Приложение

Конспект урока безопасности в интернете для родителей

Введение

Добрый день, уважаемые родители. Сегодня я бы хотел поговорить про обеспечение безопасности в интернете: как вашей, так и вашего ребенка. Мы постоянно пользуемся всемирной сетью для общения и получения информации, вступаем в сообщества по интересам, делимся последними новостями. Иными словами, интернет – это информация, обеспечивающая ежедневные потребности и доступная в любой момент.

Хотел бы отметить, что работа МВД России стала высокотехнологичной, полицейские теперь расследуют не только преступления, совершенные физически, в реальном пространстве, но и противоправные действия в сети интернет.

На сегодняшний день доля интернет-пользователей в России весьма значительна и исчисляется десятками миллионов граждан. У наших детей также есть возможность выхода во всемирную сеть.

Мы все чаще вынуждены предупреждать об опасностях виртуального мира. Преступники используют сеть Интернет для совершения противоправных действий, и наша задача - **обезопасить детей от преступных намерений других людей.** Недобросовестные граждане по-своему оценивают возможности интернета, «благодаря» ему появляется возможность действовать анонимно, поэтому небезопасное поведение в сети может нанести вред вам и вашим близким людям.

Для того, чтобы не стать жертвой мошенничества, важно серьезно отнестись к проблеме киберпреступности и соблюдать правила, о которых я сегодня расскажу. Также рекомендую вам провести беседы с детьми и рассказать им об опасностях, поджидающих на просторах сети.

Как обеспечить безопасность ребенка при использовании интернета и социальных сетей

Начать свое выступление хотелось бы с важных тезисов, которые позволят вам минимизировать риски попадания ребенка в проблемную ситуацию.

В первую очередь необходимо проинформировать ребенка как о возможностях интернета, так и об опасностях, которые он в себе хранит. Объясните ребенку, что в интернете как и в жизни надо быть осторожным с незнакомыми людьми.

Расскажите о некоторых правилах поведения в интернете, в том числе в соцсетях:

1. Никогда и ни при каких обстоятельствах не размещать в сети и не сообщать незнакомцам личную информацию (номера телефонов, адреса, место работы родителей, номер или адрес школы, любимые места для прогулок).
2. Не встречаться с онлайн-знакомыми, потому что люди могут оказаться не теми, за кого себя выдают.
3. Не посещать подозрительные сайты или страницы с противоправным контентом. Предупредите о возможных негативных последствиях открытия подозрительной почты, реагирования на рекламные сообщения. Расскажите о возможных видах интернет-мошенничества.

Не все, что можно прочитать или увидеть в интернете - правда. Порекомендуйте ребенку консультироваться с Вами относительно полученной в интернете информации.

В интернете как и в жизни необходимо соблюдать правила и нормы поведения. Обязательно рассказывать родителям о случаях проявления агрессии со стороны других людей или попытках вовлечь в подозрительные сообщества.

Установите на компьютер, планшет или смартфон ребенка специализированное программное обеспечение, позволяющее

регламентировать перечень доступных для посещения сайтов, количество времени, проведенного в Сети, а также имеющее другие настраиваемые параметры для обеспечения максимально безопасного пребывания ребенка в интернете.

Самое главное - постарайтесь поддерживать доверительные отношения с ребенком и замечать любые малейшие изменения в его поведении.

Защита компьютеров и мобильных устройств

В настоящее время мы выходим в сеть со смартфона, планшета, ноутбука, персонального компьютера, иногда даже умных часов. Нам удобно находить информацию в интернете через эти устройства: они небольшие, удобные, стильные.

Для защиты собственных гаджетов, а также устройств, принадлежащих вашим детям, от вторжения, необходимо:

1) Использовать сложные и различные пароли для доступа к своим аккаунтам и личным кабинетам.

