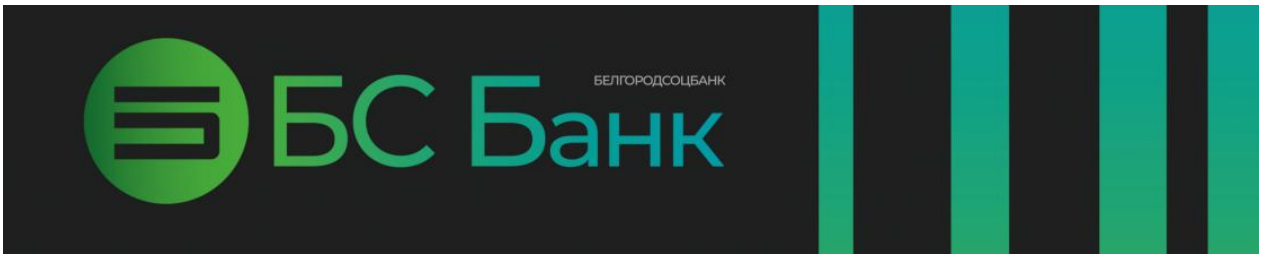

Как мошенники обманывают детей

Дети из-за небольшого жизненного опыта доверчивы, и если их не научить, как распознавать мошенников, последствия могут быть катастрофическими для семейного бюджета. Задача взрослых — объяснять, почему нельзя разговаривать с незнакомыми людьми по телефону, почему важно держать персональные данные втайне, не заводить знакомства в онлайн-играх, форумах, не совершать покупки в Интернете без разрешения родителей.

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.

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

1. Фишинговый сайт

Мошенники создают фишинговые сайты, где детям предлагают с большой скидкой купить игры и «бусты» к этим играм, либо приобрести модные наушники или другие гаджеты. Как и в настоящих интернет-магазинах, на фишинговых сайтах нужно вводить данные банковской карты для оплаты. Но после «покупки» деньги уйдут мошенникам.

Лайфхак: оформите ребенку собственную карту. По ней можно установить лимиты на операции. Например, можно поставить запрет на покупки в Интернете, а дневной лимит по карте — 500 рублей. Это поможет избежать списаний всех денег с карты.

Признаки фишингового сайта

— ошибки в адресной строке сайта (например, лишние символы или буквы). Лучше всего сохранять адреса банков, госорганов, любимых интернет-магазинов в закладках;
— небезопасное соединение. Перед его адресом сайта обязательно должно стоять "https" и значок закрытого замка. Буква s и закрытый замок означают, что соединение защищено:

когда вы вводите на сайте данные, они автоматически шифруются и их не могут перехватить;
— непрофессиональный дизайн. В большинстве случаев мошенники не мудрят с дизайном и структурой сайта. Небрежная верстка, орфографические ошибки, неработающие разделы и ссылки, видоизмененные логотипы;
— отсутствие контактной информации. На таких сайтах нет адресов офисов, складов;
— много запросов на ввод личных и финансовых данных. Главная цель фишинговых

сайтов — собрать конфиденциальные данные.

Как защитить себя

— не переходите по ссылкам из сообщений от незнакомых адресатов. Тщательно проверяйте адрес, с которого пришло письмо. Если он даже чуть-чуть отличается от официального адреса магазина, банка, авиакомпании и другой организации, такое письмо не стоит открывать
— платите безопасно. После ввода реквизитов карты сайт магазина должен направить вас на отдельную страницу для подтверждения платежа. Это страница - платежный шлюз. Он соединяет владельца карты с банком при проведении платежа. Там вы вводите код из СМС, которую присылает банк для подтверждения платежа.
— заведите отдельную карту для интернет-платежей, чтобы держать на ней только такие суммы, которые вам нужны в ближайшее время.

2. Онлайн-работа

Дети хотят заработать собственные деньги и ищут разные варианты. В сети ребенок может наткнуться на очень привлекательные предложения удаленной работы. Например, писать отзывы на товары. Для получения выплаты нужно оплатить небольшую комиссию, а для этого ввести данные карты, которые, как и в предыдущей схеме, уходят мошенникам.

3. Розыгрыш призов

Злоумышленники делают рассылку от имени известных людей (знаменитостей, блогеров) о выигрыше приза. Ребенку нужно оплатить комиссию за доставку. Итог: вместо приза - списание денег на счет мошенников.

4. Фейковый аккаунт друга

Взламывают аккаунты в соцсетях и мессенджерах, пишут контактам с просьбой занять деньги. Суммы могут быть маленькие, но знайте, что даже 500 рублей для мошенников — хороший улов.

5. Обналичить Пушкинскую карту

Согласно условиям программы, картой можно оплачивать билеты на культурные мероприятия: театры, музеи, кинотеатры, выставки. Но мошенники уверяют, что обходными путями с карты можно выводить деньги, и предлагают купить «руководство» за символические деньги. Естественно, никакой инструкции ребенок не получает.

6. Дропперские счета

Попадаясь под влияние мошенников, можно не только потерять деньги, но и самому «случайно» стать преступником или дроппером — человеком, который через свой счет проводит операции с украденными деньгами. Мошенники предлагают подросткам оформлять банковские карты, на которые аферисты переводят деньги. Эти деньги нужно обналичить или перевести другим мошенникам, то есть ребенок становится посредником,

который доставляет украденные деньги от мошенника к мошеннику. Естественно, за вознаграждение. За такую «помощь» подростку грозит уголовная ответственность.

7. Ответы по ЕГЭ

Легкая добыча для мошенников в конце учебного года — переживающие за баллы на ЕГЭ выпускники. Именно на их страхе получить низкий балл на экзаменах аферисты и зарабатывают. В соцсетях появляются группы, в которых можно купить ответы по выпускным экзаменам. После оплаты школьнику присылают ответы на прошлогодние вопросы, и чаще всего, мошенники сразу исчезают.

8. Новые «друзья» в онлайн-играх или форумах

Мошенники втираются в доверие и заводят онлайн-дружбу с подростками, чтобы в дальнейшем получить от них информацию, например, банковские реквизиты карт родителей, номера телефонов, фото паспортов родителей и другие данные. Благодаря этой информации аферисты могут украсть деньги с карты, оформить кредит и другими способами незаконно обогатиться.

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.

Подключите Родительский контроль

Включите функцию Родительского контроля в сервисах, которыми пользуется ребенок. Отключите отображение рекламы на компьютере, чтобы ребенку не попадались вредные баннеры. Функция Родительского контроля не гарантирует полной безопасности, а служит скорее дополнительной мерой защиты.

8 800 707-39-39/bsbank.ru