ГБОУ СОШ «Оц» с. Богатое
3А класс

Учебный курс для родителей «Цифровая гигиена»

Тема 1.

Лекция по теме:

«История возникновения Интернета. Понятия Интернет - угроз. Изменения границ допустимого в контексте цифрового образа жизни».

Цель:

Расширить представление родителей о безопасности в интернете; возможных интернет – угрозах.

Способствовать формированию навыков безопасного поведения в информационном обществе.

Задачи:

1. Привлечение внимания родителей к проблеме информационной безопасности.
2. Ознакомление с перечнем опасностей, которые несет электронный мир.
3. Совместное сотрудничество учителей и родителей в целях изучения цифрового пространства.

Оформление и оборудование:

- Компьютер и мультимедийный проектор;
- Видеоролики:

«Самые распространенные вирусы» https://youtu.be/xC0wf0igiu8,

«Электронные деньги»
https://youtu.be/hb-gLiLagC8,

-Презентация «Фишинг»
https://infourok.ru/prezentaciya-na-temu-fishing-v-internete-5499207.html

«Как реагировать на кибербуллинг»
https://youtu.be/L0mE3sNYxWA

Ход

- С каждым годом молодежи в интернете становиться больше, и это одна из категорий самых активных пользователей Интернета.

- Казалось бы, чем можно навредить человеку, сидя за монитором? Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

Наша лекция посвящена теме: «История возникновения Интернета. Понятия Интернет - угроз. Изменения границ допустимого в контексте цифрового образа жизни».

История Интернета началась в конце 50-х годов XX века, а именно, когда в 1957 году в СССР запустили первый искусственный спутник. В разгар холодной войны «захват» Советским Союзом космического пространства представлял серьезную угрозу для США. Необходимо было ускорить темпы разработок новейших систем защиты. С этой целью в 1957 году было создано Агентство перспективных исследований Министерства обороны США – ARPA. Эту организацию интересовал вопрос, можно ли соединять расположенные в разных местах компьютеры с помощью телефонных линий. Их целью являлась организация сети передачи данных, способной функционировать в условиях ядерного конфликта. В январе 1969 года впервые была запущена система, связавшая между собой

4 компьютера в разных концах США. А через год новая информационная сеть, названная ARPAnet, уже приступила к работе.
С каждым годом ARPAnet росла и развивалась и из военной и засекреченной сети становилась все более доступной для различных организаций.
В 1973 году сеть стала международной.
В 1983 году был введен в строй новый механизм доступа к ARPAnet, названный «протоколом TCP/IP». Этот протокол позволял с легкостью подключаться к Интернету при помощи телефонной линии.
В конце 80-х годов терпению военных пришел конец, так как сеть превратилась из секретной в общедоступную. Поэтому они отделили от сети часть для своих нужд, получившую название MILNet.
В конце 90-х годов стало возможным передавать по сети не только текстовую, но и графическую информацию и мультимедиа.
Одной из первых российских сетей, подключенных к Интернету, стала сеть Relcom (Релком), созданная в 1990 году на базе Российского центра «Курчатовский институт». В создании сети принимали участие специалисты кооператива «Демос» (сейчас это компания «Демос-Интернет»). Уже к концу года к Интернету было подключено 30 организаций. В 1991 году в компьютерной сети Relcom появился первый сервер новостей (электронных конференций). И очень скоро она объединила многие крупные города России (Екатеринбург, Барнаул и др.), а также некоторых других стран СНГ и стран Балтии.
Сегодня Интернет состоит из миллионов компьютеров, подключенных друг к другу при помощи самых разных каналов, от сверхбыстродействующих спутниковых магистралей передачи данных до медленных коммутируемых телефонных линий.

1) Компьютерные вирусы
Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю. В большинстве случаев распространяются вирусы через интернет.
Как понять, что компьютер заражен
Есть определенные признаки, которые являются ярким доказательством того факта, что на ПК был занесен вирус:
- объем оперативной памяти без объективных причин внезапно и ощутимо уменьшается;
- замедляется работа программ, которые раньше функционировали быстро;
- увеличиваются размеры файлов; - появляются необычные файлы, которые ранее не были замечены в системе;
- могут возникать как звуковые, так и видеоэффекты, а также другие отклонения.
Словом, в работе операционной системы при заражении наблюдаются заметные сбои. Если подобные признаки были зафиксированы, то стоит проверить насколько эффективна действующая защита информации. Антивирусные программы постоянно совершенствуются, а это значит, что стоит оставить в стороне приверженность конкретному продукту и периодически искать наиболее эффективные системы защиты ПК.

Методы защиты от вредоносных программ:
• Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
• Постоянно устанавливай обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

• Ограничь физический доступ к компьютеру для посторонних лиц;
• Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
• Работай на своем компьютере под правами пользователя, а не администратора.
• Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
• Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

2)СетиWI-FI

Да, бесплатный интернет-доступ в общественных местах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

• Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
• Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
• При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
• Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
• Ипользуй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
• В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.
(показ презентации или ролика)

3) Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

• Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
• Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
• 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;
• Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
• Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
• 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. (показ ролика)

4) Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Основные советы по безопасной работе с электронными деньгами:

• Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

• Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

• Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль.

• Не вводи свои личные данные на сайтах, которым не доверяешь.

(показ презентации или ролика)

5) Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

• Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

• Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;

• Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

• Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

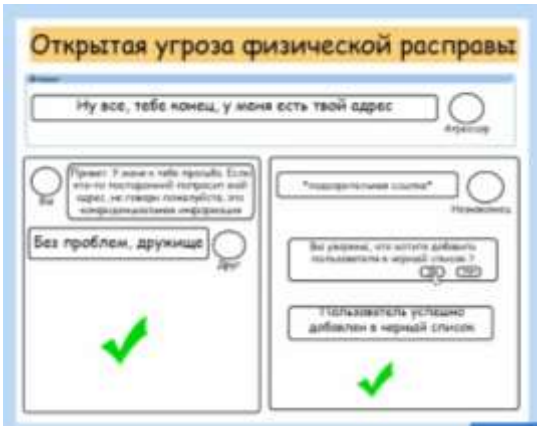
• Если есть возможность написать самому свой личный вопрос, используй эту возможность;

• Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

• Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

• После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

6) Кибербуллинг или виртуальное издевательство



Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

• Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
• Управляй своей киберрепутацией;
• Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
• Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
• Соблюдай свой виртуальную честь смолоду;
• Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
• Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
• Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

7) Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

• Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
• Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
• Необходимо обновлять операционную систему твоего смартфона;
• Используй антивирусные программы для мобильных телефонов;
• Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
• После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
• Периодически проверяй какие платные услуги активированы на твоем номере;
• Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

• Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

8) Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей.

Основные советы по борьбе с фишингом:

• Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
• Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
• Используй сложные и разные пароли.
• Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
• Установи надежный пароль (PIN) на мобильный телефон;
• Отключи сохранение пароля в браузере;

II Памятка
по безопасному поведению в Интернете

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- Используйте нейтральное экранное имя, не выдающее никаких личных сведений.
- Защитите свой компьютер.
- Используйте надежные пароли и храните их в секрете.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Не допускайте грубости в интернете, блокируйте веб-агрессоров.
- Не добавляйте незнакомых людей в свои контакты
- Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились 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.

III. Рефлексия.

Каждый родитель заканчивает предложение на выбор:

- - Лекция была мне полезна, потому что…
- - Я сегодня узнал…
- - Теперь я буду…
- Возможны свои варианты предложений.