Муниципальное автономное общеобразовательное учреждение

средняя общеобразовательная школа № 2

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПО ОБУЧЕНИЮ УЧАЩИХСЯ ПРАВИЛАМ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ, ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. Рекомендации разработаны на основании письма Министерства образования и науки Мурманской области от 12.12.2014 №17-02/9115-ИК «О методическом обеспечении деятельности по противодействию экстремизму среди обучающихся и профилактике интернет-зависимости».

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 No 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

- школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;

- ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю;

- лучше работать за компьютером в первой половине дня;

- комната должна быть хорошо освещена;

- при работе за компьютером следить за осанкой, мебель должна соответствовать росту;

- расстояние от глаз до монитора – 60 см;

- периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиа- безопасности»); знакомить родителей с современными программно- техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.

В основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

- познакомить учащихся с ответственным, достойным поведением в Интернете;

- рассказать об основных опасностях и правилах безопасного использования сети Интернет;

- убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;

- объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;

- убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.

ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование модерируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.

Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Обсудите с подростками азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися: рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся.

**Родителям могут быть даны следующие рекомендации по формированию у учащихся навыков безопасного поведения в сети Интернет:**

Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.

Научите детей не загружать программы, музыку или файлы без вашего разрешения.

Позволяйте заходить на детские сайты только с хорошей репутацией и контролируемым общением.

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.

Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Единство родительских и педагогических усилий поможет оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

Информационная памятка для обучающихся

С каждым годом молодежи в Интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, Интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

*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, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через Интернет.

*Методы защиты от вредоносных программ:*

Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

Постоянно устанавливай почти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

Ограничь физический доступ к компьютеру для посторонних лиц;

Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;

Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

*Сети WI-FI*

Wi-Fi — это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «WirelessFidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFiсети не являются безопасными.

*Советы по безопасности работе в общедоступных сетях Wi-fi:*

Не передавай свою личную информацию через общедоступные Wi-Fiсети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

При использовании Wi-Fiотключи 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-FIдля передачи личных данных, например, для выхода в социальные сети или в электронную почту;

Используй 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-Fiавтоматически». Не допускай автоматического подключения устройства к сетям Wi-Fiбез твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebookуже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. 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.

Электронные деньги

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

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов — анонимные и не анонимные. Разница в том, что анонимные — это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

**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. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;;

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

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. 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».

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.

*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.

Online-игры

Современные онлайн-игры — это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

**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;

Не устанавливай неофициальные патчи и моды;

Используй сложные и разные пароли;

Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

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. На английском языке phishingчитается как фишинг (от fishing— рыбная ловля, password— пароль).

**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. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

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;

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.

Цифровая репутация

Цифровая репутация — это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в Интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» — это твой имидж, который формируется из информации о тебе в Интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких — все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

**Основные советы по защите цифровой репутации:**

Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;

Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники — активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права — это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

**Методические и справочные материалы**

***Классный час***

***«Безопасный интернет в начальной школе»***

Цель: Познакомить учащихся с опасностями, которые подстерегают их в сети Интернет, и помочь избежать этих опасностей.

Задачи: познакомить с правилами поведения в информационном обществе с целью обеспечения информационной безопасности; способствовать расширению кругозора учащихся.

Форма: беседа.

Ход занятия

I. Организация класса

2.Сообщение темы

Учитель: Сегодня мы поговорим на очень важную для всех нас тему.

Я вам загадываю загадки, а вы отвечаете.

1.Что за чудо-агрегат

Может делать все подряд -

Петь, играть, читать, считать,

Самым лучшим другом стать? (Компьютер.)

2.Не зверушка, не летаешь, а по коврику скользишь

И курсором управляешь.

 Ты – компьютерная... (мышь).

3.Сетевая паутина оплела весь белый свет,

 Не пройти детишкам мимо.

 Что же это? (Интернет).

– Кто догадался, о чём мы будем говорить сегодня на классном часе? О компьютере, интернете, безопасности в интернете.

Тема классного часа«Безопасность в Интернете».

