

Обачність

Пильність

Захист

Доброзичливість

Сміливість

Представляємо вашій увазі навчальний посібник із безпеки дітей в Інтернеті, розроблений компанією Google у співробітництві з організаціями The Net Safety Collaborative та Internet Keep Safe Coalition. Цей посібник створено для того, щоб допомогти вчителям навчити дітей необхідним навичкам, завдяки яким вони зможуть користуватись Інтернетом безпечно й обачно.

Цього року ми додали до навчального посібника 10 нових занять. У співпраці з неприбутковою організацією Committee for Children ми створили нові соціально-емоційні навчальні заняття, які допоможуть дітям у подорожах цифровим світом. Крім того, ми додали нові уроки, присвячені навичкам пошуку, та оновили заняття з безпеки й захисту відповідно до потреб сучасного цифрового світу. Ми також класифікували заняття за певними рівнями (класами), врахувавши широкий спектр етапів розвитку дитини.

Посібник із безпеки дітей в Інтернеті було оцінено Науковим центром «Злочини проти дітей» Університету Нью-Гемпшир. За результатами дослідження, проведеного центром, це перший посібник із безпеки дітей в Інтернеті, який має доведений позитивний вплив на навчання дітей темам безпеки в мережі та цифрового громадянства.

Посібник із безпеки дітей в Інтернеті є самодостатнім ресурсом. Усі практичні завдання можна виконувати без спеціальних професійних навичок, з мінімальною підготовкою до занять та без спеціального обладнання чи інших ресурсів для навчання. Крім того, матеріал, пройдений на уроках, можна весело й цікаво закріпити на практиці завдяки пригодницькій онлайн-грі Interland.

Посібник охоплює п'ять фундаментальних тем щодо цифрового громадянства та безпеки:

- **Діліся з обачністю.** Цифровий слід і відповідальне спілкування
- **Не дай себе обманути.** Фішинг, шахрайство та надійні джерела
- **Бережи свої таємниці.** Безпека в Інтернеті та паролі
- **Круто бути доброзичливим!** Боротьба з негативною поведінкою в Інтернеті
- **Сумніваєшся? Спитай!** Сумнівний контент та сценарії

Цей посібник створено для 2–6 класів, однак уроки стануть у пригоді вчителям як старших, так і молодших дітей, зокрема розділи, присвячені термінам, обговоренням у класах та іграм. Радимо вам експериментувати та підібрати програму, що найкраще підходить для ваших учнів. Наприклад, ви можете пройти всю програму від початку до кінця або зосередитися на кількох уроках, які найбільше потрібні вашим учням. Додатково ви можете скористатися ресурсами для вчителів та батьків: готовими слайдами, роздруковками, посібником та порадами для сім'ї, які можна застосовувати вдома.

Міжнародна спілка International Society for Technology in Education (ISTE) провела незалежний аудит посібника з безпеки дітей в Інтернеті та визнала його ресурсом, що допомагає підготувати учнів на рівні Стандартів ISTE 2021, а також відзначила грифом матеріалів підготовчого рівня (Seal of Alignment for Readiness).



Зміст

Інструкції для вчителів

Ресурс 1 Викладання навчальної програми.....	4
Ресурс 2 Словникові вправи	
Ресурс 3 Шаблон ознайомчого листа/електронного листа для батьків	
Ресурс 4 Поширені запитання	

Ділися з обачністю Модуль 1

Урок 1 Чи вмієте ви зберігати таємниці?	12
Урок 2 Конфіденційність на практиці	
Урок 3 Я не це маю на увазі!	
Урок 4 Правильне формулювання	
Урок 5 Хто взагалі ця людина?	
Урок 6 Як інші нас бачать в Інтернеті?	
Урок 7 Interland. Уважна гора	

Не дай себе обманути Модуль 2

Урок 1 Спливаючі вікна, підроблені облікові записи та інші шахрайські дії	35
Урок 2 Хто це зі мною «розмовляє»?	
Урок 3 Це дійсно правда?	
Урок 4 Виявлення недостовірної інформації в мережі	
Урок 5 Якби ми були пошуковою системою	
Урок 6 Практика з пошуку в Інтернеті	
Урок 7 Interland. Річка реальності	

Бережи свої таємниці Модуль 3

Урок 1 Це був не я!.....	72
Урок 2 Як створити надійний пароль	
Урок 3 Як керувати налаштуваннями конфіденційності	
Урок 4 Interland. Вежа зі скарбами	

Круто бути доброзичливим! Модуль 4

Урок 1.1 Звертаємо увагу на почуття.....	85
Урок 1.2 Практикум з емпатії	
Урок 2.1 Трішечки доброти Урок	
2.2 Як проявити доброту	
Урок 3 Від негативу до доброзичливості	
Урок 4 Тон має значення	
Урок 5 Як слова можуть змінити загальну картину	
Урок 6 Interland. Королівство доброти	

Сумніваєшся? Спитай! Модуль 5

Урок 1 Що означає бути сміливою людиною?.....	113
Урок 2 Від байдужості до допомоги	
Урок 3 Помічники мають варіанти!	
Урок 4.1 Коли ви бачите щось, що вас засмучує: що робити?	
Урок 4.2 Коли вас щось засмучує в Інтернеті: що робити?	
Урок 5.1 Що робити з недоброзичливим контентом	
Урок 5.2 Як поводитися, якщо ви стикнулися з ворожою поведінкою в Інтернеті	
Урок 6 Коли треба звернутися по допомогу	
Урок 7 Повідомте про порушення онлайн	

Викладання навчальної програми

Навчальна програма в цьому посібнику досить гнучка, тому ви легко можете адаптувати її в класі до потреб вашої групи учнів. Радимо підлаштовувати уроки відповідно до вашого розкладу занять і готовності ваших учнів. Наприклад, ми можемо порадити провести практичне заняття з усім класом, але ви краще знаєте своїх учнів і можете відчувати, що це заняття було б краще провести в невеликих групах.

Проводьте заняття так, як, на вашу думку, буде найкраще для учнів. Прислухайтесь до свого вчительського досвіду!

Стисло про навчальну програму:

1. Кожен модуль містить список словникових слів, які зустрічатимуться в уроках. Цей список можна роздрукувати та видати учням. Обов'язково перегляньте **Словникові вправи** на наступних сторінках!

2. Кожен із 5 модулів містить різну кількість уроків.

Кожен урок має таку структуру:

- ✓ **Цілі для учнів**
- ✓ **Обговорення** — довідкова інформація для вчителів, написана мовою, зрозумілою для учнів (якщо ви просто хочете зачитати їх своїм учням).
- ✓ **Практичне завдання** — деякі завдання можуть мати різні варіанти адаптації відповідно до класу.
- ✓ **Висновки** — підсумок змісту уроку та можливість для роздумів.

3. Поруч із кожною назвою уроку є символ, який позначає, для яких класів рекомендовано цей урок. Якщо це урок із медіаграмотності та/або соціально-емоційне навчальне заняття, ви побачите відповідний символ.

2-6

2-6
класи

2-3

2-3
класи

4-6

4-6
класи

ML

Медіаграмотність

SEL

Соціально-емоційне
навчальне заняття

4. Цей навчальний посібник розроблено таким чином, щоб ви могли викладати програму будь-яким із двох способів: у порядку розташування уроків або в порядку, який відповідає потребам у навчанні цифровій грамотності ваших учнів. Модулі розташовані в порядку, у якому можна вивчати теми з нуля, але багато учнів початкових класів уже знають певну інформацію з цієї області, тож запитайте в них, що саме їх цікавить і які навички вони хочуть розвивати. Для початку було б чудово обговорити з ними, що вони знають, а чого не знають. Бажаємо успіхів в опануванні програми безпеки дітей в Інтернеті разом!

Словникові вправи

Терміни, які використовуються в цих заняттях, наведені на початку кожного модуля.

Розкажи мені більше



Необхідні матеріали

- Дошка, щоб записувати слова зі словника (грифельна дошка, ватман, магнітна дошка тощо)

Інструкції

1. Учні розбиваються по парах.
2. Учень 1 повертається спиною до дошки (учні можуть сидіти або стояти).
3. Учитель показує на дошці від трьох до п'яти слів зі словника.
4. Учень 2 дивиться на дошку та пояснює перше слово зі словника Учні 1, **не називаючи самого слова**.
5. Учень 1 намагається вгадати словникове слово.
6. Як тільки Учень 1 правильно вгадає перше словникове слово, Учень 2 переходить до пояснення наступного слова.
7. Продовжуйте кроки 3–6, доки Учень 1 правильно не вгадає всі слова на дошці.
8. У наступному раунді Учні 1 та 2 міняються місцями. Повторіть заняття з новими словами зі словника.

Бінго



Необхідні матеріали

- Роздатковий матеріал: Картки бінго зі словниковими словами з посібника
- Ігрові фішки (усе, що можна використати для позначення слів — маленькі кубики, скріпки, квасолини тощо)

Інструкції

1. Роздайте картки бінго (оберіть картки 5 x 5 або 3 x 3) та ігрові фішки кожному учню.
2. Учні заповнюють картки бінго словниковими словами із заданого модуля.
3. Учитель зачитує **визначення** словникового слова. *Учитель може випадковим чином вибрати визначення зі списку словникових слів модуля.*
4. Учні шукають, чи є слово, яке відповідає визначенню, на їхніх картках та кладуть на нього ігрову фішку.
5. Учень може вигукнути «Бінго!», коли у кожному полі рядка, стовпчика чи діагоналі буде ігрова фішка.
6. Продовжуйте грати з виданими картками бінго або попросіть учнів зняти всі ігрові фішки та зіграти знову.

Мережа слів



Необхідні матеріали

- Роздатковий матеріал: Мережа слів (сторінка 8)

Інструкції

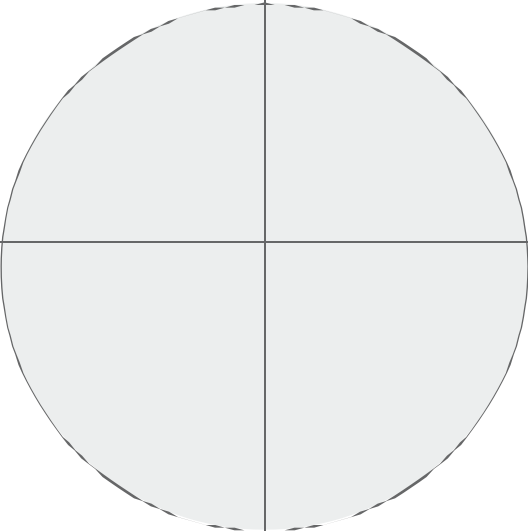
1. Учні розбиваються по парах.
2. Роздайте матеріали **Мережі слів** кожній групі (учні також можуть намалювати мережу слів самостійно на папері).
3. Учні пишуть одне слово зі словника в колі на роздатковому матеріалі. Цей крок можна реалізувати трьома різними способами:
 - призначте те саме слово для всіх груп учнів;
 - призначте кожній групі своє слово;
 - учні самі вибирають словникові слова зі списку модуля.
4. Потім учні в парах заповнюють роздатковий матеріал.
5. Після заповнення можна доповнити вправу таким чином:
 - учні заповнюють іншу картку мережі слів для нового слова зі словника;
 - зберіть заповнені роздаткові матеріали та розмістіть їх у класі на стіні;
 - проведіть прогулянку, як по галереї, щоб учні розглянули картки мережі слів своїх однокласників.

Картка бінго (5 x 5)

Картка бінго (3 x 3)

Мережа слів

Визначення	Характеристики
Приклади	Не є прикладом



Шаблон ознайомчого листа/електронного листа для батьків

Нижче наведено шаблон листа, який можна надіслати електронною чи звичайною поштою батькам учнів, щоб ознайомити їх із програмою з безпеки дітей в Інтернеті, яка допоможе їхнім дітям навчитися поводитися безпечно та обачно в цифровому світі. Вміст листа за потреби можна змінювати.



Шановні батьки!

Коли наші діти ще маленькі, ми робимо все можливе, щоб допомогти їм отримати якомога більше користі від Інтернету, при цьому дбаючи про їхню безпеку онлайн. Коли діти стають підлітками, наша роль змінюється — ми маємо допомогти їм навчитися безпечно та обачно орієнтуватися в цифровій частині свого життя.

У [назва школи] ми віримо, що завдяки співпраці з батьками ми можемо підготувати наших учнів [клас] класу та навчити їх:

- критично мислити й оцінювати додатки, веб-сайти та інший цифровий контент;
- захищатися від інтернет-загроз, у тому числі від цькування та шахрайства;
- ділитися з обачністю й розуміти, чим, коли, як та з ким це можна робити;
- бути добрими та ввічливими до інших людей в Інтернеті, у тому числі поважати їх приватність;
- просити про допомогу в складних ситуаціях у батьків або інших дорослих, яким вони довіряють.

Цього року ми викладатимемо комплексну навчальну програму безпеки дітей в Інтернеті, щоб дати дітям навички, необхідні для того, щоб дбати про свою безпеку в мережі Інтернет. Одним із ресурсів програми є браузерна гра Interland, яка допомагає навчатися в інтерактивному й цікавому форматі. У цю гру також можна грати вдома (ваша дитина зможе показати вам, як це робиться). Програма безпеки дітей в Інтернеті розроблялася компанією Google разом із викладачами, дослідниками та експертами з питань інтернет-безпеки з організацій The Net Safety Collaborative та iKeepSafe.org. Це веселе навчання, що відповідає віку дітей і побудоване на базі п'яти основних уроків:

- Ділися з обачністю
- Не дай себе обманути
- Бережи свої таємниці
- Круто бути доброзичливим
- Сумніваєшся? Спитай!

Обачне та безпечне використання технологій може мотивувати учнів навчатися самостійно та зробити заняття в класі ще ефективнішими. Ми віримо, що ця програма стане важливим кроком у досягненні нашої мети — зробити так, щоб усі учні [назва школи] навчались, досліджували та залишались у безпеці в Інтернеті як у школі, так і за її межами.

Ми будемо раді поділитися додатковою інформацією про цю нову програму й ознайомити вас із деякими ресурсами, які ваша дитина почне використовувати в класі, а також пропонуємо вам переглянути супутні ресурси програми на сайті [g.co/BeInternetAwesome](https://www.google.com/BeInternetAwesome). Радимо вам запитати свою дитину про те, що вона вивчає; і хто знає, можливо, ви також дізнаєтеся для себе щось нове та корисне про конфіденційність і безпеку!

З повагою, [Ваше ім'я]

Поширені запитання

Чи потрібно пройти з учнями весь урок, перш ніж вони зможуть грати в Interland?

Ні, але це може бути корисно. Гра приносить найбільшу користь тоді, коли вона закріплює вивчену навчальну програму. А ще буде цікавіше, якщо учні матимуть нагоду обговорити тему з вами до того, як почнуть грати.

Чи потрібні учням облікові записи Google, щоб займатися за цією навчальною програмою?

Ні! Посібник із безпеки в Інтернеті доступний кожному, хто заходить на сайт. Оскільки Google не збирає жодних даних про учнів, для навчання за програмою не потрібні імена користувачів, паролі чи електронні адреси.

На яких пристроях можна грати в Interland?

Interland працює на будь-якому пристрої, який має підключення до Інтернету та веб-браузер. Це означає, що майже будь-який комп'ютер, ноутбук, планшет або мобільний телефон підходить для занять за цією навчальною програмою.

Де можна ознайомитися з основними ресурсами програми?

- Сайт програми безпеки дітей в Інтернеті: g.co/BeInternetAwesome.
- Гра Interland: g.co/Interland.
- Посібник із безпеки дітей в Інтернеті: g.co/BeInternetAwesomeEducators.
- Ресурси для сім'ї: g.co/BeInternetAwesomeFamilies.

Чи потрібно мені пройти спеціальний тренінг або чи маю я бути вчителем певної спеціалізації, щоб навчати цій програмі?

- По-перше: будь-який учитель, від дошкільної освіти до старших класів, може викладати цю програму для своїх учнів.
- По-друге: кожен учитель — особливий. :)
- По-третє: уроки передбачають веселу, розслаблену двосторонню взаємодію між учителем і учнями; в ідеалі це має бути неупереджене активне слухання з боку вчителя.

Для якого класу найкраще підходить програма безпеки дітей в Інтернеті? Повна програма, що включає навчальні матеріали, гру та ресурси на веб-сайті, була розроблена для учнів 2–6 класів (7–12 років). Однак залежно від того, як викладачі адаптують навчальну програму, її теми можуть бути корисними для будь-якого класу.

Як діти вчать за допомогою гри?

Гра в безпечному навчальному середовищі закріплює концепції навчальної програми, допомагаючи дітям у формі гри навчитися правильно поводитися в цифровому світі та зрозуміти, як пов'язані дії в цифровому просторі (і їх наслідки).

Чи можна кожен урок використовувати в Google Classroom?

Так, так, і ще раз так. Ви можете призначати гру Interland як заняття для певних класів або груп чи зробити її доступною для всіх своїх учнів.

Чи є спільна папка або веб-сайт із роздатковими матеріалами для вправ, які можна було б вивести на дошку через проєктор?

Так, у формі презентацій. Разом із Pear Deck ми зробили уроки доступними також на слайдах, щоб їх було зручніше презентувати, розповсюджувати та надсилати. Їх можна знайти тут: g.co/BeInternetAwesomeEducators.

Чи потрібно мені бути експертом із питань цифрового громадянства, щоб викладати за цим посібником?

Зовсім ні. Посібник розроблено таким чином, щоб кожен учитель міг викладати програму у своєму класі. Крім того, якщо вам цікаво дізнатися більше про цифрову безпеку та громадянство, ви можете пройти наш онлайн-курс для вчителів за цим посиланням: g.co/OnlineSafetyEduTraining.

Чи узгоджується навчальна програма безпеки дітей в Інтернеті з будь-якими національними стандартами?

Чудове питання. Так. Навчальна програма узгоджується як зі стандартами ISTE (Міжнародна спілка з використання технічних засобів у сфері освіти), так і зі стандартами AASL (Американська асоціація шкільних бібліотекарів).

Чи можуть мої учні зберегти свій прогрес у грі Interland?

Не в поточній версії, і це, швидше за все, не зміниться. У рамках програми безпеки дітей в Інтернеті не зберігається жодна персональна інформація. Це стосується і файлів зберігання. На те є вагомі причини: ми не збираємо дані учнів і хочемо, щоб гра була доступна кожному, тому не обов'язково створювати обліковий запис, ім'я користувача чи пароль.

Це добре, але багато моїх учнів пишуться тим, що пройшли гру, і тим, що вони дізналися.

