Классный час

по теме: «Безопасность в сети Интернет».

Класс: 8 класс

Цель:

Познакомить с основными правилами пользования интернета.

Расширить представление детей об интернете.

Формировать основы коммуникативной грамотности, чувства ответственности за своё поведение.

Сформировать у учащихся понятия о принципах безопасного поведения в сети Интернет.

Обеспечить информационную безопасность ребенка при обращении к ресурсам Интернет.

Воспитывать внимательное отношение к информационным ресурсам.

Задачи:

Образовательная:

- познакомиться с понятием «Интернет», «Интернет-угроза»;

- изучить приемы безопасности при работе в сети Интернет.

Развивающая:

- формирование приёмов логического мышления;

- развитие способности анализировать и обобщать, делать выводы.

Воспитательная:

- воспитание аккуратности, точности, самостоятельности;

- привитие навыка групповой работы, сотрудничества.

Здоровьесберегающая:

- оптимальное сочетание форм и методов, применяемых на занятии.

Здравствуйте ребята. Я предлагаю вам поприветствовать друг друга. Как мы это можем сделать? Подавая друг другу руку мы передаем каждому радость общения друг с другом.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники.

Как много информации про человека мы можем узнать от рукопожатия или ника? …

Всегда знайте, что рядом есть люди, которым можно доверять, которые вас любят которые всегда рядом.

Кто это? Родные, близкие, одноклассники, друзья.

Сегодня мы с вами поговорим об интернете.

Плюсы и минусы интернета.

Как любое глобальное явление, существенно влияющее на развитие человеческого общества, Интернет имеет свои плюсы и минусы.

К плюсам можно отнести следующее:

- оперативность получения любой информации – пользователю интернет нет необходимости идти в библиотеки, искать необходимый материал, достаточно только открыть любую поисковую систему и задать в строке поиска условие и из предложенных вариантов выбрать то, что необходимо;
- информативность – на любую предложенную тему можно найти несколько точек зрения, сравнить их, получить полную информацию;
- технологичность - использование новейших достижений информационных и телекоммуникационных технологий;
- творчество - пользователь может использовать в своей работе готовые наработки, предлагаемые для свободного доступа в сети Интернет, а может

на основе предложенной информации представить что-то свое, непохожее на то, что было предложено, таким образом самовыразиться;

- общение на расстоянии (социальные сервисы и форумы, электронная почта) – возможность общения, обмена опытом, знаниями;
- формирование информационной компетентности, включая умение работать с информацией (находить, получать, анализировать, систематизировать и использовать);
- возможность постоянного самообразования, самореализации.

И все же есть и очевидные минусы:

- при поиске информации пользователь встречает много ненужной, беспорядочной, сопутствующей информации, формирующей недостоверные понятия об объектах, явлениях, процессах. При этом тратиться время на просмотр открывающихся ссылок, проверку содержимого сайтов, отсеивание ненужного «мусора».
- отсутствие очного общения – очень часто в интернет можно найти целые блоки обучающих программ, которые предполагают самостоятельное изучение и рассмотрение предложенной темы, но все-таки общение с преподавателем, который может объяснить непонятный материал, не заменишь никакой машиной;
- ухудшение здоровья пользователя: потеря зрения (компьютерный зрительный синдром), гиподинамия, искривление осанки, психические и интеллектуальные нарушения развития, подростковая агрессия.

Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)

Интернет, как и все в жизни, имеет две стороны - черную и белую. Сегодня попробуем лучше разобраться в том, что происходит в интернете, узнать, что в нем есть интересного и полезного, а также опасного и неприятного.

Просмотр социального ролика. http://www.youtube.com/watch?v=789j0eDglZQ

Угрозы, исходящие из сети Интернет можно разделить на онлайн и оффлайн.

Давайте начнем с первой группы угроз – онлайн угрозы. Онлайн угрозы – любые проблемы, которые опасны для вашего компьютера.

