МЕДОТИЧНИЙ ПОСІБНИК ДО ОНЛАЙН-КУРСУ

ОСНОВИ КІБЕРБЕЗПЕКИ ДЛЯ ШКОЛЯРІВ

ДЛЯ 10-11 КЛАСІВ

2023

Методичні посібники розробила громадська організація “Смарт освіта”

Курс “Основи кібербезпеки для школярів” розроблений CRDF Global в Україні в співпраці з ГО “Смарт Освіта” та технічними експертами компанії Technomatix за підтримки Державного департаменту США (Офіс із координації допомоги Європі та Євразії).

Мета курсу – зміцнення рівня обізнаності та підвищення загального рівня знань у сфері кіберзахисту здобувачів освіти, їхніх батьків та вчителів.
Курс розміщений на платформі за посиланням: cyberkidsukraine.org

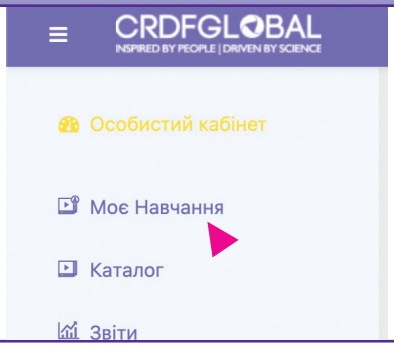
Для його проходження / використання матеріалів необхідно зареєструватися.
З огляду на вікові особливості школярів, матеріали курсу адаптовані для учнів 1-2 класів, 3-4 класів, 5-6 класів, 7-9 класів, 10-11 класів.

ДЛЯ УЧНІВ 10-11 КЛАСІВ КУРС СКЛАДАЄТЬСЯ З ТАКИХ НАВЧАЛЬНИХ МОДУЛІВ:

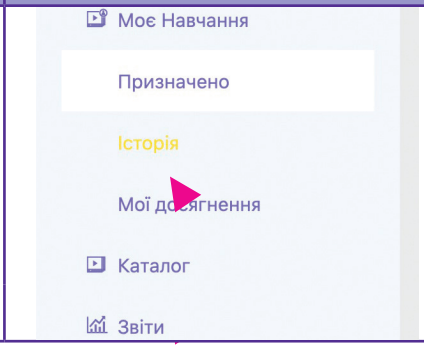
Модуль 1. Основні помилки користувачів	**Модуль 2. Безпечне використання мобільного телефону**
• Як зловмисники отримують доступ до наших персональних даних і носіїв інформації. • Які наслідки можуть мати кібератаки для користувачів. • Як убезпечити себе та свої дані в цифровому світі.	• Які існують загрози для мобільних носіїв інформації. • Як захистити телефон та дані на ньому від зловмисників.
Модуль 3. Безпечне використання комп'ютерів	**Модуль 4. Безпечне використання електронної пошти**
• До яких наслідків призводить порушення правил безпеки під час використання комп'ютерів. • Що робити, аби не стати жертвою хакерської атаки.	• Які атаки можуть здійснюватися через електронну пошту. • Як убезпечити свій обліковий запис та повідомлення від дій зловмисників.
Модуль 5. Безпека в соціальних мережах	**Модуль 6. Інтернет-безпека**
• Яка особиста інформація користувачів потрапляє в соцмережі. • До чого призводять витоки даних. • Як налаштувати параметри конфіденційності.	• Якої шкоди може завдати порушення правил безпеки під час використання інтернет-ресурсів. • Яких рекомендацій треба дотримуватися, щоби захиститися від нападів зловмисників.
Модуль 7. Типи шкідливих програм	**Модуль 8. Фейкові новини**
• Які існують типи шкідливих програм та яку небезпеку вони несуть. • За якими ознаками можна розпізнати небезпечне ПЗ і як вберегтися від атак хакерів.	• Які існують різновиди фейкових новин. • Які причини виникнення та канали поширення неправдивих новин. • Як розпізнати інформаційну маніпуляцію.
Модуль 9. Основні правила захисту інформації	**Модуль 10. Що робити, якщо кіберзлочин все-таки стався**
• Фізичні аспекти безпеки інформації. • Поради з використання паролів, створення резервних копій даних. • Важливість використання ліцензійного ПЗ, антивірусів та фаєрволів. • Безпекові аспекти користування соціальними мережами.	**Як діяти в таких ситуаціях:** • обліковий запис був зламаний; • електронний пристрій заражений вірусом; • зловмисник дізнався дані банківської картки; • гаджет викрали; • були викрадені персональні дані.

Зареєстровані користувачі платформи матимуть доступ до кожного навчального модуля. У такий спосіб, учні та їхні батьки можуть проходити курс самостійно, а вчитель матиме можливість використовувати деякі модулі під час навчання.
Після успішного проходження тесту, кожен користувач отримає сертифікат про те, що він опанував навчальний онлайн-курс «Базові правила інформаційної безпеки».
ПРИМІТКА. Якщо ви вже завершили курс для 10-11 класів, але хочете повернутися до якоїсь частини (наприклад, на уроках чи класних годинах), виконайте наступні дії.