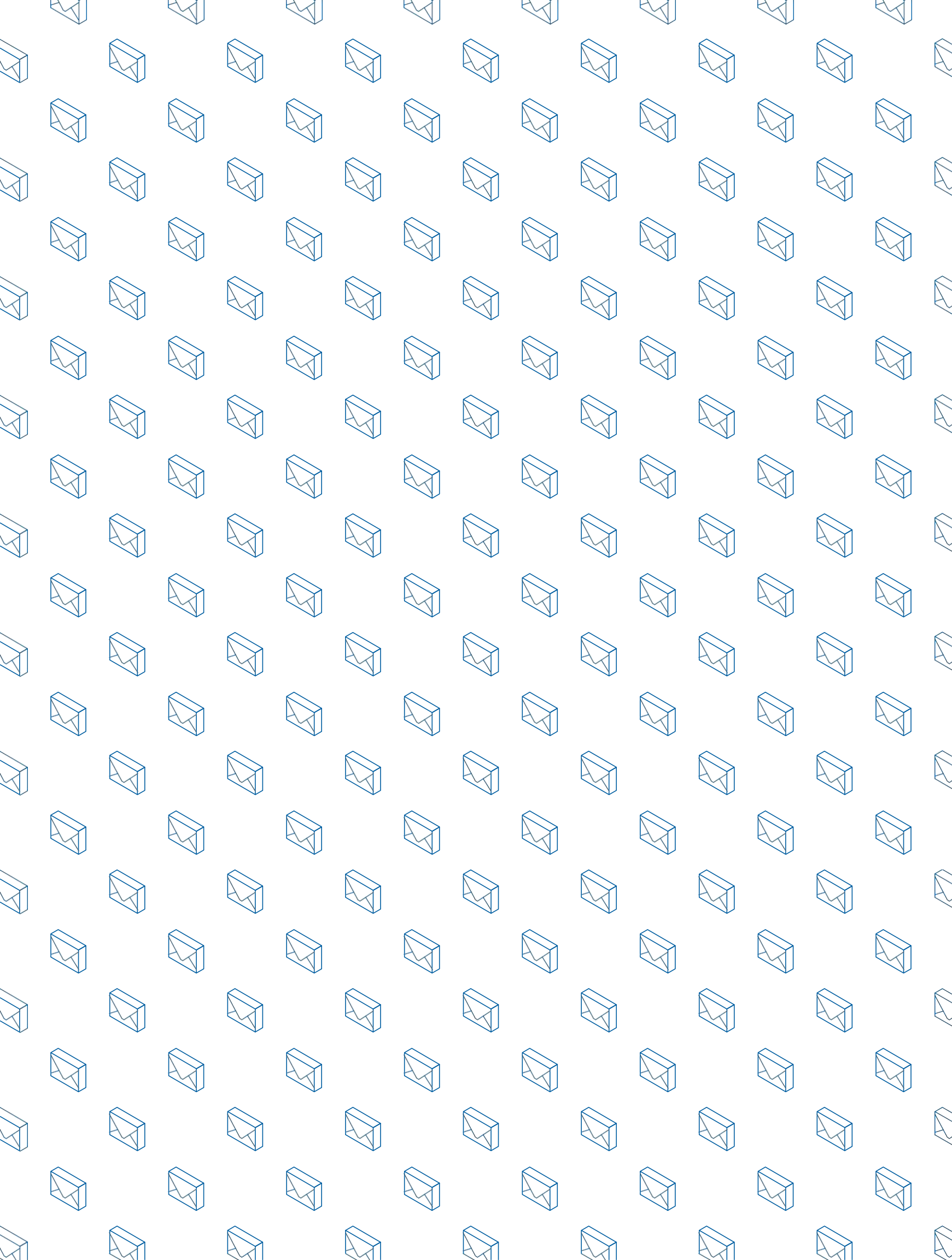
Ми це розуміємо й тому створили сертифікат про завершення курсу. Шаблон сертифіката можна заповнити, роздрукувати та вручити кожному учню або учениці, які пройшли курс.

Де я можу знайти інші матеріали для вчителів?

Усі матеріали програми безпеки дітей в Інтернеті можна знайти на цій сторінці: g.co/BeInternetAwesomeEducators.

Чи є онлайн-спільнота людей, які використовують цю програму, діляться ідеями чи шукають допомоги?

Так! (І це нам дуже подобається.) Ми часто ділимося ідеями та спілкуємось з учителями у Твіттері. Підписуйтеся на нас, щоб дізнатися більше про програму безпеки дітей в Інтернеті та поспілкуватись на інші теми: @GoogleForEdu.



Ділися з обачністю

Як захистити себе, свою інформацію та конфіденційність в Інтернеті

Огляд уроку	Урок 1	Чи вмієте ви зберігати таємниці?		2–6 класи
	Урок 2	Конфіденційність на практиці		2–6 класи
	Урок 3	Я не це маю на увазі!	ML	2–6 класи
	Урок 4	Правильне формулювання	ML	2–6 класи
	Урок 5	Хто взагалі ця людина?		2–6 класи
	Урок 6	Як інші нас бачать в Інтернеті?		2–6 класи
	Урок 7	Interland. Уважна гора		2–6 класи

Теми

Учителі й батьки знають, як необачні дії в мережі можуть вплинути на репутацію в майбутньому. Однак дітям важко пояснити, що нібито цілком невинний допис колись можуть побачити та неправильно зрозуміти люди, для яких він не призначався.

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

Цілі для учнів

- ✓ **Навчитися** створювати та підтримувати позитивну репутацію як у мережі, так і в реальному житті.
- ✓ **Навчитися** поважати конфіденційність і межі приватного життя інших.
- ✓ **Навчитися** розуміти можливі наслідки необачних дій у мережі.
- ✓ **Навчитися** звертатися по допомогу до дорослих у делікатних ситуаціях.

Застосовні стандарти

Стандарти ISTE для вчителів: 1a, 1b, 2a, 2c, 3b, 3c, 3d, 4b, 4d, 5a, 6a, 6b, 6d, 7a

Стандарти ISTE для учнів: 1c, 1d, 2a, 2b, 2d, 3b, 3d

Навчальні стандарти AASL: I.a.1, I.b.1, I.c.1, I.d.3, I.d.4, II.a.2, II.b.1, II.b.2, II.b.3, II.c.1, II.c.2, d.2., III.a.1, III.a.2, III.a.3, III.b.1, III.c.1, III.c.2, III.d.1, III.d.2, IV.a.1, IV.a.2, V.a.2, VI.a.1, VI.a.2, VI.a.3

Ділися з обачністю Словник

Уроки 1 і 2

Конфіденційність в Інтернеті. Широкий термін, який зазвичай означає можливість контролювати, яку інформацією про себе ви розміщуєте в мережі та хто може її бачити й ділитися нею.

Особиста інформація. Особистою (або конфіденційною) вважається інформація, яка вас ідентифікує — наприклад, ваші ім'я та прізвище, адреса, номер телефону, номер соціального страхування, електронна адреса тощо. Краще за все не ділитися такою інформацією в мережі.

Репутація. Ідеї, думки, враження чи переконання, які мають про вас інші люди. Ви не можете знати напевно, яку маєте репутацію, але зазвичай хочете, щоб вона була позитивною й гарною.

Урок 3

Код. Слово чи фраза, зображення (наприклад, логотип чи смайлик) або інший символ чи набір символів, що представляють певне значення або повідомлення. Іноді це секретний код, який розуміють лише певні люди; часто це просто символ, який означає щось, що розуміють майже всі.

Контекст. Інформація, яка оточує повідомлення, або щось, що ми бачимо, що допомагає нам зрозуміти його. Контекстом може бути місце, де розміщене повідомлення, час, коли воно з'явилося, або особа, від якої воно надійшло.

Тлумачення. Те, як людина розуміє повідомлення, або значення, яке вона від нього отримує.

Представлення. Фото, символ або опис, що багато говорить (або відображає правду) про особу або групу.

Урок 4

Кадр. Коли ви робите фотографію або відео пейзажу, людини чи об'єкта, кадром буде те, що зможе бачити глядач. Те, що ви вирішите залишити поза кадром, ваш глядач не зможе побачити.

Уроки 5 і 6

Припущення. Те, що ви або інші люди вважаєте правдою про когось або щось, але немає жодних доказів того, що це правда.

Ретельно добирати. Вирішувати, що розміщувати в мережі (текст, фотографії, звуки, ілюстрації чи відео), і думати про те, як це може вплинути на людей, які це побачать, або що вони можуть про вас подумати.

Цифровий слід (або цифрова присутність).

Це всі дії людини в Інтернеті, з яких складається її електронний портрет. Коли ви публікуєте фотографії, аудіозаписи, відео, текстові повідомлення, дописи в блозі чи пишете щось на сторінках друзів, то залишаєте в мережі так званий слід.

Факт. Щось, що є насправді дійсним або правдивість чого можна довести.

Думка. Те, що ви чи інші люди думаєте про когось або щось. Це не обов'язково є фактом, оскільки думку неможливо довести.

Урок 7

Надмірна відвертість. Коли ви забагато ділитесь інформацією в мережі. Зазвичай це означає повідомляти забагато особистого або просто забагато говорити про себе в певній ситуації чи розмові в мережі.

Чи вмієте ви зберігати таємниці?

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

Інформація про урок. Це базовий урок, присвячений конфіденційності в мережі для людей різного віку. Цей урок про те, що майже неможливо забрати назад те, чим ви поділилися, або контролювати, хто побачить цей контент та як надовго він буде видимий у мережі. Корисно буде спочатку запитати в учнів, які технології вони використовують, а потім згадувати ці додатки чи пристрої під час виконання завдання. Якщо ви не знайомі з цими додатками й пристроями, не проблема! Вашим учням, скоріш за все, сподобається, якщо ви попросите їх допомогти вам із цим.

Цілі для учнів



- ✓ Зрозуміти, яку особисту інформацію слід зберігати в таємниці і чому.
- ✓ Запам'ятати, що кожен має право на збереження своїх таємниць.

Обговорення



Чому конфіденційність має таке велике значення?

Завдяки Інтернету тепер дуже легко спілкуватися з родиною, друзями — з будь-ким. Ми надсилаємо повідомлення, ділимося фотографіями, приєднуємося до чатів та прямих трансляцій, та часто не замислюємося про те, хто їх може побачити просто зараз або колись у майбутньому. 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. Чийсь почуття можуть постраждати. Людина, яка не зрозуміла жарту, може подумати, що ви злий лише тому, що не знайома з вами. Якщо щось з'явилося в мережі, забрати це назад буде важко, а люди зможуть копіювати, робити знімки екрана та надсилати цей контент іншим. Тож пам'ятайте:

- те, що ви публікуєте або чим ділитесь у мережі, може побачити хто завгодно;
- контент, опублікований у мережі, важко або навіть неможливо видалити з неї назавжди — навіть якщо хтось просто зробить знімок екрана й поділиться ним з іншими (це як перманентний маркер: його дуже важко стерти);
- уся ця інформація про вас, яку бачать інші люди в Інтернеті та яку так важко видалити, — це і є ваша репутація (те, що люди думають про вас), тож краще вам контролювати те, чим ви ділитесь.

Ось чому так важливо піклуватися про свою конфіденційність. Щоб захистити її, публікуйте лише те, що вважаєте цілковито безпечним для себе та своєї репутації (інакше кажучи, ретельно думайте про те, що ви говорите, публікуєте або надсилаєте в Інтернеті).

Також добре знати, коли взагалі нічого не публікувати — не реагувати на чийсь пост, фото чи коментар; не писати щось, що може бути неправдою (навіть якщо це просто жарт); не бути занадто відвертим та не публікувати особисту інформацію. Є дуже гарна порада: «Перш ніж публікувати, подумай». Поважати

власну та чужу конфіденційність — це замислюватися над тим, що можна публікувати, хто може бачити те, що ви публікуєте, який вплив це може мати на вас та інших людей (завтра чи коли вам буде аж 16!), а коли взагалі краще нічого не розміщувати.

Нижче наведено деякі питання для подальшого обговорення (ці питання також можна дати учням додому для подальшого обговорення в сім'ї).

- Чому ніколи не слід розміщувати своє повне ім'я, адресу, номер телефону та іншу особисту інформацію в мережі?
- Коли можна ділитися фотографією чи відео когось іншого?
- Чи можна взагалі повідомляти чужу конфіденційну чи приватну інформацію — чому/чому ні? А якщо ви думаєте, що це жарт?
- Якщо близька вам людина публікує приватну інформацію, яка змушує вас думати, що ця людина в небезпеці — ви б розповіли про це комусь? Якщо так, то чи повинні ви сказати цій людині, що хвилюєтеся? Чи потрібно сказати їй, що ви думаєте про те, аби повідомити дорослого, який піклується про неї?

Практичне завдання



1. Вигадайте таємницю

Це має бути щось **вигадане**, а не ваш справжній секрет.

2. Розкажіть таємницю своєму партнеру

Розказали? Тепер розбийтеся на пари, обміняйтеся таємницями й обговоріть наведені далі запитання.

- Чи поділилися б ви з кимось цією таємницею?
- Якщо так, то з ким і чому?
- Як би ви почувались, якби хтось розповів усім вашу таємницю без вашого дозволу?

3. Розкажіть класу

Розкажіть класу, яка ваша вигадана таємниця, з ким ви нею поділилися б і чому. Клас може обговорити свої відповіді на запитання, наведені вище.

Висновки

Таємниці — один із багатьох різновидів особистої інформації, яку ми не розголошуємо в мережі та якою варто ділитися лише з найближчими рідними та друзями. Поділившись таємницею, ви більше не контролюєте, куди вона піде далі. Ось чому кажуть, що завжди слід подумати, перш ніж щось публікувати

(і це правда!). Інші види інформації, які ніколи не слід розміщувати в мережі:

- домашня адреса й номер телефону
- електронна пошта
- паролі
- повне ім'я та прізвище
- оцінки та домашнє завдання

Конфіденційність на практиці

Клас розглядає чотири сценарії й обговорює, як зберегти інформацію конфіденційною в кожному випадку.

Цілі для учнів



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

Обговорення



Практичні приклади: що робити?

Ознайомтеся з наведеними нижче прикладами, щоб дізнатися більше.

Практичне завдання



Розгляньмо п'ять практичних прикладів і поговоримо про те, якого рішення щодо конфіденційності вимагає кожен із них. Ми поділимося на чотири групи, обговоримо по одному прикладу в кожній групі, а потім усім класом обговоримо отримані висновки.

Необхідні матеріали

- Конспект для вчителя: «Конфіденційність на практиці»

Сценарії

Сценарій 1. Хтось сказав Дитині А, що корисно час від часу міняти паролі та коди входу на телефоні. Тому вона вирішує змінити свій пароль в улюбленій грі.

Найкращий друг Дитини А, Дитина Б, теж любить грати в цю гру, але не має власних даних для входу, тому Дитина Б грає в цю гру через ім'я та пароль для входу Дитини А. Дитина А ділиться новим паролем з Дитиною Б.

- Чи вчинила Дитина А правильно, змінивши пароль?
- Чи вчинила Дитина А правильно, коли дала свій пароль Дитині Б? Чому так або чому ні?

А якби Дитина А поділилася паролем для входу у свій обліковий запис соціальної мережі? Та сама відповідь? Та сама відповідь, якщо діти навчаються в школі та мають різних друзів?

Сценарій 2. Один з учнів веде щоденник. Ви дізнаєтесь, що друг знайшов його, коли вони ночували в нього вдома, і подумав, що буде дуже смішно, якщо він опублікує кілька уривків зі щоденника в мережі.

- Чи був друг неправий, розмістивши цю інформацію в мережі? Чи було це смішно? Чому так або чому ні?
- Як би ви почувалися, якби це був ваш щоденник?

Сценарій 3. Хтось написав на сторінці вашого друга в соціальній мережі:

«Гарного відпочинку!»

- Чи розповідав друг усім, що він збирається кудись їхати?
- Чи хотів він, щоб усі на світі про це дізналися? (Ну, можливо, не всі на світі, але хто знає.)
- Чи можна було побажати гарного відпочинку більш конфіденційним способом?

Сценарій 4. Ви знаєте, що один учень створив підроблений обліковий запис у соціальній мережі та видає себе за іншого учня так, щоб той виглядав погано.

- Чи має право учень, який став жертвою, знати про це? Чи ви б сказали йому про це?
- Важко з'ясувати, хто це зробив, але ви знаєте, хто це. Чи попросили б ви цього учня видалити підроблений профіль?
- Чи розповіли б ви про це вчителю чи іншому дорослому, якому довіряєте?

Сценарій 5. Діти у вашому домі по черзі використовують планшет вашої мами, тому всі знають пароль. У вашої сім'ї також є один обліковий запис для онлайн-покупок на одному веб-сайті. Усе було добре, поки одного разу до вашого брата не прийшов у гості друг, і вони через планшет вашої мами розглядали геймерські навушники на цьому сайті. Ваш брат пішов перекусити на кухню, а потім вони пішли на вулицю погуляти. Через кілька днів вам додому доставили посилку.

У ній були навушники. Ваш брат сказав, що не замовляв їх. Ви йому вірите.

- Ваші батьки, звичайно ж, запитують, як ці навушники потрапили у ваш дім. Що ви та ваш брат будете робити?
- А як щодо пароля? Чи бачите ви проблему в тому, що всі у вашій сім'ї використовують однакові паролі для сімейних пристроїв та облікових записів, якщо друзі також можуть користуватися цими пристроями та обліковими записами? Не хочете обговорити це зі своєю сім'єю?

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.

Конфіденційність на практиці

Примітка для вчителів. Цей аркуш допоможе вам провести обговорення в рамках цього уроку; він не є роздатковим матеріалом для учнів. Запишіть їхні правильні та/або найкращі відповіді на дошці та обговоріть.

Сценарій 1

- **Чи вчинила Дитина А правильно, змінивши пароль?**

Так, базовою рекомендацією щодо забезпечення конфіденційності є мати різні паролі для різних пристроїв та сервісів, а також змінювати їх принаймні раз на рік.

- **Чи вчинила Дитина А правильно, коли дала свій пароль Дитині В?**

Чому так або чому ні?

Ні. Ми знаємо, що діти часто діляться паролями з друзями, і вони мають знати, що це погано для конфіденційності та безпеки в мережі. Тут ви можете допомогти дітям назвати причини, чому саме це погано. Поставте їм таке запитання: «Чи можете ви придумати ситуацію, у якій ви б не хотіли, щоб хтось, крім дорослого, якому ви довіряєте, завжди знав би ваш пароль?»

Нижче кілька прикладів таких ситуацій.

- Іноді дружба закінчується і люди зляться. Чи хотіли б ви, щоб хтось, хто дуже злий на вас, мав змогу передати ваш пароль комусь іншому?
 - А якби ваш друг знав пароль від вашого телефона і увійшов у систему, прикинувшись вами, та заради жарту сказав би щось дивне чи образливе про когось, кого ви обидва знаєте? Це виглядало б так, ніби це сказали ви.
 - Якби ви поділилися своїм паролем з кимось, хто переїхав, чи хотіли б ви, щоб ця людина мала доступ до ваших облікових записів та приватної інформації назавжди?
 - Ви граєте в гру, а інший гравець просить ваш логін, щоб грати під виглядом вас. Чи повідомили б ви йому свій логін, навіть якщо це друг? Подумайте, що ви можете робити в цій грі та як він міг би робити у вашому обліковому записі все замість вас. Це нормально? Це буде нормальним наступного тижня чи наступного року?
- **А якби Дитина А поділилася паролем від свого облікового запису соціальної мережі? Та сама відповідь? Та сама відповідь, якщо вони навчаються в школі та мають різних друзів?**
 - Так, відповідь та сама, оскільки не можна давати паролі від будь-яких облікових записів друзям, навіть найближчим, оскільки, як вже говорилося в першому пункті вище, друзі змінюються; іноді друзі стають колишніми друзями, а вам не дуже захочеться відкривати свій обліковий запис чи профіль для когось, кому ви байдужі. Хтось може змінити вашу інформацію, виставити вас у поганому світлі або зробити так, ніби це ви пишете щось погане про когось іншого.

