі? Що ви відчували з цього приводу?
- Як найпростіше спрямувати негативне висловлювання в позитивне русло?

На негативні емоції можна реагувати конструктивно – наприклад, перефразовуючи неприязні коментарі та стежачи за тоном спілкування в мережі.

Практичне завдання

Необхідні матеріали:

- дошка чи проектор;
- роздруківки "Ввічливість в Інтернеті";
- стікери чи пристрої для учнів.

1. Прочитайте коментарі

Прочитаймо ці негативні коментарі.

2. Виправте ці коментарі

А тепер розіб'ємося на групи по троє та спробуймо продумати дві можливі реакції на вказані далі коментарі.

- Як можна сформулювати ту саму чи схожу думку більш позитивно та конструктивно?
- Якби так висловився хтось із ваших однокласників, що б ви сказали, щоб спрямувати розмову в більш доброзичливе русло?

3. Представте свої відповіді

А тепер кожна група представить свої реакції в обох ситуаціях.

Висновки

Якщо відповісти на негативне висловлювання позитивним, можна зробити спілкування цікавішим і приємнішим, а це набагато краще, ніж сварки й образи.

Аркуш із вправами. Заняття 2

Ввічливість в Інтернеті

Прочитайте наведені нижче коментарі. Після кожного з них обговоріть:

1. Як можна сформулювати ту саму чи схожу думку більш позитивно та конструктивно?

2. Якби так висловився хтось із ваших однокласників, що б ви сказали, щоб спрямувати розмову в більш доброзичливе русло?

Запишіть свої ідеї під кожним із коментарів.

"Ха-ха, Костя єдиний з усього класу не їде на екскурсію".

"Усі вдягніть завтра синє. Тільки Люді не кажіть!"

"Вибач, я не зможу запросити тебе на мій день народження, бо вийде задорого".

"Без образ, але ти геть не вмієш малювати. Ми не хочемо робити з тобою стінгазету".

"Жах, мене аж тіпає. Чого вона вирішила, що вміє співати?"

"Ти зможеш вступити в нашу групу, тільки коли даси мені ім'я користувача та пароль від свого облікового запису".

"Я одна думаю, що Жанна схожа на смурфика?"

"👎👎👎"

Тон має значення

Учні намагаються визначити, які емоції автор вклав у текстове повідомлення, і вчаться критично мислити, щоб уникнути неправильного тлумачення чужих висловлювань і виникнення інтернет-конфліктів.

Цілі

- ✓ **Навчитися** правильно добирати слова та розуміти, коли краще промовчати.
- ✓ **З'ясувати**, у яких ситуаціях краще не писати повідомлення чи SMS, а почекати й поговорити особисто.

Обговорення

Проблема непорозуміння

Молодь постійно використовує для спілкування різні види комунікації, однак SMS і повідомлення в чаті часом сприймаються по-іншому, ніж усні висловлювання.

- Чи траплялося, що адресат неправильно розумів ваше SMS (наприклад, ви надіслали жарт, а друг подумав, що ви пишете серйозно)?
- Чи траплялося вам неправильно зрозуміти чиєсь SMS або повідомлення в чаті? Що ви тоді зробили, щоб прояснити непорозуміння? Що б ви зараз зробили інакше?

Практичне завдання

Необхідні матеріали:

– приклади SMS (на класній дошці чи проекторі).

1. Прочитайте повідомлення

Погляньмо на ці приклади на дошці:

- "Це так круто"
- "Як хочеш"
- "Я на тебе страшенно зла"

2. Зачитайте повідомлення вголос

Тепер зачитайте ці SMS (по одному учню на кожне повідомлення) з різними інтонаціями: сердитою, саркастичною, дружньою тощо.

Що ви помітили? Як інші люди можуть сприйняти ці повідомлення? Як відправнику краще донести те, що він насправді мав на увазі?

Висновки

Часом із письмового тексту важко зрозуміти, які емоції за ним стоять. Тож завжди намагайтеся вибрати для кожної бесіди оптимальний вид зв'язку й пам'ятайте, що часом не варто шукати в Інтернет-повідомленнях підтекст, якого там немає.

Круто бути доброзичливим! Заняття 4

Батьки і діти

Клас обговорює, як діти можуть вплинути на поведінку дорослих.

Цілі

- ✓ **Проаналізувати** поведінку дорослих у мережі.
- ✓ **Подумати**, як поведінка дорослих впливає на дії дітей.

Обговорення

Чого дорослі можуть навчити дітей

Прищеплювати дітям доброзичливість – важлива справа, але її варто робити не словом, а ділом. Агресія та залякування характерні не лише для дітей: достатньо поглянути, як дорослі розмовляють одне з одним у мережі чи в заторах.