Часто мы не слишком задумываемся о своих личных данных, устанавливаем один и тот же пароль для входа в личные кабинеты банков, аккаунты социальных сетей. Не рекомендуем этого делать, поскольку утечки и взломы известных сайтов нередки. В такой ситуации, зная один пароль, злоумышленник сможет войти во все ваши личные кабинеты, похитить информацию или финансовые средства. Также исключите использование паролей по умолчанию и не сохраняйте их в ваших гаджетах и браузерах. Понимаю, что это не всегда удобно, но только так можно обеспечить полную безопасность своих данных. Примерно раз в год необходимо осуществлять смену паролей. Сложный пароль должен содержать сочетание цифр, прописных и строчных букв, а также специальных символов.

Очевидно, что запоминание нескольких сложных паролей для различных аккаунтов – непростая задача. В такой ситуации на помощь могут прийти менеджеры 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 на новые.

ВАЖНО: Современные дети регистрируются на огромном количестве всевозможных ресурсов, зачастую используя одни и те же данные для входа. Сообщите своему ребенку, что для доступа к основным аккаунтам *(вКонтакте, Facebook, Twitter, Instagram, TikTok, Snapchat, электронный дневник)* рекомендуется использовать разные пароли, привязанные к личному адресу электронной почты.

Для максимальной защиты учетной записи рекомендуется использовать двухэтапную аутентификацию (для входа в аккаунт кроме логина и пароля необходимо ввести одноразовый код или подтвердить действие на электронных устройствах, подключенных к вашему аккаунту).

2) Использовать лицензионные антивирусные программы.

Вредоносные программы создаются для того, чтобы похищать личную информацию с различных устройств, тем самым причиняя ущерб пользователю. Они в состоянии скопировать, повредить или уничтожить важные сведения, отследить ваши действия, украсть денежные средства. В новостях мы слышим различные названия: «черви», «трояны», «шпионы», «вредоносы», но суть одна – все это вирусы. Для защиты компьютера или смартфона на них устанавливаются защитные программы и фильтры. Настоятельно рекомендуем использовать только лицензионное программное обеспечение с актуальными обновлениями.

ВАЖНО: Также настоятельно рекомендую вам настроить контент-фильтр для ребенка: существует 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 либо некорректным содержимым.

3) Внимательно оценивать, какие именно конфиденциальные данные вы передаете третьим лицам.

Часто мы сталкиваемся с ситуацией, когда необходимо направить копии, сканы, фотографии каких-либо документов другому человеку или в организацию. Если сведения, планирующиеся к отправке, действительно важные, рекомендуется передавать их лично, а не через интернет. Если же такой возможности нет, безопаснее всего делать это посредством электронной почты или мессенджеров.

Никогда не отправляйте логины, пароли и данные банковских карт, такая информация должна храниться только у вас.

ВАЖНО: Расскажите детям, что необходимо дважды подумать, прежде чем оправлять друг другу различные фотографии и видеозаписи. Цифровые следы тянутся за ними всю жизнь, могут навредить в будущем: например, при приеме на работу. Дети должны запомнить простое правило: «Документы всегда хранятся в сейфе».

Если они публикуют какую-либо информацию на своей странице в социальной сети, необходимо проверить настройки конфиденциальности на сайте и убедиться, что данные не доступны для просмотра широкой публике. Сообщите своему ребенку: то, что он публикует в интернете, останется там навсегда, даже если он удалит эти сведения впоследствии.

Телефонное мошенничество

Телефонное мошенничество возникло достаточно давно, вскоре после массового распространения домашних телефонов. Но сегодня, когда смартфон есть у каждого, случаи такого мошенничества все так же нередки. Чаще всего жертвами мошенников становятся пожилые или доверчивые люди, а также *дети школьного возраста.*

Так как дети зачастую не имеют личной банковской карты, либо их социальная карта привязана к покупкам на территории школы, целью мошенников являются финансовые средства, хранящиеся на балансе мобильного телефона ребенка.