Сценарій 2

- **Чи був друг неправий, розмістивши цю інформацію в мережі? Чи було це смішно? Чому так або чому ні?**

Деякі учні можуть сказати, що це смішно, якщо те, чим він ділиться, смішне, тому заглибтеся в цю тему та поставте учням наступне запитання...

- **Як би ви почувалися, якби це був ваш щоденник?**

Сценарій 3

- **Чи розповідав друг усім, що він збирається кудись їхати?**

Якщо діти відповіли «так», тоді запитайте їх...

- **Чи хотів він, щоб усі на світі про це дізналися?**

Ні. (Ймовірно)

- **Чому ні?**

Наприклад: його сім'я, можливо, не хотіла повідомляти про своє місцеперебування або турбувалася про безпеку будинку, коли в ньому нікого немає.

- **Чи можна було побажати гарного відпочинку більш конфіденційним способом?**

Діти, скоріш за все, придумують кілька гарних відповідей, наприклад надіслати приватне повідомлення, SMS, зателефонувати тощо.

Сценарій 4

- **Чи має право учень, який став жертвою, знати про це? Чи ви б сказали йому про це?**

У вас буде власна відповідь на першу частину цього запитання, але було б цікаво почути відповіді учнів та обговорити, чи розповіли б вони жертві та що саме розповіли б.

- **Важко з'ясувати, хто це зробив, але ви знаєте, хто це. Чи попросили б ви цього учня видалити підроблений профіль?**

Не всім було б комфортно протистояти агресору, і це нормально. Запитайте клас, чи хтось міг би це зробити й чому. Подивіться, чи виникне дискусія між учнями.

- **Чи слід сказати про це вчителю чи іншому дорослому, якому ви довіряєте?** Так, якщо ніхто не скаже агресору припинити це або якщо хтось скаже про це, але він не видалить підроблений обліковий запис.

Допоможіть учням зрозуміти, що захищати інших від шкоди, у тому числі від переслідувань, соціального відчуження, знущання та цькування, дуже важливо. Це не означає «ябедничати».

Важливо розуміти, що це робиться для того, щоб захистити когось, а не завдати шкоди іншій людині.

- **Що може статися, якщо цього ніхто не зробить?**

Шкода, яку завдають іншій людині, не припиниться. Це гарний привід поговорити з класом про те, що турбуватися про інших важливо. Більше про це в розділі Доброзичливість в Інтернеті.

Сценарій 5

- **Ваші батьки, звичайно ж, запитають, як ці навушники потрапили у ваш дім. Що ви та ваш брат будете робити?**

Ваші учні можуть рефлексивно зосередитися на тому, що правильно і що неправильно робити та говорити. Це цілком нормально. Стисло обговоріть це та подивіться, чи досягнуть вони згоди в цьому питанні.

- **А як щодо пароля? Розкажіть мені, наскільки ризиковано те, що вся сім'я використовує однакові паролі для сімейних пристроїв та облікових записів.**

Учні мають подумати та обговорити наступне: 1) захист паролів сім'ї, коли приходять друзі, 2) чому важливо не ділитися сімейними паролями з друзями та іншими людьми за межами сім'ї та 3) які інші проблеми можуть виникнути, крім того, що друзі можуть замовляти щось через сімейні облікові записи.

Я не це маю на увазі!

Використовуючи лише смайлики, учні створюють футболки, щоб зобразити себе. У процесі вони дізнаються, що різні люди можуть по-різному тлумачити одне і те ж повідомлення.

Довідка для вчителів стосовно медійної грамотності. Коли ми одягаємо футболки з логотипами компаній, спортивних команд, шкіл, з музикантами, політиками тощо, ми, по суті, є ходячою рекламою. Це практичне заняття показує, що футболка є одночасно і прямим повідомленням, і носієм інформації. Це допоможе учням зрозуміти, що носії інформації — не тільки на екранах.

Цілі для учнів



- ✓ **Зрозуміти**, що важливо запитувати себе: як інші люди можуть по-іншому тлумачити це повідомлення?
- ✓ **Дізнатися** про те, як багато візуальних сигналів використовують люди для комунікації.
- ✓ **Переконатися**, що те, чим вони діляться в мережі, так само як і на футболці, є носієм інформації.
- ✓ **Дізнатися**, що означає «контекст» та «представлення».

Обговорення



Чи траплялося таке, що хтось колись неправильно зрозумів те, що ви сказали, зробили, написали чи розмістили в мережі? Вам довелося пояснювати, що ви мали на увазі зовсім інше, бо ця людина засмутилася або розізлилася?

Спілкуючись, зазвичай **ми** знаємо, що маємо на увазі, але люди, з якими ми спілкуємося, іноді цього не розуміють, особливо якщо ми не поруч один з одним. Це відбувається тому, що досвід людей впливає на те, як вони тлумачать зображення та слова.

Ще більше непорозуміння додає те, що існує багато повідомлень, які ми передаємо, навіть не підозрюючи про це. Ми говоримо людям, ким ми є, і судимо, ким є вони, використовуючи такі сигнали, як наш одяг, зачіска і навіть те, як ми ходимо або жестикулюємо. Це називається «представленням» — вираженням чогось про річ, особу чи групу шляхом використання зображень, символів, стилю та слів.

Ось приклад: якби ви побачили в мережі фото людини, одягненої у спортивний костюм із логотипом відомої команди, то ви, скоріш за все, подумали б, що ця людина є фанатом цієї команди (і, мабуть, мали б рацію). Це тому, що більшість із нас розпізнає дизайн спортивного одягу — ми знаємо, що це спортивний «код».

Тож навіть якщо ми не впевнені, яка команда має такий логотип, ми знаємо, що це, скоріш за все, спортивна команда.

А що як ви б побачили фото людини з трикутним шматком сиру на голові? Що б ви подумали про цю людину? Якщо ви живите у штаті Вісконсин або ви — футбольний фанат, то ви знаєте, що «сирна голова» — це прізвисько футбольних фанатів Green Bay Packers. Людина на фото одягла капелюх зі шматком сиру, щоб представити команду Packers.

Можливо, у вас навіть виникла б спокуса якось прокоментувати цей дивний капелюх. Це могло б розлютити фанів Packers. Для них ваш коментар грубий, і у них може виникнути спокуса також відповісти вам злим коментарем. Це, у свою чергу, розізлить вас і може викликати цілий потік негативних коментарів та ображених почуттів.

То як ми можемо бути впевнені, що інші люди зрозуміють, що ми маємо на увазі, розміщуючи повідомлення в мережі? Один із способів — уявляти, що ми створюємо контент, а не просто спілкуємося чи граємо в ігри. Щоразу, коли ми створюємо профіль у мережі, надсилаємо комусь повідомлення, залишаємо коментар в ігровому чаті або ділимося фото, ми створюємо контент. Як і всі успішні творці контенту, ми думаємо про те, який контент ми створюємо та яким контентом ділимося, тому робимо паузу, перш ніж щось опублікувати, і питаємо себе: «Чи може хтось не схожий на мене зрозуміти моє повідомлення якось інакше?»

Практичне завдання



Необхідні матеріали

- Роздатковий матеріал «Пуста футболка» (одна для кожного учня)
- Роздатковий матеріал «Табличка зі смайликами» (її можна вивести на екран через проектор або надрукувати й повісити так, щоб усі бачили)
- Маркери, кольорові олівці або воскові олівці для малювання
- Скотч (або щось інше, що допоможе закріпити малюнки на стіні)

1. Опишіть себе за допомогою смайлів

Щоб ми могли краще уявити себе вмілими творцями контенту, ми будемо прикрашати футболки. Використовуючи роздатковий матеріал у вигляді футболки, намалюйте своє представлення, використовуючи лише смайлики. Ви можете використовувати один, два або три смайли, але не більше. Ви можете скопіювати смайли з таблички або намалювати власні.

2. Покажіть і розкажіть

Розбийтеся на пари і спробуйте вгадати, про що говорять смайли на футболці вашого партнера. Чи вдалося вам точно вгадати, чи доводилося пояснювати один одному, що означає ваш вибір смайликів?

3. Дізнайтеся щось один про одного

Розвісьте «футболки» у класі, щоб усі могли подивитися на футболки інших. Чи можете ви точно сказати, яка футболка кому належить?

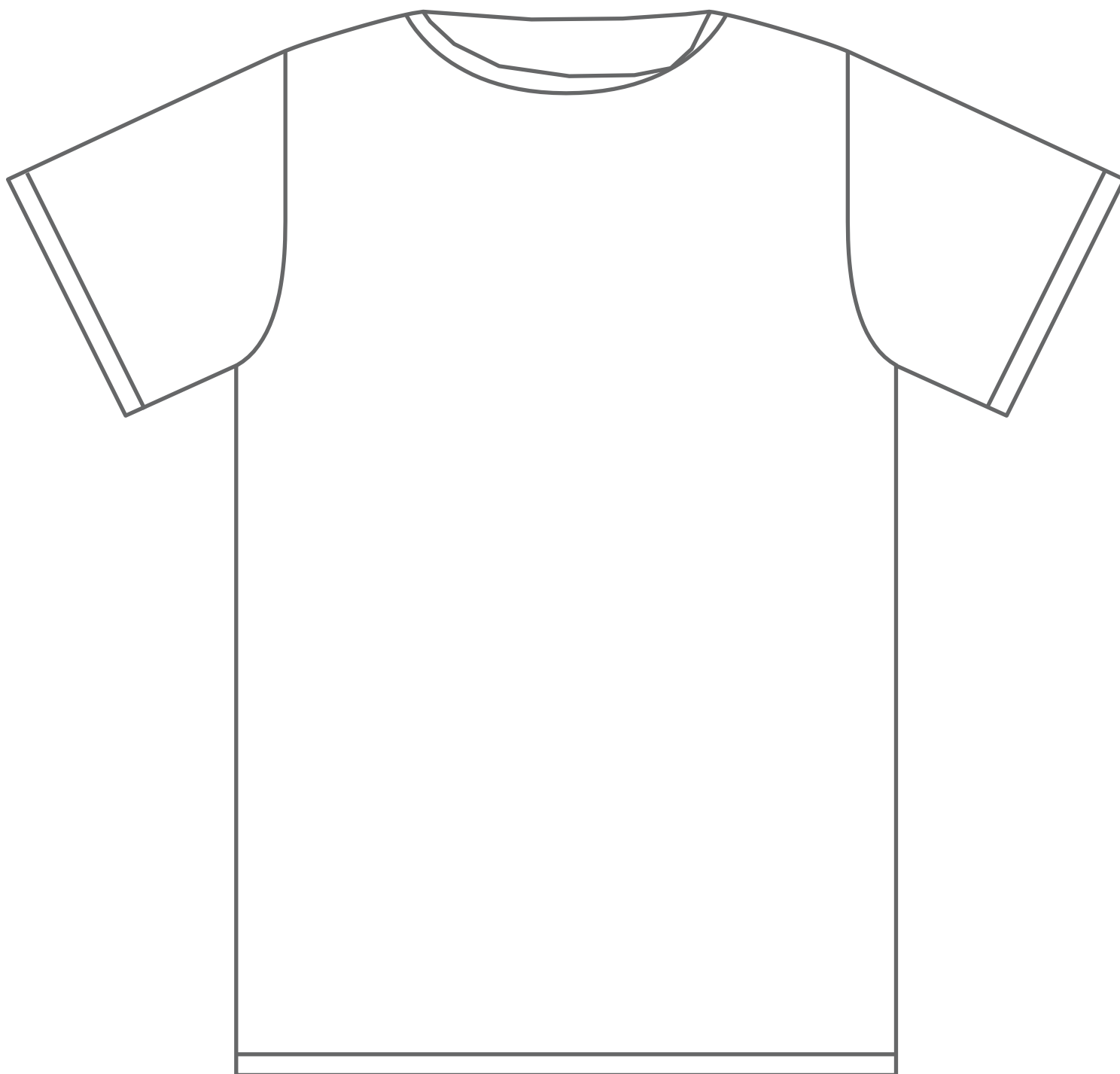
4. Обговоріть усім класом:

- Що допомогло, а що навпаки заважало зрозуміти, де чия футболка? Які символи на футболках було легко зіставити з учнями? Чи були смайли, які використовувало багато учнів? Чи були смайли, які використав лише один учень?
- Чи всі погодилися із значенням кожного смайла? Як контекст може змінити значення смайла? Подивіться на смайл руки з двома пальцями. Звідки ви знаєте, чи означає він мир, перемогу чи число 2? А як щодо смайла вогню? Чи означає він небезпеку/надзвичайну ситуацію? Справжню популярність чи успіх («Чувак, це вогонь!»)? Чи змінюється значення залежно від того, де з'являється смайлик (наприклад, смайлик із посмішкою на домашньому завданні може означати, що ваш учитель вважає, що ви добре попрацювали, але в текстовому повідомленні від друга цей смайл може означати, що він щасливий чи жартує)? Чи змінюється значення залежно від того, з якими іншими смайлами поєднується той чи інший смайл?

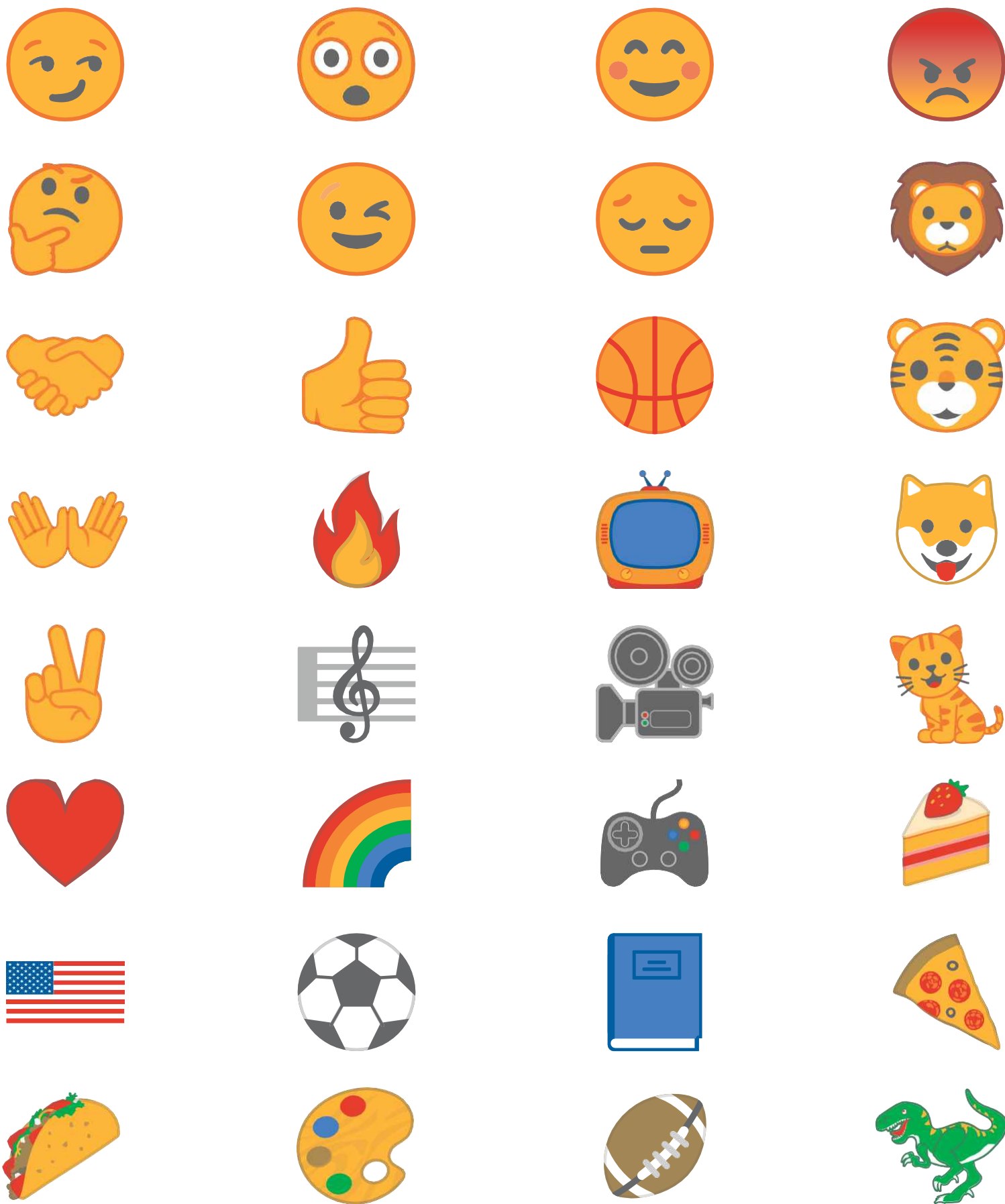
Висновки

«Чи може хтось не схожий на мене зрозуміти це якось інакше? Чи впевнений(-а) я в тому, що інші зрозуміють те, що я маю на увазі? Чи можуть вони зрозуміти це неправильно?» Так само потрібно запитувати себе про це, перш ніж самому щось коментувати. «Чи впевнений(-а) я в тому, що розумію те, що інші мають на увазі? Звідки я це можу знати?»

Пуста футболка



Табличка смайлів



Правильне формулювання

Довідка для вчителів. *Контент створюють люди, які роблять вибір. Основний вибір — це що залишити, а що прибрати. Цей урок допомагає учням подивитися на себе як на творців контенту, які приймають рішення, чим ділитися в мережі.*

Цілі для учнів



- ✓ **Уявити** себе творцем контенту.
- ✓ **Зрозуміти**, що люди, які створюють контент, роблять вибір, що показувати, а що залишити за кадром.
- ✓ **Використовувати** концепцію формування кадрів, щоб зрозуміти різницю між тим, що робити видимим та публічним, а що — конфіденційним чи невидимим.

Обговорення



Люди, які створюють візуальний контент, контролюють кількість інформації, якою вони бажають поділитися, через **формування кадру**. Вони вирішують, що включити **в кадр** (те, що ми можемо бачити), а що залишити **поза кадром** (невидимим).

Практичне завдання



Виконайте кожне завдання в класі, а потім обговоріть:

1. Формування кадрів

Увесь контент — результат цілого ряду вибору, який роблять його творці. Важливим вибором є те, що включити в кадр, а що залишити невидимим. Коли ми робимо фото чи відео, є те, що потрапляє в кадр, і те, що лишається поза кадром.

Щоб побачити, як це працює, візьміть індексну картку та виріжте прямокутник із центру, щоб зробити рамку.

Тримайте рамку на відстані витягнутої руки й повільно переміщуйте її в напрямку до обличчя та назад (це можна також спробувати зробити за допомогою функції наближення на камері).

На що ви звернули увагу, поки дивилися в середину рамки? А якщо рухати її зі сторони в сторону? Чи можна тримати рамку так, щоб бачити деяких зі своїх однокласників, а інших — ні, або деякі речі на стіні, а інші — ні?