Целеполагание: Какие цели поставим перед собой сегодня на уроке? Компьютер и Интернет приносят пользу или вред? Какой вред может нанести компьютер и Интернет человеку? Можно ли пользоваться Интернетом так, чтобы было безопасно?

Работа по теме.

Учитель. Ещё несколько десятков лет назад компьютер был диковинкой, а сегодня он стал доступен обычной семье.

-Ребята у кого дома есть компьютер? Кто им пользуется?

-А как вы пользуетесь компьютером? (Слушаем музыку, играем, выполняем задания, готовим сообщения).

Каждое современное предприятие внедряет компьютерные технологии в производственный процесс.

-Ребята, где вы видели компьютер? (В школе, банках, магазинах, поликлинике, на работе у родителей).

2. Работа в парах.

1. Что такое Интернет для вас? (дети высказываются). После обсуждения на доске появляются таблички («Средство для поиска информации», «Место, где можно играть», «Большой магазин», «Источник учебной информации», «Средство для поиска друзей, место общения»).

2. Какие угрозы вас могут ожидать при работе в сети Интернет?

(1. Угроза заражения вредоносным программами. 2. Доступ к нежелательной информации. 3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. 4. Неконтролируемые покупки).

 - Что такое Интернет?

Интернет – обширная информационная система, которая стала наиболее важным изобретением в истории человечества. Хотя сеть интернет построена на основе компьютеров, программ и линий связи, в действительности она представляет собой систему взаимодействия людей и информации. Это всемирная электронная сеть информации(паутина), которая соединяет всех владельцев компьютеров, подключенных к этой сети. Сеть Интернет представляет собой информационную систему связи общего назначения. Получив доступ к сети, можно сделать многое. При помощи Интернета можно связаться с человеком, который находится, на другом конце света. В Интернете собрана информация со всего мира.

- Как вы понимаете значение слова БЕЗОПАСНОСТЬ?

Безопасность – отсутствие угроз, либо состояние защищенности от угроз. Положение, при котором не угрожает опасность кому-нибудь или чему-нибудь.

- Что вы понимаете под угрозой?

Угроза – запугивание, обещание причинить кому-нибудь неприятность, зло.

(После обсуждения на доске появляется определение).

- Откуда может исходить угроза в Интернете? (ответы детей)

(от взрослых, сверстников при личном общении, через мобильную связь, через ИНТЕРНЕТ).

 Часто в ИНТЕРНЕТЕ встречаются материалы, которые противоречат закону, нарушают права и достоинство человека.

Наш классный час направлен на то, чтобы помочь вам сориентироваться в ИНТЕРНЕТЕ, научиться извлекать из общения с ним пользу. Мы поговорим с вами о том, как защититься от ИНТЕРНЕТ-угроз, о безопасности, бдительности, познакомимся с правилами сетевого общения.

**Классный час на тему: «Информационная безопасность несовершеннолетних»**

Цель: научить подростков правильно пользоваться интернетом; познакомить детей с опасностями сети Интернет; дать рекомендации по безопасному использованию всемирного источника информации.

Задачи:

- выявить отношение подростков к интернету;

- сформировать у подростков знания правильного поиска информации в интернете;

- проинформировать подростков об отрицательных и положительных сторонах интернета;

- развивать умения видеть положительные и негативные стороны в работе с компьютером,

Ход мероприятия

1.Организационный момент

Учитель: Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Интернет - это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины. 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.

«Нам в интернете всё знакомо! Мы в интернете словно дома!»

Международные стандарты в области информационной безопасности детей нашли отражение и в российском законодательстве. Федеральный закон Российской Федерации № 436-ФЗ от 29 декабря 2010 года "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию", направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Закон устанавливает порядок прекращения распространения продукции средства массовой информации.

***Тест на знание правил поведения в интернете:***

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.

A) Попрошу его фото, и потом отправлю своё.

B) Посоветуюсь с родителями.

2)В чате тебя обозвали очень грубыми словами.

A) Скажу в ответ: «Сам дурак».

B) Прекращу разговор с этим человеком.

3)Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

A) Потребую доказательств, что она плохая.

B) Сразу откажусь.