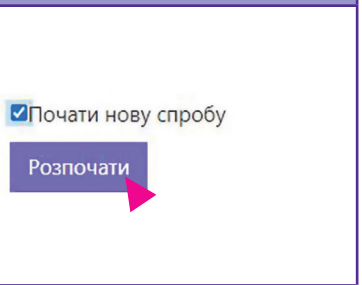
1. Після входу в систему, оберіть меню «Моє навчання» (зліва на панелі навігації сайту).



2. Відкрийте меню «Історія», у якому знайдете завершені курси.



3. Відкрийте курс, наприклад, за 1-2 клас, оберіть потрібний модуль і зробіть позначку в клітинці.



4. Натисніть «Розпочати».

ПРИКЛАДИ ВИКОРИСТАННЯ ОКРЕМИХ МОДУЛІВ КУРСУ НА УРОКАХ

Запропоновані матеріали розроблені на основі діяльнісного, особистісно орієнтованого та компетентнісного підходів. Враховані такі наскрізні змістові лінії: «інформаційне середовище» (вміння критично аналізувати інформацію, висловлювати зважені судження), «здоров'я і безпека», «громадянська відповідальність» (формування відповідального члена суспільства).

Формування компетентностей

Вільне володіння державною мовою
• вміння доступно й переконливо висловлювати думки, вести аргументовану дискусію відповідно до теми.
Інформаційно-цифрова компетентність
• дотримання правил безпеки в мережах та мережевого етикету.
Ініціативність і підприємливість
• використовувати досвід діяльності в інтернеті для вибору життєвих стратегій; • виявляти можливості й загрози використання інтернету (у тому числі й для майбутньої професійної та підприємницької діяльності); • уміння визначати всі можливі варіанти причин виникнення проблем та їх розв'язання (які пов'язані з використанням мережі Інтернет).
Соціальна та громадянська компетентності
• вміння комунікувати та працювати з іншими; • критично аналізувати джерела масової інформації для протистояння деструктивним і маніпулятивним технікам впливу.
Навчання впродовж життя
• використовувати різноманітні підходи й форми навчання, можливості сучасних навчальних середовищ (зокрема, онлайн-середовищ) для побудови власної траєкторії розвитку.

ВЧИТЕЛЮ ІНФОРМАТИКИ

ТЕМА. «ОСНОВНІ ПОМИЛКИ КОРИСТУВАЧА ТА ЇХ МОЖЛИВІ НАСЛІДКИ»

ПРИМІТКА. За основу розробки взято матеріали 2, 3, 4 модулів курсу.

Мета:
• формування предметних, міжпредметних і ключових компетентностей в учнів; • формування культури інформаційної безпеки для запобігання можливим негативним наслідкам.
Завдання:
• навчити учнів оцінювати ризики під час використання онлайн ресурсів, пристроїв, програм, аналізувати рівень безпеки в різних ситуаціях; • розвивати в учнів навички роботи в групі; • розвивати навички ефективного пошуку та аналізу інформації; • розвивати вміння аналізу помилкової поведінки в цифровому світі, що може призвести до негативних наслідків.
Необхідне обладнання:
• телевізор / проєктор і екран для перегляду відео; • комп'ютери / смартфони / планшети з доступом до інтернету в дітей, роздаткові матеріали.

РЕКОМЕНДАЦІЇ ДЛЯ ПРОВЕДЕННЯ ТЕМАТИЧНОГО УРОКУ З ОСНОВ КІБЕРБЕЗПЕКИ У 10-11 КЛАСАХ (В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ)

За тиждень до уроку запропонуйте учням:
1. об'єднатись у п'ять груп;
2. самостійно ознайомитися з матеріалами курсу «Основи кібербезпеки для учнів» (1-2 групи – 2 модуль, 3 група – 3 модуль, 4 група – 4 модуль, 5 група «Психологи» виконує окреме завдання);
3. за допомогою жеребкування визначити номер групи;
4. виконати завдання.

Завдання для груп (див. додаток 1) і правила роботи в групі (див. додаток 2) розмістіть на Google Диску (чи іншому сервісі хмарного зберігання), надайте дітям до них доступ.
Під час дистанційного навчання, вчитель / вчителька створює додаткові ресурси для роботи кожної групи (наприклад, групові чати, сесійні зали в Zoom тощо).

ПРИМІТКА. Якщо діти навчаються офлайн, усі завдання вони можуть виконувати на уроці. Підготуйте роздруківку з QR-кодами, за допомогою яких учні отримають доступ до матеріалів.

Тривалість уроку: офлайн – 45 хв, дистанційне навчання – відповідно до санітарних норм.

ХІД УРОКУ

I. Організаційний момент (до 1 хв)

II. Актуалізація опорних знань (до 3 хв)

Запитання до учнів:
1. Світ навколо нас стрімко переносить інформацію з аналогових джерел у цифровий вигляд. Чи створює це додаткові ризики в нашому повсякденному житті?
2. Чи можна користуватися інтернетом без ризику постраждати від шахраїв чи хакерів?
3. Чи все ми робимо для того, щоб захистити наші персональні дані та іншу приватну інформацію?