Коли ви контролюєте, що буде в кадрі, ви — виробник цифрового контенту.

Ви маєте право вирішувати, що залишити, а що прибрати з кадру. Те, що ви вирішили залишити поза кадром, усе одно існує в реальному житті, але люди, які переглядають створений вами контент, не зможуть цього побачити.

2. Залишити в кадрі чи поза кадром?

Візьміть роздатковий матеріал і подивіться на малюнок 1А. Як ви думаєте, на що ви дивитесь і звідки ви це знаєте? А тепер подивіться на малюнок 1В. Як додаткова інформація допомагає вам краще зрозуміти, на що ви дивитесь?

Продовження на наступній сторінці →

Спробуйте ще раз із малюнком 2А. Як ви думаєте, що кидає тінь? Які ваші докази? Малюнок 2Б додає більше інформації. Чи правильним було ваше припущення?

3. Забагато інформації?

Додаткова інформація — це не завжди добре. Іноді вона відволікає увагу та не дає нам насолодитися меншим зображенням або правильно його зрозуміти. Погляньте на приклад №3 на роздатковому матеріалі.

Іноді цікаво спостерігати, як створюються ті чи інші речі. Але що було б, якби кожного разу, коли ви дивитесь фільм, телевізійну програму або відео, ви бачили б не лише маленький кадр, але камери, мікрофони, знімальну групу та край сцени? Думаєте, вам так само сподобався б сюжет?

4. Вирішуйте ви

Щоразу, коли ви ділитесь чимось у мережі, ви створюєте цифровий контент. Як і продюсери фільму, відео чи телевізійної програми, ви можете вирішити, що бачитимуть люди в кадрі, а що залишиться поза кадром.

Висновки

Створюючи цифровий контент, ви ніби накладаєте рамку навколо того, чим ділитесь в мережі, щоб інші люди бачили лише те, що ви хочете, щоб вони бачили.

Що в кадрі?



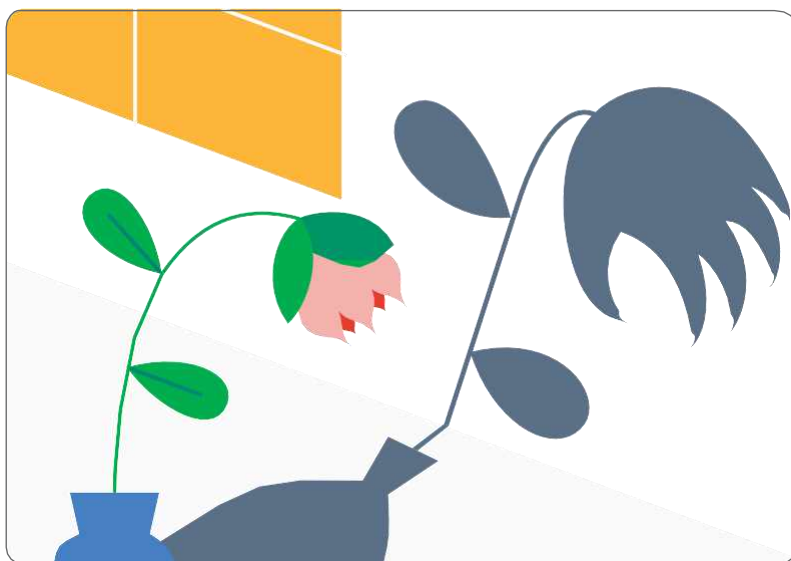
1А



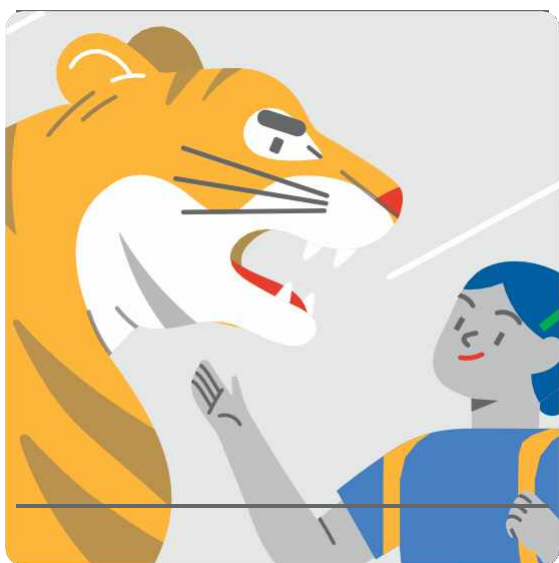
1Б



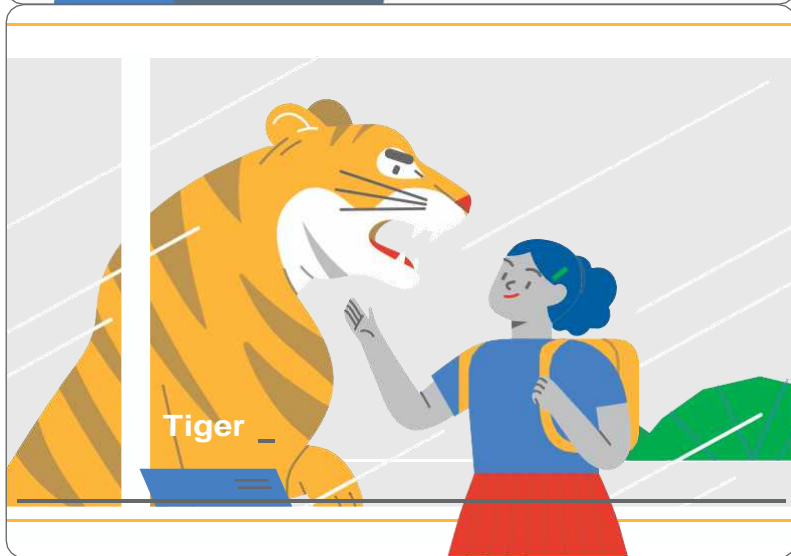
2А



2Б



3А



3Б

Хто взагалі ця людина?

У цьому уроці наведено приклади того, як насправді виглядає «цифровий слід».

Учні аналізуватимуть особисту інформацію вигаданих людей (частину їх цифрового сліду) і намагатимуться скласти про них уявлення.

Цілі для учнів



- ✓ **Визначити**, якими способами можна знайти в мережі інформацію про людину.
- ✓ **Поміркувати**, як на основі інформації, яку людина розміщує в мережі (тобто на основі її цифрового сліду), з'являються різні судження про неї.
- ✓ **Визначити** точність інформації й зрозуміти різницю між припущенням, думкою та фактом.

Обговорення



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

У мережі можна знайти багато особистих даних, і часом на їх підставі ми робимо не зовсім правильні припущення. Тож давайте обговоримо наведені далі запитання..

- Що можна дізнатися про людину на основі її особистої інформації або публікацій?
- Які припущення можна зробити про людину з її особистої інформації, навіть якщо ми в них не впевнені?
- Чи завжди ми знаємо, звідки з'явилася ця інформація? Як ми можемо визначити джерело?

Практичне завдання



Необхідні матеріали

- Аркуш із вправами: «Хто взагалі ця людина?» (один для кожного учня).

Можливі модифікації для 2-3 класів. Якщо ви вважаєте, що учні 2 або 3 класу готові говорити про «цифровий слід», можливо, вам стане в пригоді стратегія «Я роблю, ми робимо, ви робите» (де ви моделюєте перший приклад на аркуші, другий приклад виконуєте всім класом, а потім учні виконують завдання самостійно, після чого ви разом його обговорюєте).

1. Вивчіть людину

Усі мають прочитати інформацію про Кароліну, Лізу, Макса або вигаданого персонажа, якого учні створили самі.

2. Опишіть людину

Розділіться на групи, по одному персонажу на групу. Кожна група складає короткий опис цього персонажа, відповідаючи на запитання: «Як ви думаєте, хто ця людина?»

3. Прочитайте опис

Кожна група читає опис, який вона створила для свого персонажа.

4. З'ясуйте правду

Хто ж наші персонажі насправді? Давайте порівняємо надану інформацію з тим, що, на вашу думку, говорить про них інформація, яку вони розмістили:

- **Кароліна** — випускниця. Наступного року вона планує вступити в університет на факультет хімічної інженерії, а в майбутньому мріє започаткувати власну компанію. Її основні захоплення — це родина, волонтерство, поп-культура та мода.
- **Лізі** 15 років. Вона живе в Києві, ходить до школи й займається баскетболом. У неї є восьмирічна сестричка. Основні захоплення – баскетбол, мистецтво, гра на гітарі та спілкування з друзями.
- **Максу** 14 років. Він має двох котів і нещодавно приєднався до шкільної футбольної команди. У нього чудові інженерні здібності, і у вихідні він любить збирати роботів. Основні захоплення — це техніка й футбол, а ще тварини та захист їхніх прав.

5. Обговоріть

Наскільки близькі були ваші описи персонажів до фактів про них? Чому, на вашу думку, ви склали саме такі описи? Чи є ваші описи думками, припущеннями чи фактами? Поясніть чому. Що ви дізналися з цього уроку?

Висновки

Коли ми бачимо дописи, коментарі, фотографії та відео, які публікують інші люди, ми робимо щодо них припущення, які не завжди є правильними, особливо якщо ми не знаємо цих людей. Це тому, що в мережі або в певний момент часу ми лише частково бачимо, ким вони є і чим цікавляться. Також людина може лише прикидатися кимось, ким не є насправді, або виражати емоції, що відчуває лише в момент публікації. Ми не можемо насправді знати, хто ці люди і що насправді вони відчувають, доки не познайомимося з ними особисто — і навіть тоді потрібен час, щоб їх зрозуміти!

Хто взагалі ця людина?

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?


Кароліна


Ліза

Макс

Наклацала трохи фото зі шкільної дискотеки. Народ, ви всі красунчики!

Ми виграли! Ще один матч – і ми в національному турнірі. Треба ще трохи попрацювати над блокшотами.


 Царство бургерів


 5 секретних засобів, які назавжди позбавлять тебе від прищів


Ненавиджу шкільні дискотеки. #бойкот


Пропустив переможний гол, хай би йому грець. Добре, що хоч витягнули нічию.


Мій менший брат Алекс ТААК мене дратує. Може він прибулець?


 Національний науково-природничий музей

 25 неймовірно милих фото цуценят

 Київська лазертаг-арена

 Їду до Одеси на мій золотий день народження! Не можу дочекатися.


 Випуский фізико-математичного ліцею

 Конференція молодих хіміків в Університеті Томпсона

Збираюся грати в мяч з татом в Парку Партизанської Слави! Буде круто

Зацініть сайт мого друга! Це я його розробив.

НАРЕШТІ ПОДИВИЛАСЯ НОВИЙ ФІЛЬМ «ВІЙНИ ШПИГУНІВ». Це просто щось неймовірне!

 Мистецький ярмарок на Подолі

Новий рекорд!!! Тааак! Обожаю батуту!!!

Як інші нас бачать в Інтернеті?

Учні обговорюють, яке уявлення про персонажів із попереднього заняття склалося б у різних людей: батьків, роботодавців, друзів, поліцейських, або те, як елементи цифрового сліду можуть характеризувати їх.

Цілі для учнів



- ✓ **Зрозуміти** точку зору інших людей, вирішуючи, чи ділитися тією чи іншою інформацією в мережі.
- ✓ **Обміркувати** можливі наслідки оприлюднення особистої інформації (як те, чим ви поділилися, стає частиною вашого цифрового сліду) та її вплив на свою репутацію (часто незворотний).
- ✓ **Почати** думати про те, що означає ретельно добирати, що публікувати в мережі, та як це пов'язано із цифровим слідом.

Обговорення



Нова точка зору

Цифровий слід може розказати про людину набагато більше, ніж вона сама того хотіла. Ми розглянемо наслідки цього.

Давайте виберемо одного з цих персонажів та уявимо, що це ми розмістили ті коментарі. Ми будемо приміряти їхню точку зору.

- Як ви думаєте, чи хотів би ваш персонаж, щоб інші люди знали всю його особисту інформацію? Чому так або чому ні? Ваш персонаж хотів би, щось якись певні типи людей бачили (або не бачили) цю інформацію?
- Як, на вашу думку, інші люди **бачили б** цю інформацію?
- Як, на вашу думку, інші люди могли б використати цю інформацію?

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

Практичне завдання



Можливі модифікації для 2–3 класів. Якщо ви вважаєте, що учні 2 або 3 класу готові говорити про те, як їх бачать у соціальних мережах, спробуйте зменшити кількість різних точок зору. Наприклад, обговоріть, як би цю інформацію сприйняли їхні батьки, друзі, працівники органів правопорядку або вони самі через 10 років.

1. Розгляньте різні точки зору

Ми обійдемо клас і порахуємо від 1 до 3, а потім сформуємо три групи. Перша отримає профіль Кароліни, друга — Лізи, а третя — Макса. Потім учитель підходить до кожної групи та вдає із себе когось із перелічених нижче людей (зачитайте список). Група учнів має обговорити, як їхній персонаж сприйняв би те, як людина, якою прикидається вчитель, відреагувала б на інформацію в профілі. Як учитель ви будете грати роль батька/матері, працівника органів правопорядку, однолітка, іншого учня тощо та вдавати, як би вони відреагували на інформацію кожного персонажа (виберіть 2–3 ролі або запитайте групи, кого ви маєте вдавати). Коротко (не більше 2 хв на роль).

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

Необхідні матеріали

- Аркуш із вправами: «Хто взагалі ця людина?» з Уроку 5 (один для кожного учня).

Продовження на наступній сторінці →

2. Обговорення в групі

Протягом 5–10 хв кожна група обговорюватиме вибір, який робив їхній персонаж, реакцію людей, яких грав учитель, і те, як вони ставились до цих поглядів Кароліни, Лізи та Макса. Потім учитель просить кожену групу поділитися з усіма тим, що вони обговорили та що дізналися про конфіденційність і вибір у мережі.

3. Обговорення в класі

Які ваші 3 основні висновки з цього заняття? Чи різні люди, які бачили вашу інформацію в мережі, робили точні припущення щодо вас? Як ви думаєте, чи сформували вони про вас позитивну чи негативну думку? Чи були ви задоволені їхніми відгуками? Які, на вашу думку, можуть бути наслідки того, що хтось сформує про **вас** негативну думку на основі інформації, яку ви розміщуєте в мережі?

Знаючи, хто бачив вашу інформацію, чи ви б інакше добирали чи публікували її?

Висновки

Різні люди роблять із тієї самої інформації різні висновки. Інші люди в мережі можуть бачити вас не так, як ви самі себе бачите.

Interland: Уважна гора

Центр гірського містечка Інтерленд — це місце, де завжди багато людей та перетинаються всі стежки. Але ви повинні бути дуже обережними щодо того, якою інформацією ділитися та з ким. Інформація рухається зі швидкістю світла, а серед ваших знайомих інтернаутів є базікало, що розповідає забагато інформації.

Відкрийте на своєму комп'ютері або мобільному пристрої (наприклад, на планшеті) веб-переглядач і зайдіть на сайт g.co/MindfulMountain.

Теми для обговорення



Запропонуйте своїм учням зіграти в «Уважну гору» і, використовуючи наведені нижче запитання, проведіть обговорення висновків, які можна зробити на базі цієї гри. Більшість учнів отримують найбільше задоволення від гри, коли грають самостійно, але ви також можете запропонувати їм пограти у парах. Це може бути особливо корисним для молодших учнів.

- З усіх постів, що ви розмістили в грі, яким типом постів, на вашу думку, ви найчастіше ділилися в реальному житті? Чому?
- Опишіть ситуацію, коли ви, можливо, випадково поділилися чимось, чим не слід було б ділитися.
- Чому, на вашу думку, персонажа з «Уважної гори» називають базікалом?
- Опишіть характер базікала та те, як його дії впливають на гру.
- Чи змінила гра «Уважна гора» вашу думку щодо того, як ви будете ділитися інформацією в мережі в майбутньому?
- Назвіть одну річ, яку ви робитимете інакше, після того як пройшли ці уроки та зіграли в гру.
- Назвіть один із прикладів можливих негативних наслідків того, щоб поділитися чимось публічно, а не лише з друзями.
- Що можна зробити, якщо ви випадково поділилися чимось особистим? А як бути, якщо хтось випадково поділиться чимось занадто особистим із вами?



Не дай себе обманути

Тримайтеся подалі від шахраїв, обманщиків, інформації, що не допомагає, та іншого контенту в мережі, який намагається ввести вас в оману, а ще дізнайтеся, як знаходити корисний контент

Огляд уроку	Урок 1	Спливаючі вікна, підроблені облікові записи та інші шахрайські дії		2–6 класи
	Урок 2	Хто це зі мною «розмовляє»?	ML	2–6 класи
	Урок 3	Це дійсно правда?	ML	2–6 класи
	Урок 4	Виявлення недостовірної інформації в мережі	ML	4–6 класи
	Урок 5	Якби ми були пошуковою системою	ML	2–6 класи
	Урок 6	Практика з пошуку в Інтернеті		2–6 класи
	Урок 7	Interland: Річка реальності		2–6 класи

Теми

Важливо, щоб діти розуміли, що контактам чи контенту в мережі не завжди можна довіряти. Часто контент публікують зловмисники з метою обману або викрадення чужої інформації, особистості чи майна. Інтернет-шахрайство націлене на те, щоб змусити користувачів (незалежно від віку) відреагувати на пропозицію від невідомої людини чи переконати їх, що вони спілкуються зі знайомими.

Цілі для учнів

- ✓ Зрозуміти, що те, що говорять вам в мережі, не завжди відповідає дійсності.
- ✓ Дізнатися, як працюють різні види шахрайства, чим вони небезпечні та як їх уникнути.
- ✓ Навчитися визначати достовірність інформації та повідомлень у мережі та розпізнавати оманливі акції, призи й інші шахрайські пропозиції.

Застосовні стандарти

Стандарти ISTE для вчителів: 1a, 2c, 3b, 3c, 4b, 5a, 6a, 6d, 7a

Стандарти ISTE для учнів: 1c, 1d, 2b, 2d, 3b, 3d, 7b, 7c

Навчальні стандарти AASL: I.b.1, I.c.1, I.c.2, I.c.3, I.d.3, I.d.4, II.a.1, II.a.2, II.b.1, II.b.2, II.b.3, II.c.1, II.c.2, II.d.1, II.d.2., III.a.1, III.a.2, III.a.3, III.b.1, III.c.1, III.c.2, III.d.1, III.d.2, IV.a.1, IV.a.2, IV.b.3, V.a.2, VI.a.1, VI.a.2, VI.a.3

Не дай себе обманути Словник

Уроки 1 і 2

Кетфішинг. Створення підробленого профілю чи облікового запису в мережі, щоб обманом змусити людей дружити чи ділитися особистою інформацією.

Зловмисний. Слова чи дії, які є жорстокими чи шкідливими. Це слово може також стосуватися зловмисного програмного забезпечення, призначеного для пошкодження пристрою, облікового запису або особистої інформації людини.

