## **Россиян предупредили о массовых потерях сбережений из-за СМС. Как действуют мошенники и как себя вести, чтобы не стать их жертвами.**

Россиян предупредили о массовых потерях сбережений из-за СМС. Новые технологии общения банка с клиентом часто оказываются отличной возможностью для злоумышленников. Россияне стали путаться в данных, которые можно сообщать, а какие — нет. Этой путаницей и пользуются мошенники. Банкиры советуют совершать операции, требующие оглашения секретных сведений, только в офисах.

Сотрудники кредитных организаций стали чаще запрашивать у клиентов коды из СМС-сообщений, что может привести к массовым потерям сбережений, пишут СМИ со ссылкой на экспертов по информационной безопасности.

Обычно эту информацию кредитные организации запрашивают для подтверждения списания денежных средств, при этом предупреждая в этих же сообщениях, что их нельзя называть никому, даже сотрудникам банка. Однако ряд банков отправляет клиентам коды, которые им необходимо называть сотрудникам в офисе при совершении отдельных операций. Это такие операции, как подключение автоплатежей, досрочное погашение кредитов, проверка корректности номера телефона и другие.

Некоторые кредитные организации используют такие практики не только в случаях, когда клиент приходит в офис банка, но и при обращении в колл-центры.

При этом привычка называть коды, присланные в СМС-сообщениях, может обернуться потерей средств.

**Эксперты по безопасности опасаются, что такое поведение банков, когда само кредитное учреждение формирует у клиентов определенные шаблоны поведения, показывая, что сообщать секретный смс-код сотруднику финансовой организации нормально, может увеличить проведение мошеннических операций.**

В Центробанке отметили, что пока к ним не поступало жалоб на подобные проблемы.

**«Банки, запрашивающие по телефону коды, в первую очередь увеличивают шансы успешных мошеннических действий против своих же клиентов, так как приучают их выполнять подобные требования», — соглашается Геннадий Николаев, эксперт Академии управления финансами и инвестициями.**

Проблему признают и сами банки. По словам Вячеслава Абрамова, директора офиса продаж «БКС Брокер», в связи с технологичным развитием онлайн-банков нужно задуматься и об усилении защиты клиентов, однако это тоже непросто.

«Нет никакой целесообразности в запросе смс при звонке в колл-центр для индентификации личности, ведь телефон мог быть украден. К тому же на практике банки все же больше запрашивают кодовое слово. Если у банка возникают какие-то подозрения в операциях, они просто блокируют карту», — говорит банкир.

Как отмечает Тимур Аитов, заместитель председателя подкомитета по платежным системам и информационной безопасности ТПП, банки уже несколько лет идут по упрощению доступа клиентов к своим продуктам в онлайне. Но при этом уровень защищенности этого доступа критически падает. Он вспоминает, что еще лет пять назад, когда клиент проводил крупный платеж, например, на сумму 80-100 тыс. рублей, ему обязательно звонил человек из колл-центра и просил подтвердить — хотя бы просто словами, что эту операцию человек совершает сам, а не злоумышленник, укравший его карту.

«Теперь же достаточно простого четырехзначного кода, полученного на телефон, и операция совершается. А вот ответственность за то, что ты сказал этот код не тому человеку или ввел не на том сайте, банки с себя сложили — теперь за безопасность своих денег, которые человек доверил банку, всецело отвечает не банк, а сам клиент.

**Кроме того, банки всегда в случае мошеннических действий рекомендуют клиентам обращаться в правоохранительные органы, а те не очень-то горят желанием возбуждать уголовные дела, зная, что мошенников они никогда не найдут. И в этой лазейке между технологичностью и несовершенством закона все новые и новые способы мошенничества множатся с катастрофической быстротой», — говорит эксперт.**

В начале этого года стало известно о резком росте мошеннических звонков клиентам якобы от банков с использованием технологии подмены номера. Такие случаи зафиксировали крупные кредитные организации.

Для клиента это выглядело как звонок банка: входящий номер принадлежит кредитной организации, представитель которой сообщал о попытке несанкционированной операции, далее выманиваются данные карты, происходит хищение.

**Звонившие представлялись сотрудниками банка, сотрудниками службы безопасности, называли имена и фамилии.**

**«Вам сообщают о якобы совершаемых по вашей карте операциях. «Мы видим, что происходит списание средств по вашей карте», «прямо сейчас мы видим, что происходит перевод ваших средств», далее сумма и регион, где якобы все происходит. Предлагается сверить ваши персональные данные: не вы, а вам называют номер вашей карты, телефон — все паспортные данные. Звучат фразы «мы действуем в целях вашей безопасности», «мы как банк обязаны обеспечить вашу безопасность» и прочие обороты со словом «безопасность», — делилась приемами, которые используют мошенники, София Иванова.**

Вас спрашивают, не забывали ли вы где-то карту, не теряли ли, не оставляли ли в банкомате, не привязывали ли к онлайн-банку дополнительные номера телефонов, говорит она.

«Далее якобы находят номер телефона, привязанный к вашему онлайн банку пару дней назад. Вы, разумеется, отрицаете, вам сообщают, что проблема обнаружена. Вам называют остаток средств на карте вплоть до копейки, чтобы удостовериться, что спохватились вовремя, и никто ничего не украл», — пишет пользователь соцсетей.

Потом мошенники с целью обмануть бдительность клиентов предупреждают, что средства, карта и онлайн-банк будут заблокированы на сутки, а деньги будут переведены на секьюритизированный счет, после чего в течение 24 часов вернутся обратно.

«При этом несколько раз мошенники предупреждают, что теперь будет звонить сотрудник банка каждый раз, когда сумма перевода будет превышать 5 тысяч рублей. Мошенники не просят называть три цифры на обороте карты, но спрашивают о кодовом слове», — рассказывала София Иванова.

**Для того, чтобы обезопасить себя от мошенников, операции, требующие оглашения секретных паролей, лучше проводить либо непосредственно в офисе банка, либо «без посредников» — с использованием интернет банкинга, советует Андрей Люшин, заместитель председателя правления Локо Банка.**

**26 мая 2019 г**

***Источник: https://professionali.ru/***

**-------------------------------------------------------------------------------------------------------------------**

Российский портал информатизации образования [содержит: законодательные и нормативные правовые акты государственного регулирования информатизации образования, федеральные и региональные программы информатизации сферы образования, понятийный аппарат информатизации образования, библиографию по проблемам информатизации образования, по учебникам дисциплин цикла Информатика, научно-популярные, документальные видео материалы и фильмы, периодические издания по информатизации образования и многое другое.](http://portalsga.ru)