**Осторожно, появились новые схемы онлайн-мошенничества**

Поделиться:

Источник: Редакция МоиФинансы

Новые способы обмана появляются в условиях санкций и нестабильной экономической ситуации. Мошенники делают ставку на то, что люди растеряны и не успевают вникнуть в суть быстро меняющихся событий. Преступники смешивают реальные информационные поводы с выдумкой. Рассказываем, как распознать обман.

**Мошенническая схема №1. Отключение от SWIFT**

Самая распространенная схема последних дней — запугивание отключением банков от системы SWIFT (СВИФТ). Евросоюз уже отключил семь российских банков от этой платежной системы. Мошенники рассказывают потенциальным жертвам, что теперь они потеряют все свои сбережения. Но есть шанс спасти деньги. Для этого, по словам преступников, надо их перевести на специальный «безопасный счет». Это обман. «Средства всех клиентов на счетах в российских банках сохранены и всегда будут доступны. Отключение некоторых банков от SWIFT на это никак не повлияет», — говорится в сообщении Банка России, размещенном в его официальном Telegram-канале.

ЧТО делать? Не выполнять никаких действий со своими счетами по инструкции посторонних. Никаких особых защищенных счетов не существует. Если клиент банка выполнит указания мошенников, то его деньги уйдут на счет преступников.

Важно! SWIFT - это финансовый мессенджер, которым пользуются банки по всему миру. Его отключение создает неудобства для международной деятельности банков, но никак не влияет на операции внутри страны. SWIFT не связан со сбережениями людей.

**Мошенническая схема №2. Снять наличные.**

Перебои с наличными в банкоматах, дефицит валюты в отделениях банках, новости о запрете Евросоюзом продавать евро в Россию подняли волну афер. Телефонные мошенники под видом сотрудников банков и финансовых организаций стали предлагать обналичить деньги с карт, в том числе и валютных. Деньги аферисты предлагают вывести через «спецсчета» и криптобиржу. Если потенциальная жертва соглашается, в ход вступает уже обкатанная схема: деньги надо перевести на «специальный счет», для чего необходимы данные карт, включая CVV-код на обороте и код смс. Получив секретную информацию, мошенники обнуляют карточные счета.

Что делать? Прерывайте любые разговоры, связанные с данными вашей карты. Не проводите операции со своими счетами по телефонным просьбам третьих лиц, даже если они представляются «сотрудниками банка», в котором у вас есть карточный счет, даже если они правильно называют ваше имя, фамилию и паспортные данные. Настоящие сотрудники банка никогда не выспрашивают сведения и коды, связанные с картами клиентов. А при возникновении вопросов относительно снятия наличных с карты обратитесь в отделение банка или позвоните в банк по телефону, указанному на оборотной стороне карты или на официальном сайте банка.

**Мошенническая схема №3. Псевдоблаготворительность.**

В интернете появились десятки псевдоблаготворительных сайтов. С этих сайтов гражданам приходят сообщения на электронную почту и в мессенджеры. Сообщения содержат эмоциональные призывы о помощи и ссылки для перечисления денег.

Что делать? Переход по ссылкам от псевдоблаготворителей может обернуться не только потерей денег. Через эти сайты на ваш компьютер может попасть вирус, в том числе и для кражи паролей и личных данных. Сайт официальной благотворительной организации должен быть зарегистрирован в России. На нем должны быть доступны все учредительные и регистрационные документы. Если эти данные скрыты, иметь дело с такой организацией не нужно.

Чтобы оказать реальную помощь, сделайте это адресно и в неденежной форме. В муниципалитетах открыты штабы по сбору гуманитарной помощи для беженцев. Там есть списки того, что действительно необходимо оказавшимся в беде людям. Ищите адреса этих пунктов на сайтах региональных администраций.

**Мошенническая схема №4. Псевдоброкеры.**

Обвал фондового рынка в последние дни оказался особенно чувствителен для частных инвесторов, не имеющих опыта работы с активами в условиях высокой волатильности. Они пребывают в панике и пытаются спасти свои деньги. Такими настроениями пользуются мошенники. Они предлагают «поправить финансовое положение» и вложиться в растущие валюты, нефть, драгметаллы и фьючерсы на них. Также в ход идет криптовалюта, которая «будет расти при любых условиях». Под видом брокеров аферисты размещают в соцсетях рекламу о выгодных инвестициях. Для инвестиций необходимо оставить заявку по форме. Далее с инвестором связывается представитель брокера, который убеждает скачать специальную программу для работы на бирже и перевести «на брокерский счет деньги». После того как преступник видит, что у жертвы заканчиваются деньги, «брокерский счет» обнуляется, а сам «брокер» перестает выходить на связь.

Что делать? Прежде чем доверить свои средства неизвестному брокеру, проверьте, находится ли он в реестрах Банка России: оказывать услуги на российском финансовом рынке могут только компании, имеющие лицензию регулятора. Сделать это можно на сайте Банка России в разделе «Реестры». «Список брокеров».

Сравните доходность финансовых инструментов из рекламы брокера с доходностью этих инструментов у известных лицензионных брокеров. Если прибыль в разы больше - это повод сомневаться.

А также следите за новостной повесткой.

Высокая волатильность последних дней — не лучший момент для торговли на фондовом рынке. Риски для неопытных инвесторов слишком высоки.

В заключение

Быстро подстраиваясь под новостную повестку, мошенники ежедневно изобретают новые способы обмана. Некоторые из них могут оказаться невероятными. Так, «Мои финансы» сталкивались с предложениями вывезти родственников из-за границы, открыть счет в европейском банке, который якобы можно привязать к российскому карточному счету, предлагали даже купить антиквариат и драгоценные камни, потому что «рубль и валюта обесцениваются».

Для таких случаев есть несколько универсальных правил. Они помогут обезопасить ваши деньги в любой ситуации:

• Не слушайте предложения от незнакомых по телефону.

• Проверяйте любую информацию от незнакомых.

Не сообщайте по телефону конфиденциальную информацию: личные данные и данные своих счетов и карт.

• Не переходите по случайным ссылкам, присланным на почту и в мессенджер.