Фішинг. Спроба виманити ім'я користувача чи іншу особисту інформацію онлайн. Зазвичай для фішингу застосовуються електронні листи, соціальні мережі, текстові повідомлення, оголошення та фіктивні сайти, за дизайном дуже подібні до тих, які часто відвідує користувач.

Шахрайство. Спроба заробити гроші нечесно, обманом змушуючи людей повідомити своє ім'я користувача, особисту інформацію, контакти тощо, або виманювати в людей гроші чи цифрове майно.

Смішинг (або SMS-фішинг). Шахрайство, яке використовує текстові повідомлення, щоб обманом примусити людину щось зробити, наприклад, повідомити логін чи іншу особисту інформацію, натиснути на посилання на зловмисний сайт чи завантажити зловмисне програмне забезпечення.

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

Довірений. Надійний; такий, що робить те, що правильно чи необхідно.

Урок 3

Надійний. Той, хто викликає довіру; хтось, хто заслуговує на довіру. Людина, яка використовує докази, і ви можете бути впевненими в тому, що вона говорить правду.

Компетенція. Спеціальні навички чи знання про певну річ; експерти мають компетенцію.

Мотив. Причина того, що хтось щось робить; намір.

Джерело. Хтось або щось, що надає інформацію.

Влогер. Людина, яка регулярно розміщує короткі відео в блозі чи соціальних мережах.

Урок 4

Оманливий. Підроблений; дія або повідомлення, мета яких — створити в користувачів хибне враження чи обманути.

Оманливі новини. Новини, які навмисно повідомляють неправду або спотворюють правду — популярна на сьогоднішній день назва: «фейкові новини».

Дезінформація. Неправдива інформація, призначена для обману або введення в оману.

Докази. Факти чи приклади, які доводять, що щось є правдивим або хибним.

Недостовірна інформація. Неправдива інформація.

Скептичний. Готовий поставити під сумнів твердження про істину.

Уроки 5 і 6

Клікбейт. Контент, який привертає увагу, використовуючи цікавий формат чи привабливі фрази, і може змусити вас натиснути посилання на певний сайт.

Ключове слово. Слово, безпосередньо пов'язане з темою вашого пошуку в Інтернеті — одне зі слів, яке вам дійсно потрібно для здійснення пошуку, оскільки жодне інше слово не описує вашу тему краще.

Запит. Ключове слово, набір ключових слів або запитання, яке ви вводите у вікно (або поле) для пошуку інформації в мережі. Іноді потрібно зробити більше одного запиту, щоб знайти те, що ви шукаєте.

Пошукова система/пошук в Інтернеті. Програма чи «інструмент», який люди використовують для пошуку інформації (а також місць, фото та відео) в Інтернеті.

Результати пошуку. Набір інформації, який ви отримуєте в пошуковій системі після того, як вводите запит і натискаєте кнопку «Пошук» або «Надіслати».

Спливаючі вікна, підроблені облікові записи та інші шахрайські дії

Учні в ігровій формі аналізують різні повідомлення, намагаючись визначити, які з них справжні, а які шахрайські.

Цілі для учнів



- ✓ Дізнатися, які є способи шахрайства в мережі чи на пристроях.
- ✓ Навчитися захищатися від крадіжки в мережі.
- ✓ Зрозуміти, що в разі підозри шахрайства в мережі важливо звернутися по допомогу до дорослого, якому довіряєте.
- ✓ З'ясувати, за якими ознаками можна виявити шахрайство.
- ✓ Усвідомити, чому ділитись особистою інформацією слід дуже обачно.

Обговорення



Що ж таке шахрайство?

Шахрайство — це коли хтось намагається обдурити вас, щоб щось вкрати, наприклад, ваше ім'я користувача, особисту інформацію, гроші чи цифрове майно. Шахраї іноді видають себе за когось, кому ви довіряєте. На них можна натрапити в спливаючому вікні, на веб-сторінці, у текстовому повідомленні чи навіть у підробленому додатку в магазині додатків. Їхні повідомлення — і небезпечні сторінки, на які вони намагаються вас відправити, — також можуть перенести віруси на ваш пристрій. Деякі з них можуть використати ваш список контактів, щоб направити подібну атаку на ваших друзів та близьких. Інші шахрайські повідомлення можуть містити сповіщення про те, що з вашими пристроєм щось не так, і змусити негайно завантажити зловмисне програмне забезпечення, яке виглядає як справжнє.

Запам'ятайте: жоден месенджер, сайт або оголошення не здатні визначити, чи правильно працює ваш пристрій чи комп'ютер! Тож якщо вони кажуть, що щось не так, вони намагаються обдурити вас. Також пам'ятайте (ви, можливо, чули це раніше, але краще повторити): якщо ви отримуєте повідомлення від когось, кого не знаєте або навіть думаєте, що **могли б** знати, і воно звучить неймовірно, захоплююче або занадто добре, щоб бути правдою, цілком імовірно, що так воно і є (занадто добре, щоб бути правдою).

Примітка для вчителя. Ви можете запитати у класу, чи чули вони коли-небудь про це, попросити підняти руки, а потім запитати, чи бачили вони самі чи хтось із їхньої сім'ї коли-небудь подібне повідомлення. Якщо ні, ЧУДОВО — якщо це відбудеться в майбутньому, вони знатимуть, як захистити себе, свою сім'ю, свої дані та пристрої.

Часом шахрайство дуже легко розпізнати, але часто воно буває складним і дуже переконливим. Наприклад, деякі зловмисники використовують у листах особисту інформацію користувачів. Це так званий цільовий фішинг, персоналізований для одного адресата, і він буває дуже дієвим. Інший вид

Продовження на наступній сторінці →

шахрайства, про який ви, напевно, чули, — це кетфішинг: це коли хтось створює несправжню сторінку або профіль, видаючи себе за когось із ваших знайомих чи підписників, щоб обдурити вас. Також є смішинг (шахрайство в текстових повідомленнях) і фішинг (в електронній пошті).

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. Завжди ставте собі наведені нижче запитання.

- Якщо це повідомлення чи лист від компанії, чи виглядають вони професійно, чи містять звичайний логотип компанії чи товару, чи немає в тексті орфографічних помилок?
- Не слід натискати посилання на веб-сайт у повідомленні. Краще відкрити браузер, знайти цю компанію та перейти на сайт із пошуку, а потім запитати себе: чи відповідає URL-адреса сайту назві товару чи компанії та інформації, яку ви шукали?
- Чи надходить повідомлення у формі надокучливих спливаючих вікон?
- Чи починається URL-адреса сторінки з префіксу `https://`, перед яким відображається значок зеленого замка? (Це вказує на те, що з'єднання безпечне та зашифроване).
- Що написано дрібним шрифтом? (Усякі хитрі нюанси та невігідні умови часто пишуть саме так. Також не дуже добре, якщо **немає** дрібного шрифту.)
- Чи пропонує повідомлення щось, що звучить занадто добре, щоб бути правдою, наприклад, шанс заробити гроші, отримати кращу цифрову штуку для аватару чи персонажа, стати знаменитим тощо? (Це майже **завжди** занадто добре, щоб бути правдою.)
- Чи звучить повідомлення дещо дивно? Наприклад, вам говорять, що знають вас, і ви думаєте, що це можливо, але ви не зовсім впевнені.

Але що робити, якщо ви попалися на гачок? Перш за все не панікуйте! Це трапляється з багатьма.

- негайно повідомте батьків, учителя чи іншого дорослого, якому довіряєте. Чим довше ви зволікаєте, тим 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

- Роздатковий матеріал: «Приклади фішингу» (відповіді на сторінці 39)

Можливі модифікації для 2-3 класів. Розділіть клас на 5 груп і призначте кожній групі по одному прикладу з аркуша із вправами. Після того як кожна група проаналізує приклад, обговоріть його в класі.

1. Розділіть клас на групи

2. Кожна група вивчає приклади

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

Відповіді на роздатковий матеріал для учнів:

«Приклади фішингу»

1. Справжній.

У повідомленні користувача просять увійти в обліковий запис самостійно, а не за наданим у повідомленні посиланням, а також не просять надіслати пароль на електронну пошту (посилання можуть переводити вас на зловмисні веб-сайти).

2. Шахрайський. URL-адреса підозріла й незахищена.

3. Справжній. Зверніть увагу на <https://> в URL-адресі.

4. Шахрайський. Підозріла пропозиція в обмін на введення банківських реквізитів.

5. Шахрайський. URL-адреса підозріла й незахищена.

6. Шахрайський. URL-адреса підозріла й незахищена.

7. Шахрайський. URL-адреса підозріла й незахищена; також підозріла пропозиція в обмін на введення банківських реквізитів.

3. Перевірка справжності (індивідуально)

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

4. Обговорення думок учнів (у групах)

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

5. Подальше обговорення

Ось ще 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 пропонують вам виправити те, що ви не вважаєте за проблему?

• Чи не виглядає цей додаток сумнівно?

Іноді у спливаючих вікнах веб-сайтів чи в магазинах додатків рекламуються фейкові додатки, які виглядають досить схоже на справжні. Під час завантаження на телефон такі додатки можуть наробити багато шкоди — викрасти вашу інформацію або контакти, установити зловмисне програмне забезпечення тощо. Зверніть увагу на орфографічні помилки, незначну кількість відгуків користувачів або недбалу (не дуже професійну) графіку.

• Чи пропонується в повідомленні щось безкоштовне?

Безкоштовні пропозиції зазвичай не зовсім безкоштовні — відправники хочуть щось отримати від вас.

• Чи просять вас указати особисту інформацію?

Деякі шахраї вимагають надати їй, щоб надсилати вам нові шахрайські повідомлення. Наприклад, усілякі тести можуть насправді збирати про вас факти, які допоможуть угадати ваш пароль тощо. Більшість реальних компаній не просять надати особисті дані в повідомленні або іншим чином, окрім як на власних веб-сайтах.

• Це ланцюгове повідомлення чи пост в соцмережі?

Якщо в листі чи публікації вимагається переслати їх, наприклад, «10 друзям», це дуже ризиковано. Робіть це тільки тоді, коли точно знаєте, від кого це повідомлення і що воно безпечне.

- **Чи є в повідомленні дрібний шрифт?**

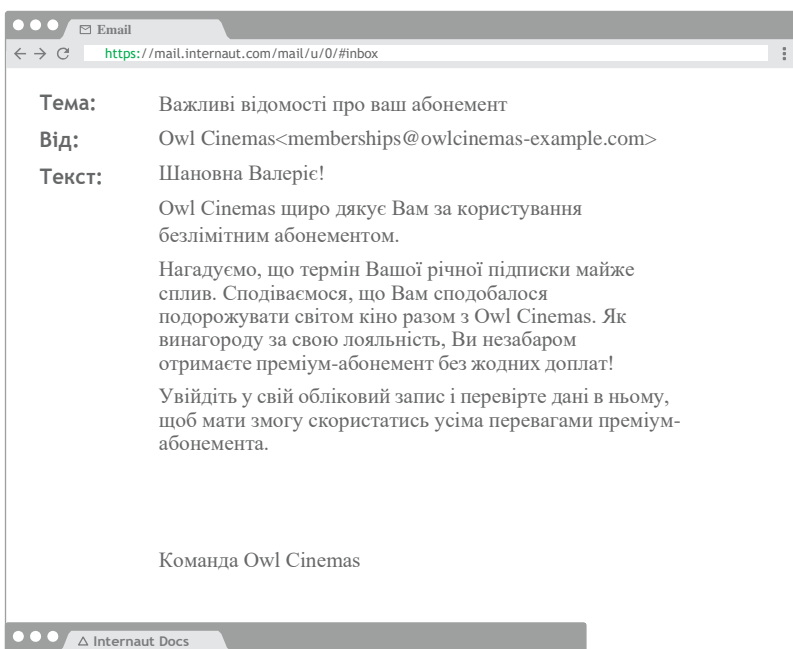
Унизу повідомлень часто вказується додаткова інформація дуже дрібним шрифтом. Зазвичай її ніхто не читає — на те вона й розрахована. Наприклад, у заголовку листа може бути вказано, що ви виграли телефон, а дрібним шрифтом унизу уточнюватиметься, що за приз доведеться щомісячно доплачувати по 200 дол. Повна відсутність дрібного шрифту також не є гарною ознакою, тому також звертайте на це увагу.

Примітка. Для цього уроку уявімо, що вигадана компанія Internaut Mail — це справжня поштова служба.

Висновки

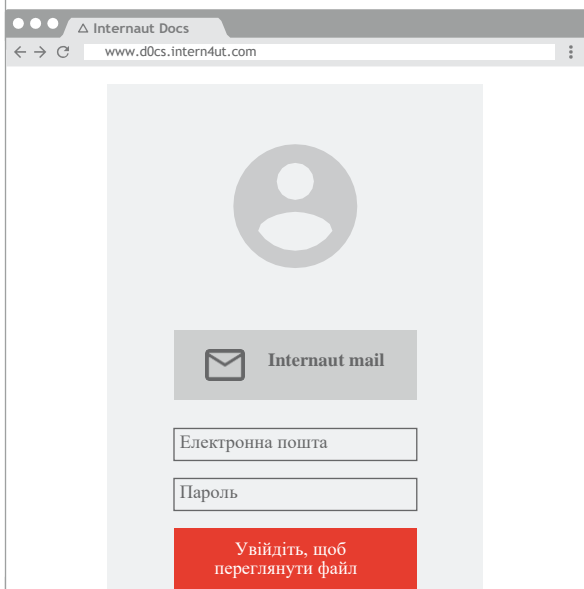
Користуючись Інтернетом, завжди будьте насторожі: пам'ятайте про загрозу шахрайства в іграх, на веб-сторінках, у додатках і повідомленнях. Пам'ятайте: якщо щось здається занадто чудовим або пропонується безкоштовно, це може бути фейк. А якщо ви все ж потрапили на гачок, негайно повідомте дорослого, якому довіряєте.

Приклади фішингу



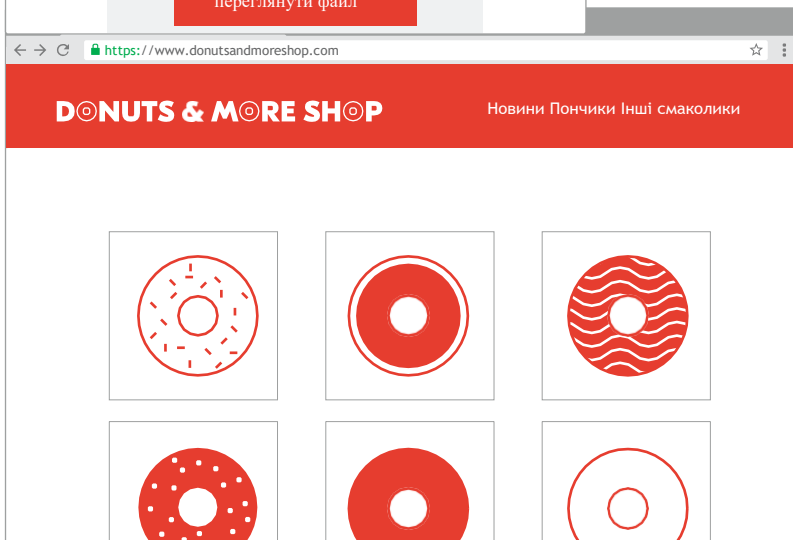
1. Справжній чи шахрайський?

Справжній Шахрайський



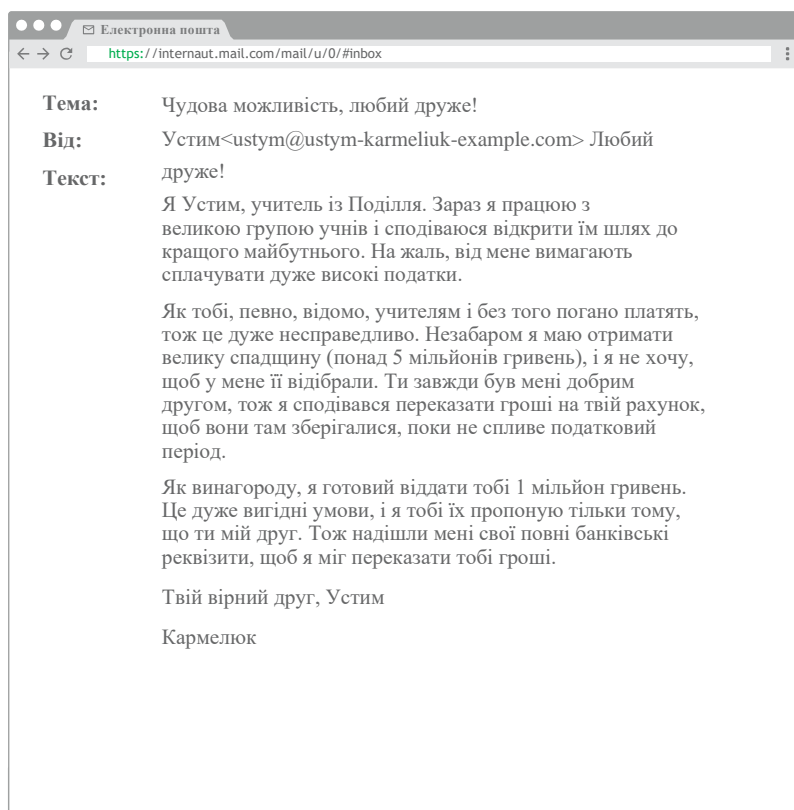
2. Справжній чи шахрайський?

Справжній Шахрайський



3. Справжній чи шахрайський?

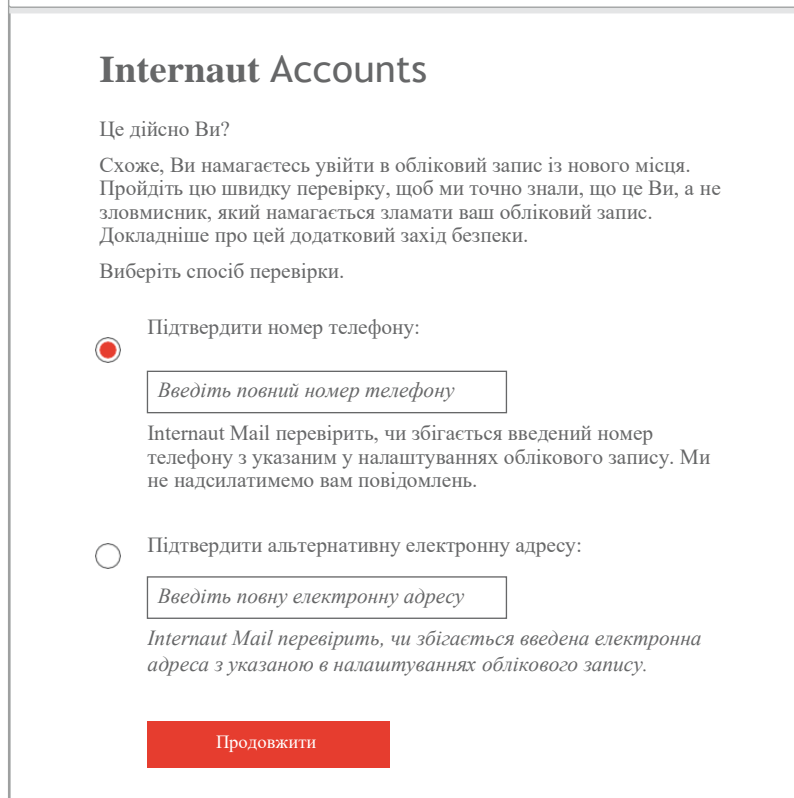
Справжній Шахрайський



4. Справжній чи шахрайський?