Відповіді школярів

Учитель / вчителька:
Безумовно, повністю виключити інтернет-загрози неможливо. Але можна максимально себе убезпечити, якщо розумієш ключові помилки користувачів інтернету.
Розгляньмо ті з них, які трапляються найчастіше, щоб зрозуміти, як робити не потрібно.

III. Визначення мети уроку (1-2 хв)

1. Запропонуйте учням визначити освітню мету уроку.
2. Узагальніть їхні відповіді.

IV. Робота в групах

(20 хвилин, якщо навчання офлайн і діти виконують завдання на уроці. В умовах дистанційного навчання, учні на уроці лише презентуватимуть свою роботу).

Учні чотирьох груп розглядають ситуації 2-4 модулів курсу. Кожна група має провести обговорення можливих наслідків конкретної ситуації.

Завдання для груп 1-4

- Ознайомтеся з правилами роботи в групі.
- Розгляньте ситуацію.
- Визначте основні поняття, які використовуються в ситуації.
- Знайдіть в інтернеті інформацію про подібні ситуації та можливі негативні наслідки.
- Презентуйте результати своєї роботи однокласникам.

ПРИМІТКА. В умовах дистанційного навчання, учні мають підготувати презентацію та продемонструвати її.

РОЛЬ УЧИТЕЛЯ / ВЧИТЕЛЬКИ

Під час роботи груп учитель / учителька консультує, за потреби надає допомогу у виконанні завдань, забезпечує морально-психологічний комфорт у групах.

Ситуація 1. Анімаційний ролик «Безпечне використання мобільного телефону 1» (01:05 хв)
Легковажний учень вихваляється на дні народження своїм новеньким смартфоном. Попередньо він не встановив захист на своєму смартфоні (код або відбиток пальця).

Ситуація 2. Анімаційний ролик «Безпечне використання мобільного телефону 2» (02:07 хв)
Дівчинка завантажує додаток із Play Market на свій телефон (розробник додатка невідомий, коментарів та відгуків про додаток немає).

Ситуація 3. Анімаційний ролик «Безпечне використання комп'ютерів» (02:17 хв)
Учениця підключає до свого ноутбука флешку, яку знайшла в публічному місці. Попередньо вона не встановила антивірус, тому на її ноутбуці з'явилося шкідливе ПЗ.

Ситуація 4. Анімаційний ролик «Безпечне використання електронної пошти» (02:02 хв)
Учениця, яка успішно веде свій блог, отримує повідомлення на пошту від імені Instagram про порушення авторських прав і про те, що вона має 24 години на відновлення акаунта. Адреса дуже схожа на реальну, наприклад, info@theinstagram.team.
У повідомленні є кнопка, щоб оскаржити видалення акаунта "Review complaint", перехід за якою веде на фішинговий сайт.
Учениця переходить за посиланням та вводить свій логін і пароль на сайті зловмисника.

ГРУПА 5 «ПСИХОЛОГИ»

ПОМІРКУЙТЕ
Що робити, якщо ви дізналися, що ваш однокласник або товариш переглядає заборонений контент, перебуває в небезпечній групі, має наміри зробити щось загрозливе?
Спробуйте розробити алгоритм «кризового реагування» в складних ситуаціях у класі.

Висловіть свою думку, пошукайте відповіді на запитання:
1. Якщо я дізнався / дізналася, що однокласник / подруга збирається зробити ризиковану дію, – як правильно мені вчинити?
2. Як зрозуміти, що однокласнику / другові погано?
3. Що я роблю, коли мені погано?
4. Як розрізнити «небезпечну інформацію»?
5. До кого можна звернутися за допомогою?
6. Що ми робимо в класі, щоби підтримувати одне одного?

IV. Презентація роботи (15 хв)

ПРИМІТКА. Усі команди-учасники можуть доповнювати запропоноване рішення, ставити запитання.

V. Рефлексія (до 5 хв)

Запропонуйте дітям поділитися враженнями від уроку.

- На скільки корисним був урок?
- Що вдалося, а що ні?
- Чи знадобляться здобуті знання та вміння в подальшому житті?
- Чи потрібно передати ці знання батькам, друзям, іншим людям?
- Які переваги й недоліки групової роботи?

VI. Оцінювання роботи

Вчитель ухвалює рішення чи буде оцінюватися діяльність учнів.
Можна запропонувати учням формат самооцінювання своєї роботи й оцінювання вчителем (див. додаток 3).

ДОДАТОК 1
ОСНОВНІ ПОМИЛКИ КОРИСТУВАЧА ТА ЇХ МОЖЛИВІ НАСЛІДКИ
ЗАВДАННЯ ГРУПАМ

Завдання для груп 1-4

Самостійно ознайомтеся з матеріалами курсу «Основи кібербезпеки для учнів» (1-2 групи – 2 модуль, 3 група – 3 модуль, 4 група – 4 модуль).

