Полиция призывает граждан быть бдительными при общении по телефону с незнакомцами, представляющимися сотрудниками банков

МВД по Республике Марий Эл призывает граждан остерегаться подозрительных звонков от лиц, в телефонном разговоре называющих себя сотрудниками банков. Как правило, ими представляются мошенники. Диалог с такими злоумышленниками может закончится потерей крупной суммы денег и большим долгом в виде кредита.

Как действуют мошенники: онзвонят своей жертве и сообщают, что с банковской карты клиента зафиксирован подозрительный перевод денежных средств и предлагают остановить транзакцию. При этом аферисты очень правдоподобно копируют манеру общения банковских работников, называют имя, отчество клиента банка, информацию о его картах и счетах, а также маскируют номера исходящих вызовов под московские номера телефонов и реально существующие номера банков и других организаций и ведомств. Далеелже-банкиры просят продиктовать коды из смс-сообщений, которые придут во время разговора. С помощью полученной информации они похищают денежные средства со счета банковской карты своей жертвы.

Во втором варианте злоумышленники просят гражданина самостоятельно перевести денежные средства с банковской карты на якобы безопасный счет.

Другая часть мошенников уговаривает клиента установить на свой телефон специальное приложение, которое, по их словам, защитит деньги пользователей от краж. Но на самом деле с помощью подобных приложений злоумышленники могут узнать пароль от онлайн-банка клиента.

Другой, не менее популярный среди аферистов способ получения персональных данных третьих лиц – это сообщение о том, что неизвестные пытаются оформить кредит на держателя карты. При этом мошенники в диалоге используют выдуманные термины, такие как «зеркальный кредит», «ответное кредитование», «резервный счет», «защищенная банковская ячейка» и так далее. Злоумышленники убеждают жертву подать онлайн-заявку на кредит, а затем перевести деньги на «безопасный счет». На самом деле это счет мошенников, с которого они тут же всё снимают. В итоге человек оформил кредит, который он должен выплатить банку, да еще и остался без заемных средств.

Полицейские акцентируют внимание граждан, что ни в коем случае не следует выполнять требований лжебанкиров. Вы можете быть уверены, что общаетесь с мошенниками, если под предлогом потери денежных средств вам предлагают совершить какие-либо действия с вашими картами. Например, просят перевести деньги на «резервные счета», срочно идти к банкомату и выполнить какие-то операции, оформить на себя кредиты или сообщить любые персональные данные и пароли из смс-сообщений банка. Настоящие сотрудники банков так не делают.

МВД по Республике Марий Эл предупреждает: мошенники используют технологию подмены телефонных номеров

Полиция предупреждает об участившихся фактах телефонного мошенничества, связанного с незаконным использованием подменных абонентских номеров. При этом номера телефонов, которые задействуются в криминальных схемах, могут быть закреплены как за банками, так и за различными подразделениями министерства.

Мошенничество происходит по следующей схеме. Гражданину звонит незнакомец, представляется сотрудником банка и сообщает, что злоумышленники пытаются оформить в банке онлайн-кредит на его имя. Якобы для того, чтобы предотвратить незаконные действия, человека убеждают в необходимости самостоятельно оформить онлайн-кредит на ту же сумму, обналичить поступившие на банковскую карту деньги и перечислить их на так называемый резервный счет для мгновенного погашения кредита.

Чтобы у потенциального потерпевшего не осталось сомнений, через несколько минут ему звонит соучастник преступной схемы, который представляется полицейским и рекомендует следовать инструкциям звонивших ранее представителей банка. При этом злоумышленники используют современную технологию подмены данных, которая позволяет имитировать звонок с номеров телефонов, указанных на официальном сайте МВД по Республике Марий Эл. Неизвестные даже предлагают гражданам сверить номер телефона входящего звонка с номером, указанным на сайте, и абоненты видят, что комбинации цифр на самом деле совпадают.

Сотрудники полиции призывают граждан быть бдительными и соблюдать простые правила. Первое из них – не совершать финансовых операций по инструкциям, полученным в ходе телефонных разговоров. Если вам звонят люди и представляются сотрудниками банка или полиции – перезванивайте по официальным номерам финансовых организаций и правоохранительных органов. Никому не сообщайте полные реквизиты банковских карт, PIN-код, CVC/CVV-коды и одноразовые пароли для подтверждения операций. Если в отношении вас или ваших близких совершены противоправные деяния, немедленно сообщите о случившемся в полицию по телефону 102.