Так, SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять юным владельцам смартфонов и планшетов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт. Обман может быть организован следующим образом: ребенок получает на мобильный телефон сообщение, якобы от родственника или друга: «У меня проблемы, кинь 500 рублей на этот номер. Мне не звони, перезвоню сам». Детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники. Если ребенок беспокоится, что с его близким человеком действительно может случиться несчастье, всегда лучше перезвонить ему лично, а не реагировать на первое же сообщение с незнакомого номера. Вы можете удивиться, однако таким нехитрым способом все еще совершается значительное количество обманов.

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Вам или вашему ребенку может прийти SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы с социальной картой, блокировка аккаунта в онлайн-игре. После того как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы прекращаете звонок – и оказывается, что с вашего счёта списаны крупные суммы. Такая ситуация происходит, потому что существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок. Мы настоятельно советуем не звонить по незнакомым номерам, и донести эту информацию до ребенка. Это единственный верный способ обезопасить себя от телефонных мошенников.

Существует еще один хорошо известный, но тем не менее до сих пор функционирующий способ мошенничества. Вам поступает звонок либо

приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными:

– предложение подключить новую эксклюзивную услугу;
– для перехода на более выгодный тариф;
– предложение принять участие в акции от вашего сотового оператора.

Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи. На самом же деле код, который вам предложат отправить, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только вы его наберёте, ваш счёт будет опустошён, никакая услуга не будет подключена. Любая упрощённая процедура изменения тарифных планов выглядит подозрительно, не ленитесь перезванивать своему мобильному оператору для уточнения условий.

Советуем вам критически относиться к таким сообщениям и не спешить выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации.

ВАЖНО: Вы можете установить запрет так называемых «платных контентных коротких номеров», то есть ограничить доступ к платным услугам, из-за которых может резко уменьшиться баланс вашего смартфона. Зайдите в личный кабинет мобильного оператора и установите запрет на платные услуги, и вы не сможете воспользоваться платными развлекательными SMS, командами, голосовыми сервисами контент-провайдеров. Такая услуга есть у всех крупных операторов мобильной связи в России.

Банковские карты

Банковская карта является инструментом для совершения платежей и доступа к наличным средствам на счёте, не требующим для этого присутствия в банке. Несмотря на постоянные усилия банков, государственных регуляторов и

правоохранительных органов, простота использования и распространенность банковских карт оставляет множество лазеек для мошенников.

Запомните правила, о которых мы будем сейчас говорить, а если у вашего ребенка уже есть собственная банковская карта, расскажите ему о потенциальных опасностях и способах противодействия им.

Думаю, все вы слышали про **PIN-код карты, а также код безопасности** – комбинацию цифр, указанную на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Напомню, что никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить PIN-код или код безопасности. Сотрудник банка может запросить у вас контрольное слово, полное Ф.И.О., в редких случаях паспортные данные или адрес проживания для изменения важной информации, но ничего более. *При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.*

Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

Если вам позвонили из банка и интересуются вашей платежной картой, разумнее всего прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты).

Также можно обратиться в отделение банка лично. Помните, что самый распространенный способ совершения хищений денежных средств с карт граждан – побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Как безопасно пользоваться интернет-банком?

1. Используйте сложный пароль блокировки экрана и качественную антивирусную программу. Несмотря на очевидное удобство, не входите в банковские приложения, используя отпечаток пальца или функцию распознавания лица.

2. Ни в коем случае не храните в телефоне логин и пароль от входа в мобильный банкинг, а также реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты.

3. Избегайте входа в систему мобильного банкинга с чужих устройств.

4. При утрате телефона немедленно обратитесь в банк для блокировки карты и в офис мобильного оператора для блокировки SIM-карты.

Как безопасно совершать платежи в интернете?

1. Используйте на устройстве антивирус с активной защитой онлайн-платежей.

2. Совершайте оплату только посредством использования защищенных соединений. Защищенное или зашифрованное подключение можно распознать по значку в виде замочка в начале адресной строки браузера и префиксу https:// перед адресом сайта.

3. Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладку браузера. Не проводите финансовые операции с общественного WI-FI в кафе, транспорте или гостиницах, это очень опасно.

