**Урок «Моя безпека в цифровому світі»**

**Мета:** ознайомити учнів із загрозами в Інтернеті, навчити цифрової грамотності, розвинути вміння розпізнавати кіберзагрози, підвищити обізнаність про безпеку особистих даних, виховувати культуру поведінки в Інтернеті.

**Час:** 90 хвилин

**Обладнання:** Презентація "Твоя безпека в цифровому світі", анкети для опитування, роздаткові матеріали, маркери, дошка.

**ХІД УРОКУ**

**I. Вступне слово вчителя. Слайд 1**

Доброго дня, діти! Сьогодні ми з вами поговоримо про дуже важливу тему – безпеку в Інтернеті. Як ви знаєте, зараз практично кожна людина користується Інтернетом: для навчання, спілкування, перегляду відео чи ігор. Але чи завжди ми задумуємося про те, що несе Інтернет – користь чи небезпеку? Сьогодні ми дізнаємося про найпоширеніші загрози у цифровому світі та навчимося, як від них захиститися.

Інтернет є частиною нашого життя, і дуже важливо знати, як користуватися ним без ризику для себе. Давайте розглянемо основні загрози та способи захисту.

❓ **Запитання для обговорення:**

* Чи знаєте ви, коли у світі відзначається День безпечного Інтернету?
* Як часто ви користуєтеся Інтернетом?
* Що вам подобається найбільше в Інтернеті?
* Чи знаєте ви, які небезпеки можуть чекати в Інтернеті?

**II. Практична частина**

Сьогодні на уроці ми розглянемо основні загрози, які можуть чекати нас у цифровому просторі.

* Кібербулінг: що це таке, його наслідки, як боротися.
* Фішинг та інтернет-шахрайство: які бувають схеми обману.
* Небезпечний контент: фейки, маніпуляції, тролінг.
* Захист персональних даних: як створити надійний пароль, які налаштування приватності використовувати.

**Небезпеки Інтернету: факти та статистика. Слайд 2**

Кількість кіберзлочинів у світі постійно зростає. Чому? Тому що зловмисники знаходять нові способи обманювати людей. Фейкові новини впливають на наші думки та рішення, а доступність персональних даних у мережі робить нас вразливими до шахрайства.

❓ **Питання:** Як ви думаєте, чи може це стосуватися кожного з нас?

**Кіберзлочини: види та наслідки. Слайд 3**

Кіберзлочини можуть мати різні форми. Розглянемо найпоширеніші.

* Фішинг – це коли вас обманом змушують ввести особисті дані на підробленому сайті.
* Віруси можуть пошкодити ваш пристрій або вкрасти інформацію.
* Кібербулінг – це переслідування в Інтернеті, яке може вплинути на психічне здоров'я людини.

Давайте розглянемо, як можна захиститися від цих та багатьох інших загроз загроз.

 **Кібербулінг. Слайд 4**

Кібербулінг – це приниження, погрози, знущання через соціальні мережі або месенджери, це форма агресії, здійснювана через цифрові платформи, такі як соціальні мережі, месенджери, ігрові платформи та мобільні телефони. Він охоплює систематичне поширення дезінформації, образи, погрози та інші дії, що мають на меті приниження або залякування людини. Він може бути анонімним, і тому ще небезпечніший.

❓ **Питання:** Чи зустрічали ви або ваші знайомі подібні ситуації? Як ви вважаєте, як можна захиститися від цього? Давайте розглянемо що робити, якщо ти став жертвою кібербулінгу?

### Статистика кібербулінгу у світі. Слайд 5

* За даними ЮНІСЕФ, приблизно третина молоді з 30 країн світу повідомляють, що вони зазнали кібербулінгу.
* В Україні 29% опитаних підлітків стали жертвами кібербулінгу, а 16% були змушені пропустити шкільні заняття через це.
* Згідно з дослідженням ВООЗ, близько 16% дітей віком від 11 до 15 років зазнали кібербулінгу в 2022 році, порівняно з 13% чотири роки тому.

### Наслідки кібербулінгу. Слайд 6

Кібербулінг може мати серйозні наслідки для психічного та фізичного здоров'я постраждалих:

* Психологічні наслідки: депресія, тривожність, зниження самооцінки, почуття ізоляції.
* Фізичні прояви: порушення сну, головні болі, проблеми з апетитом.
* Соціальні наслідки: погіршення стосунків з однолітками та родиною, зниження успішності.

