Конспект урока безопасности в Интернете

(для проведения занятий в общеобразовательных организациях)

Урок целесообразно проводить для обучающихся младших, средних или старших классов, делая акцент на наиболее актуальных проблематиках для каждого возраста.

ВВЕДЕНИЕ

Добрый день! Сегодня я хочу поговорить с вами об обеспечении безопасности в интернете. Техническое обеспечение полиции не стоит на месте, а постоянно обновляется, вместе с прогрессом всего человечества. Информационные центры, базы данных, которые хранят все сведения в цифровом формате и являются сегодня фундаментом для работы полиции, создавались в последние десятилетия, и активно функционируют в настоящее время. Работа МВД России стала высокотехнологичной, полицейские теперь расследуют не только преступления, совершенные физически, в реальном пространстве, но и злодеяния в сети Интернет. Такие правонарушения предусмотрены Главой 28 Уголовного Кодекса Российской Федерации, мы называем их «преступлениями в сфере компьютерной информации».

Компьютерная грамотность необходимое условие воспитания человека в XXI веке. Информационные технологии являются неотъемлемой частью современного общества. В России больше 80 миллионов человек выходят в интернет каждый день, и значительную часть из них составляете именно вы и другие ребята вашего возраста.

Интернет - уникальная реальность нашего с вами времени. Это безграничный мир информации, в котором есть как развлекательные и игровые порталы, так и полезные сведения для учебы и расширения кругозора. Именно с помощью интернета мы общаемся со своими друзьями в режиме онлайн, вступаем в сообщества по интересам, делимся последними новостями, веселимся и делаем домашнюю работу. Иными словами, интернет - это информация, оперативно обеспечивающая ваши ежедневные потребности и доступная в любой момент.

Однако полицейские вынуждены предупреждать об опасностях виртуального мира. Определенная часть пользователей сети ищет в интернете не друзей, а своих жертв.

Важно обезопасить себя и своих близких от преступных намерений других людей. Недобросовестные граждане (мошенники, наркодилеры, психически нездоровые люди) по своем у оценивают возможности интернета. Ведь именно сеть зачастую дает возможность преступникам действовать анонимно, поэтому небезопасное поведение в интернете может нанести вред вам, вашим родным и близким.

Необходимо себя обезопасить для этого достаточно серьезно отнестись к проблеме киберпреступности и соблюдать простые правила, о которых сегодня расскажу.

1. ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Начнем с простого вопроса, с помощью каких устройств вы, как правило, выходите в интернет?

(смартфон, планшет, ноутбук, персональный компьютер, умные часы)

Безусловно, это так. Нам удобно находить информацию в интернете через эти устройства в первую очередь потому, что они небольшие, удобные, стильные и, как ни странно, имеют экраны. Но наверняка вам известно, что уже сейчас есть холодильники, чайники, умные колонки, утюги, телевизоры, камеры, которые тоже могут иметь доступ к интернету.

Возникает проблема: если так много устройств из нашей повседневной жизни имеют или будут иметь доступ к интернету, как нам защититься от их взлома? Ведь они, как правило, подключены к домашней Wi-Fi сети, а значит, заражение способно распространиться на все устройства, подключенные к конкретному роутеру. Однозначного ответа на этот вопрос сейчас нет ни у кого. Многие эксперты считают, что интернет вещей может как вывести нашу цивилизацию на качественно новый уровень, так и погрузить ее в хаос. Но почему мы начали разговор именно с этого? Все просто: мне бы хотелось бы еще раз напомнить вам банальные, но важные истины. Для защиты себя и своих гаджетов от вторжения:

Используйте сложные пароли.

Статистика говорит о том, что люди не слишком то задумываются о своих паролях, часто ставят один и тот же пароль на множество сайтов и социальных сетей. Исключите использование паролей по умолчанию и не сохраняйте пароли в ваших гаджетах и браузерах. Да, это не всегда удобно, но мы же хотим, чтобы наши устройства были безопасными? Как вы считаете, какие два пароля до сих пор остаются самыми популярными в мире? Верно, «123456» и «qwerty». Надеюсь, что вы используете более сложные варианты, ведь подобрать простой пароль злоумышленнику действительно не доставит труда. Регулярно осуществляйте смену паролей и никому их не сообщайте. Пароль должен содержать сочетание цифр, прописных и строчных букв, а также специальных символов. Не используйте один и тот же пароль на каждом сайте, который вы посещаете.

Вы резонно можете мне возразить: все это, конечно, здорово, но как я запомню столько разных, сложных паролей для различных аккаунтов? Мой совет таков: пользуйтесь менеджерами паролей. Их можно скачать как на компьютеры, так и на смартфоны, в них несложно зарегистрироваться и

внести свои пароли. Удобство этих программ заключается и в том, что при фиксации мошеннической атаки они автоматически меняют все сохраненные пароли.