4. Не сохраняйте свои данные о карте в браузере. Это недавно появившаяся, очень удобная функция, имеющая свои слабые стороны: злоумышленнику достаточно взломать ваш аккаунт в Google, Yandex, Mail.ru, чтобы получить доступ ко всей сохраненной информации и паролям.

Какими банкоматами пользоваться?

1. Отдавайте предпочтение банкоматам, установленным в защищенных местах (например, в офисах банков, госучреждениях, крупных торговых центрах).

2. Осмотрите банкомат перед использованием. Убедитесь, что на клавиатуре и в месте для приема карт нет дополнительных устройств, следов клея и механических повреждений.

3. При наборе ПИН-кода прикрывайте клавиатуру рукой.

4. Не используйте банкомат с признаками неисправности: устройство зависает, перезагружается или на экране появляются подозрительные изображения.

5. Не используйте банкомат в присутствии подозрительных лиц и не принимайте помощь от незнакомцев.

Интернет-покупки и онлайн-игры

Наиболее часто встречающееся мошенничество заключается в предложении различных категорий товаров по ценам значительно ниже, чем среднерыночная цена.

Мошенники создают сайт интернет-магазина и активно запускают рекламный трафик, чтобы высвечиваться на первых страницах в поисковых системах. Также оплачивают услуги «профессиональных комментаторов», которые оставляют восторженные отзывы о товарах и работе магазина. При этом за товар требуется полная предоплата, а доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен. После перевода денежных средств покупателем, продавец перестает выходить на связь, а затем и вовсе удаляет сайт интернет-магазина.

Характерными показателями таких интернет-магазинов являются:

- чрезмерное занижение стоимости товара относительно среднерыночного показателя;
- телефонная связь и электронная почта в качестве способов коммуникации;
- оплата без расчетного банковского счета;
- обязательная предоплата, зачастую 100 % от стоимости товара;

– отсутствие адреса расположения магазина или его несоответствие данным интерактивных карт.

Как обезопасить себя от сделки с мошенником?

- Если в качестве способов оплаты допустимы только денежные перечисления на лицевой счет электронного кошелька, посредством терминала, либо отправки платного сообщения на телефонный номер - высока вероятность перечислить деньги мошенникам.
- Отсутствие наименования организации в любой из форм собственности (ООО, ИП, ЗАО) является еще одним поводом не совершать сделки с данным продавцом.
- Отдайте предпочтение магазину, который предлагает забрать товар самовывозом. Наличие подобной услуги подразумевает честность продавца. Вы можете заказать доставку покупки, но само по себе наличие такой услуги является плюсом;
- Лучший из способов оплаты - курьеру после получения товара. Вы внесете оплату только после визуального осмотра и проверки товара на работоспособность;
- Иногда мошенники используют копии сайтов известных магазинов. Обращайте внимание на адреса в верхней строке - у известных магазинов они, как правило, простые и запоминающиеся;
- Насторожитесь, если менеджер магазина проявляет излишнюю настойчивость или настаивает на немедленной оплате заказа.

Онлайн-игры

В настоящее активно растет игровая индустрия. Я думаю, что многие из вас играют в онлайн игры и, конечно, такое времяпровождение очень привлекает наших детей. Многие из них имеют платный аккаунт в многопользовательских играх.

К сожалению, игровое мошенничество является весьма развитым. Такие вещи, как купленный танк, игровое оружие, скин для героя в стратегии представляют собой ценность, которую можно украсть и потом перепродать за большие деньги.

ВАЖНО: Родители должны быть в курсе действий ребенка в сети, особенно связанных с онлайн-платежами. Вы можете быстро отменить ошибочный или неправильный платеж или обратиться в полицию в случае мошенничества.

Сегодня мы обсудили основные правила безопасности в сети Интернет. Зная и используя их, Вы сможете защитить себя и своего ребенка от преступных посягательств. Если у Вас есть вопросы, я с удовольствием выслушаю и отвечу на них. Большое спасибо за внимание.