Справжній

Шахрайський

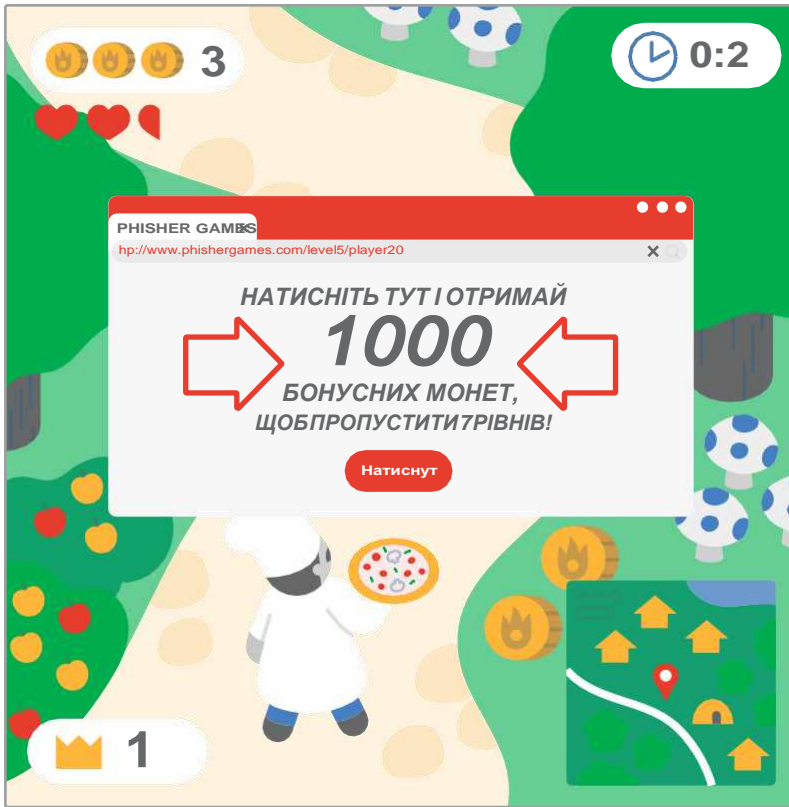


5. Справжній чи шахрайський?

Справжній

Шахрайський

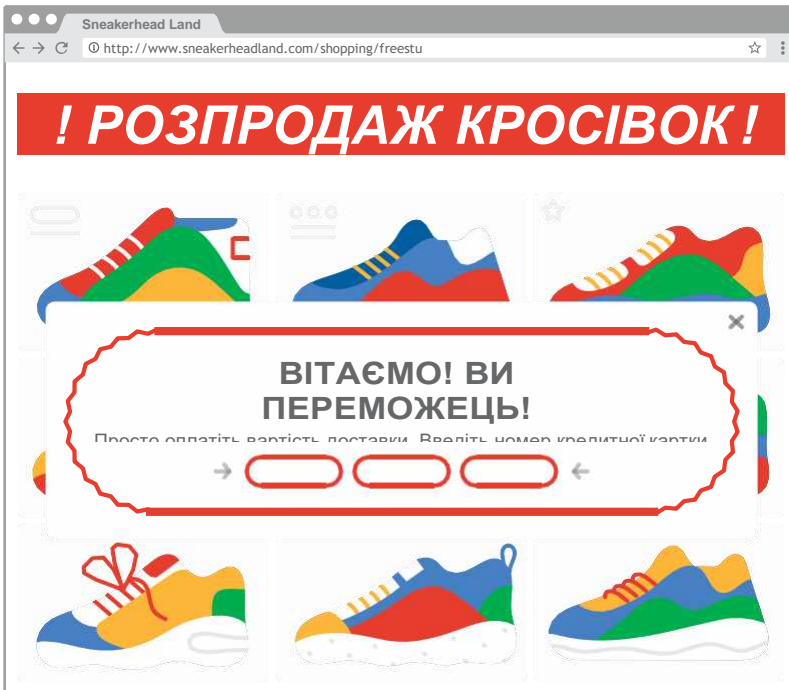
Продовження на наступній сторінці →



6. Справжній чи шахрайський?

Справжній

Шахрайський



7. Справжній чи шахрайський?

Справжній

Шахрайський

Хто це зі мною «розмовляє»?

Учні відпрацьовують навички розпізнавання шахрайства, розігруючи сценарії з підозрілими онлайн-повідомленнями, дописами, запитами друзів, додатками, зображеннями, електронними листами й обговорюють можливу реакцію на них.

Інформація про урок. *Оскільки йдеться про соціальну взаємодію, може здаватися, що цей урок більше підійде учням 5–6 класів, але оскільки все більше дітей віком 7–9 років грають в онлайн-ігри, і багато з них грають разом з іншими гравцями, а не окремо, то цей урок стане гарною підготовкою навіть для учнів 2–3 класів. Ми сподіваємося, що вчителі цих класів дізнаються, чи грають їхні учні в онлайн-ігри, і якщо так, то запитують, що їм подобається в цих іграх та чи не виникали в них якісь підозрілі ситуації. Щоб навчання було максимально ефективним, спілкування має бути простим, відкритим та неупередженим.*

Цілі для учнів



- ✓ **Зрозуміти**, що люди, які зв'язуються з нами, можуть бути не тими, за кого себе видають.
- ✓ **Переконатися**, що це саме та людина, якою вона назвалася, перш ніж відповідати.
- ✓ **Ставити** запитання чи звертатися по допомогу до дорослого, якщо важко визначити особу людини.

Обговорення



Ви певні, що це дійсно та людина?

Коли ви розмовляєте з другом по телефону, ви можете по голосу сказати, що це саме він, навіть якщо ви його не бачите. Онлайн-світ дещо інший. Іноді важко бути впевненим, що люди є саме тими, за кого себе видають. У додатках та іграх люди іноді прикидаються кимось заради жарту, щоб отримати щось від вас або просто з підлості. В інших випадках вони видають себе за інших людей, щоб викрасти особисту інформацію або цифрове майно, наприклад, скіни або ігрові гроші. Найбезпечніше — не відповідати або сказати батькам чи іншим дорослим, яким ви довіряєте, що ви не знаєте людину, яка намагається з вами зв'язатися. Але якщо ви вирішите відповісти, то непогано було б спочатку подивитися, що ви можете дізнатися про цю людину. Перевірте її сторінку чи профіль, подивіться, хто її друзі, або знайдіть іншу інформацію, яка може підтвердити, що це дійсно ця людина.

Є багато способів перевірити особу іншої людини та визначити, чи це не шахрай. Ось для початку кілька ідей.

Примітка для вчителя. *Ви можете спочатку провести мозковий штурм у класі, запитавши в учнів: «Як можна перевірити особу людини в мережі?», а потім продовжити розмову на основі отриманих ідей.*

• Якщо є фото відправника повідомлення, чи не виглядає воно підозрілим?

Можливо, фото розмито чи на ньому щось важко розібрати? Або, можливо, взагалі немає фото, а замість нього картинка чи обличчя мультиплікаційного персонажа.

Продовження на наступній сторінці →

Фото низької якості, картинки, фотографії домашніх тварин тощо допомагають людині приховати особу в соціальних мережах. Ще шахраї часто крадуть справжні фото в інших людей і використовують як зображення власного фіктивного профілю. Якщо є фото, то чи можете ви знайти більше фотографій людини з таким іменем в мережі?

• **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 користувача звать 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. Чи можете ви щось підтвердити з цієї інформації, якщо пошукаєте цю людину в Інтернеті за її іменем у профілі?

• **Як довго обліковий запис був активним? Чи має така активність сенс для вас?** Цей профіль зовсім новий чи в ньому багато активності? Чи є у вас спільні друзі з цією людиною, як ви того очікували? У фіктивних облікових записах часто мало чи зовсім немає дописів і взаємодій з іншими людьми.

Практичне завдання



Необхідні матеріали

- Аркуш із вправами: «Хто це зі мною «розмовляє?»», розрізаний на смужки, по одному сценарію на кожній смужці
- Миска чи інша ємність, з якої учні всліпу витягуватимуть смужки (одна група витягує одну смужку)
- Конспект учня на сторінці 46 (по одному на учня)

1. Групи аналізують сценарії

Добре, а тепер розбиймося на 5 груп. Кожна група витягує сценарій.

2. **Групи вибирають одну або декілька відповідей** зі шпаргалки та обговорюють, чому було вибрано таку реакцію на ситуацію. Ви можете написати більше повідомлень, які, на вашу думку, були б ще більш заплутаними.

3. Клас обговорює реакцію груп

Нарешті давайте використаємо цю шпаргалку для обговорення в класі всіх сценаріїв.

Кожна група читає свій сценарій і розповідає класу про свою реакцію й чому саме вони її обрали. Обговорення в класі.

Висновки

Уважно стежте за колом свого спілкування в мережі. Обов'язково перевіряйте, чи дійсно ваші інтернет-знайом — ті, за кого себе видають.

Хто це зі мною «розмовляє»?

Сценарій 1

Ви отримує запит від випадкового гравця в грі додати його в друзі: «Привіт, ти прикольний! Давай грати разом! Додаси мене до друзів?»

Сценарій 2

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

Сценарій 3

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 4

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 5

Хтось пише вам у соціальній мережі: «Привіт, я знайома з твоєю подругою Наталкою, вона мені багато про тебе розповідала. Я хочу з тобою дружити!»

Хто це зі мною «розмовляє»?

Ось п'ять сценаріїв повідомлень, які кожен може отримати в Інтернеті або на телефоні. До кожного з них наведено перелік варіантів реагування, деякі з яких чудові, а інші не дуже. Вам треба вирішити, який один (чи два) з них найбільш прийнятні для вас (або можете придумати інші варіанти). Назвіть їх, а потім обговоримо разом.

Зверніть увагу. Якщо один із цих сценаріїв дійсно трапляється з вами, і ви не впевнені, що робити, найпростішою реакцією є відсутність будь-якої реакції. Ви завжди можете проігнорувати або заблокувати цю людину. Також ніколи не завадить поговорити з батьками чи вчителями про це, особливо якщо це вас турбує.

Сценарій 1

Ви отримує запит від випадкового гравця в грі додати його в друзі: «Привіт, ти прикольний! Давай грати разом! Додаси мене до друзів?» Якою буде ваша реакція?

- **Проігнорувати цю людину.** Якщо ви не знаєте цю людину, то можете просто нічого не відповідати.
- **Заблокувати цю людину.** Ви більше не отримаєте від неї повідомлень — у більшості ігор та додатків ця людина навіть не знатиме, що ви її заблокували.
- **Змінити налаштування.** Зайдіть в налаштування гри, подивіться, чи зможете ви вимкнути всі запити про додавання до друзів і відмітьте цей прапорець. Таким чином вам навіть не доведеться вирішувати, приймати чи ні запити випадкових гравців.
- **Перевірити профіль цієї людини.** Подивіться, чи є в цієї людини сторінка або профіль, щоб перевірити, чи дійсно це гравець — чи є в нього ігрові досягнення, підписники, чи проводив він ігрові трансляції? Чи знають його ваші друзі? Тільки якщо дійсно схоже на те, що ця людина захоплюється цією грою, можна подумати про можливість додати її в друзі. Але дітям найкраще просто грати зі своїми реальними друзями.
- **Додати до друзів.** Це можна робити тільки тоді, коли ви впевнилися, ким ця людина є насправді, та поговорили з дорослим, якому довіряєте, або принаймні зі своїми друзями, щоб дізнатися, чи знають вони цю людину. Якщо ви граєте з нею з мікрофоном або гарнітурою, розмовляйте лише про гру — ніколи не повідомляйте своє повне ім'я та прізвище чи іншу особисту інформацію.
- **Надати особисту інформацію.** Точно ні. **Ви** знаєте: ніколи не варто давати свою особисту інформацію людям, яких ви не знаєте.

Сценарій 2

Ви отримуєте SMS із незнайомого номера: «Привіт, це Аня, ми познайомились улітку. Пам'ятаєш мене?» Якою буде ваша реакція?

- **Заблокувати Аню.** Але ви маєте заблокувати цю людину, 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, чи знайомі з нею та хочете дізнатися більше. Але не кажіть Ані, де ви були минулого літа!
- **«Я тебе не пам'ятаю, але можемо зустрітися».** Це дуже погана ідея. Ніколи не варто пропонувати незнайомій людині зустрітися.

Сценарій 3

Людина, на яку ви не підписані, надсилає вам таке повідомлення з облікового запису @soccergirl12: «Привіт! Я просто в захваті від твоїх дописів, ти такий дотепний!!! Напиши мені свій номер телефону, я хочу з тобою поспілкуватися!» Якою буде ваша реакція?

- **Проігнорувати користувача @soccergirl12.** Якщо ви не хочете відповідати цій людині, то можете просто промовчати.
- **Заблокувати користувача @soccergirl12.** Якщо ця людина видається вам підозрілою, можна просто заблокувати її, і тоді вона вам більше не писатиме, якщо тільки не створить новий фейковий профіль і не зв'яжеться з вами знову...

«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 4

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». Якою буде ваша реакція?

- **Проігнорувати.** 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. Ніколи не зустрічайтеся особисто з тими, кого ви знаєте лише зі спілкування в мережі.

Сценарій 5

Хтось пише вам у соціальній мережі: «Привіт, я знайома з твоєю подругою Наталкою, вона мені багато про тебе розповідала. Я хочу з тобою дружити! Де ти живеш?» Якою буде ваша реакція?

- **Проігнорувати.** 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).

Це дійсно правда?

Довідка для вчителів. Крім того, щоб навчити учнів ставити аналітичні запитання для оцінки надійності джерел, ми також хочемо, щоб вони розуміли, що інформація надходить із багатьох місць (а не лише з підручників). Тому їм потрібно застосовувати свої навички для аналізу всіх видів джерел інформації. Коли вони це зрозуміють, вони будуть готові перейти до аналізу особливих категорій контенту, таких як новини чи наукові дані.

Примітка. Цей урок медіаграмотності буде корисним для всіх, але може бути трохи заважким для учнів 2–3 класів, тому дивіться запропоновану модифікацію нижче в розділі «Практичне завдання».

Цілі для учнів



- ✓ **Визначити** інструменти, які ви вже використовуєте, щоб переконатися, що інформація **надійна**.
- ✓ **Розглянути** те, як певні речі, такі як **компетенція і мотиви**, впливають на надійність.
- ✓ **Дізнатися** 4 запитання, які допомагають оцінити надійність джерела.
- ✓ **Зрозуміти**, що джерело достовірної інформації з однієї теми не обов'язково заслуговує на довіру щодо інших тем.
- ✓ **Розуміти**, що перевірка у декількох джерелах часто допомагає зрозуміти, чи інформація є надійною.

Обговорення



Як зрозуміти, де правда?

Щодня ви приймаєте рішення, чому вірити, а чому — ні. Чи було достовірним відео, яке ви побачили? Вас намагалися у чомусь переконати? Ваш старший брат говорить вам правду чи дражнить? Чи є правдою ті чутки, які ви чули про друга?

Що ви робите, коли намагаєтесь вирішити, чи хтось говорить правду? Ви вже використовуєте наведені нижче підказки?

- **Що ви знаєте про людину**
Наприклад, ви знаєте, що однокласник щось уміє робити дійсно класно або завжди був чесним чи навпаки часто розігрує когось або поводить себе підло, тому ви зазвичай можете сказати, чи він каже правду, шуткує чи обманює.
- **Що людина знає про вас**
Наприклад, ваші батьки знають, від якої їжі у вас болить живіт; а реклама по телевізору — ні, тому ви дотримуєтеся порад батьків щодо того, що їсти. Шкільний бібліотекар знає ваші інтереси та які книги вам подобаються, тому ви довіряєте її рекомендаціям щодо книг.
- **Тон голосу та вираз обличчя**
Наприклад, ви знаєте, що ваш друг говорить одне, а має не увазі протилежне, якщо він закриває очі та поводить себе дещо дивно, коли говорить, що жакливо провів час у новому скейт-парку.
- **Ситуація**
Наприклад, коли друзі граються і хтось дражнить вас за вашу нову зачіску, ви розумієте, що це просто жарт. Але якщо хтось у школі каже точно такі ж слова, щоб збентежити вас перед усім класом, це образа.

Коли ми чуємо щось у засобах інформації, наприклад, у відео, від людини по телевізору чи на веб-сайті, ми особисто не знаємо це джерело, а вони не знають нас.

Навіть коли знайомий надсилає нам текстове повідомлення, ми не можемо бути впевнені, що він має на увазі, оскільки ми не бачимо його міміку чи вираз обличчя. Саме тоді нам потрібно поставити таке запитання...

Практичне завдання



Необхідні матеріали

- Роздатковий матеріал: «Визначення надійності» (один для кожного учня)

Рекомендовані модифікації для 2-3 класів. Якщо ви вважаєте, що ваші учні готові до обговорення питання надійності джерел, виконайте лише кроки 1 та 2.

1. Оцініть джерело

Якби ви хотіли отримати рекомендацію щодо чудової нової відеоігри, ви б запитали бабусю? Або, якщо сказати по-іншому, чи ваша бабуся є **надійним** джерелом інформації про відеоігри? **Надійне** джерело — це джерело, якому ми можемо довіряти в наданні нам точної та релевантної інформації.

Складіть список «за» і «проти», щоб пояснити переваги і недоліки того, щоб запитати поради про відеоігри у бабусі.

Ваш список виглядав приблизно так?

ЗА	ПРОТИ
Бабуся любить мене і бажає мені щастя	Бабуся не грає у відеоігри і не знає про них багато
Бабуся досить добре знаходить інформацію, коли сама не знає відповіді	Бабуся не знає, які ігри в мене вже є або які види ігор мені подобаються

Якщо ваш список виглядав так, то ви щойно використали два найпоширеніші інструменти прийняття рішення щодо надійності джерела: **мотив** та **компетенцію**. «Компетенція» — це спеціальні навички чи знання про певну річ; експерти мають компетенцію. «Мотив» — це чийсь намір, причина того, що людина щось говорить чи робить.

Який пункт у списку дає вам інформацію про мотиви бабусі? Які пункти говорять про її компетенцію? Виходячи з цього списку «за» і «проти», чи є бабуся надійним джерелом інформації про те, яку нову відеогру придбати? Вона не брехатиме, але чи не краще було б запитати когось, кому ви не байдужі, але хто **також** дещо знає про ігри та види ігор, які вам подобаються?

Ми можемо також знати, що тато чудово готує, але зовсім не розбирається в моді; наш тренер спеціаліст у баскетболі, але не в гімнастиці, або те, що бабуся може поремонтувати майже будь-яку іграшку, але не знає нічого про відеоігри. **Те, що людина є експертом у чомусь одному, не робить її експертом у всьому.**

2. Складіть свій список «за» і «проти»

Якщо ви вперше замислились над тим, як використовувати **мотив і компетенцію** для визначення надійності джерел інформації, можливо, ви захочете дещо попрактикуватися.