- Оберіть ситуацію, яку розглядатиме ваша команда.
- Визначте основні поняття, які використовуються в ситуації.
- Знайдіть в інтернеті інформацію про подібні ситуації та їх можливі негативні наслідки.
- Підготуйте презентацію роботи команди для ваших однокласників.

ПРИМІТКА. В умовах дистанційного навчання, команда має підготувати та продемонструвати презентацію.

Ситуація 1. «Безпечне використання мобільного телефону 1» (01:05 хв)
Легковажний учень вихваляється на дні народження своїм новеньким смартфоном. Попередньо він не встановив захист на своєму смартфоні (код або відбиток пальця).

Ситуація 2. «Безпечне використання мобільного телефону 2» (02:07 хв)
Дівчинка завантажує додаток із Play Market на свій телефон (розробник додатка невідомий, коментарів та відгуків про додаток немає).

Ситуація 3. «Безпечне використання комп'ютерів» (02:17 хв)
Учениця підключає до свого ноутбука флешку, яку знайшла в публічному місці. Попередньо вона не встановила антивірус, тому на її ноутбуці з'явилося шкідливе ПЗ.

Ситуація 4. «Безпечне використання електронної пошти» (02:02 хв)
Учениця, яка успішно веде свій блог, отримує повідомлення на пошту від імені Instagram про порушення авторських прав і про те, що вона має 24 години на відновлення акаунта. Адреса дуже схожа на реальну, наприклад, info@theinstagram.team.
У повідомленні є кнопка, щоб оскаржити видалення акаунта "Review complaint", перехід за якою веде на фішинговий сайт.
Учениця переходить за посиланням та вводить свій логін і пароль на сайті зловмисника.

ГРУПА 5 «ПСИХОЛОГИ»
ПОМІРКУЙТЕ
Що робити, якщо ви дізналися, що ваш однокласник або товариш переглядає заборонений контент, перебуває в небезпечній групі, має наміри зробити щось загрозливе?
Спробуйте розробити алгоритм «кризового реагування» в складних ситуаціях у класі.

Висловіть свою думку, пошукайте відповіді на запитання:
1. Якщо я дізнався / дізналася, що однокласник / подруга збирається зробити ризиковану дію, – як правильно мені вчинити?
2. Як зрозуміти, що однокласнику / другові погано?
3. Що я роблю, коли мені погано?
4. Як розрізнити «небезпечну інформацію»?
5. До кого можна звернутися за допомогою?
6. Що ми робимо в класі, щоби підтримувати одне одного?

ДОДАТОК 2

Правила роботи в групі

1. Розподіліть між собою обов'язки в команді згідно з видом діяльності:
- пошук інформації;
- організація роботи всіх учасників;
- систематизація інформації;
- підготовка презентаційних матеріалів.

2. Дотримуйтеся принципу обов'язковості виконання домовленостей.

3. Ставтеся з повагою до думок інших членів групи.

4. Дотримуйтеся принципу рівності сторін.

5. Будьте толерантними.

ДОДАТОК 3

ТАБЛИЦЯ САМООЦІНЮВАННЯ ТА ОЦІНЮВАННЯ ВЧИТЕЛЕМ

	Критерії самооцінювання	Максимум балів	Самооці-нювання	Оцін. вчителя
1	Повнота викладу інформації: теоретичні поняття, пояснення, терміни	5		
2	Повнота опису наслідків ситуації	4		
3	Відповідність прикладу, запропонованого командою, до теми ситуації	5		
4	Чіткість та повнота відповідей на запитання	4		
5	Рівень презентації розробки	5		
6	Креативний підхід до розробки	4		
7	Командна робота (спільне презентування, розподіл ролей, участь всіх у роботі)	5		
8	Активна участь (доповнення під час презентації розробок інших команд)	4		
	Загальна кількість балів	**12**		

ВЧИТЕЛЮ ГРОМАДЯНСЬКОЇ ОСВІТИ

Заняття 2. «ЦИФРОВА ІДЕНТИЧНІСТЬ. БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ»

ПРИМІТКА. За основу розробки взято матеріали **5 модулю «Безпека в соціальних мережах»**, які можуть бути використані вчителем / вчителькою курсу Громадянська освіта (інтегрований курс) в 10 класі як додаткове заняття, щоб учні відпрацювали практичні навички.

Предмет, розділ, тема за програмою МОН	Очікувані результати навчально-пізнавальної діяльності учнів / учениць за програмою МОН	Питання, що розглядаються в модулі 5 курсу
Громадянська освіта (інтегрований курс) 10 клас **Розділ 5 «Світ інформації, мас-медіа та медіаграмотність»** **Тема 5 «Інтернет»** • Приватність та конфіденційність у віртуальному світі. • Цифрова ідентичність. • Соціальні мережі. • Права людини в інтернеті. • Безпека та етика поведінки в мережі. • Кіберзлочинність.	**Знання і розуміння:** • Знає зміст понять: соціальні мережі. • Знає можливості Інтернету та усвідомлює небезпеки, пов'язані з його використанням. **Вміння і навички:** • Простежує переваги й ризики під час користування соціальними мережами.	• Яка особиста інформація користувачів потрапляє в соцмережі. • До чого призводять витоки даних. • Як налаштувати параметри конфіденційності.

