

# Классный час на тему: «Безопасный Интернет»

**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 (раздать каждому на память).

## 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?»**

### **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 Сети.

### **3) 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.

#### **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, связанные с выигрышем или проигрышем настоящих денег.

#### **5) Онлайнное пиратство.**

Онлайнное 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.

### **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-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.

## **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) Онлайн-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 онлайн-материалов и не доверять им.

### ***Игра-соревнование***

Учитель:

А сейчас мы проведём игру-соревнование.

Разобьёмся на две команды. При этом я выберу координатора группы.

Первая команда “Злоумышленник”

Вторая команда “Дока-пользователь”

Первая команда - это коллективный злой разум, действующий в Интернет.

Вторая команда - это добропорядочные пользователи сети.

Первая команда, при ответе на вопрос, называет негативные явления, вторая – позитивные.

Ответим на вечный вопрос “Кто победит в борьбе – зло или добро?”

Результаты фиксируются на доске.

### ***Вопросы:***

*Первая команда* - Какие существуют опасности при работе в сети?

### **Эталон ответов:**

- широкая торговля базами данных о частных лицах и предприятиях
- кража личной информации об абонентах мобильных сетей
- нарушение законодательства об охране авторских прав
- одна из важных проблем - вирусы
- спам - это различные рекламные объявления, которые приходят по электронной почте, забивая ящик и мешая загружать нормальные письма

*Вторая команда* - Какие существуют средства профилактики и борьбы с опасностями при работе в сети?

### **Эталон ответов:**

- чтобы обезопасить себя, необходимо пользоваться антивирусными программами
- не следует загружать программы с сайтов, не заслуживающих доверия
- если в тексте сайта множество грамматических ошибок, и весь он забит рекламными баннерами, то загрузка с такого сайта может быть чревата последствиями
- не открывайте подозрительных писем от неизвестных вам авторов
- осторожно относитесь к адресу своего ящика вводите свой e-mail только в том случае, если он гарантирует вашу конфиденциальность

- заведите два почтовых ящика: адрес одного говорите только друзьям и знакомым, а для регистрации в Интернете, пишите адрес второго

*Первая команда* - Какие правонарушения, связанные с работой в сети вам известны?  
(Ответы детей)

*Вторая команда* - Какие меры принимает общество и государство против правонарушений?

(Ответы детей)

*Первая команда* – Вы являетесь похитителем контента. Ваши действия.

(Ответы детей)

*Вторая команда* - Вы являетесь автором произведения. Ваши действия для его защиты. Ваши права.

(Ответы детей)

Задание командам. “Реверанс”. - Кто назовёт больше правил этикета.

### **Эталоны ответов:**

- Обращаться к незнакомым людям можно при условии, что адрес был опубликован его владельцем.
- К незнакомым людям можно обращаться с просьбами о консультации и вежливыми предложениями, не претендуя на получение ответа. Если ответ не пришел, повторять обращение не следует.
- При обращении к незнакомым людям надо воздерживаться от просьб использовать другие средства связи, например, выслать по почте автограф. Такие просьбы оставляют без ответа, а повторение рассматривают как спам.
- Отправляемое электронное письмо всегда должно быть подписано и указана тема сообщения.
- Если у вас нет возможности сразу ответить на полученное письмо, сообщите, что вы его получили и ответите позже.
- Не забудьте ответить позже, не затягивайте с ответом.
- Будьте вежливы, не отправляйте *флеймов* - написанных в запале писем.
- Шутки принято обозначать явным образом при помощи смайликов: ©, ®, и др.
- В тексте сообщения не принято выделять текст прописными БУКВАМИ. Такое выделение рассматривается как крик. В лучшем случае - как неграмотность в вопросах этикета.
- Большие файлы-вложения нужно архивировать. А для обмена очень большими файлами есть другие способы.
- Нельзя посылать рекламу в не предназначенные для этого места. Это грубое нарушение.
- Нельзя посылать незатребованную корреспонденцию. Это тоже нарушение этикета.

Задание командам. Какие профессии служат для сохранения информации, регулирования её использования?

**Эталоны ответов:** системный администратор, модератор, криптограф.

## *Подведение итогов*

Задание командам. Сделайте вывод.

(О чем мы сегодня говорили на уроке?)

Какие силы побеждают в борьбе за информацию?

Пригодятся ли знания, полученные на этом уроке в вашей жизни?)

**Вывод – “добро должно быть с кулаками”, то есть информация нуждается в эффективных методах защиты.**

**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.