В дополнение к паролю необходимо подключить двухфакторную авторизацию когда вы будете вводить регистрационные данные для входа на страницу социальной сети или в мессенджер, вам дополнительно придет СМС-сообщение с кодом доступа. Это займет лишение 10 секунд, но может обезопасить вас от больших проблем в будущем. Такая технология пришла из банковской сферы, но все вы знаете, что в настоящее время и Вконтакте, и Т1кТок настоятельно предлагают защищать свои аккаунты именно таким образом.

Пользуйтесь антивирусными программами.

И вновь банальный, но важный совет. Любому компьютеру или гаджету могут причинить ущерб вредоносные программы. Они в состоянии скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть денежные средства. Их называют «черви», «трояны», «шпионы», но суть одна все это вирусы. Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями. Также нельзя допускать истечения срока действия вашего антивируса в таком случае он будет работать неэффективно.

Не стоит скачивать программы с непонятных сайтов, открывать и сохранять подозрительные файлы, отвечать на загадочные рассылки. И главное не посещайте сайты с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения.

Думаю, все вы сможете назвать несколько антивирусных программ для компьютера и смартфона. Кстати, возвращаясь к нашему разговору про интернет вещей: если у вас есть домашняя Wi-Fi сеть, подключите роутер к стационарному компьютеру или ноутбуку по проводам. Тогда весь трафик пойдет через устройство, и антивирусной программе будет легче отражать атаки мошенников.

Никому не передавайте свои конфиденциальные данные и следите за «цифровым следом».

Это могут быть логины, пароли, данные банковских карт, свидетельство о рождении, паспортные данные, личные фотографии. Такие «цифровые следы» тянутся за вами всю жизнь, могут навредить на пути к достижению поставленной цели. Игнорируйте в интернете подобные запросы. Важно запомнить правило: «Документы всегда хранятся в сейфе».

Цифровой след уникальный набор действий в Интернете или на цифровых устройствах. Во Всемирной паутине это информация, оставленная в результате просмотра веб-страниц и сохраненная в виде cookie - файлов.

Если вы публикуете какую - либо информацию на своей странице в социальной сети, обязательно проверьте настройки конфиденциальности на сайте: убедитесь, что данные не доступны для просмотра широкой публике.

То, что вы публикуете в интернете, останется там навсегда, даже если вы удалите эти сведения. Университеты и работодатели проверяют профили соискателей в социальных сетях, поэтому убедитесь в том, что вы публикуете в Интернете, уместно и не навредит вам в будущем.

2. ОСКОРБЛЕНИЯ И НАПАДКИ В СЕТИ ИНТЕРНЕТ

Давайте поговорим о тех, кто чаще всего доставляет нам огорчение при общении в интернете. Это разнообразные вредители, главная цель которых уколоть вас, испугать, огорчить или заставить грубить в ответ. Существует такая категория интернет вредителей это граждане, имеющие преступные намерения в отношении вас лично, или просто злые люди, выходящие сначала за грань воспитанности, а затем и за грань закона. Самый распространенный вид хулиганства в сети это троллинг.

Троллинг — форма провокации или издевательства при общении в интернете, использующаяся людьми, заинтересованными в узнаваемости, публичности, эпатаже. Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это искушение, провокация и подстрекательство — то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям.

Термин «троллинг» происходит из сленга участников виртуальных сообществ. Цель тролля подбросить вам такую наживку (обидное слово, насмешка, оскорбление), чтобы вы ее заглотили (начали расстраиваться, писать ругательства в ответ). Анонимность в сети позволяет троллям представлять себя совершенно другими и быть уверенными в своей безнаказанности, поэтому они пишут и делают такие вещи, которые в реальной жизни никогда бы не рискнули сотворить в присутствии оппонента. По причине как неизвестности, так и недосягаемости, травить, оскорблять и провоцировать людей, кажется им забавным занятием. Как показывает практика, больше половины сетевых грубиянов являются детьми, скучающими в интернете или не ладящими со сверстниками.

Запомним простое правило: **не надо кормить троллей, это бессмысленно.** Если вы заметили, что кто то в сети ведет себя таким образом вы можете легко победить его: не спорьте с ним, не пытайтесь оправдаться или что -то объяснить, не обращайте внимания. Ведь единственное, что ему нужно это ваша реакция. Как только вы перестанете реагировать он очень быстро потеряет к вам интерес. Не доставить грубияну удовольствия видеть ваш гнев или обиду будет лучшим наказанием, ибо его цель не будет достигнута.

Давайте будем разделять троллинг и юмор. Безусловно, никто не запрещает вам шутить над своими друзьями, обсуждать в сети вопросы, не

обязательно используя литературный русский язык. Просто не переходите грань: юмор не должен перерастать в оскорбления, хамство и откровенную травлю.

