**Организация  профилактической работы с несовершеннолетними и их родителями по вопросу**

**«Мошенничество в сети Интернет» с использованием различных форм**

**Рекомендуемые мероприятия «Внимание:  «Интернет-безопасность»**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Название мероприятия | Содержание | Время проведения |
| 1 | Беседа «Безопасность детей в интернете» | Знакомство учащихся с опасностями, которые подстерегают их в Интернете, помощь во избежание этих опасностей | 5 апреля |
| 2 | Анкетирование обучающихся «Безопасный Интернет» | Анкета позволяет проанализировать современную ситуацию в образовательной среде | 6 апреля |
| 3 | Деловая игра «Основы безопасности в сети Интернет» | С использованием интерактивного метода разработать коллективно  в объединении «Правила работы в сети Интернет» | 7 апреля |
| 4 | Литературная гостиная   «Интернет и мое здоровье» | Составление стихов, рассказов, фельетонов, заметок, информационных сообщений | 9 апреля |
| 5 | Конкур  рисунков «Правила поведения в сети Интернет» | Создание тематических художественных буклетов из рисунков участников | 10 апреля |

**Беседа «Безопасность детей в интернете»**

**Возраст:** 11-17 лет

**Цель:** Познакомить учащихся с опасностями, которые подстерегают их в Интернете и помочь избежать этих опасностей.

Вопрос 1. «Какие опасности подстерегают нас в интернете?»

**1) Преступники в интернете. ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.**Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

**2) Вредоносные программы.** К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Cети.

**3) Интернет-мошенничесво и хищение данных с кредитной карты.** В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing»,состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

**4) Азартные игры**. Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанны с выигрышем или проигрышем настоящих денег.

**5) Онлайновое пиратство.** Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

**6) Интернет-дневники.** Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

**7) Интернет-хулиганство.** Так же как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

**8) Недостоверная информация.** Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

**9) Материалы нежелательного содержания.** К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантскими материалы, материалы с ненормативной лексикой. Мы с вами уже рассмотрели те опасности, которые нам могу встретиться в интернете. А теперь давайте посмотрим, как этих опасностей можно избежать.

**Вопрос 2. «Как этих опасностей избежать?»**

1) Преступники в интернете. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

2) Вредоносные программы. А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла. Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности. В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

3) Интернет-мошенничесво и хищение данных с кредитной карты. А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме. Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России. 4) Азартные игры. Помните, что нельзя играть на деньги. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

5) Онлайновое пиратство. Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

6) Интернет-дневники. Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую- либо личную информацию.

7) Интернет-хулиганство. Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

8) Недостоверная информация. Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам.

9) Материалы нежелательного содержания. Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.

**Анкетирование обучающихся «Безопасный Интернет»**

►Укажите свой возраст

►Что такое Интернет?

►Какие опасности существуют в Интернете?

►Использование Интернета является безопасным, если: ( выберите один или несколько вариантов из списка ответов)

-защитить свой компьютер

- защитить себя в Интернете

- соблюдать правила

-разглашать личную информацию

- заботиться об остальных

-регулярно обновлять операционную систему

-защитить компьютер

-создавать резервные копии документов

-закону надо подчиняться даже в Интернете

►Как защитить себя в Интернете? (выберите один или несколько вариантов из списка ответов)

-защитить свой компьютер

-расширять круг знакомств с неизвестными людьми

-стараться давать как можно меньше информации о себе

-размещать фотографии свои, друзей и родственников

►Как обезопасить свой компьютер? (выберите один вариант из списка ответов)

\*выключить и спрятать в шкаф

\*установить антивирусную программу

►Что надо делать, чтобы антивирусная программа была эффективной  (выберите один или несколько вариантов из списка ответов)

-лучше не иметь антивирусную программу

-обновлять антивирусную базу

-не посещать сайты, где нет достоверности, что сайт находится под защитой

►Кто создаёт опасные программы? (выберите один или несколько вариантов из списка ответов)

-чёрный властелин

- шпионы

-хакеры

 -пожиратели смерти

►Перечислите правила поведения в Интернете (если вы не знаете ответа на этот вопрос, то напишите "Без ответа")

►А что для вас является "Безопасным Интернетом?" (если вы не знаете ответа на этот вопрос, то напишите "Без ответа")

**Деловая игра «Основы безопасности в сети Интернет»**

**Цель:** формирование устойчивых жизненных навыков при работе в сети Интернет.
Проведению деловой игры предшествует предварительная подготовка обучающихся по предложенной тематике. **Перечень вопросов для обсуждения выявляется в результате анкетирования обучающихся.**

***Примерные вопросы для обсуждения:***
1.    Для чего нужен Интернет?
2.    Какие существуют риски при пользовании интернетом, и как их можно снизить

3.    Какие виды мошенничества существуют в сети Интернет?

4.    Как защититься от мошенничества в сети Интернет?
5.    Что такое безопасный чат?
6.    Виртуальный собеседник предлагает встретиться, как следует поступить?
7.    Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

*П****едагог формирует три творческие группы. Каждая группа обсуждает 2-3 вопроса  и  информирует всех ребят, представляя свой вариант решения проблемы или вопроса***

         После этого группы работают над предложением модели

«Правила поведения в сети Интернет». После совместного обсуждения принимают более эффективный вариант или составляю коллективный.         Составленный вариант правил оформляют в творческой форме и вывешивают на информационном стенде.