Мета:
• формування предметних, міжпредметної та ключових компетентностей в учнів; • формування культури інформаційної безпеки для запобігання можливим негативним наслідкам.
Завдання:
• навчити учнів розпізнавати основні помилки користувачів соціальних мереж та визначати рівень безпеки в різних ситуаціях; • розвивати вміння аналізу помилкової поведінки в цифровому світі, що може призвести до негативних наслідків; • розвивати вміння роботи в групі.
Очікувані результати:
Учень / учениця: • знає можливості Інтернету та усвідомлює небезпеки, пов'язані з його використанням під час користування соціальними мережами; • вміє налаштувати параметри приватності акаунта; • аналізує ситуації, пов'язані з можливими ризиками та запобігає їх виникненню.
Необхідне обладнання:
• телевізор / проєктор і екран (для роботи офлайн), ноутбук / комп'ютер із доступом до інтернету в учителя; • смартфони / планшети з доступом до інтернету в дітей; • листи фліпчарта, маркери (для роботи офлайн).

В умовах дистанційного навчання вчитель на власний розсуд визначає, які завдання учні будуть виконувати на уроці. Крім того, запропоновані завдання можуть бути випереджальними. У такому випадку, учні самостійно зареєструються на курс, виконають завдання п'ятого модуля, а на уроці лише презентують результати.

Тривалість уроку: офлайн – 45 хв, дистанційне навчання – відповідно до санітарних норм.

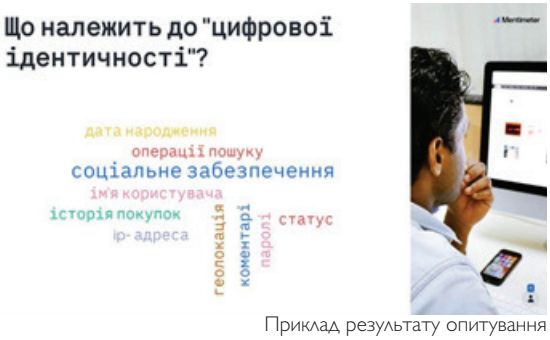
ХІД УРОКУ

I. АКТУАЛІЗАЦІЯ ЗНАНЬ (до 5 хв)

Запитайте учнів про їхню діяльність у мережі за останню добу.

Вислухайте відповіді.

Запропонуйте учням за допомогою гаджетів пригадати / визначити, що належить до цифрової ідентичності. Для цього скористайтеся сервісом для опитувань Mentimentr (учням можна надати QR-код тощо).



Приклад результату опитування

Підсумуйте відповіді, пригадайте / поясніть термін

Цифрова ідентичність (або ідентичність онлайн) – це сукупність інформації, дані, які унікально описують особу, організацію або електронне обладнання, що існує в інтернеті[1].

Запитання до учнів
- Як можуть бути використані наші особисті дані за допомогою «цифрового сліду»?
- Чи можна захистити конфіденційність в Інтернеті?

Відповіді учнів.

Запитайте, що таке соціальна мережа.

Відповіді учнів.

Якщо учні не зможуть відповісти, поясніть.

Соціальна мережа – це вебсервіс, віртуальна спільнота, що складається з людей з однаковими інтересами, нахилами, діяльністю[2].

Запропонуйте назвати найпопулярніші соціальні мережі в Україні серед дітей, підлітків і дорослих.
Відповіді учнів.

Запропонуйте дітям відповісти на запитання:

- Яку роль відіграють соціальні мережі у вашому житті?
- Чи викладали ви колись фото зроблені під час відпочинку в іншій країні?
- Чи писали в дописах про час відпочинку?
- Хто з вас викладав інформацію про місце й графік роботи батьків?
- Хто робив фото у квартирі, хизуючись дорогими подарунками?
- Чи впевнені ви у своїй безпеці, розміщуючи інформацію про себе та інших людей (наприклад, родичів чи друзів) у соціальних мережах?

Відповіді учнів

ПРИМІТКА. Під час дистанційного уроку діти можуть ставити помітки на слайді презентації біля запитання, якщо їхня відповідь «так».

II. МОТИВАЦІЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ (до 2 хв)

Запропонуйте учням визначити неприємності, на які можна натрапити, користуючись соціальними мережами.

ПРИМІТКА. Відповіді учнів можна доповнити інформацією, яка подається у вступній частині 5 модуля.

Скажіть, що знання і навички, які учні здобудуть на уроці, допоможуть убезпечити себе й інших небайдужих їм людей від багатьох проблем.

[1]Громадянська освіта. 3D Демократії: думаємо, дбаємо, діємо : методичний посібник до курсу громадянської освіти для 10-го класу закладів загальної середньої освіти : в 7-ми частинах / П. Вербицька, О. Волошенюк, Г. Горленко та ін. ; за ред. П. Кендзьора. — Львів : ВД «Панорама», 2018. Світ інформації, мас-медіа та медіаграмотність : частина 5. — 2018. — 56 с. ; іл.