4)Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.

A) Вышлю только пароль: они сами должны знать логин.

B) Отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «B».

4 «А» - Тебе ещё многому надо научиться.

3 «А» и 1 «В» - Внимательно прочитай памятку по безопасному поведению в интернете.

2 «А» и 2 «В» - Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В» - Ты почти справился, но есть слабые места.

4 «В» - Молодец! К интернету готов!

Обсуждение вопроса: «Какие опасности подстерегают нас в интернете?

- Угроза заражения вредоносным программным обеспечением;

- Доступ к нежелательному содержимому;

- Контакты с незнакомыми людьми с помощью чатов или электронной почты;

- Неконтролируемые покупки;

- Интернет-зависимость;

- Интернет – преступники и их деятельность в сети.

Учитель: Вот сколько опасностей подстерегает нас в интернете, давайте с вами подумаем и обсудим, что делать и как всего этого избежать.

1. Спрашивай взрослых

2. Установи фильтр

3. Не спеши открывать файлы

4. Не спеши отправлять SMS

5. Осторожно с незнакомыми

6. Будь дружелюбен

7. Не рассказывай о себе

Учитель: Интернет прочно вошел в жизнь практически каждого человека. Очень многие уже не представляют свою жизнь без этого достижения техники. Однако это достижение рождает множество проблем, которые требуют незамедлительного решения.

«Интернет зависимость» – это широкий термин, обозначающий большое количество проблем поведения и контроля над влечениями.

Некоторые признаки виртуальной зависимости:

· Пристрастие к виртуальным знакомствам – избыточность знакомых и друзей в сети Интернет.

· Навязчивая потребность в сети – игра в онлайновые азартные игры.

· Информационная перегрузка (навязчивый web-серфинг) – бесконечные путешествия по сети, поиск информации по базам данных и поисковым сайтам.

***Тест на интернет - зависимость***

Ответы на каждый вопрос даются по пятибалльной шкале:

1 – очень редко, 2 – иногда, 3 – часто, 4 – очень часто, 5 – всегда.

1. Как часто Вы обнаруживаете, что задержались в сети дольше, чем задумывали?

2. Как часто Вы забрасываете свои домашние обязанности, чтобы провести больше времени в сети?

3. Как часто Вы предпочитаете развлечения в интернете общению с друзьями?

4. Как часто Вы строите новые отношения с друзьями по сети?

5. Как часто Ваши знакомые жалуются по поводу количества времени, что Вы проводите в сети?

6. Как часто из-за времени, проведенном в сети страдает Ваше образование и/или работа?

7. Как часто Вы проверяете электронную почту, прежде чем заняться чем-то другим?

8. Как часто страдает Ваша эффективность или продуктивность в работе из-за использования интернета?

9. Как часто Вы сопротивляетесь разговору или скрываете, если Вас спрашивают о том, что Вы делали в сети?

10. Как часто Вы отодвигаете на второй план неприятные мысли о своей жизни, заменяя их успокаивающими мыслями об интернете?

11. Как часто Вы чувствуете приятное предвкушение от предстоящего выхода в сеть?

12. Как часто Вы боитесь, что жизнь без интернета станет скучной, пустой и безынтересной?

13. Как часто Вы раздражаетесь, кричите, если что-то отрывает Вас, когда Вы находитесь в сети?

14. Как часто Вы теряете сон, когда поздно находитесь в сети?

15. Как часто Вы чувствуете, что поглощены интернетом, когда не находитесь в сети, или воображаете, что Вы там?

16. Как часто вы замечаете свои слова «еще пару минут…», когда находитесь в сети?

17. Как часто Вы пытаетесь безуспешно урезать время пребывания в сети?

18. Как часто Вы пытаетесь скрыть количество времени пребывания в сети?

19. Как часто Вы предпочитаете находиться в сети вместо того, чтобы встретиться с людьми?

20. Как часто Вы чувствуете подавленность, плохое настроение, нервничаете, когда Вы не в сети, что вскоре исчезает, стоит Вам выйти в интернет?

Теперь подсчитайте общую сумму баллов.

