Аферисты от имени банков списывают у владельцев карт миллионы

Издание: РИА НОВОСТИ, август 2019 г.
Спикер: Виталий Малкин, директор по развитию

«Вас беспокоят из службы безопасности банка. По вашей карте зафиксирована попытка перевода денежных средств в Сингапур…» С этой фразы может начинаться разговор сотрудника финансовой организации с клиентом. А может — мошенника с потенциальной жертвой. На сегодняшний день звонок от «представителя банка» — самая распространенная схема, которой пользуются аферисты, чтобы получить доступ к чужим кредитным и дебетовым картам. Для убедительности преступники могут сообщить ваш остаток на счете, банкомат, в котором вы в последний раз снимали деньги. И вы им верите.

На днях телефонные мошенники установили своеобразный антирекорд — с карты москвича по такой схеме они сняли 3,5 миллиона рублей. Как не стать жертвой аферы — в материале РИА Новости.

«Украли 140 тысяч рублей»

Две недели назад актрисе театра и кино Александре Верхошанской позвонили «из службы безопасности банка ВТБ». Точнее, девушка представилась сотрудницей этой финансовой организации.

Роль оператора call-центра собеседница играла настолько хорошо, что даже Александра, привыкшая перевоплощаться на сцене, не заметила подвоха. Обратились по имени-отчеству. На экране мобильного высветился номер банка.

— «Оператор» спросила, осуществляла ли я несколько минут назад перевод в Самару. Причем назвала сумму, которую накануне мне перечислили из театра в качестве зарплаты. Я удивилась, ведь в тот день никаких операций с картой не проводила. Тогда девушка заявила, что доступ к моему счету, видимо, получили мошенники. И прямо сейчас они пытаются украсть деньги. «Мы можем отменить операцию, но для этого вы должны озвучить код, который придет вам в СМС», — обнадежила Александру собеседница.

Саша хотела положить трубку, перезвонить в банк самостоятельно. Но «оператор» все время торопила, убеждала, что деньги в течение нескольких минут уйдут злоумышленникам. Надо действовать быстро. В итоге Александра дважды назвала коды из СМС.

— Я не самый доверчивый человек. Но то, что звонившая обратилась ко мне по имени-отчеству, озвучила остаток на моей карте, меня подкупило. Очнулась я, только когда связь оборвалась. Тут же перезвонила в банк и узнала, что у меня украли 140 тысяч рублей. Причем сто сняли с кредитного счета.

Александра сразу же написала заявление в полицию. Там пообещали завести дело, перезвонить. Но на связь до сих пор никто не вышел. В банке отменить транзакцию также отказались, сославшись на то, что код для проведения операции пострадавшая назвала аферистам сама. «Друзья, работающие в банковской сфере, сказали, что мне еще повезло. Мол, некоторые таким

образом теряли деньги, которые выручили, продав квартиру или машину», — успокаивает себя Александра.

Звонок из «службы безопасности банка» на сегодняшний день — одна из самых распространенных мошеннических схем. Работает безотказно: мало кто успевает сориентироваться, когда тебя уверяют, что деньги вот-вот уйдут. К тому же аферисты прекрасно мимикрируют под сотрудников службы безопасности. Они знают не только паспортные данные владельцев карт, но и остаток на счете, могут назвать, в каком банкомате вы в последний раз снимали деньги.

Многие пострадавшие вспоминают: на заднем плане они даже слышали звуки call-центра, просьбы «оставаться на линии» и «оценить работу оператора».

Евгению Кротову (фамилия изменена), IT-специалисту из Москвы, позвонили в самое неудобное время, утром, когда нужно было выбегать на работу. Он уверен: если бы накануне не прочитал об этой схеме развода в соцсетях, точно бы попался. А так записал беседу на диктофон:

— Здравствуйте, Евгений Евгеньевич. Вас беспокоит отдел финансового мониторинга Сбербанка России, младший специалист Александр, — подставной оператор говорит казенными фразами, голос уставший. — Семь минут назад у нас был зафиксирован вход в ваш аккаунт Сбербанк-онлайн на территории Сочи. Подскажите, данный вход выполняете вы?

— Нет, — отвечает Евгений.

— Также после входа фиксируется попытка перевода денежных средств на сумму две тысячи рублей на электронный киви-кошелек. Имя получателя — Анатолий Бережин. Данный перевод подтверждать или отменять?

— Отменяйте, я переводов не делал, — продолжает подыгрывать Евгений.

— Фиксирую ваш ответ. Проинформируйте меня, вы карту нашего банка теряли?

— Нет.

— Третьим лицам ее передавали?

— Нет.

— Интернет-покупки часто совершаете по картам нашего банка?

— Нет, не часто, — Евгений с трудом подавляет смех. Но «оператор» не сдается.

— Информацию я зафиксировал. Сейчас мне нужно вас идентифицировать как клиента нашего банка, чтобы отменить данную операцию о списании. Для этого предоставьте либо номер вашего договора, либо номер вашей карты — как вам будет удобнее.

— Нет, такие данные я по телефону не предоставляю.

