Вишинг. Как понять, что вам звонит не банк, а мошенник

Вишинг (англ. *vishing*, от *voice phishing*) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой.

Исходя из статистических сведений, с начала 2020 года вишинг набирает все большую популярность и входит в топ самых распространенных способов телефонного мошенничества на территории нашей страны. Результаты многочисленных исследований показывают следующее:

– Во время эпидемии COVID-19 количество звонков от финансовых мошенников выросло более чем на 30%.

– Большинство звонящих в первую очередь пытаются вызвать доверие клиентов. Подавляющая часть мошенников знают, как минимум, имя человека, другие знают также фамилию и отчество, меньшинство обладают сведениями о персональных данных карты или могут назвать банк, в котором обслуживается клиент. Все эти сведения мошенники используют в беседе, и часто клиенты начинают верить в то, что общаются именно с сотрудником банковской организации.

– Персональную информацию о клиентах мошенники получают благодаря сливам баз данных банков или с помощью агрегаторов данных. Например, ФИО и номера телефонов могут быть у различных магазинов: они собирают информацию о своих покупателях для включения их в бонусные программы. Если мошенник получит доступ к этим данным, он будет знать имя и фамилию клиента, а также номер его телефона.

– Мошенники используют различные техники социальной инженерии, за основу можно выделить несколько сценариев, которыми чаще всего пользуются злоумышленники. Обычно звонящие пытаются сразу вызвать страх у клиентов: сообщают о подозрительном платеже с банковской карты или о том, что карта заблокирована. Реже мошенники звонят с «выгодным» предложением — открыть вклад или получить кредит.

– Целью мошеннических звонков в большинстве случаев являются коды из СМС, приходящие на телефон клиента. Например, если мошенники звонят и говорят, что с карты пользователя был совершен подозрительный перевод без его ведома, то позже они предложат остановить транзакцию. Чтобы ее остановить, злоумышленники попросят клиента назвать код из СМС, которая придет во время разговора. Однако на самом деле клиент не останавливает транзакцию, а подтверждает ее и деньги уходят на счет мошенников. Второй вариант — мошенники попросят клиента самостоятельно перевести деньги с карты на якобы безопасный счет. При этом злоумышленники называют реквизиты собственных карт. Некоторые мошенники заходят еще дальше и уговаривают под различными предлогами клиента установить специальное приложение на телефон, которое, по их словам, защитит деньги пользователей от краж. Но на самом деле с помощью подобных приложений злоумышленники могут узнать пароль от интернет-банкинга клиента и иные персональные данные, а также удаленно управлять мобильным устройством.

Что делать для защиты от мошенников.

В ситуации, когда самый излюбленный способ работы мошенников — звонок от имени якобы сотрудника банка, лучше вообще не вступать в такие разговоры. К сожалению, злоумышленники сейчас активно пользуются IP-телефонией. Это позволяет использовать номера, которые похожи на официальные номера банков. Иногда эти номера и вовсе могут совпадать.

Следующие советы помогут обезопасить себя при встрече с таким методом мошенничества, как вишинг:

– Ни в коем случае не перезванивайте на тот номер, с которого вам поступил звонок. Сами же при звонке в банк набирайте номер, который указан на сайте банка.

– Сотрудник банка и без звонка должен знать:

- вашу фамилию;
- паспортные данные;
- и то, какие карты у вас оформлены;
- сколько денег осталось у вас на карте.

Если кто-то по телефону начинает спрашивать у вас что-то подобное, смело завершайте разговор и сообщайте о подозрительном звонке в банк.

– Есть информация, которую должны знать только вы. Банки никогда не звонят сами и не спрашивают по телефону у клиентов:

- полный номер карточки;
- срок ее действия;

- CVC/CVV;
- логин и пароль к интернет-банкингу;
- кодовое слово, код из СМС-сообщения.

Подобные сведения банк может спросить только в том случае, если клиент позвонил сам и то, это будет только ограниченная информация, а не полные данные, которые у банка и так имеются. Если вам позвонили и просят сказать что-то из вышеперечисленного — перед вами, скорее всего, мошенник.

Если с вашей картой действительно какие-то проблемы, то банк может сам ее заблокировать (такие случаи были, например, когда резко менялась география совершения операций по карте). Но в любом случае все подобные вопросы нужно решать в отделении банка, а не по телефону.

Еще одна уловка мошенников — рассылать СМС или сообщения в соцсетях со ссылками, перейдя по которым, вы сами установите на смартфон или ноутбук вредоносное ПО для воровства персональной информации. Внешне такие лжесообщения очень похожи на реальные сообщения от банков, госорганов, операторов связи или известных магазинов. Сложность еще и в том, что злоумышленники обычно используют сервисы по сокращению интернет-ссылок и выявить подвох гораздо сложнее.

Если вы получили сообщение о выигрыше, прежде чем переходить по ссылке, узнайте, действительно ли был такой розыгрыш и, если ли информация о розыгрыше на официальном сайте. Например, были случаи, когда клиентам обещали подарки к юбилею банка, которое будет только через несколько лет, либо вообще уже давно было.

Подведем итоги и выделим основное.

В любых ситуациях, проводя какие-либо действия с денежными средствами пользователям необходимо соблюдать повышенную осторожность. Банки не запрашивают CVV-коды (с обратной стороны карты) или коды из СМС, а также иную персональную информацию. Кроме того, пользователям нельзя переходить по сомнительным ссылкам из СМС или писем в интернет-ресурсах, социальных сетях и мессенджерах: они могут вести на мошеннические сайты.

По рекомендациям банковских учреждений, клиенты, которым поступает звонок из банка, должны обращать внимание на манеру общения сотрудников. Мошенники постараются всеми способами убедить клиента

продолжать разговор. А настоящая служба безопасности банка никогда не будет возражать, если клиент захочет перезвонить позже.

Если мошенники все же украли деньги со счета клиента, нужно в кратчайшие сроки сообщить банку о несанкционированном переводе и заблокировать карту. Если пользователь не нарушил правила безопасности, банки обязаны вернуть клиенту деньги. Однако сложно говорить о возврате, когда клиент нарушает правила пользования интернет-банком: сообщает свои данные для входа в онлайн-банк и коды подтверждения мошенникам. В таких случаях все зависит от типа транзакции и удалось ли ее остановить антифрод-системам, либо она ушла.

Пользователям, столкнувшимся с неудачной попыткой мошенничества, также рекомендуется обращаться в банк. Таким образом, банк узнает о новых способах мошенничества и их предотвращает. Также имеет смысл сообщать о злоумышленниках операторам связи: у них есть возможность отследить и заблокировать звонки с номеров мошенников.

Успех или неудача вишинговых мошенников практически полностью зависит от просвещённости и грамотности в сфере информационной безопасности граждан. Таком образом, если клиент будет бдителен и осторожен, то вероятность хищения с его карты денежных средств стремиться к нулю.