Сотрудники полиции призывают жителей обратить пристальное внимание на осуществление безопасных сделок при купли-продажи товаров на сайтах бесплатных объявлений и в социальных сетях

Интернет-технологии все больше и больше позволяют активным пользователям Интернета расширять свои возможности. Не выходя из дома, вы свободно можете осуществлять общение, приобрести нужные или продать ненужные вам вещи, невзирая на время и географию. Однако такое удобство привлекает не только продавцов или покупателей, но и мошенников.

Избежать обмана при покупке онлайн легко, поскольку большинство распространенных мошеннических схем обязано своим успехом не сложным техническим уловкам, а банальной доверчивости и невнимательности пользователей.

Чтобы обеспечить себе безопасность, достаточно соблюдать несколько простых правил: никогда не вносить предоплату за товар, не переходить по ссылкам на внешние сайты, если их прислали другие пользователи, не диктовать и не высылать никому личные данные - CVV/CVC-код банковской карты, коды из SMS от банка или других сервисов.

Три самые распространенные схемы обмана:

1. Подмена страницы платежа (фишинг). Вы хотите что-то приобрести или продать на сайте объявлений, а другой пользователь предлагает провести оплату онлайн или оформить доставку. Вам через интернет-мессенджер приходит от него ссылка, якобы ведущая на страницу оформления заказа. При этом собеседник может утверждать, что на самом сайте объявлений (через который и нужно производить все операции) не работают кнопки подтверждения заказа, доставки или оплаты.

Это всегда ложь, единственная цель которой - увести вас с реального сайта на подменный и получить доступ к вашим платежным данным. Мошенники имитируют страницы известных ресурсов. Даже адрес поддельной мошеннической ссылки может быть очень похож на настоящий. Однако отличия все-таки будут. Например, если вы приобретаете или продаете что-то на "Авито", то и ссылка может вести только на сайт www.avito.ru. Если адрес выглядит чуть иначе (avitopayments.ru, avito-dostavka.ru или avitto.ru) - это точно мошенничество.

Крупные сайты объявлений блокируют возможность присылать активные ссылки на внешние ресурсы во встроенных чатах на своей платформе и предупреждают пользователей уведомлениями, что переходить куда-либо может быть небезопасно. Именно поэтому мошенники часто настаивают на том, чтобы перевести общение в WhatsApp или другой мессенджер.

Но честному продавцу или покупателю просто незачем присылать вам ссылку, так как все необходимое для оформления заказа и доставки внутри крупного сайта объявлений уже есть. Лжепродавец может сам отключить функцию доставки для своих объявлений, а потом врать, что на сайте сбой и поэтому доставка якобы недоступна. Верить такому и переходить по каким-либо ссылкам нельзя.

2. Выманивание платежных данных. Вы покупаете или продаете что-то на сайте объявлений. С вами на связь выходит другой пользователь, вроде бы готовый на сделку, и для ее оформления просит вас продиктовать реквизиты банковской карты и коды из SMS от банка.

Аргументировать необходимость предоставить эти данные мошенник будет самыми разными способами. Например, он может уверять, что согласно правилам безопасности банка это необходимо для верификации

вашей карты, или говорить, что без этих данных невозможно оформить доставку.

Предоставлять такие коды кому бы то ни было ни в коем случае нельзя. Ни покупателям, ни продавцам они не могут понадобиться никогда. Эти данные могут использоваться посторонними людьми только для получения доступа к вашему онлайн-банку с выводом денег или совершения с вашей карты покупок в интернете.

3. Требование предоплаты. На продажу выставляется востребованный товар - возможно, редкий или привлекательный по цене. Когда покупатель проявляет к нему интерес, продавец начинает торопить с решением и просит перевести предоплату - иногда полную, но чаще частичную. Мошенник просит зачислить деньги на его счет в интернет-банке или опять-таки пройдя по поддельной ссылке на страницу оплаты. Получив деньги, такой продавец пропадает из поля зрения и добавляет вас в черный список.