При сумме баллов 50-79 стоит учитывать серьезное влияние интернета на вашу жизнь.

При сумме баллов 80 и выше, у Вас с высокой долей вероятности интернет-зависимость и Вам необходима помощь специалиста.

**Рекомендации подросткам**

1. Используйте реальный мир для расширения социальных контактов. Реальный мир, жизнь человека – это постоянное освоение, расширение и преображение реальности, и внутренней, и внешней. Таким путем человек становится совершеннее.

2. Определите свое место и цель в реальном мире. Ищите реальные пути быть тем, кем хочется. Избегайте простых способов достигать цели: бесплатный сыр – только в мышеловке.

3. Виртуальная реальность заполняет «дыры» в жизни. Живите без «заплаток»!

4. Компьютер – это всего лишь инструмент, усиливающий ваши способности, а не заменитель цели.

5. Развивать в виртуальной реальности то, что для вас не важно в реальной жизни, – нельзя. Делайте то, что хотите, в реальной жизни!

6. Ищите друзей в реальности. Виртуальный мир дает только иллюзию принадлежности к группе и не развивает никаких действительных навыков общения.

7. Наполняйте жизнь положительными событиями, поступками.

8. Имейте собственные четкие взгляды, убеждения.

9. Избегайте лживости и анонимности в виртуальной реальности.

10. Пребывайте «здесь и сейчас», а не «там».

11. Научитесь контролировать собственное время и время за компьютером.

Учитель: Интернет - это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина может быть и весьма опасна.

**Самостоятельная работа по группам: «Плюсы» и «минусы» Интернета**

Задание: ученикам предлагается самим подумать и перечислить положительные и отрицательные стороны Интернета. Например, в интернете можно найти: прогноз погоды, новости, чат, магазины и др.

Заполняется таблица.

Положительные моменты интернета:

– развитие технического прогресса;

– доступ к разнообразной информации;

– доступность и легкость покупок.

Отрицательные моменты интернета:

– широкие знакомства – зависимость;

– теряется навык реального общения;

– портится язык (словарный запас);

– меняются цели человека;

– виртуальная реальность замещает действительную.

Подведем итоги классного часа.

**Памятка по безопасному поведению в интернете**

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей интернета и причинения возможного ущерба, вы должен предпринимать следующие меры предосторожности при работе 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 содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

• Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.

• Всегда сообщайте взрослым обо всех случаях в интернете, которые вызвали у вас смущение или тревогу.

• Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

• Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в интернете. О подобных предложениях немедленно расскажите родителям.

• 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. Расскажите об этом родителям.

**Тема классного часа «Безопасность в Интернете».**

Целеполагание: Какие цели поставим перед собой сегодня на уроке? Компьютер и Интернет приносят пользу или вред? Какой вред может нанести компьютер и Интернет человеку? Можно ли пользоваться Интернетом так, чтобы было безопасно?

Работа по теме.

Учитель. Ещё несколько десятков лет назад компьютер был диковинкой, а сегодня он стал доступен обычной семье.

-Ребята у кого дома есть компьютер? Кто им пользуется?

-А как вы пользуетесь компьютером? (Слушаем музыку, играем, выполняем задания, готовим сообщения).

Каждое современное предприятие внедряет компьютерные технологии в производственный процесс.

-Ребята, где вы видели компьютер? (В школе, банках, магазинах, поликлинике, на работе у родителей).

2. Работа в парах.

1. Что такое Интернет для вас? (дети высказываются). После обсуждения на доске появляются таблички («Средство для поиска информации», «Место, где можно играть», «Большой магазин», «Источник учебной информации», «Средство для поиска друзей, место общения»).

2. Какие угрозы вас могут ожидать при работе в сети Интернет?

(1. Угроза заражения вредоносным программами. 2. Доступ к нежелательной информации. 3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. 4. Неконтролируемые покупки).

 - Что такое Интернет?

