Краматорське вище професійне училище

**МЕТОДИЧНА РОЗРОБКА**

виховної години на тему

**«Безпечний Інтернет»**



Підготувала: Алла БАБАСКІНА викладач Краматорського ВПУ

Погоджено: Ірина РОЯНОВА

заст. директора з НВхР

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_2023р.

Краматорськ 2023

**Виховна година**

**Тема «Безпечний Інтернет»**

**Мета**: розширити й поглибити знання про безпечний Інтернет та соціальні мережі, сприяти обізнаності учнів про небезпеки, які існують в Інтернеті та соціальних мережах і про шляхи їх подолання, мотивувати поширювати цю інформацію у своєму середовищі, розвивати уважність, спостережливість, мовленнєві навики, пам’ять, виховувати любов до родини, навколишнього світу, етичне спілкування між товаришами, дорослими, молодшими друзями.

**Обладнання:** ноутбук, смартфони

**Хід виховної години**

**І. Організаційний момент.**

**ІІ. Основна частина виховної години.**

*Класний керівник:* Ми живемо в епоху інформаційних технологій, які увійшли в життя кожного з нас. Ніхто не заперечуватиме, що тепер Інтернет відіграє важливу роль у житті людей. Просто вражає, скільки часу у нас забирає Інтернет.

 При цьому діти потрапили в Мережу значно раніше за дорослих. У наш час сучасна молодь вільно володіє можливостями Інтернету та мобільними телефонами, а школярі, можливо, не розуміють, як без цього жив світ 20 років тому. Сьогодні Інтернетом користується кожна 3 людина на планеті.

 Розвиток сучасної глобальної мережі Інтернет дав поштовх у розвитку різного виду страхів для дітей та їхніх батьків.

Щорічно більш ніж в 100 країнах світу відзначається День безпеки в Інтернеті. У 2023 році День безпеки в Інтернеті припадає на 7 лютого. Цей день є одним із ключових для поширення ідей безпечного користування Інтернетом та сучасними цифровими технологіями.

**Вправа** Мозковий штурм «Про користь Інтернету» (учні називають позитивні та негативні можливості Інтернету).

**Загрози в Інтернеті:**

* Виготовлення, розповсюдження та використання матеріалів зі сценами насильства над дітьми
* Наполегливе чіпляння в мережі, розмови на теми сексу, насильства, "зваблення”
* Показ невідповідних віку, нелегальних та шкідливих матеріалів, що впливають на психіку, приводять до фізичної шкоди
* Переслідування і залякування

У всьому світі діти та підлітки є найбільшими користувачами інформаційно-комунікативних технологій. Вони широко користуються мобільними телефонами, шукають інформацію на Інтернет-сторінках, спілкуються «онлайн» в соціальних мережах, створюють свої блоги, спілкуються в чатах, обмінюються музикою та фільмами, обговорюють проблеми на форумах, використовують веб-камеру, skype та грають в онлайн ігри.

Ніколи раніше не було так легко, швидко та зручно знайти людей будь-якого віку, соціального статусу, статі, національності, рівня досвіду й дискутувати з ними на які завгодно теми, що є цікавим для певних груп.

В рамках програми Microsoft «Партнерство в навчанні» кафедрою превентивної роботи та соціальної політики ЮНЕСКО в Україні було проведено Всеукраїнське широкомасштабне дослідження «Рівень обізнаності українців щодо питань безпеки дітей в Інтернеті».

Ключові результати: З 96% дітей-користувачів Інтернету віком від 10 до 17 років 51% не знає про небезпеки в мережі. 52% дітей виходять в Інтернет передусім для спілкування у соціальних мережах, де залишають свій номер мобільного телефону (46%), домашню адресу (36%), особисті фото (51%). 44% дітей знаходяться у потенційній зоні ризику (розміщують особисту інформацію) і 24,3% вже були в ризикованих ситуаціях (ходили на зустріч з віртуальними знайомими).

 Найпопулярніші за відвідуваністю серед дітей ресурси в Інтернеті – соціальні мережі – містять найбільшу загрозу з точки зору доступності особистої інформації для сторонніх осіб. У соціальних мережах свій особистий номер телефону вже залишили 46% дітей 10-17 років, вказали домашню адресу – 36%, розмістили особисті фотографії – 51%.

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості, спілкування, навчання, дозвілля. Але разом з тим, в Інтернеті приховано досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути.

***1 учень Віруси.*** Комп’ютерний вірус – це невелика програма, яка написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. комп’ютерних вірусів. Дія вірусів може проявлятися по-різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації.

Основними ранніми ознаками зараження комп’ютера вірусом є:

 - зменшення обсягу вільної оперативної пам’яті;

- уповільнення роботи комп’ютера та завантаження;

- незрозумілі (без причин) зміни у файлах, а також зміни розмірів та дати останньої модифікації файлів;

 - помилки під час завантаження операційної системи;

 - неможливість зберігання файлів у потрібних каталогах;

 - незрозумілі системні повідомлення, музичні та візуальні ефекти тощо.

***2 учень Кібер-хуліганство.*** Кібер-хуліганство – термін, який використовується для того, аби описати інформаційні атаки на дитину через Інтернет. На відміну від традиційного хуліганства, якого дитина може уникнути, знаходячись вдома, стати жертвою кібер-хуліганства можна й у власній оселі на очах у батьків. Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами є наступна.