Обезопасить себя просто: передавайте деньги лично при получении товара, а если это невозможно или неудобно, пользуйтесь встроенными функциями безопасной сделки или доставки с постоплатой, которые есть на многих популярных сайтах объявлений. Такие функции замораживают на карте покупателя сумму, равную цене товара на сайте. Продавец получит деньги только после того, как покупатель подтвердит в системе, что он забрал товар и убедился, что с ним все в порядке. Если при доставке в пункте выдачи оказывается, что с товаром что-то не так, можно отказаться от покупки, и деньги автоматически вернутся на карту.

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам, значительно ниже среднерыночных.

Злоумышленники создают сайт интернет-магазина и запускают рекламный трафик, с целью появления в топе поисковых систем. Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина, требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывозе не предусмотрен.

После перевода денежных средств, мошенники перестают выходить на связь с покупателями, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

- неоправданно низкая цена на товар;

- электронная почта или мессенджеры в качестве способов коммуникации;

- оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;

- обязательная предоплата зачастую более половины стоимости товара;

- отсутствие физического адреса расположения магазина или его сомнительный интернет-адрес.

Если же решили заказать товар, то требуйте от продавца, чтобы посылку оформлял с описью вложения. Если посылка имеет опись вложения,

то она вскрывается до оплаты, содержимое проверяется согласно перечню, подписывается акт, посылка оплачивается, и адресат ее забирает.

Полиция предупреждает о мошеннических схемах при использовании онлайн-бирж

По мере расширения сферы применения Интернета растет и число людей, использующих эту информационную среду для финансовых операций. Одновременно с этим, возможности Интернета делают его очень удобным инструментом для организаторов мошеннических схем. Обещание инвесторам высокого дохода, но шанс получить его есть только у организаторов-преступников.

Как действуют жулики? Поступает звонок на телефон. Звонящий представляется сотрудником брокерской компании. Рассказывает о низких ставках по депозитам и предлагает значительно приумножить ваши вложения. Вам предлагают якобы абсолютно безопасную схему инвестирования на финансовых рынках. Для этого всего-то нужно открыть счет у брокера и пополнить его на какую-то сумму. Брокерская компания добавить к вашим деньгам свои и вы начнете зарабатывать. И поскольку мошенники умеют убеждать, человек соглашается и переводит первоначальный взнос. Конечно, в первые дни, может быть даже недели у клиента такой брокерской компании на счете образуется прибыль. Но потом под различными предлогами аферисты начинают выманивать деньги у клиента. Например, компания, в акции которой инвестировали деньги, показала убытки. И для возврата начальных вложений требуется внести на счет дополнительные деньги. Такая схема продолжается до тех пор, пока потерпевший не лишится всех своих денежных средств или не поймет, что его обманывают. Как правило, к этому моменту большинство попавших на удочку мошенников успевают расстаться со всеми своими накоплениями, а некоторые даже с деньгами, взятыми в кредит.

Как не стать жертвой мошенников? Брокеры для того, чтобы осуществлять свою деятельность на территории Российской Федерации, должны иметь лицензию на осуществление брокерской деятельности. Такие лицензии организациям выдает Центральный банк РФ. Поэтому первое, что вы должны сделать при выборе брокера, - проверить наличие у них лицензии. Сделать это можно на сайте Банка России. Если у компании, которая обещает вам огромные прибыли, нет лицензии Банка России – осторожно, это мошенники.

На что еще следует обратить внимание:

1. Навязчивые звонки в любое время суток. Помните: профессиональный и честный брокер никогда не станет навязывать свои услуги по телефону. Хорошего специалиста клиенты ищут сами.

2. Обещание брокером баснословной прибыли от вложенных денежных средств. Важно помнить, что ни один брокер не может гарантировать 100-процентное получение прибыли.
3. Отказ назвать адрес сайта брокерской компании. Отсутствие информации о ней в Интернете. Или на сайте компании нет сведений о собственнике компании, юридического адреса и контактных данных.
4. Брокер предлагает быстро открыть счет без проверки ваших документов и заверяет, что достаточно оформить личный кабинет на сайте.

Если вам поступил звонок с предложением об инвестировании, не пожалейте своего времени. Проверьте лицензию, обратите внимание на другие детали, указанные выше..Будьте бдительны, не дайте себя обмануть!