Интернет – обширная информационная система, которая стала наиболее важным изобретением в истории человечества. Хотя сеть интернет построена на основе компьютеров, программ и линий связи, в действительности она представляет собой систему взаимодействия людей и информации. Это всемирная электронная сеть информации(паутина), которая соединяет всех владельцев компьютеров, подключенных к этой сети. Сеть Интернет представляет собой информационную систему связи общего назначения. Получив доступ к сети, можно сделать многое. При помощи Интернета можно связаться с человеком, который находится, на другом конце света. В Интернете собрана информация со всего мира.

- Как вы понимаете значение слова БЕЗОПАСНОСТЬ?

Безопасность – отсутствие угроз, либо состояние защищенности от угроз. Положение, при котором не угрожает опасность кому-нибудь или чему-нибудь.

- Что вы понимаете под угрозой?

Угроза – запугивание, обещание причинить кому-нибудь неприятность, зло.

(После обсуждения на доске появляется определение).

- Откуда может исходить угроза в Интернете? (ответы детей)

(от взрослых, сверстников при личном общении, через мобильную связь, через ИНТЕРНЕТ).

 Часто в ИНТЕРНЕТЕ встречаются материалы, которые противоречат закону, нарушают права и достоинство человека.

Наш классный час направлен на то, чтобы помочь вам сориентироваться в ИНТЕРНЕТЕ, научиться извлекать из общения с ним пользу. Мы поговорим с вами о том, как защититься от ИНТЕРНЕТ-угроз, о безопасности, бдительности, познакомимся с правилами сетевого общения.

Просмотр видеролика.

3. Назовите несколько правил безопасности при работе в сети Интернет.

Не сообщайте свой электронный адрес никому, кроме людей, которым доверяете.

Тщательно обдумайте, какую информацию о себе загружать в Интернет.

 Осторожно подходите к выбору друзей, не принимайте все заявки подряд для количества.

Не открывайте доступ к своим личным страничкам незнакомым людям. Обязательно установите антивирус, обновляйте их базы.

Будьте осторожны при общении с незнакомыми людьми.

Нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работыпапы или мамы и т.д.;)

Основные правила на доске:

1. Будьте осторожны при общении с незнакомыми людьми.

2. Нельзя сообщать свои личные данные.

3. Установите антивирус.

4. НЕ запускайте неизвестные файлы.

5. НЕ открывайте письма от незнакомцев.

Работа в группах

Вначале занятия, мы говорили о том, полезен интернет или нет. Давайте еще раз вспомним полезные и отрицательные стороны интернета.

 Я предлагаю рабочим группам приступить к обсуждению. Одна группа выстраивает позицию и доказывает о «Плюсах интернета». Вторая группа отстаивает точку зрения «Минусы интернета».

Посовещайтесь несколько минут, запишите на бумаге слова защиты в свою пользу, а затем мы выслушаем обе стороны. Каждая группа отстаивает свою точку зрения. Записывает ответы на стикерах и приклеивает к плакату.

(Карточки прикреплены к доске, ниже дети записывают варианты своих ответов)

«Здоровье и Интернет»

«Время и Интернет»

 «Игры и Интернет»

«Образование и Интернет»

«Интернет и Общение»

«Здоровье»

Испортится зрение.

Народные рецепты

Можно получить облучение.

Можно посмотреть как использовать и для чего нужно это лекарство.

Нарушается осанка.

Отсутствие прогулки

«Время»

Забыл сделать домашнюю работу

Быстрый поиск (экономия)

Забыл поесть

Получаешь быстрый ответ на свой вопрос

Не погулял

Заигрался

«Игры и Интернет»

Время

Развивающие

Агрессия

Командный дух

Безразличие к судьбе героя игры

Логика

«Интернет и Образование»

Копирование информации.

Бесплатное обучение

Интернет не сможет объяснить как учитель, разными способами

Подготовка к конкурсам, поиск информации, фото.

Углубленное изучение предметов

Вопросы по хобби

Электронная библиотека

«Интернет и Общение»

Отсутствует настоящее общение

Быстрота ответов при разговоре, несмотря на расстояние

Опасные незнакомцы

Новые знакомства

Можно не только поговорить, но и увидеть своего собеседника

5 . Рефлексия

- Молодцы. Мы выслушали разные мнения и задали друг другу много вопросов. Согласимся, что Интернет даёт нам много возможностей, НО станет Интернет другом вам или врагом - зависит только от вас.

