**Противодействие мошенничеству**

Соблюдайте эти правила, чтобы не стать жертвой мошенников

**1. Не спешите отправлять деньги**
Если с вами связались по телефону, электронной почте или в сообщениях и просят срочно перевести деньги, не торопитесь. Сначала проверьте информацию. Свяжитесь с близкими или самостоятельно позвоните в нужную организацию и проверьте сведения.

**2. Не сообщайте данные карты**
Если вам звонят и просят назвать данные карты или подтвердить действия, которые вы не совершали (денежный перевод, оформление кредита, смену номера телефона, привязанного к карте и т. д.), сразу положите трубку. Настоящие сотрудники банка/службы безопасности ни по телефону, ни в письмах такую информацию не запрашивают.

**3. Проверяйте сайты**
Не переходите по ссылкам из SMS. Не вводите данные карты на подозрительных сайтах. Поддельные сайты бывают очень похожи на официальные, но используются мошенниками для кражи данных карт. Если вы хотите совершить покупку, убедитесь, что это официальный интернет-магазин.

**4. Сохраняйте платёжные документы**
Не выкидывайте документы, которые вы получили после отправки денежного перевода: квитанции, чеки и т. д. Они понадобятся, если вы решите обратиться в правоохранительные органы по факту мошенничества.

**5. Никогда не сообщайте никому:**
– паспортные данные (а также данные любых других документов), кодовое слово, логин и пароль для доступа в личный кабинет интернет-банка, коды из СМС, 16-значный номер карты и срок ее действия, ПИН-код, CVC/CVV/ СVP-код (защитный код из 3 цифр, который написан на обороте карты).
Если вам звонят и просят назвать данные карты или подтвердить действия, которые вы не совершали (денежный перевод, оформление кредита, смену номера телефона, привязанного к карте и т.д.) СРАЗУ ПОЛОЖИТЕ ТРУБКУ!!!

Противодействие мошенническим практикам

Информация с сайта Банка России - https://cbr.ru/information\_security/pmp/

Для хищения денег у граждан злоумышленники используют все более изощренные сценарии. В результате тысячи людей страдают от их действий, теряют деньги, которые в некоторых случаях копили годами. Знания о том, как противодействовать мошенникам, помогут в нужную минуту принять правильное решение. В этом разделе Банк России представляет распространенные мошеннические схемы, которые будут регулярно дополняться, а также рекомендации по защите от них.

Мошенники специально оказывают психологическое воздействие на человека таким образом, чтобы он раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Они могут неоднократно звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Злоумышленники всячески пытаются вывести человека из спокойного состояния и отключить у него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Такое психологическое воздействие представляет собой методы социальной инженерии.

Банк России ведет работу по выявлению мошеннических схем, информирует о них правоохранительные органы, которые занимаются расследованием хищений денежных средств.

**Как не стать жертвой мошенников: общие рекомендации**

Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

Если с неизвестного номера звонит якобы сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Самостоятельно позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

Не совершайте каких-либо действий по счету, если вам звонят с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет Центробанка, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

По возможности установите антивирус на все устройства и обновляйте его.

Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Если вы стали жертвой мошенников:

**Шаг № 1**
Немедленно заблокируйте карту с помощью мобильного приложения или личного кабинета на сайте банка. Заблокировать ее также можно через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.

**Шаг № 2**
В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение полиции.

**ПОМНИТЕ:** если вы самостоятельно перевели деньги мошенникам или предоставили им банковские данные, то банк не обязан возвращать похищенную сумму.

Количество IT-преступлений в отношении пользователей интернет-магазинов, маркетплейсов и сайтов объявлений ежегодно растет. Вместе с этим растут число пострадавших и заработки мошенников. К сожалению, эффективных инструментов борьбы с интернет-злоумышленниками пока не изобрели. Поэтому, чтобы не стать их жертвой, и покупателям, и магазинам следует знать основные мошеннические схемы и понимать, как не попасться на них.

Самые распространенные схемы

Если не рассматривать уже ставшие привычными звонки по телефону от «представителей банков», которые донимают и наших клиентов, то самой распространенной схемой кибермошенничества можно назвать создание фишинговых сайтов. Она заключается в том, что мошенники имитируют доменные имена известных брендов. Покупатель думает, что делает заказ в проверенном и известном интернет-магазине.

Мошенники заманивают покупателей фальшивыми объявлениями, обычно с заниженной ценой. После этого они переводят общение с клиентом в сторонние мессенджеры якобы «для удобства» или под каким-то другим предлогом. Уже там они отправляют покупателю ссылку на фальшивый сайт, который внешне напоминает сайт известного бренда. Клиент проводит там оплату, вводит данные своей карты и попадает на деньги.