Уявіть, що ви хочете знати, як стати кращим футболістом. Складіть списки «за» і «проти» для наступних джерел, щоб вирішити, чи вони є надійними:

- ваша бабуся
- блог тренера з баскетболу, команда якого здобувала перемоги
- найкращий гравець у вашій команді
- веб-сайт, на якому продається футбольне взуття та даються рекомендації
- відео, у яких вчать техніці гри у футбол

Що ви помітили стосовно сильних та слабких сторін кожного джерела?

- Чи є серед них хтось, хто вміє вчити, але не знайомий з навичками гри у футбол?
- Чи є серед них експерт з футболу, який не знає, як вчити?
- Чи є таке джерело, яке, скоріш за все, порадить щось купити?
- Чи є таке джерело, що знається на футболі, але не знає вас чи не знає, над якими навичками вам треба працювати?

Обговоріть, до якого джерела краще було б звернутися і чому ви так вважаєте?

Надійність рідко означає «все або нічого». Більшість джерел мають свої переваги та недоліки. Саме тому **найкращі відповіді часто можна отримати, якщо пошукати інформацію в різних джерелах і порівняти її.**

3. Скористайтесь простими кроками

Надійність — це не тільки про те, **кому** ми віримо. Це також і про те, **у що** ми віримо. Ми отримуємо уявлення про світ з різних місць, а не лише безпосередньо від людей. Фільм про цунамі показує, як гігантська хвиля — вища за хмарочос — рухається до людей на березі. Невже цунамі **насправді** так виглядають? З реклами випливає, що більшість вчених — це чоловіки із скуйовдженим волоссям, які постійно носять товсті окуляри та білі халати. Це правда?

Ми можемо перевірити будь-яке джерело завдяки 3 кроками **Визначення надійності**. Вони базуються на тому, що ми вже знаємо про мотиви та компетенцію.

Крок 1. Користуйтеся здоровим глуздом

Запитайте себе: «Це логічно? У цьому є сенс?» Якщо а) те, що ви бачите, не має сенсу, б) ви знаєте, що це неправда з вашого власного досвіду або в) це суперечить фактам, які вже вам відомі, не потрібно виконувати будь-яких додаткових кроків. Це джерело ненадійне.

Крок 2. Ставте запитання

Не просто будь-які запитання, а такі чотири запитання:

Компетенція

а) Чи знає мене це джерело та чи піклується про мене? Відповідь на це запитання залежить від інформації, яку ви шукаєте. Якщо ви перевіряєте якусь інформацію про пластикові пляшки для води, які забруднюють океан, насправді неважливо, знає вас джерело чи ні. Але якщо сайт обіцяє, що вам сподобається їхня нова іграшка, йому потрібно було б знати, які іграшки, ігри чи заняття вам подобаються, аби обіцянка була надійною.

б) Чи багато знає джерело про цю тему? Звідки вони знають те, що їм відомо?

Деякі люди вважають, що найпростіший спосіб знайти надійну інформацію — запитати цифрового голосового помічника. Цифрові асистенти, здається, знають усе! Ви коли-небудь цікавилися, звідки вони можуть знати всі ці відповіді? Вони використовують математичні розрахунки (так звані «алгоритми») для пошуку відповідей.

Для простих запитань, на які є лише одна можлива відповідь (наприклад, температура на вулиці або ім'я знаменитості, яка виконує конкретну пісню), вони, як правило, є надійним джерелом. Але якщо запитання складне, краще почати з людей, які мають великий досвід, здобули якісь нагороди або є кандидатами наук у вашій темі. **Після цього** ви можете скористуватися голосовим помічником, щоб підтвердити цю інформацію (див. Крок 3).

Мотив

в) Що це джерело хоче, щоб я зробив, або вважає, що я зроблю, і для чого це йому? Чи заробить це джерело гроші, якщо я скористаюся його порадою? Наприклад, чи вважаєте ви, що лідер думок заробить гроші, якщо ви придбаєте товар, у який він одягнений чи про який розповідає? Чи носить професійний спортсмен певну марку взуття чи футболки лише тому, що йому подобається ця марка, або тому, що йому платять за це?

Гроші часто можуть бути однією з причин, чому ви бачите логотип чи назву бренду у відео чи рекламі — вони можуть вплинути на те, що лідер думок чи спортсмен вам говорить (і те, чого він вам не говорить). Скоріш за все, людина, яка рекламує товар, не хоче вам зашкодити, але цілком можливо, що отримати гроші для неї набагато важливіше, ніж повідомити вам усі факти або сказати, що буде кращим для вас.

г) Хто виграє, а хто може постраждати, якщо люди повірять цьому джерелу?

Це не завжди легко сказати. Ось приклад.

Уявіть собі рекламу додатка, який обіцяє зробити вас кращим учнем.

Які можливі переваги? Розробник додатка виграє, якщо ви придбаєте додаток, оскільки він заробить гроші. І ви можете отримати користь, якщо додаток дійсно допоміг вам.

- Хто може постраждати, якщо ви повірите цій рекламі? Можливо, ви даремно витрачаєте гроші, якщо купите цей додаток. Ви також можете витратити час, займаючись не тим, чим потрібно, а потім ваша успішність у школі знизиться.

Або, можливо, ви довіритесь додатку, який не знає напевно, що саме вам потрібно, замість того, щоб звернутися по допомогу до вчителя, який це добре знає.

Крок 3. Підтверджуйте інформацію

Запитайте: «Чи інші надійні джерела підтверджують те, що говорить це джерело?» Завдання полягає не лише в тому, щоб перевірити **більше** джерел. Потрібно шукати різноманітні джерела. Якщо ви не можете знайти декілька надійних джерел, які погоджуються з джерелом, яке ви перевіряєте, не слід вірити цьому джерелу.

4. Перевірте свої джерела

Тепер, коли ви все зрозуміли, прийшла черга практикуватися. Виберіть запитання, пов'язане з чимось, що ви вивчали в класі або бачили в мережі. Знайдіть джерело, яке дає відповідь на це запитання, і в невеликих групах ставте запитання з роздаткового матеріалу, щоб вирішити, чи є джерело надійним.

Пропонуємо вам кілька ситуацій нижче.

- Вам потрібні ідеї подарунка на день народження для вашого друга. Реклама місцевого магазину стверджує, що їхній інструмент для пошуку допоможе вам переглянути всі товари, які пропонує цей магазин, і знайти подарунок для будь-кого. Це підійде вам?
- Ви читаете в Інтернеті відгуки про нову піцерію та звертаєте увагу на те, що три із шести відгуків з оцінкою «5 зірочок» залишили люди, прізвище яких збігається з назвою ресторану. Двоє інших кажуть, що це найкраща піца у світі, а один каже, що піца досить непогана за свою ціну. Також є чотирнадцять негативних коментарів. Чи переконали б вас позитивні відгуки спробувати їхню піцу?
- У спливаючій рекламі повідомляється, що вас відібрали до невеликої групи людей, яким дадуть спробувати спеціальну «таблетку русалки», що дає можливість дихати під водою без аквалангу. Усе, що вам потрібно зробити, це надіслати 9,99 доларів для оплати доставки. Ви б це зробили?
- Вам подобається багато відеороликів популярного влогера, оскільки вони смішні, але він також говорить неприємні речі, які вам не подобаються, і ображає групи меншин. Чи купите ви те, що рекомендує цей влогер, тому що він дійсно веселий і популярний? Думаєте, це впливає на людей?

Висновки

Запитання — наші друзі. Якщо ви ставите правильні запитання про джерела та інформацію, яку вони надають, ви отримаєте більш якісну інформацію. Чим більше джерел ви використовуєте, тим краще. І пам'ятайте, що джерело, яке чудово висвітлює одну тему, не обов'язково є надійним джерелом інформації на інші теми.

Визначення надійності

Корисні кроки, які допоможуть відрізнити надійні джерела від ненадійних.

Крок 1

Користуйтеся здоровим глуздом

Це логічно?

Крок 2

Ставте запитання

Не просто будь-які запитання, а такі чотири запитання:

Компетенція

- Чи знає мене це джерело та чи піклується про мене (і чи це важливо)?
- Чи багато знає джерело про цю тему? Як вони дізналися те, що знають?

Мотив

- Що це джерело хоче, щоб я зробив, або вважає, що я зроблю, і для чого це йому?
- Хто виграс, а хто може постраждати, якщо люди повірять цьому джерелу?

Крок 3

Підтвердьте інформацію

Чи інші **надійні** джерела підтверджують те, що говорить це джерело? Скористайтеся пошуком в Інтернеті або працюйте в шкільній бібліотеці, щоб знайти інші джерела інформації на вашу тему (такими джерелами можуть бути книги, новини чи статті в журналах, як онлайн, так і офлайн). Виконайте кроки 1 і 2 — поставте ті самі запитання про ці джерела. Якщо вони дають таку саму інформацію на вашу тему, цілком ймовірно, що вони підтверджують надійність вашого джерела.

Виявлення недостовірної інформації в мережі

Довідка для вчителів. Запитання щодо медіаграмотності та методи спостереження — це інструменти, які допомагають учням протидіяти дезінформації, не потрапляти в суперечки та не шкودити відносинам із друзями та сім'єю. Але учні мають ставити запитання та звикати застосовувати критичне мислення щодо інформації, яка трапляється їм на шляху.

Цілі для учнів



- ✓ **Навчитися** виявляти підказки, які свідчать про те, що новина чи джерело інформації є неправдивими.
- ✓ **Використовувати** аналітичні запитання та спостереження для оцінки надійності джерела.
- ✓ **Розуміти**, що важливо перевірити надійність джерела, перш ніж розповсюджувати інформацію з нього.
- ✓ **Виробити** звичку аналізувати **всі** новини та інформацію, а не лише історії, які ми вважаємо підозрілими.

Обговорення



Чи грали ви колись в гру, де потрібно знайти помилки, приховані на малюнку? Іноді з новинами трапляється те саме. Існує багато людей і груп, які настільки захоплені тим, у що вони вірять, що перекручують правду, аби примусити нас погодитися з ними. Коли таке перекручування правди маскується під новину, це дезінформація.

Деякі люди не знають, як розпізнати неправдиву інформацію, але все одно діляться нею. Саме так вона і поширюється. І коли люди сліпо вірять такій дезінформації, їм може бути дуже важко слухати один одного спокійно, поважати думку іншої людини, розуміти один одного краще та вирішувати проблеми.

Отже якщо щось виглядає або звучить як новина, як нам зрозуміти, чи вона реальна й достовірна, чи фальшива й оманлива? Є підказки, завдяки яким ми можемо навчитися це помічати — прийоми, які використовують люди, які намагаються ввести вас в оману. І є запитання, які ми можемо поставити, щоб розпізнати історії, які не базуються на фактах.

Практичне завдання



Необхідні матеріали

- Зображення: «Що не так з цією картинкою?»
- Роздатковий матеріал: «Визначення надійності» з Уроку 3 (стор. 54)
- Аркуш із вправами: «Виявлення фальшивих URL-адрес»

Відповіді для вправи: «Виявлення фальшивих URL-адрес»

Справжня abcnews.go.com
bbc.com/news/nbcnews.com
nytimes.com
washingtonpost.com
usatoday.com

Фальшива

abcnews.com.co abcnews-us.com nbc.com.co
nytimesofficial.com
bbc1.site/business-news
washinqtonpost.com
washingtonpost.com.co
usatosday.com

1. Що не так з цією картинкою?

Погляньте на зображення нижче. Подивіться уважно. Чи можете ви помітити відмінності між цими двома малюнками?



Тут є 9 відмінностей, ви знайшли їх усі?



Спроба визначити, чи є новина реальною чи фальшивою, схожа на цю гру. Подивившись дійсно уважно, можна знайти важливу інформацію. І набагато простіше, якщо ви знаєте, на що звертати увагу.

Отже, ось кілька підказок щодо пошуку дезінформації. Якщо ви помічаєте ці речі, то ви, вірогідно, дивитесь на фальшиву або оманливу історію.

Роздатковий матеріал «Виявлення фальшивої URL-адреси»

Перше, на що слід звернути увагу, це URL-адреса (веб-адреса) сайту, який опублікував інформацію. Деякі фейкові сайти намагаються обдурити вас, вибираючи назви, що імітують реальні сайти, але з невеликими відмінностями. Більшість компаній використовують короткі URL-адреси, оскільки їх легше запам'ятовувати та вводити, тому URL-адреси з доданими непотрібними літерами часто виявляються сайтами з неправдивою інформацією.

Погляньте на роздатковий матеріал.

- Обведіть усі URL-адреси, які, на вашу думку, є реальними.
- Коли всі закінчать, подивіться на відповіді. Ви правильно обрали?

Як ви могли перевірити, чи є URL-адреса справжнім сайтом новин? Один із способів — пошукати цю організацію або URL-адресу в Інтернеті. Якщо організація надійна, праворуч від результатів пошуку на багатьох платформах з'являється поле з її описом, включно з адресою веб-сайту. Якщо URL-адреса ненадійна, часто можна знайти в результатах пошуку інформацію про те, що цей сайт виявився фальшивим або що сайт більше не доступний.

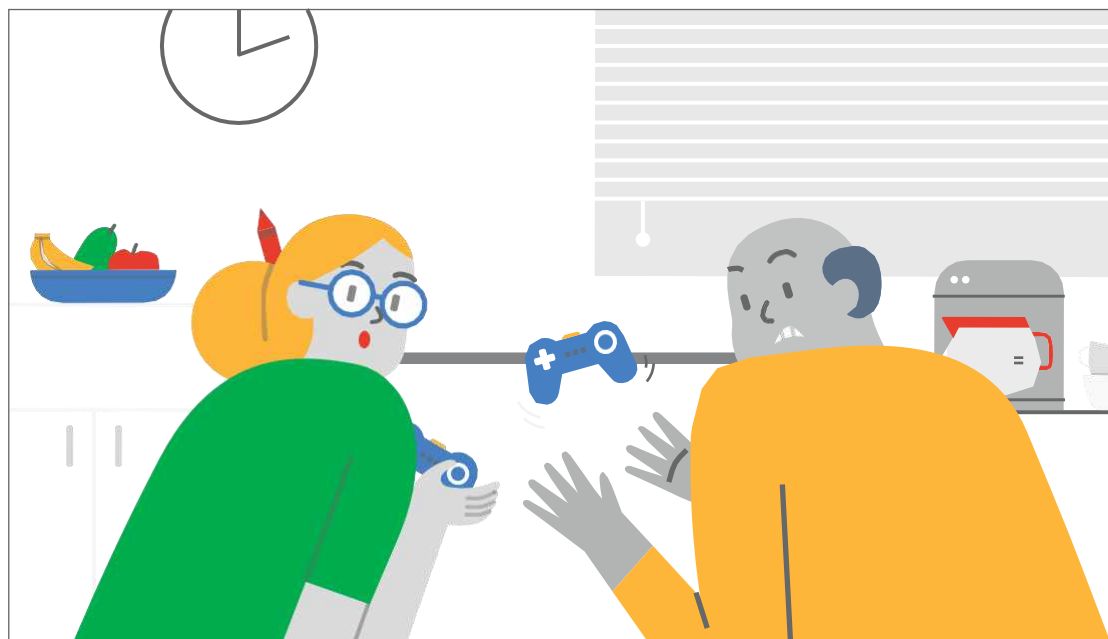
Продовження на наступній сторінці →

2. Перевірка заголовків

Іноді хтось ділиться новиною без URL-адреси. Нижче кілька підказок, які можна використовувати в таких ситуаціях.

- а) На початку новини ми бачимо фотографію чогось, що могло б нас зацікавити (наприклад, милого песика, знаменитості або незвичайного трюку). Але коли ми натискаємо на посилання, новина не має майже нічого спільного із зображенням.
- б) Замість того щоб дозволити вам вирішувати самостійно, деякі сайти намагаються переконати вас погодитися з ними, використовуючи жирний шрифт, УСІ ВЕЛИКІ ЛІТЕРИ, підкреслення або знаки оклику, щоб змусити вас думати, що це щось важливе, і переконати натиснути посилання. Це називається клікбейт.
- в) Щоб змусити вас прочитати новину, деякі люди включають у заголовок такі слова, як «шокуючий», «неймовірний» чи «надзвичайний». Вони знають, що такі слова змушують нас зацікавитися. Але **справжні** журналісти дозволяють новинам говорити самим за себе. Вони розповідають історію, і ми вирішуємо, шокує вона чи дивує.

Наприклад, подивіться на це зображення та заголовок:



Шокуюча правда: що вчителі роблять після школи

Не читаючи наперед, про що, на вашу думку, ця новина? Чому ви так думаєте? Які ваші докази?

Ось новина:

«Нещодавнє опитування викладачів університетів показало, що 86% із них роблять після роботи те саме, що і всі інші. Вони їздять у справах, готують вечерю, проводять час із родиною, займаються домашніми справами й готуються до наступного дня. Але останнім часом багато вчителів роблять дещо несподіване.

Десять років тому проблеми з економікою призвели до того, що багато країн скоротили бюджети на освіту. Це означало роки без підвищення заробітної плати для вчителів. Не в змозі покрити основні витрати через низьку зарплату, багато вчителів зараз працюють на другій роботі. У деяких країнах учителі навіть страйкують, вимагаючи підвищення заробітної плати, аби мати змогу покинути другу роботу й присвятити більше часу своїм учням».

Чи була ця новина такою, як ви думали? Ви вважаєте, що зображення та заголовки були точними чи оманливими? Які ваші докази?

3. Перевірка джерел

Коли ми аналізуємо новини, підказки можуть бути корисними, але їх не завжди достатньо. Іноді надійні новини використовують прийоми, щоб привернути нашу увагу, і через це вони можуть виглядати як неправдиві. А іноді фейкові джерела настільки добре копіюють справжні, що важко сказати, що вони такими не є. Їх важко відрізнити. Наприклад...

Чи здаються вам наступні джерела новин такими, яким можна довіряти?

American News

National Review

News Examiner

World News Daily Report

Weekly World News

NewsWatch33

Насправді, реальним є лише National Review. Звідки ви могли б про це дізнатись? Можна почати з пошуку компанії в Інтернеті. Подивіться, де ще згадується ця назва, крім як на власному веб-сайті організації. Якщо організація згадується у Вікіпедії чи статті на сайті газети або журналу новин, вона, скоріш за все, заслуговує на довіру. Але подивіться, що ці статті говорять про цю організацію! Можливо, усі вони пишуть, що це фейкова організація.

Знайдіть у новинах статтю про свою школу, район, останню модну дієту чи іншу тему, яка вас цікавить. Скористайтеся 3 кроками з роздаткового матеріалу **Визначення надійності**, а також новими підказками, щоб вирішити, реальна ця новина чи оманлива.

Крок 1. Користуйтеся здоровим глуздом

Запитайте себе: Це логічно? Це має сенс?

Іноді все очевидно. Якщо ви бачите заголовок: **ЗНАМЕНИТІСТЬ ТАЄМНО НАРОДИЛА НЕМОВЛЯ ВІД ПРИБУЛЬЦЯ**, логіка, мабуть, говорить вам, що це не реально.