К ним, во-первых, относятся различные категории компьютерных вредителей и вирусов, которые могут просочиться на ваш компьютер во время путешествия по просторам социальных сетей. Для этого порой достаточно нажать на ссылку, содержащуюся в письме от «мнимого» друга. Например, получив письмо или найдя сообщение на стене следующего содержания: «Нашел твою фотку!» или «Ты тут неплохо получилась!», или «Смотри какой котеночек!». Заинтересовавшись содержанием письма, вы кликнете на ссылку, которая переведет вас на загадочный сайт, попутно загружающий на компьютер всевозможные зловредные программы. Среди них могут быть:

- программы-шпионы (будут отслеживать все ваши действия на компьютере, вводимую информацию с целью ее похищения).

Общение в интернете - это хорошо или плохо, почему?

(ответы детей) – это хорошо в меру, но не стоит заменять живое общение виртуальному.

Интернет - магазины это хорошо или плохо, почему?

(ответы детей) – это плохо, потому, что это наиболее популярный вид жульничества в Интернете.

Но кроме нужной информации в Интернете есть и разные опасности.

Риски и угрозы интернета

Что можно встретить опасного

Иногда наше неразборчивое общение, игры, и наша безответственность в интернете делает опасной не только вашу жизнь, но и жизнь ваших родственников.

Фильм: http://www.youtube.com/watch?v=789j0eDglZQ

- А теперь давайте перейдем к самому опасному виду угроз, который может принести ущерб не только вашему имуществу, но и жизни – это оффлайн-угроза. Она включает все то, что может случиться в реальной жизни. К ней относятся предложения о встрече от неизвестных «друзей», телефонный шантаж, мошенничество, вымогательство и даже ограбление квартиры или кража другого имущества.

Зачастую мошенникам даже не нужно ломать голову над тем, как получить заветную информацию от пользователя – он сам предоставляет ее на тарелочке. Например, при регистрации в социальной сети и составлении личного профайла предлагается внести информацию о своем годе рождение, номер телефона, адрес электронной почты, адрес проживания и работы. К сожалению, дети воспринимают такие «требования» как необходимость, и заносят личную информацию во все графы. Это первая и сама главная ошибка! Мы советуем вносить как можно меньше личной информации. Почему? Вот простой пример: ребенок в ожидании долгожданных каникул с родителями и всей семьей в какой-нибудь заморской стране каждый день обновляет свой статус: «Ура, до путешествия осталось три дня!», «Осталось два дня, не могу дождаться!», а на третий-четвертый день, после того, как дни закончились, квартиру обворовывают. Причина в том, что помимо ежедневного обновления статусов ребенок добавил в профиль домашний адрес и фотографии из квартиры, в которой мошенника, а уже и «домушника», заинтересовал интерьер и домашняя аппаратура.

И, наконец, социальные сети могут быть рассадником людей с более серьезными отклонениями. Создав поддельный профиль ребенка, и втершись

в доверие к вам, они могут предложить встретиться, но на встречу уже придет взрослый человек с корыстными или «больными» планами.

Давай попробуем составить свод правил по технике безопасности в сети Интернет.

Зачитайте и продолжите фразу

Никогда не сообщайте свои…

Если вас что-то пугает в работе компьютера, немедленно…

Всегда сообщайте взрослым обо всех случаях в Интернете, которые …

Никогда не соглашайтесь на личную встречу с людьми, с которыми …

Прекращайте любые контакты в социальных сетях или в чатах, если кто-нибудь …

Познакомился в сети и хочешь встретиться – …

Помните, что виртуальные знакомые могут быть не теми …

Никогда не поздно рассказать взрослым, если вас …

Не доверяйте людям, с которыми вы познакомились в социальной сети, ведь они могут быть …

Помните, то, что когда-либо было опубликовано, …

- Сейчас я расскажу вам о том, как обезопасить себя и свой компьютер от сетевых угроз.

Итак, как же бороться с сетевыми угрозами?

1. Установите комплексную систему защиты.

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

2. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

3. Не отправляйте SMS-сообщения.

Очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

4. Используйте сложные пароли.

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

5. Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.
6. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .
7. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

8. При регистрации на сайтах, старайтесь не указывать личную информацию
9. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.
10. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
11. Не добавляйте в друзья в социальных сетях всех подряд.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.

Видеоролик.

Помните! ИНТЕРНЕТ может быть прекрасным и полезным средством для обучения, отдыха или опасным, как для вас и ваших близких. Все зависит от того как вы его будете использовать!