Любое громкое событие может обернуться шквалом регистраций фишинговых сайтов, которые отрабатывают резонансный инфоповод. Например, в июне сотрудники СберБанка бесплатно накормили пиццей промоутеров Альфа-Банка, которые раздавали листовки у входа в офис конкурента. После этого мошенники стали использовать пиццу в качестве приманки. Создавали фейковые сайты, на которых «разыгрывали» от имени банков бесплатную пиццу. Они предлагали своим жертвам для получения «приза» ввести номер банковской карты и телефона, а затем дважды передать код из СМС. Этих данных было достаточно для входа в личный кабинет онлайн-банка.

В сентябре мошенники провели самую массированную за весь год атаку на клиентов российских интернет-магазинов и маркетплейсов, свидетельствуют данные компании в области кибербезопасности Infosecurity. В Интернете появилось несколько десятков фишинговых сайтов, копирующих как минимум 15 крупных торговых брендов, таких как «Ашан», «О'Кей», Wildberries, DNS, «Связной», «Ситилинк», «Дочки-сыночки», Tele2 и другие. Таких сайтов появляется по три — пять в день.

Вторая часто встречающаяся схема — поддельные накладные. Мошенники отправляют покупателю скан или фотографию поддельной накладной с предложением перевести оплату за товар. При покупке товаров в Интернете многие вносят предоплату или полностью оплачивают товар. Но если вы попались на мошенников, можно получить совершенно не то, что купили, или вообще ничего не получить.

Как защититься покупателю интернет-магазина

Обращайте внимание на цену товара на сайте, она не должна быть слишком низкой. Однажды мой знакомый потерял почти 60 тыс. рублей, когда пытался купить игровую консоль последнего поколения по цене более чем втрое ниже среднерыночной.
Общайтесь с продавцом только на сайте системы, где выставлен товар, не переходите по ссылкам, которые отправляют в сторонних мессенджерах, используйте для оплаты товаров и услуг только официальные сайты компаний.
Следите за поведением продавца. Попытки ускорить момент оплаты могут быть подозрительными.
Не переходите по неизвестным и сомнительным ссылкам, которые пересылают для оплаты услуг доставки.
Внимательно проверяйте адреса сайтов, на которых вводите персональную информацию и данные карт. Адреса фальшивых доменов могут отличаться даже на одну букву.
Отслеживайте путь товара только в личном кабинете интернет-магазина.
Внимательно изучайте копии документов. Номера накладных смотрите на сайте транспортной компании.
Не выполняйте операции с картами, если приходит СМС-уведомление или поступает звонок от якобы работников банка с извещением, что банковская карта заблокирована, произошло списание денег или необходимо подключить какую-либо услугу.
Никогда не переводите деньги на неизвестные расчетные счета! И не выполняйте инструкции по телефону от неизвестных лиц.
Если возникают сомнения по любому из перечисленных пунктов, связывайтесь с официальным контакт-центром компании для проверки предоставленной информации.
Как защититься продавцу интернет-магазина

Следует использовать штрихкоды или собственную маркировку. Стоит также добавить номер товара в квитанцию заказа. Тогда при возврате курьер, почтовая служба и сотрудник магазина смогут проверить подлинность товара.
Если вы предлагаете услугу примерки и возврат, научите курьера отличать настоящую вещь от подделки.
Перезванивайте покупателям, чтобы подтвердить заказ по телефону, уточняйте, правильный ли размер и цвет выбрал клиент.
Продумайте политику возврата и расскажите, при каких условиях вы примете товар обратно. Укажите сроки возврата, перечислите документы для подтверждения покупки, просите заполнить бланк возврата. В нем покупатель к тому же должен будет указать свои данные.
Ознакомьтесь с политикой защиты клиентов компании

К сожалению, эффективных инструментов борьбы с фишингом пока нет. Можно лишь сократить время существования сайтов, сообщая о новых случаях и схемах мошенничества и отслеживая их появление в Интернете.

Компании регулярно мониторят фейковые сайты. В этом им помогают современные аналитические сервисы, которые по запросу находят всё, что связано с названием бренда, а также при необходимости делают поиск по ключевым словам.

Бренды также отслеживают обращения в соцсетях, так как под постами обычно большой поток комментариев. Но менеджеры могут просто не успеть отсмотреть и проверить их все. Из-за этого появляется риск, что мошенники будут «красть» клиентов. При этом сервисы могут подгружать упоминания, чтобы на них можно было моментально отвечать и блокировать пользователей, которые притворяются сотрудниками бренда.

Службы доставки, в частности, борются с фейковыми фишинговыми сайтами с помощью специализированных подрядчиков. Компании также реструктурируют свои процессы внутри систем, чтобы усложнить мошенникам возможность противоправных действий.

Компании помогают своим клиентам информационно, они регулярно выкладывают в соцсетях тексты о мошенничествах и о том, как их распознать.
Подробнее на сайте Banki.ru https://www.banki.ru/news/columnists/?id=10954005