ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОКУРАТУРА МУРМАНСКОЙ ОБЛАСТИ

ПРОКУРАТУРА ГОРОДА КИРОВСКА

Обратная сторона информационно-телекоммуникационных технологий

С каждым годом количество преступлений в сфере информационно-телекоммуникационных технологий растет.

Под влиянием мошенников граждане начинают оформлять кредиты на большие суммы и переводить деньги злоумышленникам.

Для того, чтобы погасить бдительность людей и ввести их в заблуждение мошенники с использованием специальных программных средств подменяют абонентский номер, который определяется мобильным устройством как входящий. К примеру, от мошенника может поступить звонок с номера телефона банка или правоохранительного органа.

Буквально на днях на официальном сайте Сбербанка опубликована информация о том, как устроена новым схема мошенничества в мессенджерах. Она состоит из четырех этапов.

#1 Мошенник создаёт в мессенджере аккаунт, якобы принадлежащий Сберу, — с названием, имитирующим номер 900 и лого банка. С этого профиля злоумышленник делает первый звонок, представляясь сотрудником банка, и спрашивает человека, обновлял ли он мобильное приложение в последнее время.

#2 Если ответ отрицательный, «работник» сообщает, что необходимо дождаться звонка от профильного специалиста банка, который поможет обновить приложение.

Сообщник мошенника звонит с другого аккаунта или даже в другом мессенджере, где есть функция трансляции экрана во время видеозвонка. Такая путаница с разными «специалистами» нужна, чтобы дезориентировать человека и заставить действовать по указке.

#3 Второй «сотрудник» объясняет, что звонит по видеосвязи для идентификации клиента по биометрии. А потом просит включить режим

демонстрации экрана. Благодаря этому, по словам мошенника, подключается некая «роботизированная система для диагностики счёта».

#4 После этого человека просят зайти в мобильное приложение банка. Мошенник уверяет, что это абсолютно безопасно, так как экран будет видеть только робот, а сам сотрудник — нет.*

Как уверяет кредитная организация, трансляция экрана позволяет мошеннику увидеть номера карт, суммы на счетах, коды в СМС от банка, которая помогает злоумышленнику заполучить доступ к личному кабинету клиента в приложении на своем устройстве и украсть его деньги — или убедить его перевести их на «безопасный счёт».

Призываем граждан быть бдительными и воздержаться от передачи своих мобильных данных неизвестным лицам.

---

*https://www.sberbank.ru/ru/person/kibrary/investigations/skhema-moshennichestva-zvonok-ot-sotrudnika-banka