— Смотрите, если мы сейчас не идентифицируем вас, мы не сможем отменить данный перевод, и в течение трех минут у вас спишут две тысячи рублей. Вы это понимаете?

— Да, да, пусть списывают… — Евгений кладет трубку.

«Пройдите биометрическую идентификацию по телефону»

Это классический сценарий развода. Но есть и другие. Например, маме Андрея Громова аферисты представились «сотрудниками правительства Москвы». Обратились по имени-отчеству, обрадовали, что в качестве компенсации ей причитаются 13 тысяч рублей. Пенсионерка так опешила, что даже не запомнила за что. Далее мошенники попросили продиктовать номер карты, а также код с обратной стороны, чтобы перевести деньги.

— Причем у преступников были не только паспортные данные мамы, но и мои. Примерно в середине разговора у нее возникли сомнения в порядочности звонивших. Сказала, что хочет посоветоваться с сыном. «Громовым Андреем Аркадиевичем? Он в курсе. Мы ему уже звонили», — ответили в трубке. И это окончательно убедило маму, что с ней говорят честные люди из правительства Москвы, — переживает Андрей.

Опомнилась пенсионерка через пятнадцать минут, но этого времени мошенникам хватило, чтобы перевести с ее счетов (не только пенсионного, но и других) порядка 200 тысяч рублей. А вот в банке пострадавшим еще семь дней не могли выдать справку о движении денег на счете, требующуюся для возбуждения уголовного дела.

Москвичу Филиппу Высоцкому мошенники даже не потрудились звонить — просто прислали СМС. Но выбрали очень «удачное» время — пять утра.

— Меня разбудило сообщение якобы от моего банка. В нем говорилось, что на данный момент кто-то пытается снять с моей карты 100 долларов наличными. Потом пришло предупреждение о следующей операции на ту же сумму. В третьем было сказано: «Если транзакцию осуществляете не вы, отправьте цифру «1» на этот номер». Филипп уточняет: если бы его попросили прислать некий четырехзначный код, он бы распознал мошенническую схему. Но здесь просто была безобидная единица. В итоге со счета у него дважды сняли по сто долларов, причем операцию проводили в банкомате на Филиппинах.

Филиппу в итоге повезло: деньги банк через месяц вернул. «Я так и не понял, по какой схеме в моем случае работали мошенники. Мне лишь объяснили, что ранее я скомпрометировал свою карту».

А вот заявление в полицию еще от одного пострадавшего. Ему посоветовали защитить карту с помощью процедуры биометрической идентификации данных.

«Звонившая представилась: сотрудница Сбербанка Мила. Предложила пройти биометрическую идентификацию по телефону. В ответ на мой вопрос, чем она может подтвердить, что является сотрудницей банка, назвала номер моей карты, баланс на ней и мои паспортные данные: ФИО, серию и номер документа, а также указала, что я владею еще одной картой в другом банке. Я поверил ей и согласился на запись биометрии. Во время процедуры меня соединили с голосовым роботом, который попросил назвать пароль из СМС-сообщения и CVV-код с обратной стороны карты. Далее «Мила» проинформировала, что в течение десяти минут карта будет недоступна, а для проверки спишется сумма и вернется на счет. В 21:50 я попробовал зайти в свой аккаунт через персональный компьютер и обнаружил, что логин и пароль изменены неизвестными. А с моей карты списали 3636 рублей».

«Ваши данные мошенники покупают за копейки»

Все схемы объединяет одно — аферисты располагают персональными данными владельцев карт. Это не так уж и сложно — в теневом сегменте интернета торговля такой информацией процветает. Месяц назад на сайте РИА Новости было опубликовано большое расследование на эту

Всего за полторы тысячи рублей обозреватель агентства купила полное досье на себя, в котором были данные как российского, так и загранпаспорта, адрес прописки, даже фото из этих документов. На том же сайте предлагали приобрести сведения о счетах в банках, информацию о балансе карты, о последних операциях, о том, в каком банкомате человек снимал деньги и сколько.

Впрочем, телефонные мошенники предпочитают пользоваться базами данных, которых на специализированных форумах масса.

— Можно купить «готовую» базу, а можно заказать по конкретным параметрам, например «вкладчики Сбербанка с остатком на карте 50 тысяч рублей». Есть предложения по ВИП-клиентам, выборка по определенному региону, городу, — объяснил РИА Новости эксперт по системам предотвращения утечек данных, основатель и технический директор компании DeviceLock Ашот Оганесян. — Причем эти сведения мошенники покупают за гроши. Одна запись стоит от 70 до 120 рублей — за совсем уж эксклюзивные подборки. Вечером ты заказываешь базу, утром тебе присылают архив. Занимаются этим инсайдеры из числа сотрудников финансовых организаций — как действующие, так и бывшие.

Еще меньше сил аферисты тратят на то, чтобы при звонке у жертвы на мобильном высвечивался реальный номер банка. «Множество АТС позволяют осуществлять звонки с подменой А-номера. Раньше это было проблематично из-за сложного телекоммуникационного оборудования. Теперь — дело пяти минут. Подобные услуги также предоставляют на всевозможных нелегальных форумах в интернете».