Гораздо опаснее ситуация, когда вас начинают обижать люди, которые знают вас лично. В случае, когда вы видите, что против вас начинается коллективная травля ни в коем случае не расстраивайтесь и не замыкайтесь. В сети людям свойственен стадный инстинкт, и многие из тех, кто включается в травлю, лично против вас ничего не имеют. Они просто пошли на поводу у группы людей, и это говорит о них очень красноречиво значит, у них нет своего мнения, они являются послушными куклами в чужих руках.

Тебя начинают атаковать в мессенджерах, социальных сетях или модных приложениях? Требовать фотографии или персональные данные, угрожать с разной аргументацией, против тебя организуется коллективное преследование? Оскорбления, угрозы, искажение твоих изображений все это не безобидные шутки, это буллинг.

Кибербуллинг — агрессивное преследование в сети Интернет одного из членов коллектива со стороны остальных членов коллектива или его части.

При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от конфликта, где силы сторон примерно равны. Буллинг приводит к тому, что жертва теряет уверенность в себе. Также это явление может приводить к психическим отклонениям и явиться причиной жестокой агрессии в сторону тех, кто занимается травлей.

Существует несколько видов кибербуллинга:

- *Пападки:* постоянные изнурительные атаки, повторяющиеся оскорбительные сообщения, направленные на жертву;

- *Клевета:* распространение оскорбительной и ложной информации;

- *Самозванство:* перевоплощение в определенное лицо, когда мошенник позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях;

- *Обман:* выманивание конфиденциальной информации и ее распространение, получение персональных данных и их публикация в сети Интернет или передача тем, кому она не предназначалась.

В этих случаях очень важно объяснить человеку, что его травят злоумышленники, причем травят безосновательно и нет причин для расстройства, снижения самооценки. Надо показать, как действовать в сложившейся ситуации. И вы не должны допускать такого в своем коллективе, друзья!

Обязательно сообщите взрослым (родителям, родственникам, учителям) о преследовании вас или ваших одноклассников в сети интернет и примите вместе решение об обращении в полицию. Храните подтверждения фактов нападений в сети. Не переживайте в тайне от родителей такие

ситуации. Если для травли используют ваши прошлые ошибки или неправильное поведение гораздо проще сразу признаться в этом перед старшими, чем загонять проблему внутрь. Не спешите выбрасывать свой негатив в киберпространство, создавайте собственную онлайн- репутацию . И никогда не принимайте сами участие в травле кого-либо. Ваше достойное поведение является главной защитой и гарантом спокойствия вас и ваших близких.

3. ЗЛОУМЫШЛЕННИКИ в СЕТИ

Настало время поговорить об очень опасном уровне интернет угроз , где целью являетесь вы, а не ваш кошелек. Именно вас хочет виртуальный злодей вовлечь в преступную деятельность.

Рекламируя замечательный заработок по распространению наркотиков, запрашивая у вас личные фото за большие деньги, или требуя сфотографировать банковскую карту родителей, эти личности нарушают закон. Все это реальные наказуемые деяния, и интернет в таком случае лишь виртуальная рука к вам, протягиваемая настоящими преступниками.

За последнее время резко возросло количество преступлений с использованием переписок в социальных сетях или мессенджерах. Большая часть детей, ставших объектом такого виртуального насилия, не достигли 16летнег о возраста. Обращаю ваше внимание на то, что в Российской Федерации установлен общий 16летний возраст уголовной ответственности, а за отдельные преступления с 14летнего возраста.

Широкое распространение смартфонов, доступность использования интернета, неограниченная возможность анонимного общения и быстрого обмена фото и видео позволяют лицам, имеющим преступные намерения, совершать противоправные действия в отношении вас. Очевидно, что в силу возраста, любопытства и чувства безопасности в домашних условиях вам легко вступать в разговоры на любые запретные темы, в том числе развращающего характера.

У вас могут обманным путем узнать номер банковской карты, которую возможно дали вам родители, и это вызовет финансовые потери в семье. Также вас могут склонить к совершению поступков, нарушающих права других людей, что в конечном счете приведет к возникновению у вашей семьи проблем, связанных с нарушением законов, а я уверен, что вы совсем этого не хотите. Иногда из за вашей невнимательности можно открыть непонятное вложение электронной почты или загрузить с сайта небезопасный файл, и в компьютер может попасть вредоносный код, разработанный со злым умыслом.

Одной из важнейших угроз является вовлечение в распространение наркотиков через различные социальные сети. Подростки и даже их родители не до конца осознают всей полноты ответственности, которая может последовать. Более того, на самом первом этапе некоторые «закладчики»

воспринимают происходящее как некий увлекательный квест. Как правило, сами они наркотики не употребляют, многие из вполне благополучных семей. А вот срок, который грозит им по статье за сбыт и распространение наркотиков: 8-15 лет. Немало, правда?