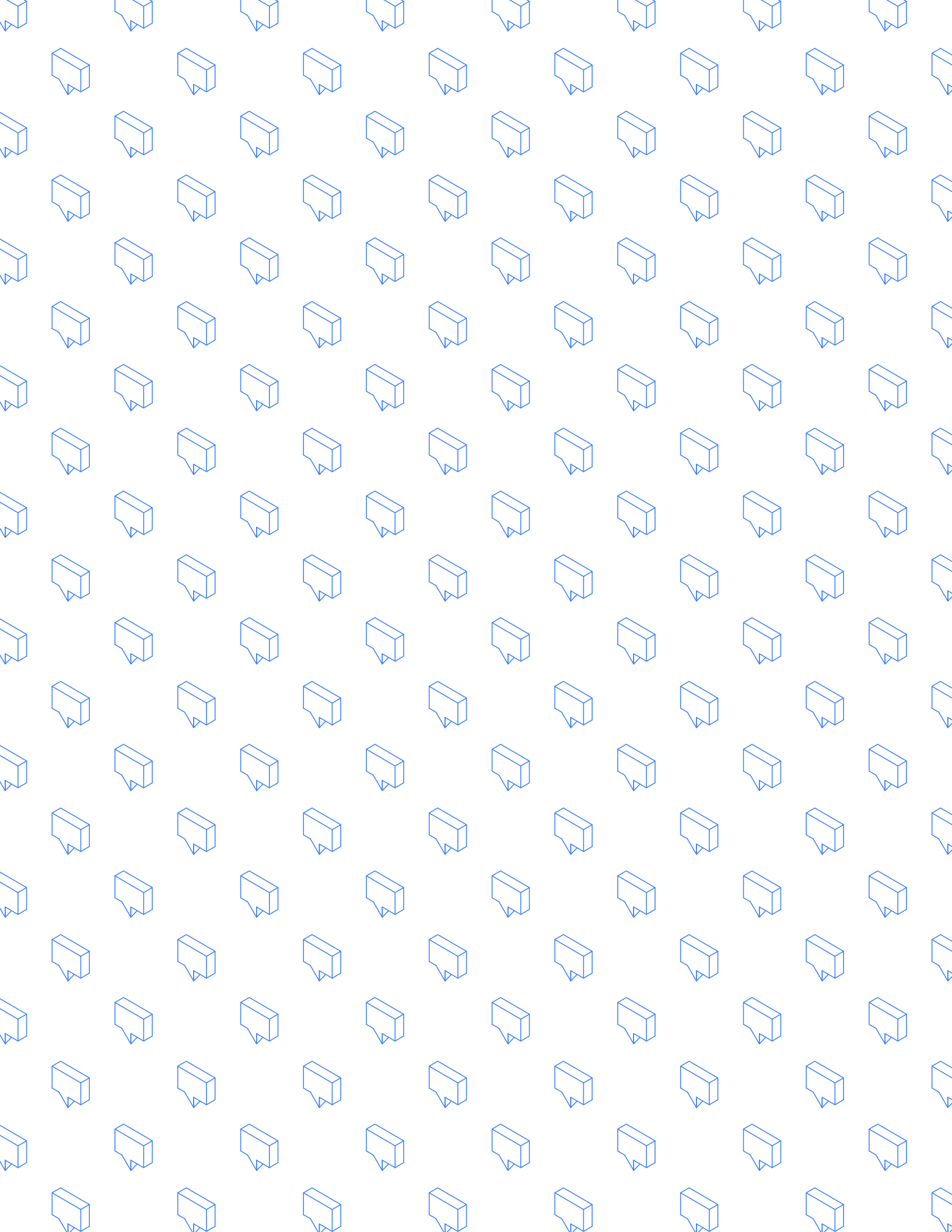
Ми вже говорили про те, чому важливо бути доброзичливими до своїх друзів і однокласників як у віртуальному, так і в реальному світі. А тепер подумайте, чи бачили ви колись, щоб дорослі ставились одне до одного зневажливо або агресивно, залякували й ображали співрозмовника? (Пам'ятайте, що імен називати не треба – достатньо обговорити дії).

Як ви думаєте, чи можуть деякі діти ображати й залякувати інших тільки тому, що дорослі показують їм саме такий приклад?

Висновки

Те, як ви та ваші друзі ставитесь одне до одного в мережі, матиме великий вплив на цифровий світ майбутнього. Як ви думаєте, чи зможе ваше покоління збудувати Інтернет, який буде добрішим і приязнішим за сьогоднішній?

Багато дорослих думають, що вам це вдасться набагато краще за них…



Сумніваєтеся? Спитайте!

Короткий огляд того, як навчити дітей не боятися звертатися по допомогу

Огляд

У цьому посібнику ми регулярно згадували одну пораду, яка насправді стосується будь-яких дій в Інтернеті: "Якщо ви побачите щось підозріле, поговоріть про це з дорослим, якому довіряєте". Цьому потрібно вчити на всіх уроках, але для зручності нижче наведено перелік ситуацій, у яких учням необхідно звертатися по допомогу.

Учням слід звертатися по допомогу до дорослого, якому довіряють, в будь-якій ситуації, яка викликає в них острах або сумнів. Далі наведено кілька таких поширених ситуацій:

- Учень підозрює, що його обліковий запис зламано (з цього приводу варто провести обговорення на тему "Як забезпечити надійніший захист облікового запису?". Деталі наведено на стор. 29-30).
- Учень забув пароль і потребує допомоги дорослого.
- Учень підозрює, що його намагаються ошукати або він уже став жертвою шахрайства (з цього приводу варто провести обговорення на тему "Які тривожні дзвіночки можуть свідчити про шахрайство?". Деталі наведено на стор. 16-17).
- Хтось у мережі заводить розмову на некомфортні для учня теми.
- Незнайома людина надсилає учню підозріле повідомлення.
- Учень хоче поговорити про доброзичливість і агресію в Інтернеті.
- Учень боїться, що опублікував в Інтернеті інформацію, яку не варто було розкривати.

Ваша місія як учителя – стимулювати відкритий діалог у класі та бути завжди готовими підтримати своїх учнів. Діти мають знати, що ви на їхньому боці. Для виховання культури безпечної поведінки в Інтернеті особливо ефективні такі форми навчання, як дискусії й робота в групах (особливо якщо учні вже достатньо дорослі).