**Кібербулінг: Що робити, якщо ти став жертвою? Слайд 7**

Є три основні кроки: по-перше, зберегти докази (скріншоти повідомлень), по-друге, повідомити адміністрацію сайту, по-третє, звернутися за допомогою до дорослих. Важливо не залишатися наодинці з проблемою.

Зважаючи на сумну статистику, ми пройдемо невеличке анкетування «Кібербулінг у моєму житті». Відповідайте «так» або «ні».

1. Чи отримували ви систематично образливі, неприємні повідомлення або повідомлення з погрозами в інтернеті?
2. Чи критикували ваш зовнішній вигляд або поведінку у відкритих коментарях?
3. Чи поширював хтось про вас неправдиву інформацію онлайн?
4. Чи були випадки, коли хтось публікував ваші фото або іншу інформацію без вашого дозволу з метою висміяти чи принизити?
5. Чи були випадки створення фейкових акаунтів з використанням вашого імені або фото?
6. Чи ігнорували ваші повідомлення або видаляли їх, щоб викликати у вас відчуття ізоляції, наприклад у групах вашого класу тощо?
7. Чи змушували вас щось зробити через шантаж або погрози в інтернеті?
8. Чи відправляли вам відео або фото принизливого характеру, яке б висміювало вашу вимову, зовнішність чи соціальний статус тощо?

Опрацювання результатів:

0 так - ТИ В БЕЗПЕЦІ! Ти навряд чи стикався з кібербулінгом. Продовжуй дотримуватись правил безпечного користування інтернетом.

1-3 так - БУДЬ УВАЖНИМ! Деякі ознаки кібербулінгу можуть бути присутніми у твоєму онлайн-житті. Спробуй уникати спілкування з людьми, які можуть тебе ображати, і поділися своїми переживаннями з батьками чи друзями.

4-8 так - ПОТРІБНА ДОПОМОГА! Можливо, ти переживаєш кібербулінг. Не мовчи про це! Звернися за допомогою до батьків, вчителів або шкільного психолога. Пам'ятай, ти не один, і разом можна знайти рішення.

**Фішинг: Як не потрапити на гачок? Слайд 8**

Поговоримо про ще один поширений спосіб обману – фішинг.

❓ **Питання:** Чи відомо вам що таке фішинг?

Фішинг – це форма інтернет-шахрайства, метою якого є виманювання у користувачів конфіденційної інформації (логіни, паролі, банківські дані тощо) шляхом обману.

Фішингові атаки маскуються під повідомлення від банків, соцмереж або знайомих.

Щоб не потрапити на гачок шахраїв, ніколи не переходьте за підозрілими посиланнями, перевіряйте веб-адресу, звертайте увагу на помилки в текстах повідомлень.

**Хейт і тролінг в Інтернеті. Слайд 9**

❓ **Питання:** З’ясуймо поняття «хейт» та «тролінг». Чи доводилося вам зустрічати ці явища у житті?

Тролінг – це провокування людей для сварок та конфліктів. Хейт – це агресивні коментарі, які можуть завдати емоційної шкоди. Що робити? Найкращий спосіб – ігнорувати або блокувати хейтера, не відповідати агресією.

Наприклад, такі коментарі притаманні хейтерам:

* «Та що ти можеш! Краще не публікуй цього!»
* Такі, як ти, не заслуговують на увагу! Подивись на себе!»
* «Ти просто дурний, якщо так вважаєш! І всі це знають!»

Коментарі, притаманні тролінгу:

* «Звідки ти дізнався такі новини? З космосу?»
* «Твій допис про котів? Може, ти таємний агент котячого клубу?»
* «Ти реально думаєш, що це цікаво? Ну нехай…»

Як реагувати на хейт і тролінг? **Слайд 10**

* Ігноруйте
* Блокуйте
* Зверніться за допомогою

**Інтернет-шахрайство: Як захистити себе? Слайд 11**

Інтернет-шахрайство - це спроби обманути користувачів онлайн, щоб викрасти гроші, особисті дані або завдати шкоди. Шахраї вигадують хитрі способи, щоб обдурити навіть уважних користувачів, тому важливо знати, як діяти безпечно.

❓ **Питання:** Чи отримували ви або ваші знайомі такі повідомлення як зображено на слайді? Що у цих повідомленнях спільного?