Іноді все не так очевидно. Якщо:

- а) те, що ви бачите, не має сенсу,
- б) ви знаєте, що це неправда з власного досвіду, або в) це суперечить фактам, які вам уже відомі,
...це вірогідно джерело фейкових новин.

Крок 2. Поставте запитання щодо компетенції та мотивів

(див. сторінки 52 та 53)

Крок 3. Підтвердьте інформацію

Запитайте себе: «Чи інші надійні джерела підтверджують те, що говорить це джерело?»

Хто ще пише про цю новину? (Ви можете скористатися пошуком в Інтернеті, щоб перевірити, чи згадується ця новина в інших джерелах...) Які інші новини розміщено на цьому сайті? Усі вони підтримують однакову точку зору чи представляють різні погляди? Якщо ви не можете знайти декілька достовірних джерел, у яких також є ця новина, слід скептично поставитися до такого джерела.

Висновки

Ви вже знаєте, як виявляти дезінформацію, тож зможете щодня ставити правильні запитання й уважно вивчати інформацію в мережі та з часом перетворитися на справжнього експерта з виявлення фейку онлайн. Тепер ви знаєте, як аналізувати інформацію, яку ви отримуєте в Інтернеті. Це називається критичним мисленням, і це суперсила споживачів цифрового контенту.

Якби ми були пошуковою системою

Без використання жодних технологій (ми зробимо це в наступному занятті) учні разом створюють «результати пошуку», щоб дізнатися, як працює пошук в Інтернеті «із середини».

Цілі для учнів



- ✓ **Вивчити** основи пошуку в Інтернеті.
- ✓ **Шукати** інформацію по тій чи іншій темі.
- ✓ **Розуміти**, що результати пошуку — це набір інформації, а не відповіді на запитання.

Обговорення



Що таке пошук?

Інтернет — це місце, де зібрано величезну кількість (мільйони та мільярди) одиниць інформації. Пошук в Інтернеті, який іноді називають пошуковою системою, допомагає нам звузити той шалений обсяг інформації, що надходить з усього світу. Це програмний інструмент, який люди використовують для пошуку інформації на будь-які теми.

Можливо, ви вже знаєте: щоб скористатися цим інструментом, потрібно ввести кілька ключових слів по темі, про яку ви хочете дізнатися більше, у рядок пошуку (порожнє поле на сторінці пошукової системи) або у вікно браузера (там, де ви вводите веб-адреси). Потім натискаєте клавішу вводу або пошуку, і пошукова система чаклує (приблизно півсекунди), а ви отримуєте результати пошуку.

Гаразд, насправді це не зовсім магія. Інтернет-пошук використовує алгоритми, які створили спеціалісти з пошукових систем, щоб навчити програму знаходити та показувати вам інформацію. Але зараз вам не потрібно думати про те, як працюють алгоритми. Вам просто потрібно знати, що пошукова система здійснює пошук для вас.

Також добре знати, що результати пошуку — це не обов'язково відповіді на запитання. Це лише набір інформації, яка вас цікавить або яку ви шукаєте. Якщо у вас є запитання, яке ви вводите в пошукову систему, ви часто можете знайти відповідь у результатах пошуку, але іноді для отримання потрібної відповіді потрібно кілька запитів. Це називається «уточненням» пошуку.

Тож давайте потренуємось, як працює пошук, уявивши, що ми і є пошукова система...

Практичне завдання



Необхідні матеріали

- Аркуш із вправами: «Якби ми були пошуковою системою» (один для кожного учня)

1. Розбийте учнів на групи по 2 учня в кожній.
2. Роздайте копію аркуша із вправами кожному учню.
3. Задайте тему для пошуку всьому класу. Ось деякі можливі варіанти:

• піца	• сонячна система	• вулкани	• баскетбол
• торнадо	• фермер	• кулінарія	• стоматолог
• літак	• футбол	• акули	• будівництво

4. Учні працюють разом у парах, створюючи можливі «результати пошуку» у кожній категорії на роздатковому матеріалі: «Веб-сайт», «Зображення», «Карта» та «Відео». Результати можна представити у вигляді слів або малюнків, залежно від ситуації.

Заохочуйте учнів проявити креативність і пояснить їм, що немає «неправильних» відповідей. Наприклад, якщо тема «акули», учні можуть придумати такі результати пошуку:

- Веб-сайт: інформація про різні види акул
- Зображення: малюнок акули
- Відео: акули плавають в океані
- Карта: розташування пляжу, де люди бачили акулу

5. Коли учні заповнять усі чотири категорії результатів пошуку для заданої теми, виберіть, яку категорію (веб-сайт, зображення, відео чи карту) обговорити в класі.

6. Один учень із кожної пари розповідає про їхній приклад одного з результатів пошуку.

Наприклад, тема «піца». Ви можете попросити кожну групу поділитися результатами зображень піци. Учні можуть підняти малюнок та пояснити, що вони створили. Це дозволить учням побачити всі результати пошуку, які можуть бути сформовані з одного запиту.

7. Після того як учні поділяться прикладами, поставте класу такі запитання для обговорення:

- Скільки приблизно результатів ми отримали?
- Скільки приблизно результатів були подібні?
- Якби ми змінили тему на _____, як, на вашу думку, це змінило б результати? Наприклад, якщо темою пошуку була «піца», як змінилися б результати, якби ми змінили запит на піца «**пепероні**»?

Порада. Виконайте в цілому 4 раунди...

- Виберіть іншу тему з кожного раунду та повторіть зазначені вище кроки.
- Пройдіть 4 раунди, щоб обговорити 4 основні типи результатів пошуку.

Висновки

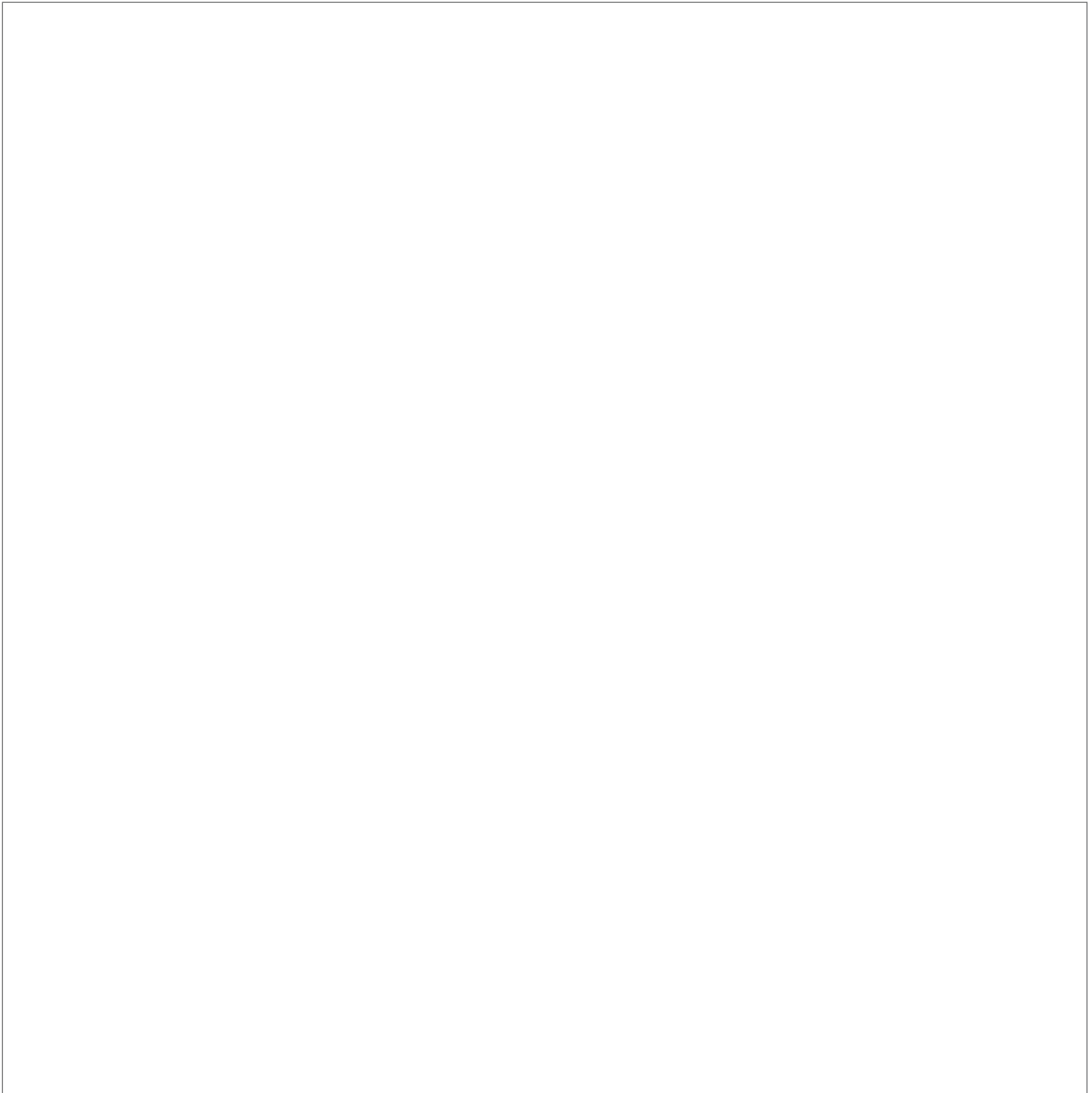
Пошук в Інтернеті — це інструмент, за допомогою якого можна знайти інформацію в мережі. Інформацією може бути текст на веб-сайті, відео, зображення, карта тощо. Ключові слова, які ви вводите в пошукову систему, визначають результати, які ви отримаєте.

Якби ми були пошуковою системою

Тема для пошуку

Веб-сайт

Зображення | Відео | Карта



Практика з пошуку в Інтернеті

Використовуючи пристрій, підключений до Інтернету, учні вивчають роботу пошукових систем та вчаться створювати все більш ефективні пошукові запити.

Цілі для учнів



- ✓ **Орієнтуватися** в пошукових системах.
- ✓ **Практикуватися** у пошуку інформації на задану тему.
- ✓ **Створювати** пошукові запити.
- ✓ **Змінювати** ключові слова та помічати відмінності в результатах пошуку.

Обговорення



Пошук — це інструмент, який допомагає знаходити інформацію в Інтернеті. Щоб скористатися пошуком, можна відкрити пошукову систему та ввести запит — запитання чи ключові слова — у поле пошуку, щоб отримати інформацію на тему, про яку ви хочете дізнатися більше. Іноді використовувати ключові слова краще, ніж просто ставити запитання. Це тому, що **слова, які ви використовуєте** у своєму пошуку, і **порядок цих слів** дуже важливі. Якщо ви просто ставите запитання, у ньому може не бути саме тих слів і порядку, які допомагають пошуковій системі підібрати результати, які ви шукаєте. Але якщо хочете, то можете ввести запитання. Головне — просто почніть шукати, адже часто потрібно ввести більше одного запиту, щоб дістатися до потрібної вам інформації. Тож введіть своє запитання в пошукову систему й подивіться на результати пошуку. Якщо вони вам не зовсім підходять, ви можете на основі цих результатів створити ще кращий запит і ще більше наблизитися до того, що шукаєте.

Приклад. Скажімо, я хочу посадити город. Я хочу вирощувати овочі, які потім можна готувати на кухні.

- Я не уявляю, як це зробити, тому я збираюся шукати інформацію в Інтернеті. Я заходжу в пошукову систему і пишу запитання: «Як посадити город?» *Покажіть екран свого комп'ютера, аби учні могли побачити ваш пошук.*
- Добре, давайте подивимось на ці результати.
Розгляньте результати в класі. Обов'язково зверніть увагу, що є веб-сайти, зображення, відео та інші типи результатів. Також покажіть результати пошуку, які не зможуть допомогти у вирощуванні овочів та спецій для приготування їжі.
- Я бачу, що багато з цих результатів стосуються різних видів городу, але мені потрібна інформація щодо вирощування овочів на своєму городі. Крім того, я хочу вирощувати лише те, що я можу їсти. Напевно, мені слід додати ключове слово про овочі, так? Гаразд, спробуємо пошукати так: «овочі для домашнього городу»
Покажіть екран свого комп'ютера, аби учні могли побачити ваш пошук.
- Погляньте на ці результати. Що ви помітили?
Нехай учні розкажуть, що вони помітили в результатах пошуку.

Обидва набори результатів пошуку дали мені інформацію те, як посадити город, так? Але перший набір стосувався різноманітних видів городу. Він показав, що мені потрібно було додати пару важливих ключових слів до мого оригінального запиту та отримати результати пошуку, які мені потрібні, щоб дізнатися, як посадити овочі для приготування їжі.

Продовження на наступній сторінці →

Що більше ви практикуватиметеся у створенні пошукових запитів, тим легше ви знаходитимете інформацію. Ви завжди можете почати із запитання, і навіть якщо ви не отримаєте відповіді, результати пошуку дадуть вам ключові слова, за якими ви можете продовжити пошук, щоб наблизитися до потрібної інформації. Якщо ви хочете почати з ключових слів і не впевнені, які саме використовувати, просто знайте, що немає «неправильних» ключових слів. Просто почніть шукати! Ви завжди можете спробувати ввести інший запит, якщо не побачили результатів, на які сподівались. Давайте спробуємо...

Практичне завдання



Необхідні матеріали

- Аркуш із вправами: «Практика з пошуку в Інтернеті» (один примірник для кожного учня)
- Пристрій, підключений до Інтернету

1. Створіть перший пошуковий запит

Поясніть учням, що вони вивчатимуть роботу пошукових систем та практикуватимуться у створенні пошукових запитів. На роздатковому матеріалі представлено чотири персонажі, кожен з яких думає (у бульбашці) про щось, що він хоче дізнатися. Потім нехай учні...

- Введуть початковий пошуковий запит (зазначений на роздатковому матеріалі) та розглянуть результати пошуку.
- Запишуть 4–5 результатів пошуку на роздатковому матеріалі.

2. Створіть власний (другий) пошуковий запит

Нехай учні ще раз подивляться на те, що хоче дізнатися персонаж (у бульбашці). Запитайте учнів, чи дали початкові результати пошуку достатньо інформації стосовно цієї теми?

- Запропонуйте учням змінити початковий запит, включивши ключові слова, які дадуть їм більш корисні результати пошуку.

Підказка. Учні можуть знайти ключові слова в перших результатах пошуку або в бульбашці думок персонажа.

- Попросіть учнів ввести другий пошуковий запит у пошукову систему та розглянути результати пошуку.
- Нехай учні запишуть 4–5 результатів пошуку на роздатковому матеріалі.

3. Обговоріть

Попросіть учнів розбитися по двоє та обговорити в парах, як вони змінили початковий пошуковий запит і які типи результатів вони отримали за зміненням пошуковим запитом. Попросіть їх поділитися висновками під час короткого обговорення в класі.

4. Повторіть кроки 1–3 для решти персонажів

Висновки

Що більше ви практикуватиметеся у створенні пошукових запитів, тим легше ви знаходитимете інформацію у пошуковій системі.

Практика з пошуку в Інтернеті

Шукаю, що б почитати.
Я люблю таємниці! Мені також подобаються книги,
де є уявні персонажі, що живуть у майбутньому.
Здається, мій учитель називає це науковою фантастикою.



Я хочу приготувати торт до дня народження сестри.
Вона не любить шоколад, але любить фрукти.
Цікаво, який торт мені спекти.



Вихідний пошуковий запит

Книжки про вигаданих персонажів і таємниці

Результати пошуку

Змінений пошуковий запит

Результати пошуку

Вихідний пошуковий запит Торт
з фруктами без шоколаду

Результати пошуку

Змінений пошуковий запит

Результати пошуку

Продовження на наступній сторінці →

Вихідний пошуковий запит

Робота з відеоіграми

Результати пошуку

Змінений пошуковий запит

Результати пошуку

Вихідний пошуковий запит

Що потрібно для риболовлі?

Результати пошуку

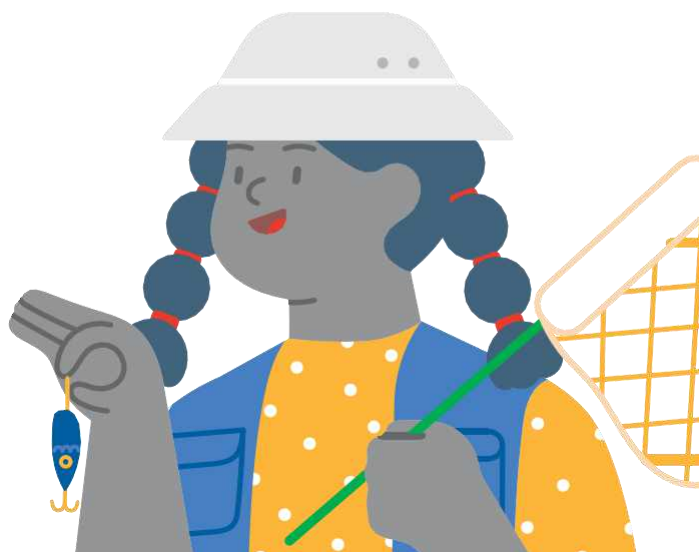
Змінений пошуковий запит

Результати пошуку

Я люблю грати у відеоігри.
Може, коли я виросту, то буду працювати в компанії,
що займається відеоіграми.
Було б так класно, якби колись це стало моєю роботою!



Двоюрідний брат запросив мене порибалити.
Я ніколи раніше не ловила рибу, тому не знаю,
яке спорядження потрібно взяти із собою.



Interland: Річка реальності

Річка, що тече через Інтерленд, несе у собі факти та вигадки. Але все не завжди так, як здається. Щоб подолати бурхливий потік, використовуйте здоровий глузд і не ведіться на оманливі витівки тих, хто виловлює в цих водах приватні дані, тобто займається фішингом.

Відкрийте на своєму комп'ютері або мобільному пристрої (наприклад, на планшеті) веб-браузер і зайдіть на сайт g.co/RealityRiver.

Теми для обговорення



Запропонуйте своїм учням зіграти в «Річку реальності». Використовуючи наведені нижче запитання, обговоріть, які висновки можна зробити з цієї гри. Більшість учнів отримують найбільше задоволення від гри, коли грають самостійно, але ви також можете запропонувати їм пограти у парах. Це може бути особливо корисним для молодших учнів.

- Опишіть випадок, коли вам довелося вирішувати, чи було щось в онлайні справжнім чи шахрайським. Які знаки чи ознаки ви помітили?
- Що таке фішер? Опишіть його дії й те, як він впливає на гру.
- Чи вплинула гра в «Річку реальності» на те, як ви оцінюватимете речі та людей онлайн у майбутньому? Якщо так, яким чином?
- Назвіть одну річ, яку ви робитимете інакше, після того як пройшли ці уроки та зіграли в гру.
- Які можуть бути ознаки того, що щось «не так» із певною ситуацією онлайн або що вона є загрозовою?
- Що ви відчуваєте, коли стикаєтеся в онлайні з чимось сумнівним?
- Якщо ви не впевнені, чи щось є справжнім, що вам варто зробити?

