Как защитить детей от интернет-мошенников

Главное, что может во многом защитить ребенка от мошенников в интернете — это его осведомленность о схемах обмана и доверительные отношения с родителями. Важно рассказывать детям, как распознать обманщика и что делать, если в друзья набивается неизвестный человек из интернета. Рассказываем об основных схемах обмана детей и о том, как родители могут минимизировать риски лишиться денег или пострадать от утечек персональных данных.

Что нужно мошенникам и как они обычно связываются с детьми

Основные цели мошенников — кража персональных или платежных данных, паролей от аккаунтов, фото документов. Получив эту информацию, преступники могут обчистить счета родителей и ближайших родственников ребенка, взять на их имя кредиты, получить доступ к личным фото или перепискам, чтобы шантажом вымогать деньги.

Дети из-за небольшого жизненного опыта доверчивы, и если их не научить, как распознавать мошенников, последствия могут быть катастрофическими для семейного бюджета.

Чаще всего мошенники связываются с детьми:

- **В играх**. Обманщики заводят дружбу с детьми в чатах мобильных или компьютерных игр. Нередко выдают себя за популярных игровых блогеров и просят выполнить «задания», чтобы получить подарки, редкие игровые артефакты, игровую валюту или скины. Задания обычно заключаются в том, чтобы прислать фото документов, личные фото, данные банковских карт родителей

- **В мессенджерах и соцсетях**. Преступники могут выходить на детей в Telegram-чатах, в группах в популярных соцсетях. Намерения те же — выудить информацию, которую можно использовать для своего обогащения

Как мошенники обманывают детей

Нужно как можно раньше рассказать ребенку о том, кто такие мошенники и как они действуют, научить с осторожностью относиться к любым заманчивым предложениям в сети. Как правило, киберворы используют следующие схемы:

Просят перейти по ссылке, скачать файл или приложение

Мошенник, установив контакт с ребенком, может отправить ему ссылку или файл и попросить открыть, чтобы «выполнить задание» и получить за это подарки. Часто ссылка имитирует страницу банковского сайта. Мошенники в качестве задания могут попросить ребенка ввести на этой странице данные банковских карт родителей. После этого с деньгами на карте можно попрощаться.

Злоумышленники также могут предложить считать QR или сформировать QR в приложении и переслать его им. Могут попросить подтвердить действие с телефона родителей или попросить сообщить код под предлогом авторизации, регистрации или участия в розыгрыше или опросе.

Еще одна распространенная схема — при переходе по ссылке на компьютер попадает вирус. Когда пользователь открывает свой онлайн-банк и вводит пароль, вирус считывает нажатия на клавиатуру. Так мошенники получают пароли от банковских аккаунтов.

Предлагают купить внутриигровую валюту, артефакты, скины

Среди детей популярны мобильные игры, многие из них имеют собственные магазины, где продают внутриигровую валюту, скины, артефакты. Мошенники заводят дружбу с ребенком и предлагают купить у них цифровой контент дешевле, чем в магазине. Или приобрести аккаунт с кучей уже купленных артефактов. Ребенок переводит деньги, но никакого цифрового контента или аккаунта, естественно, не получает.

Обещают легкий заработок или призы в интернете

Часто мошенники предлагают подросткам подработку в интернете и обещают легкий и быстрый заработок. Они могут присылать подобные предложения в мессенджер, в чаты, зазывать детей через короткие ролики на популярных видеосервисах, всплывающие рекламные баннеры и т.д.

Работу предлагают действительно несложную — например, установить приложение, ежедневно посещать определенные сайты. Также предлагают зарабатывать на ставках или криптоторговле, обещая выигрыши и сверхдоходы. Еще ребенку могут прислать сообщение, что он выиграл суперприз (например, популярную игрушку или ролики), но чтобы получить его, нужно заплатить.

Втягивают в дропперство

Дропперство — это вывод денег с чужих банковских карт через подставных лиц. Работает это так: подростку предлагают оформить дебетовую карту (ее можно оформить с 14 лет) и за денежное вознаграждение отдать ее мошенникам. Затем злоумышленники переводят на нее украденные с чужих карт средства и снимают.

Подросткам также предлагают «привести друга», то есть вовлечь других детей в дроппинг, за каждого обещают заплатить пару тысяч рублей.

Участвуя в подобных схемах, подросток может получить наказание за соучастие в мошенничестве. Для граждан от 16 лет и старше в России предусмотрена уголовная ответственность за подобные преступления.

Взламывают аккаунты друзей и с них просят о помощи

Мошенники, заполучившие доступ к аккаунту подростка, рассылают его друзьям сообщения с просьбой одолжить денег или перейти по ссылке, чтобы проголосовать за знакомого в онлайн-конкурсе.

Открыто угрожают и манипулируют

Некоторые преступники предпочитают действовать более грубо и прямолинейно — шантажируют, манипулируют, угрожают. Например, могут написать, что родителям или кому-то из друзей угрожает опасность, и нужно срочно прислать деньги или данные банковских карт.

Часто киберворы, завоевав доверие ребенка, вытягивают из него личную информацию или фото, а потом шантажируют, угрожая разослать компрометирующие данные его друзьям и родственникам.

Как родители могут оградить ребенка от мошенников

Вот несколько советов, что можно сделать, чтобы оградить ребенка от влияния интернет-мошенников.

Выстраивайте доверительные отношения с ребенком

Для того, чтобы действительно быть в курсе происходящего в жизни ребенка, — с кем общается, чем увлекается, на что тратит свои карманные деньги — нужно планомерно выстраивать с ним доверительные отношения. Важно, чтобы он сам рассказывал родителям о новых знакомствах и событиях в своей жизни. При этом не стоит нарушать его личное интернет-пространство, мониторя все переписки и устанавливая жесткие ограничения. Это приведет к обратному результату — ребенок закроется, и рассчитывать на его доверие в этом случае будет уже бесполезно.

Расскажите ребенку об основных схемах обмана

Первым делом нужно объяснить ребенку, как распознать мошенника, какие уловки используют преступники, чтобы втереться в доверие, и почему ко всем знакомствам в интернет-пространстве нужно относиться критически. Следует рассказать про опасность перехода по ссылкам, про вирусы и коды подтверждения, про основы финансовой и компьютерной грамотности. Еще следует рассказать, что делать, если ребенок заподозрил преступника в своем новом знакомом — нужно сразу же сообщить об этом родителям.

Защитите свою банковскую карту и карту ребенка

Карты для детей до 14 лет привязывают ко счету одного из родителей. В этом случае стоит настроить на своем смартфоне уведомления о тратах ребенка. Если суммы увеличились или значительно выросла частота трат, имеет смысл аккуратно поинтересоваться у ребенка, в чем причина. Можно также ограничить сумму, доступную ребенку для ежедневных трат.