

Кошелёк

С появлением цифровых активов и возможности совершения банковских операций онлайн для преступников наступили золотые времена. Достаточно грамотно «развести» жертву, и она сама принесёт (точнее, переведёт) деньги «на блюдечке с голубой каёмочкой». О том, как защитить себя от телефонного мошенничества, подробно рассказал старший вице-президент Банка «КУБ» (АО) Александр Лазуткин.

– Поток мошеннических звонков клиентам не ослабевает, при этом преступники постоянно адаптируют свои схемы под текущую ситуацию, – объясняет Александр Анатольевич. – Ежедневно фиксируем по десять–двадцать попыток обмана клиентов. Но растёт и уровень защиты банковских операций. В работе банки используют антифрод-систему мониторинга и предотвращения списания средств злоумышленниками. При проведении операции программа анализирует данные устройства и IP-адрес, и, если определяет их как нетипичные, перевод блокируется. Кроме того, Банк России фиксирует реквизиты, на которые уже были переводы по мошенническим схемам. Антифрод проверяет получателя, и, если его реквизиты в чёрном списке, перевод также не будет осуществлён. Но такие системы не позволяют выявить абсолютно все преступные схемы: к сожалению, мы не можем повлиять на случаи, когда клиент самостоятельно передаёт свои реквизиты карты и коды подтверждения, поддавшись на уловки мошенников.

Психологическая атака

Для того чтобы ввести в заблуждение потенциальную жертву, мошенники активно используют современные технологии. Самая распространённая – подменные номера. С помощью специальных программ можно сделать так, что человек будет видеть на экране реальный номер организации. Кроме того, **злоумышленники применяют приёмы социальной инженерии и психологического манипулирования, вводя человека в состояние страха и паники, лишая его способности анализировать происходящее.** Чтобы вывести жертву из равновесия, ей постоянно звонят с разных номеров, торопят, говорят, что если не выполнить требования, человек лишится сбережений прямо сейчас. Для того чтобы ещё больше запугать и лишить возможности проверить информацию, мошенники утверждают, что доступ получил кто-то из сотрудников кредитной организации, а потому звонить в отделение банка нельзя ни в коем случае. Более того, если вы положите трубку, деньги с вашего счёта сразу спишут. Запрещают общаться кому-либо о звонке, угрожают, что за «нарушение тайны следствия» последует наказание, оперируя номерами статей из Уголовного кодекса. К сожалению, очень часто на уловки мошенников попадают пенсионеры. Пожилые люди плохо разбираются в современных устройствах и привыкли доверять госструктурам.

Схемы злоумышленников

Чаше всего мошенники представляют себя специалистами службы безопасности банка или сотрудниками правоохранительных органов: полиции, ФСБ, прокуратуры.

«Вас беспокоит служба безопасности...»

Сколько существуют деньги – столько существуют и нечестные люди, пытающиеся завладеть чужими сбережениями



ры, следственного комитета, и сообщают о том, что кто-то хочет похитить ваши деньги. Например, по нотариальной доверенности пытаются снять денежные средства со счёта или оформить на вас кредит. Дальше мошенники сообщают: для того чтобы это предотвратить, нужно срочно снять средства с карты или оформить «встречный» кредит, а деньги перевести на некий «безопасный счёт». **Хотя если подумать логически – если снять наличные, они будут у вас в полной безопасности, на руках, зачем их ещё куда-то переводить?**

– Помните: такого понятия, как «безопасный счёт», не существует в принципе, нет и никакого единого счёта в Банке России, – подчеркнул Александр Лазуткин. – Центральный банк не работает с физическими лицами. Если вы услышали словосочетание «безопасный счёт» – значит с вами общаются преступники. И если звонящий представляется сотрудником ведомственных структур и хочет решить вашу проблему по телефону – это тоже мошенник. Сотрудники правоохранительных органов никогда не ведут расследования по телефону, они присылают повестку и приглашают на личный приём.

При «обработке» жертвы мошенники придумывают всё новые уловки. Например, в последнее время широкое распространение получила легенда о том, что со счёта хотят перевести деньги в поддержку ВСУ, а это преступление, отвечать за которое придётся

вам. Также появляются случаи, когда мошенники сообщают, что родственник, находящийся на специальной военной операции, попал в беду, и срочно нужны деньги для решения проблемы.

Ещё один вариант – вам звонит «менеджер» банка и просит сообщить номер банковской карты и CVV-код. Причинами могут служить якобы сбой программного обеспечения, попытка проведения подозрительной транзакции, восстановление счёта, возврат денег или заполнение протокола безопасности. Мошенник убеждает, чтобы восстановить информацию или разблокировать карту, вы должны продиктовать её данные: номер, срок действия и трёхзначный CVV-код – этих данных достаточно, чтобы списать деньги с вашего счёта.