4. МОШЕННИКИ В СЕТИ

И мы, наконец, переходим к заключительной части нашего разговора. Интернет стал местом, где многие проводят большую часть своей жизни. Помимо общения, интернет дает очень много возможностей: совершение покупок, платежи за различные услуги, использование государственных порталов для обращений граждан.

В последние годы появилось много мошенников, которые выманивают у людей деньги, пользуясь их неграмотностью, да и просто невнимательностью при работе в интернете. Самый распространенный вид интернет мошенничества, про который вы уже наверняка слышали не один раз, это фишинг. Кто-нибудь сможет сказать мне, что это такое, или привести пример фишинга?

Спасибо. Фишинг - это кража любых персональных данных, от которых преступники могут получить выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к личным кабинетам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Как защитить себя от спама и фишинга? Заведите себе несколько адресов электронной почты. Лучше всего иметь по крайней мере два адреса. Личный адрес электронной почты должен использоваться только для личной корреспонденции, а «публичный» электронный адрес используйте для регистрации на общедоступных форумах и в чатах, а также для подписки на почтовую рассылку и другие интернет услуги .

Сейчас активно растет игровая индустрия. Поднимите руки, кто из васактивно играет в онлайн игры? А кто из вас имеет платный аккаунт?

Имейте в виду, что игровое мошенничество тоже очень развитый бизнес. Такие вещи, как купленный танк, игровое оружие, скин для героя в стратегии представляют собой ценность, которую можно украсть и потом перепродать за большие деньги.

Запомните очень четко родители должны быть в курсе всех вашихдействий в сети, связанных с онлайн платежами. Они смогут быстро отменить ошибочный или неправильный платеж или обратиться в полицию в случае мошенничества. Никогда, ни при каких обстоятельствах не сообщайте никому

реквизиты пластиковых карт, ваших или родительских. Особенно защищенными должны быть PIN-коды и CVV-коды , написанные на обороте карты. Обратите внимание, что личную информацию можно вводить только при безопасном соединении. **Всегда смотрите в адресную строку адрес вебсайт а должен начинаться с «https://», а в интерфейсе браузера должна появиться иконка замка.**

Еще несколько советов от меня, если позволите.

Регулярно выполняйте резервное копирование важной для вас информации, чтобы перезагрузка вашего компьютера, или вынужденная смена программного обеспечения вашего компьютера (атаки злоумышленников это нередкость и не фантастика), не стала для вас слишком чувствительной. ***Есть очень хорошая фраза: «Если что-то звучит слишком хорошо, чтобы быть правдой, скорее всего это неправда».*** Все мы получали письма по электронной почте с обещанием чего-нибудь бесплатного, например, мобильного телефона или билетов на концерт. Это трюки, призванные заставить вас передать личные сведения, не покупайтесь на них. Еще одно правило, которое следует запомнить: «Посмотрите в обе стороны, прежде чем переходить улицу». Воспринимайте ее не только в буквальном, но и в переносном смысле. Например, прежде, чем скачать приложение из App1e Store или Goog1e P1ay, посмотри его рейтинг, почитай отзывы: убедись, что оно не навредит твоему устройству. Принцип «подумай, прежде чем сделать» будет актуален всегда. И последнее. Сейчас для разблокировки смартфонов очень популярны отпечаток пальца и разблокировка по лицу. Это очень удобно и стильно, но если вы храните большой объем личной, важной, конфиденциальной информации в телефоне используйте пароль из 4 цифр. Он гораздо надежнее и безопаснее новых способов разблокировки, хоть и не столь быстр и удобен.

ЗАКЛЮЧЕНИЕ

Подводя итог всему сказанному, я попрошу вас будьте бдительны в сети точно так же, как и в реальной жизни. Для наглядности продемонстрирую небольшую подборку новых типов мошенничеств и наглого обмана граждан, которые появились в последние два года:

1) Мошеннические телеграмм-каналы.

Предлагают вносить финансовые средства на расчетный счет и делать ставки в букмекерских конторах, не зарегистрированных на территории Российской Федерации и действующих без лицензий. Такие каналы часто продвигают блогеры, получая за рекламу значительные суммы денег, при этом рядовые пользователи становятся жертвами обмана.

2) «Суперприбыльные» инвестиции.

Предложения о вложении в ценные бумаги банков или телекоммуникационных компаний. Такие инвест-проекты «гарантируют» безусловный возврат вложенного капитала и высокие прибыли, вместе с тем капитал в последующем не возвращается.

3) Интернет магазины с необоснованно низкими ценами.

Мошенники создают сайт интернет магазин а и активно запускают рекламный трафик, чтобы высвечиваться на первых страницах в поисковых системах. За товар требуется полная предоплата, а доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен. После перевода денежных средств покупателем, продавец перестает выходить на связь и удаляет сайт интернет магазина.