**Кібер-булінг**. Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину (фото, відеозйомки тощо). З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, форуми та чати.

***3 учень Грифери.*** Інтернет-шахраї, які заважають учасникам он-лайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

***Виманювання інформації*** про дитину та її сім’ю з метою подальшого пограбування, шантажу. Це відбувається завдяки використанню певних Інтернет-технологій.

**Шпигунське програмне забезпечення**. Це комп’ютерні програми, які збирають інформацію без відома власника комп’ютера. Зібрана інформація може містити:

- список рекламних сайтів, на які переходить користувач під час серфінгу в Інтернеті;

 - особисту інформацію: ім’я, адресу та номер телефону;

 - Web-сторінки, які відвідує користувач, та відомості форм, які він заповнює на цих сторінках (треба пам’ятати про обережність при повідомленні паролів своєї електронної пошти та акаунтів у соціальних мережах; не слід називати дівоче прізвище матері – подібна інформація використовується при оформленні банківських документів у якості ключових слів);

***4 учень. Фішинг*** – технологія Інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фішинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та онлайн-фішинг (створення ідентичної копії відомих сайтів Інтернет-магазинів з метою обманювання покупців).

***5 учень*** ***Фармінг.*** Різновид шахрайства в Інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім відбувається зараження комп’ютера вірусами та шпигунським програмним забезпеченням.

***6 учень*** ***Он-лайн-хижаки*** «Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються онлайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в он-лайні, щоб знайти вразливих жертв. Онлайн-хижаки виявляють по відношенню до них увагу та турботу, пропонують подарунки і таким чином намагаються поступово спокусити своїх жертв, не шкодуючи для цього ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які найчастіше цікавлять дітей. Вони вислуховують дітей і «співчувають» їхнім проблемам. Вони намагаються позбавити комплексів молодих людей. Хижаки також можуть спонукати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

***7 учень*** ***Спам.*** Це масова розсилка комерційної, політичної та іншої реклами (інформації) або іншого виду повідомлень (у тому числі й підроблених) особам, які не висловлювали бажання їх отримувати. Фішинг також іноді може вважатися спамом. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку. Таке повідомлення, зазвичай, маскується під офіційний лист від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблоковано, і наводиться адреса сайту, що належить спамерам, з формою, яку треба заповнити. Серед даних, які просять повідомити, є ті, що потрібні шахраям. Для того, щоб жертва не здогадалася про обман, оформлення цього сайту також імітує оформлення офіційного сайту банку чи установи.

**ПРАКТИЧНЕ ЗАВДАННЯ**

* Яку відповідь Ви дасте на такі листи. Обґрунтуйте вашу відповідь:

**Лист 1.**

Привіт мене звати Сашко. Мені 15 років. Я живу в Києві. Шукаю друзів по переписці. Я полюбляю комп’ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні ....

**Лист 2.**

Привіт мене звати С. Я хочу з тобою познайомитися Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та адресу.

**Лист 3.**

 Всім!!!
 Наша організація займається збиранням коштів для потерпілих від повені в N. Ми купуємо їду, теплі речі для тих, хто втратив домівки. Не будьте байдужими до чужого горя! Хто скільки може. Наш рахунок № 123456789.
 Вдячні діти Вас ніколи не забудуть. Дякуємо

Треба бути дуже обережним, користуючись Інтернетом.

* + не надавати нікому свої паролі;
	+ не повідомляти про себе і батьків приватну інформацію,
	+ без гострої необхідності не надавати особисту інформацію по електронній пошті, в чат-кімнатах;
	+ не надавати відповіді на послання непристойного та грубого змісту;
	+ повідомити старшим про отримання інформації, яка примусить почуватись незручно або налякано;
	+ не вір всьому, що кажуть про себе віртуальні знайомі.
	+ не погоджуватись на зустріч з випадковим онлайновим другом. Якщо все ж таки це необхідно, то зустріч повинна відбуватися в громадському місті або у присутності друзів чи батьків;
	+ не відправляти нікому своє фото;
	+ не здійснювати комерційні операції через мережу Інтернет,

**ВІДЕО «НАЙЖАХЛИВІШИЙ ТИЖДЕНЬ ПЕТРИКА»**

<https://www.youtube.com/watch?v=CmD5TzdTbF4>

**Правила безпеки в інтернеті**

<https://www.youtube.com/watch?v=D3-gzPt-R9s>

**ІІІ. Підведення підсумків.**

Наше життя вирує все швидше та швидше. Інтернет уже зараз став невід’ємною його частиною. Цілком ймовірно, що у найближчому майбутньому Всесвітня мережа повністю замінить усі інші засоби зв’язку. Та давайте зупинимось на мить і замислимось, чи дійсно ми хочемо провести усе життя у віртуальному світі? Бачити аватарки – замість живих облич, смайлики – замість живих посмішок.

В решті решт як та на що втрачати власний час - це вільний вибір кожного. Але пам’ятайте, що Інтернет - це лише інструмент, яким Ви користуєтесь, щоб отримати відповіді на свої питання, підготувати реферати та доповіді, спілкуєтесь, якщо між вами величезні відстані. Вчиться користуватись Інтернетом із розумом.

Життя людини – це найдорожчий Божий дар на Землі. Будьте обережними з безпечним Інтернетом!