– Главное – правильно им воспользоваться.

- Наша встреча подошла к концу мне хочется, чтобы вы выразили свое отношение к уроку при помощи жетонов. Вы сможете подойти к нашему сундучку и выбрать себе жетон. Если Вы считаете занятие полезным, выбирайте – желтый цвет, если считаете урок бесполезным, то красный. Жетоны складываем у меня на столе.

**Дополнительные методические материалы**

Родительское собрание на тему "Безопасность детей в сети Интернет"

XXI век на дворе: Интернет вошел в каждый дом.

Сеть информирует, учит, продвигает, рекламирует, продает, покупает, следит, контролирует, консолидирует, словом, живет, как настоящее живое общество.

Мы, наши дети, и даже их бабушки и дедушки активно пользуемся всеми возможностями Интернета: участвуем в социальных сетях, смотрим фильмы, клипы, слушаем музыку, играем, пишем в блоги; сеть предлагает все больше и больше возможностей.

Среда Интернета может оказаться небезопасной для ребенка: контакты с незнакомыми людьми с помощью чатов или электронной почты, доступ к нежелательному содержимому, угроза заражения вредоносным ПО, другие опасности.

Родители должны быть информированы не только о возможной опасности для ребенка, но и способах обеспечения его безопасности в сети Интернет.

Цель: просвещение родителей по теме “Безопасность детей в сети Интернет”.

Подготовительные мероприятия:

- анкетирование учащихся по теме собрания;

- подготовка буклета для родителей по теме собрания.

 Ход родительского собрания

I. Мотивация к деятельности. Тренинг.

Родители рассаживаются по кругу лицом друг к другу, передавая из рук в руки приятный на ощупь мягкий мячик, высказывают свою точку зрения и аргументы по предлагаемому вопросу. Первый вопрос – мячик передают по часовой стрелке, второй вопрос - мячик передают против часовой стрелки и т.д.

Вопросы.

Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.

Что сделаем, чтобы не повторять ежедневно: “Ты опять весь день просидел (а) за компьютером”?

Какую пользу извлекает Ваш ребенок при использовании сети Интернет?

Какие опасности ждут Вашего ребенка в сети Интернет?

II. Анализ, обсуждение ситуаций и разработка рекомендаций.

Еще недавно компьютеры были скорее роскошью, но уже сейчас являются чуть ли не “предметом первой необходимости”.

Результаты анкетирования детей класса показали, что:

75 % детей имеют дома компьютер

В среднем ежедневно дети проводят за ним по 4 часа в день

Из видов деятельности, преобладающих в общении с компьютером, дети на первое место поставили – компьютерные игры. 80% из них каждый день играют в компьютерные игры, причем 51% может начать играть, даже не пообедав.

На втором месте – общение в Сети. 70% пользуются Интернетом – из них 100% общаются в социальных сетях, 63% - играют в сетевые онлайн игры.

Далее дети выбирают прослушивание музыки, рисование, печать документов соответственно 46%, 135 и 1%

 38% -при определении рейтинга использования свободного времени на I место поставили компьютер, исключив при этом занятия спортом, прогулки на воздухе, общение с семьёй.

Сегодня мы с вами остановимся на особенно важной проблеме современных школьников – зависимости от сети Интернет.

Зависимость в медицинском смысле определяется как навязчивая потребность в приеме привычного вещества, сопровождающаяся ростом толерантности и выраженными симптомами. Рост толерантности означает привыкание ко всё большим и большим дозам.

Интернет-зависимость – это навязчивая потребность в использовании Интернета.

Существует 5 типов Интернет-зависимости:

бесконечный веб-серфинг — постоянные «путешествия» по Интернету с целью поиска информации.

пристрастие к виртуальному общению и виртуальным знакомствам, характеризуется большими объёмами переписки, постоянным участием в чатах, форумах, избыточностью знакомых и друзей из Интернета.

игровая зависимость — навязчивое увлечение сетевыми играми.

навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах.