[2]Підручник: Т. В. Бакка Громадянська освіта (інтегрований курс, рівень стандарту): підруч. для 10 кл. закл. загал. серед. освіти / Т.В. Бакка, Л.В. Марголіна, Т.В. Мелещенко. — Київ : Вид-во «Оріон», 2018.

III. ВИЗНАЧЕННЯ МЕТИ УРОКУ (1-2 хв)

Запропонуйте учням визначити освітню мету уроку.

Узагальніть відповіді.

IV. АНАЛІЗ СИТУАЦІЙ (до 10 хв)

Розкажіть старшокласникам про курс.
CRDF Global в Україні (Фонд цивільних досліджень та розвитку США – некомерційна організація) у співпраці з ГО «Смарт Освіта» розробили курс «Основи кібербезпеки для школярів». Для учнів 10-11 класу розроблено 10 модулів. За допомогою модулю 5 «Безпека в соціальних мережах» ми можемо перевірити свої знання (повторити те, що вже знаємо).

Запропонуйте розглянути прикрі ситуації, які трапилися з користувачами соціальних мереж і визначити, що було зроблено неправильно і як має бути правильно.

1. Перегляд відео «Історія Асі» та «Історія Аліни» (частина модуля «Поміркуємо разом»).
2. У парах або групах (поділ здійснює вчитель / вчителька) діти визначають помилки користувачок соціальних мереж.

Ситуація 1 – «ІСТОРІЯ АСІ»

ТЕКСТОВА ІНФОРМАЦІЯ АНІМАЦІЇ (ВЧИТЕЛЮ ДЛЯ ПІДГОТОВКИ УРОКУ)

Сторінка Асі в Instagram не захищена налаштуваннями конфіденційності. Ася збирається відвідати великий концерт. Старшокласниця змінила аватарку на фотографію, на якій вона тримає квиток на вказаний вище захід з усіма видимими атрибутами (у тому числі й QR-кодом). Оскільки в публікації фотографія була розміщена у високій якості, зловмисник зміг скопіювати QR-код і зробити підроблений квиток. Ася не змогла потрапити на фестиваль, тому що її квиток уже був використаний зловмисником.

Алгоритм роботи з анімаційним роликом
1. Вчитель / вчителька демонструє анімацію.
2. Вчитель / вчителька пропонує учням визначити помилки в діях дівчини та як потрібно було вчинити правильно.

Можливі варіанти відповідей учнів

Помилки
1. Ася публікує фотографію з квитком у соціальних мережах.
2. Профіль облікового запису в налаштуваннях конфіденційності встановлено як "Публічний".

Як має бути правильно
1. Перш ніж опублікувати інформацію в соціальних мережах, потрібно проаналізувати її зміст.
2. Профіль облікового запису в налаштуваннях конфіденційності має бути "Тільки для друзів".

Ситуація 2 «ІСТОРІЯ АЛІНИ»

ТЕКСТОВА ІНФОРМАЦІЯ АНІМАЦІЇ (ВЧИТЕЛЮ ДЛЯ ПІДГОТОВКИ УРОКУ)

Аліна є користувачкою соціальної мережі. У стрічці дівчинки зберігається багато її особистих даних. Стрічка дозволяє визначити інтереси, місце навчання, місце проживання, улюблені місця дозвілля тощо.
На основі історичних даних у профілі, зловмисник складає портрет Аліни та визначає ключові області її інтересів. Зловмисник створює новий обліковий запис, який наповнює різним вмістом, у тому числі на теми, які близькі дівчині. Потім зловмисник додається в друзі до Аліни та обговорює з нею спільні інтереси, встановлюючи довірчі відносини. Після кількох днів інтенсивного спілкування, Аліна повідомила «новому другу» про те, що її батьки запланували відпочинок за кордоном для всієї сім'ї. Завдяки великому досвіду й ретельному опрацюванню легенди, зловмисник переконує дівчину, що відпочивав із батьками майже в 36 країнах світу й дає свої «поради» щодо відпочинку. Учениця розповідає куди, коли та на який час її родина їде на відпочинок. Зловмисник отримує інформацію про рівень заможності родини та час, коли нікого з родини не буде у квартирі.
Як висновок, через необережність дівчинки квартирні крадії "обчистили" помешкання її родини.

Алгоритм роботи з анімаційним роликом
1. Вчитель / вчителька демонструє анімацію2.
2. Вчитель / вчителька пропонує учням визначити помилки в діях дівчини та як потрібно було вчинити правильно.

Можливі варіанти відповідей учнів

Помилки
1. Аліна вказує всю інформацію про себе й не конфігурує налаштування конфіденційності.
2. Аліна додає в друзі зловмисника, не перевіряючи термін життя сторінки.
3. Аліна разом зі зловмисником обговорює терміни та умови відпочинку.

Як має бути правильно
1. Варто чистити, мінімізувати або узагальнено вказувати персональні дані в усіх соціальних мережах.
2. Потрібно перевіряти термін життя сторінки «нового друга» й ставити собі питання, чи бувають люди, наприклад, які репостять 400 дописів за 2 дні, але не роблять жодного репосту раніше?
3. Ставитися з підозрою до «нових друзів», які пропонують обмінятись інформацією про паролі, заробітну плату батьків, майбутній відпочинок (Де? Коли? На скільки? Хто залишиться вдома?)

