**Методическая разработка**

**классного часа во 2 Б классе на тему: «Безопасный Интернет»**

**Зубкова С.А.**

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

**Подготовительная работа**: классный руководитель проводит опрос учащихся по вопросам:

1. У вас на домашнем компьютере установлен Интернет?

2. Что вам больше всего нравится в Интернете?

3. Как ваши родители воспринимают ваши занятия в Интернете? Почему?

**Оборудование:** компьютер, проектор, презентация, памятка учащимся.

**Ход занятия**

**Учитель**: Раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. И ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?» нам поможет этот классный час.

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

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 негатива, пытаясь ослабить моральные запреты.

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.

Интернет-мошенничество 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.

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, связанные с выигрышем или проигрышем настоящих денег.

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.

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.

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.

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.

Материалы нежелательного содержания.

К материалам нежелательного содержания относятся: материалы ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

**Учитель**: А сейчас мы немного отдохнём. Музыкальная пауза.

 (Во время музыкальной паузы учащиеся поют и выполняют движения.)

Частушки:

 (Руки на пояс, поднимаем плечи по очереди, голову слегка влево, вправо).

 Пропоем сейчас частушки,

 Чтоб чуть-чуть нам отдохнуть.

 Про здоровый образ жизни

 Не забудем намекнуть.

 (На первые две строчки частушки закрывать глаза руками и открывать, на другие две - потягиваться).

 На компьютере играли,

 Наши глазоньки устали,

 А теперь мы отдохнем

 И опять играть начнем.

 (Руки на поясе, наклоны влево, вправо.)

 Нужно спортом заниматься

 И в жару нам, и в мороз,

 Если где-то ты не сможешь,

 То не хмурь уж ты свой нос.

 (Хлопать в ладоши.)

 Мы пропели вам частушки

 Хорошо ли, плохо ли,

 А теперь мы вас попросим,

 Чтобы вы похлопали.

**Учитель:** Мы с вами уже рассмотрели те опасности, которые нам могут встретиться в Интернете. А теперь давайте посмотрим, как этих опасностей можно избежать.

Вопрос 2. «Как этих опасностей избежать?»

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. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

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.

Интернет-мошенничество 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.

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, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

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.

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.

Интернет-хулиганство.

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

Недостоверная информация.

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

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.

**Учитель:** А теперь подведём итоги нашего классного часа. У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.

 Классный час понравился. Узнал что-то новое.

 Классный час понравился. Ничего нового не узнал.

 Классный час не понравился. Зря время потерял.

**Учитель:** А на память об этом классном часе я хочу подарить каждому из вас памятку по безопасному поведению в Инернете.

**Джентельменское соглашение родителей, учителей и детей**

Перед первым выходом в Интернет как можно четче оговорить правила пользования сетью. Обсудить с ребенком, куда ему можно заходить (возможно, на первых порах стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.

Сообщить ребёнку о том контроле, который взрослый намерен осуществлять: проверка посещенных ребенком страниц, контроль времени, проведенного в Сети, проверка адресов электронной почты. Объяснить ребенку, что доверяете ему и заботитесь о его безопасности.

**Памятка «Безопасный интернет»**

1. Сообщить родителям свое регистрационное имя и пароль, если тебе разрешено участвовать в чатах или блогах, e-mail адрес и пароль почтового ящика.

 2. Никому, кроме родителей, эти сведения сообщать категорически нельзя.

 3. Не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей).

 4. Не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет.

 5. Сразу обратиться к родителям, если увидишь нечто неприятное, тревожащее, угрожающее на сайте или в электронной почте.

 6. Не соглашаться лично встретиться с человеком, с которым ты познакомился в Сети.

 7. Если кто-то предлагает тебе какой-то "секрет" - тут же сообщить об этом родителям.

 8. Не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай.

 9. Не делать без разрешения родителей в Интернете ничего, что требует оплаты.

 10. Проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека.