Вишинг. Как не попасть на уловки кибермошенников

В этой статье мы расскажем более подробно о способе применения наших украденных или случайно утекших данных, который, несмотря на множество предупреждений в СМИ и от банков, по-прежнему приносит легкие деньги мошенникам.

Речь пойдет о **вишинге** (англ. vishing, от Voice phishing) — методе мошенничества с применением социальной инженерии, суть которого заключается в телефонной коммуникации, введении в заблуждение, претворяясь сотрудником банка, покупателем и так далее, и выманивании под разными предлогами у держателя платежной карты конфиденциальной информации или стимулировании к совершению определенных действий со своим банковским счетом и/или платежной картой.

Данный тип мошенничества стал очень активно применяться в отношении граждан Республики Беларусь с 2019 года. Звонят чаще всего со скрытого, похожего на настоящий номер банка либо подмененного с помощью специального программного обеспечения (то есть отображается при звонке настоящий номер банковской службы). Причем стоит отметить очень важный момент, который значительно повышает доверие к мошеннику. Звоня, он уже знает часть или весь номер карточки, услугами какого банка пользуется человек, а также может обратиться по имени и отчеству.

Сразу возникает логичный и резонный вопрос: откуда у мошенника может быть столько информации о человеке? Ответ на него прост, вишинг всегда начинается с получения сведений о будущей жертве. Источники могут быть самые разнообразные:

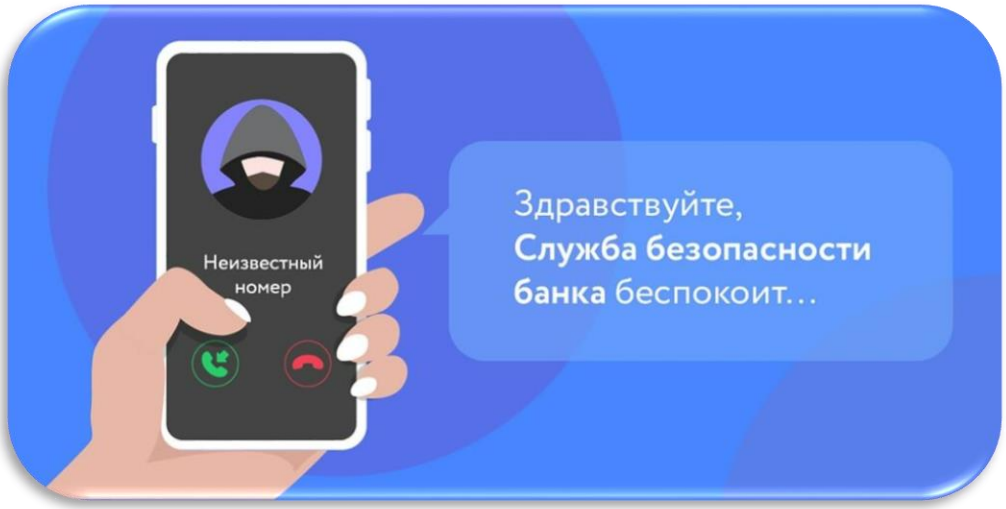
- **Утечки** клиентских и/или пользовательских баз сайтов, форумов, чатов, сообществ в соцсетях, торговых площадок, онлайн игр, интернет-магазинов, банков и многих других, не обеспечивающих должный уровень защиты для предоставленной информации или торгующие/обменивающиеся ею. Халатное отношение владельцев указанных баз к доверенным данным позволяет злоумышленникам постоянно обновлять и пополнять свои списки жертв, так как сейчас во всем мире, начиная от индивидуального предпринимателя и заканчивая крупными организациями частного и государственного секторов, все собирают и хранят наши персональные данные, в том числе паспортные и банковские, но не все используют их в заявленных целях или защищают как следует.
- Получение сведений из **открытых источников**, например, открытых страниц соцсетей или объявлений торговых площадок. Распространены случаи вишинговых звонков после публикации объявлений якобы по поводу покупки товара.
- **Фишинг**.
- **Облачные хранилища**. Из-за ненастроенных функций приватности, где могут храниться фотографии документов и иные персональные данные.
- **Социальные сети**. На страницах пользователей социальных сетей в открытом доступе находится огромное количество личной информации, данную информацию, пользователи, не задумываясь о последствиях, предоставляют в открытом виде злоумышленникам.
- Различные сомнительные и непроверенные **форумы**, **площадки**, **сайты**, **интернет-магазины**, **онлайн игры** собирают ваши регистрационные данные о банковских картах и другие, не обеспечивая должный уровень защиты для предоставленной информации либо банально торгуя ею.
- **Кража данных с пользовательских устройств** (телефон, планшет, ПК и т.д.) после заражения вредоносными приложениями, распространяемыми киберпреступниками.

В качестве примера вишинга можно привести случай, когда клиенту одного из банков позвонил неизвестный мужчина и представился сотрудником службы безопасности. Он сообщил о том, что аккаунт интернет-банкинга взломан и сейчас происходит кража денег со счета. Для того, чтобы заблокировать банкинг, необходимо сообщить логин и пароль, а потом для подтверждения того, что именно клиент является владельцем

аккаунта, назвать «секретный код», который придет ему на телефон. Испугавшись, клиент сделал все, как просил «сотрудник банка», и после этого ему пришло оповещение о списании со счета крупной суммы денег.

Таким образом, всегда нужно быть начеку и помнить, банкам нет необходимости так поступать, потому что, во-первых, абсолютно вся информация о своих клиентах (счета, номера карт, баланс, коды и т. д.) у них есть, во-вторых, они способны без вашего участия проводить операции по блокировке переводов, счетов, аккаунтов и не только.

В случае возникновения малейшего подозрения, что вы разговариваете не с сотрудником банка, просто завершите разговор и сами перезвоните по номеру телефона с официального сайта для уточнения всех вопросов либо сообщите о попытке украсть у вас данные или деньги. Также, если вам удалось пресечь такую попытку либо преступнику все же удалось получить от вас желаемое, можно обратиться в правоохранительные органы с заявлением о попытке/совершении в отношении вас преступления.



Рекомендации

В современном мире невозможно гарантированно уберечь себя от утечки персональных данных, а, следовательно, и попыток использовать их против нас (обмануть, украсть деньги или подставить), так как в тех или иных ситуациях их предоставление обязательно, а скомпрометирована может быть информационная система любой компании или организации. Но можно значительно снизить вероятность возникновения подобных ситуаций. Достичь этого можно лишь за счет ответственного и внимательного отношения к своим данным:

- Всегда соблюдать меры цифровой гигиены.
- Быть бдительным в отношении передачи и предоставления любых персональных данных.
- Не выкладывать в публичный доступ.

- Не передавать и не отправлять по почте или в мессенджерах сведения из документов, а также их сканы и фотографии сомнительным и непроверенным сервисам, магазинам, организациям, незнакомым людям.
- Постараться исключить случаи пересылки данных даже знакомому и надежному контакту, которому они необходимы, например, для оформления документов, поскольку вы не сможете проследить, будут ли ваши данные переправлены далее посторонним людям. Если альтернативного способа передать данные нет, то после использования отправителю и получателю необходимо удалить их с почтового сервера, а при пересылке сканов и фотографий документа рекомендуется ставить непосредственно на них пометку (например, водяной знак), с какой целью они пересылаются, чтобы сложнее было использовать в преступных целях.

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.