**Мошенничество с использованием удаленного доступа к телефону**

В России появилась новая схема мошенничества, включающая в себя использование одновременно средств социальной инженерии и информационных технологий. В результате чего теперь в зоне риска находятся даже самые осторожные и подозрительные клиенты банков. Для реализации данной схемы, направленной на хищение денежных средств физических лиц, мошенники взяли на вооружение общедоступное программное обеспечение, позволяющее удаленно управлять смартфоном, например, «TeamViewer».

Программное обеспечение «TeamViewer» является легальным и популярным среди пользователей инструментом, предоставляющим такие удобные функции как: удаленный контроль компьютеров и смартфонов, обмен информацией между устройствами, проведение видеосвязи и веб-конференций. Однако злоумышленники стали использовать данную программу в преступных целях.

Об особенностях работы преступной схемы и способах защиты рассказывает управляющий отделением по Курской области ГУ Банка России по Центральному федеральному округу Евгений Викторович Овсянников.

Мошенник звонит потенциальной жертве, представляется банковским работником и говорит о том, что банк якобы зафиксировал попытку несанкционированного вывода средств с её счета и в целях безопасности заблокировал эту операцию до тех пор, пока не получит подтверждение от верифицированного клиента. Но при этом злоумышленник не требует раскрыть номер, срок действия и секретный код на карте. Даже наоборот – предупреждает, что эти сведения нельзя выдавать посторонним, чем повышает доверие к себе.

Далее лжесотрудник «банка» заявляет, что операция похожа на техническую атаку, и похоже, что телефон «клиента» заражен вирусом, просит установить «специальную программу», чтобы удалить вирус из операционной системы.

Жертва устанавливает программу, даже не подозревая, что это программа удаленного управления телефоном. Мошенник получает полный доступ к смартфону жертвы и может перехватить SMS-сообщения от банка и различных онлайн-сервисов типа «Мобильный банк», авторизоваться в личном кабинете и вывести денежные средства на свой счёт.

Еще один вариант атаки выглядит следующим образом: на телефон жертвы отправляется фейковое SMS-сообщение (якобы от лица банка) о списании средств. Зачастую такое сообщение предваряет телефонный звонок

мошенников. Далее пользователю звонит лжесотрудник банка, говорит, что зафиксировал попытку вывода денежных средств и тут же уточняет: получал ли пользователь оповещение? Жертва отвечает, что сообщение приходило. В ответ мошенник сообщает, что на смартфоне зафиксирована вредоносная активность, и чтобы ее прекратить, нужно установить все ту же программу «TeamViewer» для получения удаленного доступа.

Мошенники зачастую бывают достаточно убедительными в своих обращениях. Также во время разговора на заднем плане раздаются голоса других сотрудников «call-центра», жертву переключают с линии на линию, включают автоответчик – все это делается, чтобы создать полную иллюзию официальной организации.

Доказать несанкционированный доступ к банковскому счёту в данном случае практически невозможно, поскольку фактически его не было. Жертва сама по своей воле предоставила мошеннику полный доступ к своему смартфону, а также возможность запускать любые приложения и посещать любые сайты.

Чтобы обезопасить себя от упомянутых мошеннических схем Евгений Овсянников настоятельно рекомендует:

*«Если вам звонит человек, который представляется сотрудником банка и сообщает о несанкционированном списании с вашего счета денежных средств – кладите трубку, независимо от того, с какого номера поступил звонок. Для проверки информации – перезвоните в свой банк самостоятельно по телефону, указанному на вашей карте».*

**Отделение Курск ГУ Банка России**

**по Центральному федеральному округу**

**Тел.: 36-12-20, 36-20-24;**

**е-mail: 38media@cbr.ru**