Приложение

Конспект урока безопасности в интернете
(для проведения занятий в общеобразовательных учреждениях)

ВВЕДЕНИЕ

В прошлом году российская полиция отметила свое 300-летие. Уже три столетия полицейские охраняют граждан, общественный порядок, раскрывают преступления и разыскивают тех, кто их совершает.

Сегодня я хочу поговорить с вами про обеспечение безопасности в интернете. Причем тут полиция, можете спросить вы?

Дело в том, что охрана законности нс стоит на месте, развиваясь вместе с прогрессом всего человечества. Например, только сто лет назад появилась экспертная служба, без которой сегодня трудно себе представить работу полицейского. Информационные центры, которые хранят все сведения в цифровом формате и являются сегодня фундаментом для работы полиции, создавались в последние десятилетия. Работа МВД России стала высокотехнологичной, полицейские теперь расследуют не только преступления, совершенные физически, в реальном пространстве, но и злодеяния в сети интернет.

Компьютерная грамотность - необходимое условие воспитания человека XXI века. Информационные технологии являются неотъемлемой частью современного общества. В России десятки миллионов интернет- пользователей, и значительную часть из них составляют несовершеннолетние граждане нашей страны.

Интернет - уникальная реальность нашего с вами времени. Это безграничный мир информации, в котором есть как развлекательные и ш-ровые 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. Иными словами, интернет - это информация, 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.

Вся история нашей цивилизации- это борьба добра со злом. Ни одна из сторон не добьется сокрушительной победы, но этого и не требуется. Важно другое - обезопасить себя и своих близких от преступных намерений других людей. Недобросовестные граждане (мошенники, наркодилеры, психически нездоровые люди) по-своему 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.

Но не стоит переживать: врага необходимо встречать во всеоружии. Необходимо себя обезопасить - для этого достаточно серьезно отнестись к проблеме киберпреступности и соблюдать простые правила, о которых я сегодня расскажу.

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Сегодня я бы хотел вести с вами диалог. Понимаю, как сложно воспринимать информацию, когда перед тобой 40 минут стоит человек и непрерывно подает новые и новые сведения. Уверен, нам есть чему научиться друг у друга, поэтому я с удовольствием вас выслушаю. Итак, начнем с простого вопроса, с помощью каких устройств вы, как правило, выходите в интернет? *(смартфон, планшет, ноутбук, персональный компьютер, умные часы)*

Для защиты себя и своих гаджетов от вторжения:

1) 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, вот уже пятый год подряд? 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 эго, конечно, здорово, по как я запомню столько разных, сложных паролей для различных аккаунтов? Мой совет таков: пользуйтесь менеджерами паролей. Их можно скачать как на компьютеры, гак 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 на новые.

2) Пользуйтесь антивирусными программами.

Опять банальный совет, но как же без них? 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.

Ребята, сможете ли вы назвать пять антивирусных программ для компьютера и смартфона?

(Avast, Norton, Dr Web, Kaspersky, защитник Windows, 360 Total Security)

Отлично, спасибо. 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.

Также настоятельно рекомендую Вам использовать контент-фильтр: программное обеспечение для фильтрации сайтов по их содержимому', которое не позволяет получить доступ к определённым сайтам или услугам сети Интернет. Система автоматически блокирует веб-сайты с опасным содержимым.

3) Никому не передавайте свои конфиденциальные данные.

Это могут быть логины, пароли, данные банковских карт, свидетельст во 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».

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.

Многие программы (особенно программы для обмена мгновенными сообщениями, такие как What's App) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в программу без ввода логина и пароля. Конечно же. не оставляйте без присмотра компьютер с важными сведениями на экране. А если вы работаете за компьютером в классе на информатике, заканчивая работу, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться ваша личная информация.

ХУЛИГАНЫ В ИНТЕРНЕТЕ

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. В дословном переводе trolling означает «ловлю рыбы на блесну». То есть 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 - требовать фотографии или персональные данные, начинают 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 (получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, задирать, провоцировать, донимать, терроризировать). 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 отклонениями явиться причиной жестокой агрессии в сторону тех, кто занимается травлей или даже самоубийства.

Существует несколько видов буллинга:

- Нападки, постоянные изнурительные атаки, повторяющиеся оскорбительные сообщения, направленные на жертву;
- Клевета, распространение оскорбительной и неправдивой информации.
- Самозванство, перевоплощение в определенное лицо: хулиган позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях, ведет переписку;
- Надувательство, выманивание конфиденциальной информации и се распространение: получение персональной информации и публикация ее в интернете 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 кибер-пространство, 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.

ЗЛОУМЫШЛЕННИКИ В СЕТИ

Настало время поговорить об очень опасном уровне интернет-угроз, где целью является 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 здесь 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 16-летнего возраста. Обращаю ваше внимание на то, что в Российской
Федерации установлен общий 16-летний возраст уголовной ответственности, а за отдельные преступления с 14-летнего 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. Понятно, 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 нс 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 не до конца осознаю! 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?

МОШЕННИКИ В СЕТИ

И мы, наконец, переходим к заключительной часта 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.