**Як захистити себе? Слайд 12**

Не розголошуйте персональні дані, перевіряйте джерела інформації, не довіряйте занадто вигідним пропозиціям, використовуйте антивірусний захист.

**Спам: Як розпізнати? Слайд 13**

Спам - це небажані повідомлення, які надходять на вашу електронну пошту, у месенджери, соціальні мережі чи навіть через SMS.

Спам часто містить занадто гарні пропозиції, орфографічні помилки, надсилається з невідомих джерел. Якщо щось виглядає підозріло – не відкривайте!

**Слайд 14** Зараз проведемо невеличку перевірку. Пропоную прочитати наведені нижче повідомлення та спробуйте визначити, які з них є спамом.

* Привіт! Надішли це повідомлення 10 друзям, щоб отримати подарунок! **СПАМ**
* Ваш акаунт заблоковано. Увійдіть за посиланням, щоб відновити доступ. **СПАМ**
* Гей, дивись, я знайшов твоє відео! Ти тут? https://nirngromorgo **СПАМ**
* Тільки сьогодні! iPhone 15 за 1 гривню! Отримай тут: https://bgnu9inuy **СПАМ**
* Привіт, Макс! Напиши, будь ласка, домашнє завдання з математики на вівторок. Дякую! **НЕ СПАМ**
* Подивись, ти потрапив у новини! Неймовірно! https://8954dgj **СПАМ**
* Привіт, як справи? Зустрінемося сьогодні після школи на майданчику? Візьми футбольний м'яч. **НЕ СПАМ**
* Я щойно заробив 1000 грн у цій грі! Перевір сам: https://grght **СПАМ**
* Привіт! Сьогодні отримала фото від фотографа з мого Дня народження! Вони чудові! Приходь до мене подивитися! **НЕ СПАМ**
* Ваш комп'ютер заражений вірусом! Завантажте цю програму, щоб вирішити проблему. **СПАМ**
* Ваша посилка заблокована на митниці. Щоб її отримати, сплатіть 50 грн за цим посиланням: https://b4567i **СПАМ**

**Небезпечний контент та челенджі. Слайд 15**

Небезпечний контент включає будь-яку інформацію, відео чи повідомлення, які можуть:

* провокувати ризиковану поведінку;
* спричиняти психологічну або фізичну травму;
* підштовхувати до участі у небезпечних челенджах.

Перед тим як брати участь у будь-якому онлайн-челенджі, подумайте про наслідки. Деякі з них можуть бути небезпечними для здоров’я або навіть незаконними.

**Грумінг: Як уберегти себе? Слайд 16**

Грумінг – це коли незнайомці в Інтернеті завойовують довіру дітей з метою маніпуляцій. Не діліться особистою інформацією, не погоджуйтеся на зустрічі з незнайомцями.

### Пропоную потренуватись, та разом обговорити як поводити себе у подібних ситуаціях. *(Метод мозкового штурму)*

### Твої дії, коли:

* Невідомий користувач додає тебе в друзі і починає відразу запитувати про твої особисті дані.
* Хтось з друзів пропонує тобі подарунок в обмін на зустріч або надсилання фото.
* Новий знайомий у чаті постійно робить компліменти і запрошує на приватні розмови.
* Ровесник починає надсилати тобі повідомлення з непристойним або дивним змістом.

**Як уберегти себе? Слайд 17**

* Будьте обережні з незнайомцями, ніколи не спілкуйтеся з незнайомцями онлайн.
* Не діліться особистою інформацією, наприклад, адресою або номером телефону.
* Якщо хтось робить вам неприємні пропозиції, заблокуйте його і повідомте про це дорослому.

**Фейкова інформація: як розпізнати? Слайд 18**

Фейкова інформація – це неправдиві новини, чутки або повідомлення, які спеціально створюються для того, щоб обдурити людей.

Фейкові новини можуть викликати паніку, маніпулювати людьми. Завжди перевіряйте джерело інформації, шукайте підтвердження в інших надійних джерелах.