Иногда перед тем, как совершить звонок, с помощью подменного номера вам могут прислать смс якобы из банка о попытке списать с вашей карты денежные средства, или о покупке, которую вы не совершали, где будет указано: «Если вы не совершали операцию, обратитесь в финансовую службу банка по такому-то номеру телефона». Если перезвонить по этому номеру, ответят мошенники.

Или же звонящий представляется сотрудником соцзащиты или пенсионного фонда и рассказывает о положенной вам выплате. Вот только для получения выплат необходимы данные карт и коды из смс. В этом случае сразу можете класть трубку: государственные

выплаты просто так никому не предоставляют, для их получения необходимо ваше заявление и целый пакет документов.

Также сюда можно отнести рассылки со взломанных страниц по спискам друзей в социальных сетях с просьбой перевести денежные средства на карту, мошенничества на сайтах с объявлениями, рассылки сообщений со ссылками на фишинговые (поддельные) сайты, копирующие страницы реальных интернет-магазинов, сервисов по продаже билетов.

Как вычислить мошенников

Просто запомните: если во время разговора у вас пытаются узнать данные карты, коды из смс или пароли, а также выполнить какие-то транзакции или снять деньги со счёта – это мошенники. Как только вы услышите, что нужно сообщить данные вашей банковской карты (номер, CVC-код, код из смс) – сразу кладите трубку. Банки никогда не запрашивают у клиентов такую информацию!

Если вы получили тревожный звонок от «сотрудника банка» или «прокуратуры», не выполняйте никаких инструкций. Прервите разговор, наберите ручную официальный номер банка, который можно найти на обороте карты или на сайте, и уточните информацию. Не нужно верить утверждениям, что нельзя вешать трубку или сообщать кому-то о факте звонка. Это стандартные уловки, цель которых – не дать прийти в себя.

– Сотрудники Банка «Куб» никогда не звонят клиентам с личных сотовых номеров, только с официальных номеров банка (так называемых «городских», первые цифры номера +73519), – объяснил Александр Лазуткин. – Если вам позвонили из банка, правоохранительных органов или просто незнакомые люди по телефону или через мессенджеры и просят совершить какие-то операции по вашей карте или счёту – кладите трубку. Достаточно сообщить: «Мне сейчас неудобно разговаривать, я вам перезвоню». После этого вручную наберите официальный номер банка или ведомства, по записанному у вас в телефонной книге номеру знакомому, которому срочно понадобились деньги, и выясните, что произошло. В 99,9 процента случаев окажется, что вас хотели обмануть. Даже если это реальный звонок из банка – положить трубку нормально, человек может быть занят. Если звонок был официальным, вас свяжут со специалистом, чтобы решить все вопросы.

Не перезванивайте на незнакомые номера, в том числе и номера из смс-сообщений, не переходите по отправленным ссылкам. Если в сообщении говорится о попытке снятия средств или блокировке карты, зайдите в личный кабинет мобильного банка и проверьте баланс. Если была попытка списания, она обязательно отразится в истории операций.

Помните, что трёхзначный код с обратной стороны карты, код 3-D Secure (при покупках в Интернете), пароль из СМС (для входа в интернет-банк/ для подтверждения операции), PIN-код – всё это ваши конфиденциальные данные, которые никому нельзя сообщать!

Что делать, если вас обманули

– Если клиент собственноручно перевёл деньги мошенникам, вернуть денежные средства достаточно сложно, – уточнил Александр Лазуткин. – Здесь наша рекомендация – обращаться в правоохранительные органы. Помогут следствию сохранённые переписки с мошенниками, номера исходящих звонков, скриншоты экрана телефона. Также в любом случае, даже если вы распознали мошенников и сохранили средства, обратитесь в банк. При этом постарайтесь зафиксировать номер телефона, с которого поступил звонок, – номера телефонов фиксируются в единой базе и используются всеми банками при работе с антифрод-системами.

Финансовая грамотность – залог безопасности

– С совершенствованием схем противостоять мошенникам сложно, но благодаря постоянной работе с клиентами, реализации большого количества программ по защите финансовых операций, жертв преступных схем становится всё меньше, – отметил Александр Лазуткин. – Всё чаще клиенты обращаются с тем, что их пытались обмануть, но они правильно отреагировали: просто прекратили общение со злоумышленниками и связались со специалистами банка. Мы рады видеть результаты проделанной работы в цифрах: с начала года нам удалось предотвратить мошеннические операции на сумму более семи миллионов рублей. Это и попытки оформить кредит, и попытки досрочного снятия денежных средств с вкладов с последующим переводом на счета мошенников.

Мария Митлина