На следующем, более технологичном уровне в сети возникает угроза несанкционированного доступа к вашим интернет-ресурсам, компьютерам, гаджетам, банковским и иным каргам, даже к вашим аккаунтам в онлайн-играх (уверен, у многих из вас они есть). Все это работа мошенников, цель которых проста - материальная нажива, незаконная деятельность
по отъему виртуальным способом денег у 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, эго фишинг. Кто-нибудь сможет сказать мне, что эго такое, или привести пример фишинга?

Спасибо. Вот еще пример от меня: вам на почту приходит с виду совершенно безобидное письмо, например, от интернет-провайдера, о том, что необходимо заполнить какие-то данные у них на сайте. Вы проходите по ссылке в письме - и попадаете на сайт, внешне неотличимый от настоящего, один в один. Вы заполняете форму, оставляете свои личные данные, номер телефона, реквизиты банковской карты - и с нее разом списываются почти все деньги. Оказывается, что сайт поддельный, и к настоящему сайту никакого отношения не имеет. Найти таких мошенников бывает очень сложно - ведь таких сайтов они создают десятки тысяч, и существуют они один-два дня, после чего исчезают вместе с вашими деньгами.

Фишинг - это кража любых персональных данных, с помощью 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 вас активно 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 ваших действий в если, 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 карг, 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 веб-сайта должен начинаться с «https://», а в интерфейсе браузера должна появиться иконка замка.

Не используйте общественные беспроводные сети и устройства для работы с личной информацией и не вздумайте посылать по почте и через интернет-мессенджеры копии своих документов, даже родственникам и друзьям.

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 не рсдкостьи не фантастика), не стала для вас слишком чувствительной.

Мне нравится 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 Apple Store или Google Play, посмотри его рейтинг, почитай

отзывы: убедись, что оно нс 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 горазд надежнее и безопаснее новых способов разблокировки, хоть и не столь быстр и удобен.

ТВОРЧЕСКОЕ ЗАДАНИЕ

Спасибо за внимание, друзья. А теперь я предлагаю вам провести небольшое соревнование. У меня в руках три листка, на которых описана определенная ситуация. Вам необходимо разбиться на три группы и выбрать один из листков. Представьте, что вы лично попали в эту ситуацию. В течение 5 минут каждая группа должна продумать ответ, а потом вы расскажете, как поступить в описанном случае.

Ситуация № 1

В соседнем классе учится школьник, которого в социальных сетях травят и оскорбляют его одноклассники. Они издеваются над ним по разным причинам, но в первую очередь потому, что он замкнутый, не может и не хочет дать отпор коллективу. Сам школьник ничего не говорит об этой ситуации ни учителям, ни родителям, и травля продолжается. Кроме того, он отличник - знает все предметы (в том числе информатику) и легко решает контрольные работы, но никому не даст списывать у себя.

Видя эту ситуацию, что вы будете делать? Оставите все как есть, поговорите с задирами, сами присоединитесь к травле, или что-то еще?

Ситуация № 2

Ученик 7 класса увлекается собиранием специальных карт для ролевых игр. Он очень хочет заполучить в свою колоду карту с особым магическим заклинанием, однако ему никак не удается ее купить. Поэтому подросток решает найти через интернет человека, который бы согласился обменять такую карту на какую-нибудь из карт школьника. После длительных поисков такого человека удалось найти. Алексей (23 года) согласился поменяться. Алексей предлагает встретиться сегодня в 21:00 около клуба, где проходят турниры по карточным ролевым играм.

Стоит ли школьнику согласиться на встречу? Доверяете ли вы Алексею?

Какие могут быть последствия встречи? Какими способами ученик мог бы себя обезопасить?

Ситуация № 3

В школе, в девятом классе, учились две подруги, Лиза и Даша. Под большим секретом Лиза рассказала Даше, что ей нравится один парень из одиннадцатого класса. Даша не удержалась и рассказала об этом одной знакомой в социальной сети, и скоро это стало известно всем. Над Лизой стали смеяться, Лиза очень разозлилась и стала писать про Дашу некрасивые посты в Интернете. Родители Даши обратились к классному руководителю и директору школы. В итоге Лиза была вынуждена перейти в другую школу.

Как вы думаете, реальна ли эта история? Как чувствуют себя Лиза и Даша? Кто пострадал в этой ситуации, а кто поступил неправильно? Как вы бы поступили в данной ситуации на месте Даши?

ПОДВЕДЕНИЕ ИТОГОВ

Подводя итог всему сказанному, я попрошу вас - будьте бдительны в сети точно так же, как и в реальной жизни.

Незнакомец - каждый, кого вы не знаете лично. Не доверяйте интернет-знакомствам. И не ждите, что преступник сразу покажет свое лицо. Подсказкой вам должно стать содержание первой же просьбы или предложения.

Что-то вас насторожило? Прекратите общение, никаких дискуссий, снимите скриншот, заблокируйте этого собеседника и сообщите родителям об этом факте.

А теперь я готов ответить на ваши вопросы и о киберпреступности, и о службе в полиции.