**Як розпізнати фейк? Слайд 19**

* Сенсаційний заголовок. Наприклад: "Терміново! Усі школи закриваються через невідому хворобу!"
* Незрозуміле джерело. Якщо не вказано, хто саме написав статтю, або сайт виглядає підозріло.
* Заклик до дій. Наприклад: "Перешліть це 10 друзям, інакше станеться біда!"
* Немає підтверджень. Якщо інформація не підтверджена іншими джерелами чи офіційними організаціями.
* Фото чи відео з інших подій. Іноді фейки використовують зображення, які насправді були зроблені за інших обставин.
* Інформація містичного або загадкового характеру.

**Як протистояти ворожій пропаганді та вербуванню? Слайд 20**

Сьогодні, в умовах війни росія використовує інтернет як інструмент для поширення пропаганди та вербування українських дітей. Це небезпечно і може призвести до серйозних наслідків для вас, вашої родини та країни.

**Як це працює?**

* Ворожі агенти створюють фейкові акаунти. Вони можуть писати вам у соціальних мережах, видаючи себе за друзів, блогерів чи навіть військових.
* Пропонують «допомогти». Наприклад, сфотографувати позиції ЗСУ, передати координати чи щось підпалити.
* Обіцяють гроші чи винагороду. Часто такі обіцянки – брехня.
* Використовують страх чи маніпуляції. Наприклад, залякують, якщо ви відмовитесь співпрацювати.

**Що робити, якщо вам пишуть з такими пропозиціями?**

* Не відповідайте на повідомлення;
* Повідомте батьків чи дорослих;
* Зверніться до кіберполіції;
* Заблокуйте і поскаржтеся;
* Не переходьте за підозрілими посиланнями.
* Будьте критичними до інформації, перевіряйте факти, не поширюйте сумнівні новини.

**Захист особистих даних у мережі Слайд 21**

Щоб захистити себе від усіх цих загроз, дотримуйтесь простих правил:

* використовуйте VPN
* уникайте публічного Wi-Fi
* регулярно перевіряйте налаштування конфіденційності
* використовуйте двофакторну аутентифікацію
* використовуйте складні паролі та регулярно їх міняйте
* Ніколи не переходьте за підозрілими посиланнями.
* Не додавайте у друзі незнайомців у соцмережах.
* Не поширюйте фейкову інформацію, перевіряйте факти.

# Пропоную переглянути відеоурок, як створити НАДІЙНИЙ ПАРОЛЬ який ЛЕГКО ЗАПАМʼЯТАТИ?

<https://youtu.be/USqFYyDjhqE?si=5ca0bdYMd6FcihZy>

**Правила безпечного використання Інтернету. Слайд 22**

Отож, надійні паролі, оновлення програмного забезпечення, перевірка джерел інформації, обережність із особистими даними – усе це основи цифрової безпеки.

**Етика та культура поведінки в Інтернеті Слайд 23**

**Також д**отримуйтеся правил етики: поважайте інших, думайте про наслідки своїх дій, дотримуйтеся здорового балансу між реальним життям та онлайн-активністю.

**ІІІ Закріплення матеріалу**

**Гра "Безпечний Інтернет"**

Зараз ми пограємо у гру. Я описуватиму ситуацію, а ви повинні вибрати правильний алгоритм дій.

* Вам надійшло підозріле посилання. Що робити?
* Незнайомець просить ваші персональні дані. Як реагувати?
* Ви побачили образливі коментарі під фото друга. Як вчините?

Обговорення правильних відповідей та висновки.

**VI. Рефлексія та підведення підсумків**

❓ **Питання:** Під кінець уроку я хочу почути вашу думку:

* Що нового ви дізналися сьогодні?
* Як тепер будете поводитися в Інтернеті?
* Які правила цифрової безпеки ви готові пояснити своїм друзям?

**Домашнє завдання**

**Метод "Сенкан":** Учні складають сенкан (п’ятирядковий вірш) про Інтернет-безпеку:

1. Одне слово – ключове поняття.
2. Два слова – означення.
3. Три слова – дії.
4. Чотири слова – фраза про тему.
5. Одне слово – висновок.

**Поради батькам щодо контролю за дітьми онлайн Слайд 24**

Батьки повинні розмовляти з дітьми про ризики в Інтернеті, налаштовувати батьківський контроль та стежити за активністю дітей у мережі.

**Заключне слово вчителя:** Інтернет – це чудовий інструмент для навчання та розвитку, але важливо використовувати його безпечно. Дотримуючись простих правил, ви можете захистити себе та своїх близьких. Пам’ятайте: ваша безпека в Інтернеті залежить від вас!