ГКОУ «Максатихинская школа – интернат»

«Безопасность в сети» для 5-9 классов

Презентацию подготовила:
Алексеева Н.А.

Цели: - уточнить знания учащихся о понятии «Интернет», о правилах ответственного и безопасного поведения в современной информационной среде, о способах защиты от противоправных посягательств в сети Интернет;

- развивать внимание, память;
- воспитывать внимательное отношение к работе в интернете.

Ребята, посмотрите на слайд и догадайтесь о чем сегодня мы будем говорить?

Что такое Интернет?

Это всемирная система объединённых компьютерных сетей для хранения и передачи информации.

Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. На основе Интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных.

Самые опасные угрозы сети Интернет

1. Вредоносные программы – вирусы.
2. Сайты-подделки
3. Спам
4. Кража информации
5. Online - игры.
6. Социальные сети

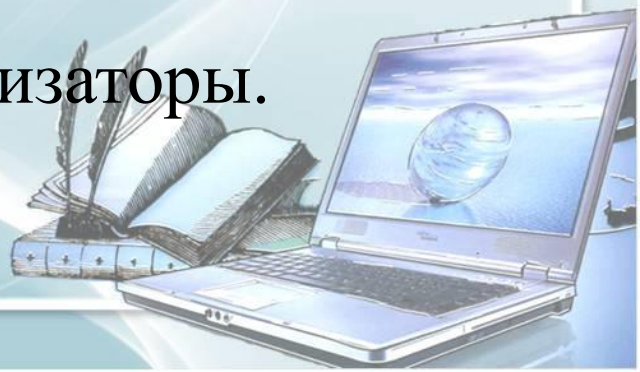
Вредоносные программы – вирусы.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным.

Защита и уничтожение вирусов

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

— программы-детекторы;
— программы-доктора, или фаги;
— программы-ревизоры;
— программы-фильтры;
— программы-вакцины, или иммунизаторы.



Профилактика

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

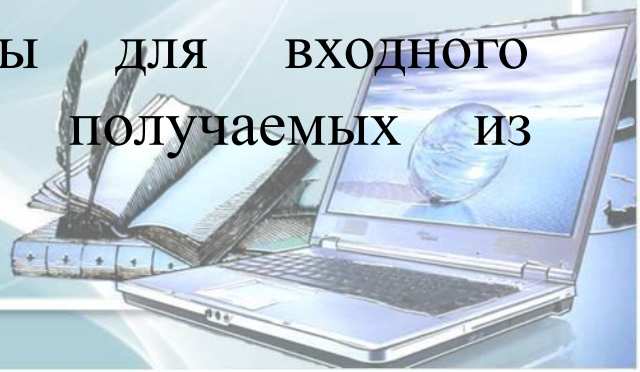
- оснастите свой компьютер современными антивирусными программами

-перед считыванием съемного диска всегда проверяйте эти дискеты на наличие вирусов

-периодически проверяйте на наличие вирусов жесткие диски компьютера,

-обязательно делайте архивные копии на дискетах ценной для вас информации;

-используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;



Сайты-подделки

Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносное ПО
- навязывают платные услуги

Как не стать жертвой мошенников?

1. Используй функционал браузера: «избранное», «закладки»!
2. Проверяй адрес сайта!
3. Обрати внимание на настоящий адрес сайта! При наведении мыши реальный адрес отображается во всплывающей подсказке.

Спам

Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.

ПОМНИ: идя на поводу у СПАМа есть риск:

- Отправить платное СМС, оплатить навязанную услугу.
- Получить платную подписку на ненужную информацию.
- Потерять учётные и (или) иные данные.
- Стать жертвой обмана.

Как себя обезопасить?

- Настрой безопасность браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты)!
- Используй дополнительные расширения браузеров, например AddBlock (позволяет блокировать СПАМ и рекламные блоки), WOT (показывает рейтинг сайта среди интернет-пользователей)!
- Используй Антивирус и файерволл!