V. ВИКОНАННЯ ПРАКТИЧНИХ ЗАВДАНЬ (до 10 хв)

1. Запропонуйте старшокласникам перевірити, як вони засвоїли правила безпеки користування соціальними мережами.

Практичне завдання 1 «Безпека в соціальних мережах»
доступ https://learningapps.org/watch?v=paemr6m8t22

ТЕКСТОВИЙ ВАРІАНТ ЗАВДАННЯ 1 «БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ» (ВЧИТЕЛЮ ДЛЯ ПІДГОТОВКИ УРОКУ)

Ви вирішили зареєструватися в одній із соціальних мереж. Яка інформація, вказана в профілі, не зашкодить вашій безпеці?
Варіанти:
- *Завантажте вашу фотографію*
- *ПІБ * – обов'язкове поле*
- *Дата народження*
- *Стать*
- *Номер телефону*
- *Електронна пошта * – обов'язкове поле*
- *Адреса проживання*
- *Місто проживання*
- *Сімейний стан*
- *Родичі (посилання на сторінки родичів)*
- *Ваше місце навчання / роботи*
- *Ваша освіта*
- *Ваші інтереси*

Якщо діти обрали всі поля крім червоних, то при натисканні кнопки «Перевірити» з'являється повідомлення «Розумний вибір. Телефон і адреса мають бути недоступні для широкого загалу».

2. Запропонуйте дітям допомогти користувачу вибрати параметри конфіденційності при створенні профілю в соціальній мережі.

Для цього вчитель має підготувати до уроку віртуальну дошку Jamboard.
Приклад дошки Jamboard
https://jamboard.google.com/d/1BW6VUiLDZ6W22K5hdONNFq-FgMhG3Gx79of_RIVy-CM/edit?usp=sharing

ПРИМІТКА. Можна створити п'ять груп (діти кожної групи будуть працювати на своїй сторінці), або ж робота буде фронтальною (з усіма учнями одночасно).

ТЕКСТОВИЙ ВАРІАНТ ПРАКТИЧНОГО ЗАВДАННЯ (ВЧИТЕЛЮ ДЛЯ ПІДГОТОВКИ УРОКУ).

Допоможіть користувачу вибрати параметри конфіденційності при створенні профілю в соціальній мережі.
Коментарі до виконання завдання:
Зелений статус означає, що налаштування конфіденційності сконфігуровані безпечним чином. Конфіденційна інформація про вас доступна тільки вашим друзям.
Помаранчевий статус означає, що конфіденційність сторінки знаходиться на середньому рівні й деякі персональні дані можуть бути доступні широкій аудиторії користувачів.
Червоний статус означає, що налаштування конфіденційності вашого профілю роблять ваші персональні дані доступними широкій аудиторії користувачів, що полегшує потенційним зловмисникам збір інформації про вас для здійснення зловмисних дій.
1. Хто може переглядати вашу сторінку?
- *Тільки я*
- *Мої друзі*
- *Усі користувачі*

2. Хто може переглядати ваші фотографії?
- *Тільки я*
- *Мої друзі*
- *Усі користувачі*

3) Хто може надсилати вам повідомлення?
- *Тільки я*
- *Мої друзі*
- *Усі користувачі*

4) Хто бачить місце розташування ваших фотографій?
- *Тільки я*
- *Мої друзі*
- *Усі користувачі*

5) Хто може переглядати ваші контактні дані (якщо такі вказані)?
- *Тільки я*
- *Мої друзі*
- *Усі користувачі*

3. Ознайомте учнів із ситуацією та запропонуйте скласти правильний, на їхню думку, алгоритм дій.

ПРИМІТКА. У розв'язанні ситуації можуть брати участь усі учні (фронтальна робота), або вчитель організовує роботу в групах.

ТЕКСТОВИЙ ВАРІАНТ ЗАВДАННЯ (ВЧИТЕЛЮ ДЛЯ ПІДГОТОВКИ УРОКУ)

В одній із соціальних мереж ви побачили повідомлення (пост) від свого друга з проханням допомогти благодійному фонду.
Повідомлення (пост) містило картинки тварин, що страждають, і дані банківської картки для збору коштів.
Ви перерахували гроші на вказаний рахунок. Через деякий час з'ясувалося, що це була шахрайська організація, яка зламала акаунти в соцмережі та відправляла повідомлення від імені користувачів їхнім друзям.

Правильний алгоритм дій у подібних ситуаціях:
1. Зв'язатися з другом за допомогою альтернативних каналів зв'язку для уточнення деталей.
2. Перевірити відгуки в інтернеті щодо благодійної організації.
3. Виконати пошук за картинками з повідомлення (поста) для перевірки достовірності фото.
4. Перед тим як перерахувати кошти, перевірити, кому належить рахунок. Якщо рахунок належить фізичній особі, то скасувати платіж.