киберсексуальная зависимость — навязчивое влечение к посещению порносайтов.

Интернет-зависимость характеризуется сильным желанием ребенка быть в сети, что приводит к нежеланию проводить время с семьей и друзьями, спать, посещать и делать уроки. Ребенок может перестать следить за своим внешним видом, начинает болезненно реагировать на просьбы отвлечься от компьютера, терять контроль за своим временем, лгать, причем уход от реальности может усиливаться день ото дня.

Родители должны уметь распознать признаки надвигающейся зависимости, прежде чем она станет реальной проблемой. Но это легче сказать, чем сделать.

Зависимость от Интернета все чаще называют чумой XXI века. В отличие от сигарет или наркотиков запретить Интернет нельзя – глобальная Сеть прочно вошла в нашу жизнь. Интернет – необходимый инструмент, которым ребенку в новом тысячелетии предстоит пользоваться постоянно.

 Подростковый возраст — время быстрых изменений в жизни. Хотя дети все еще сильно зависят от своих родителей, они уже хотят некоторой свободы. Ребята начинают интересоваться окружающим миром, и отношения с друзьями становятся для них по-настоящему важными.

Дети этого возраста используют Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и заходят на фанатские сайты своих кумиров. Их любимый способ общения — мгновенный обмен сообщениями.

Данные, показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте, и роль, которую Глобальная сеть играет в жизнях подростков, значительна.

Дети опережают взрослых по количеству времени, которое они проводят в Интернете. В возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернета

Более 90% подростков 8-16 лет сталкивались с порнографией в сети

44 % детей, регулярно использующих Интернет, хоть один раз подвергались сексуальным домогательствам при виртуальном общении, 11 % подверглись этому несколько раз.

14.5 % детей назначали встречи с незнакомцами через Интернет. 10 % из них ходили на встречи в одиночку, а 7 % никому не сообщили, что с кем-то встречаются.

38% детей просматривают страницы о насилии

16% детей просматривают страницы с расистским содержимым

Согласно исследованию, проведенному в 2006 году в Польше, почти 1/3 родителей (28,4%) не осознает опасностей, с которыми могут встретиться их дети в Интернете

Сегодня мы с вами вместе попробуем разобраться в том, какие опасности ждут ребенка в сети и как его от них оградить.

Основные угрозы для детей в сети Интернет

1. Системы мгновенного обмена сообщениями

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.

Одна из самых опасных угроз заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле.

В этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Выобмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.

Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.

Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.

Другой потенциальный риск в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.

Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

2. Электронная почта

Электронная почта – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:

Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвержены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже наркотики с большим риском для своего здоровья.

Далее, существуют ложные предложения работы. Это не представляет серьезную опасность для детей, но может являться таковой для подростков. Обычно эти сообщения содержат фантастические условия работы. Они обещают большие зарплаты без каких-либо усилий. Все, что в таких случаях необходимо, - это номер банковского счета, куда будут перечисляться деньги, а затем, в обмен на комиссию, получателя попросят перевести эти средства на другой банковский счет. Это выглядит слишком хорошо, чтобы быть правдой, и любой здравомыслящий взрослый человек насторожиться от такого предложения. Однако молодые люди ищут легких денег. В результате этого они непроизвольно становятся соучастником преступления, т.к. целью подобных финансовых переводов является «отмывание» преступных денег.

Другой риск связан с вирусами и вредоносными программами, которые могут попасть на компьютер. Как правило, они распространяются через сообщения в электронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям нажать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техника известна как «социальная инженерия». Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это научить их быть бдительными по отношению к письмам из неизвестных источников. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не

должны открывать файлы или нажимать на ссылки в письмах подобного рода.

3. Программы обмена файлами

Обмен файлами в P2P-сетях является еще одним из основных источников распространения инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это проверять каждый скаченный файл с помощью решения безопасности до момента их первого открытия / запуска.

Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия должны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл содержит в себе вирусы или другое вредоносное программное обеспечение.

4. Социальные сети и блоги

Сайты социальных сетей (например, Facebook, MySpace, одноклассники, Вконтакте) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а также свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.

Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.

Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.

5. Мобильные телефоны с выходом в Интернет

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.

В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.

В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

Итак. вот несколько рекомендаций общих психологов для профилактики Интернет-зависимости у детей:

Ограничьте количество времени, которое дети могут проводить в Интернете. Убедитесь, что ребенок пользуется Сетью во время, отведенное домашнему заданию, для учебы, а не для развлечений. Вместе с ребенком составьте подробный план с указанием, на что тратится время, проводимое за компьютером. Это поможет сократить время на бездумное обновление странички одноклассников в ожидании нового сообщения, чтение новостей ради самого процесса чтения и т.д.

Не ставьте компьютер в комнате ребенка. Установите компьютер в гостиной или в своей комнате – там, где вы сможете легко контролировать то, что ваш ребенок делает в Интернете. С помощью современных мобильных телефонов можно подключиться к Сети для общения, игр и просмотра сайтов. Неважно, с помощью какого устройства ребенок будет уходить в виртуальный мир. Важно не допустить, чтобы виртуальная реальность не стала для него домом.

Выясните, что ваш ребенок любит делать в Интернете. Некоторые онлайн-игры, в которых действие происходит в фантастических мирах с тысячами игроков по всему миру, например, World of Warcraft, действительно увлекают. Известны случаи, когда взрослые люди достигали крайней степени истощения, не в силах оторваться от любимой игры, не говоря уже о таких «мелочах», как разводы, потеря работы и т.д. Кроме того, во многих играх, чтобы добиться успеха, нужно не только проводить в игре много часов в день, необходимо также вкладывать в своего персонажа реальные деньги, обменивая их на игровую валюту. Не получив денег на игру от родителей, ребенок может пойти на обман или воровство.

Не подавайте детям плохой пример. Не проводите слишком много времени у компьютера, не берите с собой за город ноутбук или планшет. Активный отдых всей семьей поможет ребенку переключиться на реальную жизнь. Займите ребенка другими вещами, настольными или спортивными играми. Найдите ему занятие по душе. Тогда Интернет станет подспорьем в учебе, вспомогательным средством поиска информации и общения, а не способом ухода от реальности и бегства от проблем.

Советы по безопасности, или Как Вы можете защитить своих детей

Создайте список домашних правил Интернета при участии детей.

Используйте программы по защите детей в сети.

Существует ряд программ, позволяющих защитить собственного ребенка от посещения, нежелательных сайтов.

Программа «Интернет-Цензор» – Интернет—фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.

Хотите оградить ребенка от опасных и вредных сайтов? Используйте бесплатное программное обеспечение «Интернет Цензор» - это быстро и очень просто!

Лучшее решение для защиты ребенка в Интернете! В основе работы Интернет Цензора лежит технология "белых списков", гарантирующая 100% защиту от опасных и нежелательных материалов. Программа содержит уникальные вручную проверенные "белые списки", включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации.

Более подробную информацию о программе, возможность бесплатно скачать программу вы можете на странице http://www.icensor.ru/soft/

Родителям демонстрируется работа с данной программой, показывается, как можно добавить сайт в «белый» или «черный» список.

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы вы говорили о чем-то другом.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

Позволяйте детям заходить на детские сайты только с хорошей репутацией.

Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.

Научите детей не загружать программы без вашего разрешения — они могут ненарочно загрузить вирус или шпионскую программу.

Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома, создайте для него учетную запись с ограниченными правами.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Расскажите детям о порнографии в Интернете и направьте их на хорошие сайты о здоровье и половой жизни.

Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.

Расскажите детям об ответственном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, сплетен или угроз другим.

Если вы обеспокоены безопасностью ребенка при его работе в Интернете или при использовании мобильной связи;

Если ребенок подвергся опасности или стал жертвой сетевых преследователей и мошенников;

Обратитесь на линию помощи «Дети онлайн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и Интернет;

Позвоните по телефону 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск).

Или направьте Ваше письмо по адресу: helpline@detionline.com

Подробнее о Линии помощи вы можете узнать на сайте <http://detionline.com>

И последний совет – будьте внимательны к своим детям!