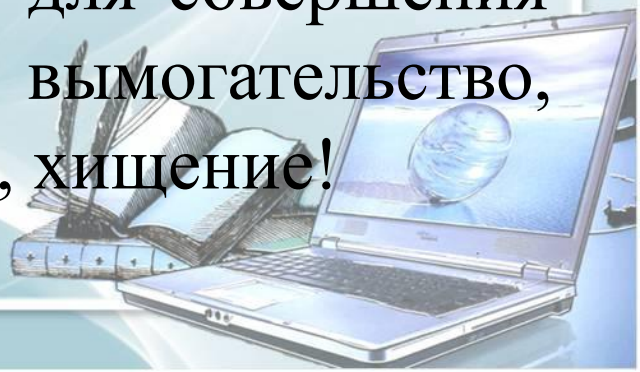
Мы все вместе улыбнемся,
Подмигнем слегка друг другу,
Вправо, влево повернемся
И кивнем затем по кругу.
Все идеи победили,
Вверх взметнулись наши руки.
Груз забот с себя стряхнули
И продолжим путь науки.

Кража информации

Персональные данные – твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Кому и зачем нужна твоя персональная информация?

- 80% преступников берут информацию в соц. сетях.
- Личная информация используется для кражи паролей.
- Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг , хищение!



Как себя обезопасить?

- При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!
- Настрой приватность в соц. сетях и других сервисах
- Не публикуй информацию о своём местонахождении и (или) материальных ценностях!
- Хорошо подумай, какую информацию можно публиковать в Интернете!
- Не доверяй свои секреты незнакомцам из Интернета!

Online - игры

Основные советы по безопасности твоего игрового аккаунта

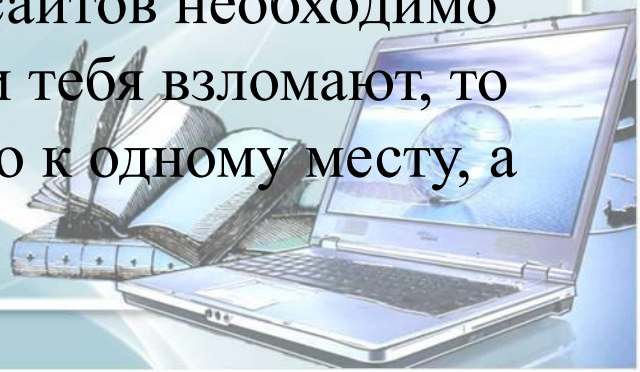
- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
  Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
  Не указывай личную информацию в профайле игры;
  Уважай других участников по игре;
- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Социальные сети

Основные советы по безопасности в социальных сетях

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8

  Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.



Рекомендации, с помощью которых посещение Интернет может стать менее опасным:

- Посещайте Интернет вместе с родителями, или делитесь с ними успехами и неудачами в деле освоения Интернет;
- Если в Интернет вас что-либо беспокоит, то вам следует не скрывать этого, а поделиться своим беспокойством со взрослыми;
- При общении в чатах, использовании программ типа ICQ, использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Выберите регистрационное имя (псевдоним), не содержащее никакой личной информации;

- Нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию;
- Уважайте собеседников в Интернет. Правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
- Никогда не стоит встречаться с друзьями из сети Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
- Далеко не все, что можно прочесть или увидеть в Интернет – правда. Спрашивайте у взрослых о том, в чем вы не уверены.

ПОМНИТЕ О НАШИХ СОВЕТАХ

И ТОГДА ИНТЕРНЕТ СТАНЕТ ВАШИМ НАДЕЖНЫМ И ПОЛЕЗНЫМ ДРУГОМ

Спасибо за внимание!

Использованы материалы:

- Блинков И.А.: Безопасность детей и молодежи в сети Интернет
- Википедия – свободная энциклопедия
- Брошюра "Безопасность детей в сети Интернет» http :// molod-nv.ru/content/page/23
- «Безопасность детей в Интернете» http :// www.soprotivlenie.org/files/all/book099.pdf