Стоит услуга копейки. «За подключение к серверу просят тысячу рублей, звонок на любой номер России — 12 рублей. Оплата в биткоинах, — озвучивает реальное предложение с теневого сайта Оганесян. — Получается, что за сто рублей они покупают одну запись из банка, еще 12 тратят на звонок. В 150 рублей укладываются. При этом обманным путем снимают у людей сотни тысяч».

«Перевел по ошибке, верните»

Впрочем, знать ваши данные мошенникам вовсе необязательно. Екатерине Савельевой (фамилия изменена) пришло СМС о переводе десяти тысяч рублей с незнакомого номера. Отправителем значился некий Мурад Х. Спустя несколько минут с этого номера перезвонили, собеседник начал заверять, что он хотел перечислить деньги племяннику, но ошибся. Всего на одну цифру. Слезно просил вернуть.

«Все родственники уговаривали меня так и сделать, мол, ошибиться может каждый. Но я все же решила обратиться в банк, где перевод отменили. Уже потом узнала, что, если бы вернула деньги, могла стать фигурантом уголовного дела», — заключает Екатерина.

Перевод средств с незнакомого номера — еще одна популярная схема обмана. Как объясняет руководитель отдела анализа защищенности компании «Информзащита» Виталий Малкин, есть два сценария развития ситуации. Первый — самый простой, что называется, на дурака.

— Вам приходит СМС о том, что на телефон зачислена энная сумма, обычно небольшая — две-три тысячи рублей. Спустя еще несколько минут вам звонит незнакомец и уверяет, что ошибся. Деньги просит вернуть. Не каждый решит проверить баланс. Многие возвращают. А оказывается, мошенники просто подделали СМС от сотового оператора, — говорит Малкин.

Вторая схема — более опасная. Вам, как правило, переводят крупную сумму, и деньги действительно приходят на счет.

— Обычно в этом случае используют чужую карту, зачастую украденную. С одной стороны, таким образом отмывают деньги. Но в итоге если владелец украденной карты обратится в суд, сумму будут взыскивать именно с вас. И фигурантом уголовного дела станете именно вы, — уточняет эксперт.

Есть и другой вариант: мошенник дает объявление о продаже товара в интернете, указывает номер вашей карты. И через некоторое время вам начинают сыпаться переводы от незнакомых людей — тех самых покупателей. Затем вам звонит аферист и просит вернуть деньги — мол, перевел по ошибке. Вы возвращаете. А в итоге реальный покупатель, который так и не дождался своего товара, подает на вас в суд.

Еще одну схему описал блогер Леонид Фадеев:

«Сегодня утром мне позвонили на сотовый телефон. Женский голос автоинформатора сообщил, что меня беспокоят из Сбербанка. «Собеседница» акцентировала внимание на том, что наш разговор записывается, после чего спросила: «Могу ли я услышать Фадеева Леонида Вячеславовича?» Далее последовала пауза для записи моего ответа. <…> Когда мне позвонили в следующий раз, я стал слушать, какие еще будут вопросы. Автоматическая женщина попросила меня назвать число, месяц и год рождения».

Леонид замешкался, стал мямлить что-то невнятное. Тогда уже «человеческий» голос уточнил, что его плохо слышно, попросил повторить фразу. В этот момент блогер понял, что его хотят обмануть, и сбросил вызов.

Как объясняет Виталий Малкин, эта схема достаточно новая. Появилась после того, как банки начали внедрять механизмы идентификации по голосу.

— Преступники записывают ваши ответы, после чего звонят в банк и от вашего имени пытаются совершить мошеннические действия либо выведать у оператора необходимые данные о вашем счете, например остаток, количество карт. Получив эти сведения, они могут повторно позвонить держателю карты и попытаться его обмануть, — говорит Малкин.

К слову, записывать конкретные фразы необязательно. «Есть системы, которые на основе некоего набора голосовых данных синтезируют голос. Потом аферист произносит слова, а они звучат вашим голосом».

Как не стать жертвой

Чтобы не потерять деньги, эксперты в сфере интернет-безопасности советуют:

— ни в коем случае не сообщайте никаких данных банковской карты или личного кабинета по телефону. И неважно, кто звонит: «сотрудник отдела финансового мониторинга», «оператор call-центра правительства Москвы», «представитель налоговой службы». Помните, у настоящих сотрудников финансовых организаций, где вы оформляли карту, все эти данные есть;

— если вам звонят из банка, скажите, что вы сами перезвоните и положите трубку. Только набрав номер самостоятельно, вы можете быть уверены, что не разговариваете с мошенником;

— занесите в память телефона номера вашего персонального менеджера или call-центра банка;

— о любых сомнительных зачислениях на счет сообщайте оператору кредитной организации.

Подробнее: https://ria.ru/20190812/1557302039.html?fbclid=IwAR2Jb0xBLm9t_ehyM_K7uWV-VhHA5A_rHUzQIoBhp8CUeEkqBIf48uuNs6A