VI. РОБОТА В ГРУПАХ над «Порадами користувачу-початківцю» (до 12 хв)

ПРИМІТКА. Щоб розробити поради, можна застосувати метод фасилітації «Світове кафе». В умовах дистанційного навчання, можна скористатися дошкою Jamboard.

1. Розділіть клас на дві групи.
2. Кожній із груп дайте лист для фліпчарту й маркери.
3. Одна група має записати «Перелік правильних дій користувача в соціальних мережах», а інша група працює над «Переліком заборон для користувачів соціальних мереж».
4. Для спільної роботи виділіть 5 хвилин, а потім групи мають обмінятися листами. Кожна група отримує ще 3 хвилини для того, щоб учні «допомогли» іншій групі та доповнили їхній список порад.
5. Далі діти знову обмінюються листами й презентують свою роботу.
6. Після учнівської презентації вчитель може вивести на екран рекомендації курсу.

ІНФОРМАЦІЙНИЙ БЛОК РЕКОМЕНДАЦІЙ МОДУЛЯ 5 (ТЕКСТОВИЙ ВАРІАНТ)
1. У соціальних мережах треба додавати в список «друзів» тільки тих, кого ви знаєте.
2. Обліковий запис у соціальних мережах повинен бути захищений налаштуваннями конфіденційності, які передбачені в соціальній мережі (особиста / персональна інформація має бути відкрита лише «друзям» власника).
3. Місцезнаходження власника облікового запису не повинно використовуватися і відображатися над фотографіями та постами в соціальних мережах.
4. Номер мобільного телефону або домашня адреса не повинні вказуватися на сторінці користувача в розділі «Про себе».
5. Доступ до акаунтів у соціальних мережах повинен бути захищений надійним паролем (двофакторна аутентифікація, якщо сервіс це дозволяє).
6. Для різних акаунтів варто генерувати різні паролі.
7. Пароль від облікових записів у соціальних мережах повинен знати лише власник облікового запису.
8. При використанні соціальних мереж на комп'ютері, завжди виходьте з облікових записів після завершення сеансу.
9. Часто зловмисники використовують соцмережі для продажу товарів. Не робіть дорогі покупки через соціальні мережі. А якщо й купуєте, то оплачуйте товар тільки після отримання та огляду.
10. Уважно вивчайте сторінки гостей і сторінки магазинів / продавців у соцмережах. Якщо вас насторожують атрибути сторінки, такі як недавня дата створення профілю, активність тільки в останній час, відсутність друзів, багато хороших відгуків / оцінок, то слід відмовитися від спілкування з таким користувачем та від покупки в такому магазині.

VII. РЕФЛЕКСІЯ (до 3 хв)

Запропонуйте дітям відповісти на запитання:
- Що для вас було новим?
- Чи було заняття зрозумілим і цікавим?
- Як використовувати набуті знання та вміння в подальшому житті?
- Що з почутого змусило задуматися? Чи зміните щось у своїй поведінці, як користувача соціальних мереж, після уроку?
- Які виникли нові запитання?
- Чому б ви насамперед навчили ваших молодших братиків, сестричок, батьків (можливо)?

ДОМАШНЄ ЗАВДАННЯ
Запропонуйте старшокласникам самостійно опрацювати **модуль 4 «Безпечне використання електронної пошти».**

РЕКОМЕНДАЦІЇ ПРОХОДЖЕННЯ МОДУЛЮ 8
Проходження **модуля 8 «Фейкові новини»** можна запропонувати учням 10 класу як домашнє завдання після вивчення теми 3 «Маніпулятивний вплив медіа».

Предмет, розділ, тема за програмою МОН	Питання, що розглядаються в модулі 8 курсу
Громадянська освіта (інтегрований курс) 10 клас **Розділ 5 «Світ інформації, мас-медіа та медіаграмотність»** **Тема 3 «Маніпулятивний вплив медіа»** • Маніпуляції в медіапросторі. Як розпізнати фейкову інформацію, пропаганду. • Роль медіа в провокуванні конфліктів та поширенні стереотипів. Що таке «мова ворожнечі» і як її розпізнати.	• Що таке фейкові новини та які їх різновиди. • Які є джерела виникнення й канали поширення неправдивих новин. • Як перевірити інформацію та розпізнати маніпуляції.

ДЖЕРЕЛА:

1. Громадянська освіта. 3D Демократії: думаємо, дбаємо, діємо : методичний посібник до курсу громадянської освіти для 10-го класу закладів загальної середньої освіти : в 7-ми частинах / П. Вербицька, О. Волошенюк, Г. Горленко та ін. ; за ред. П. Кендзьора. — Львів : ВД «Панорама», 2018. Світ інформації, мас-медіа та медіаграмотність : частина 5. — 2018. — 56 с. ; іл.
2. Підручник: Т. В. Бакка Громадянська освіта (інтегрований курс, рівень стандарту): підруч. для 10 кл. закл. загал. серед. освіти / Т.В. Бакка, Л.В. Марголіна, Т.В. Мелещенко. — Київ : Вид-во «Оріон», 2018.