

## «Установите приложение, чтобы обезопасить свои деньги»

Валерий, Смоленск

Только что столкнулся с ситуацией, звонок на телефон, человек представился сотрудником банка и рассказал, что к моему счету подключился сторонний телефон и попытался перевести деньги, эта попытка заблокирована. Далее «специалист» предложил поменять антивирус и установить стороннее приложение. Насколько я понял, что это приложение удаленно мониторит ваш экран, возможно что-то еще.

Соответственно, можно получить доступ ко всем функциям и настройкам и приложениям банков. В середине разговора я бросил трубку и перезвонил в банк, так как меня насторожило стороннее программное обеспечение, которое предлагалось установить, но все было очень правдоподобно, вплоть до фонового шума других телефонистов, сидящих вокруг. Будьте внимательны!

### Совет эксперта по противодействию мошенничеству:

Мошенники попытались получить доступ к счету Валерия с помощью легальной программы, которая позволяет основному пользователю или постороннему человеку подключиться к телефону или компьютеру и управлять им удаленно. Обычно это приложение используют в компаниях для дистанционной техподдержки сотрудников — например, для настройки оборудования или устранения проблем.

Злоумышленник использовал психологические уловки, чтобы вызвать доверие у Валерия. Он представился сотрудником банка и попытался убедить, что действует в интересах безопасности клиента. На самом деле мошенник собирался получить доступ к телефону Валерия. В частности, он мог бы выведать пароль от его мобильного банка, получить доступ к чтению одноразовых паролей из СМС и украсть деньги.

При этом настоящей службе безопасности банка сложно распознать подобное мошенничество и оперативно его пресечь. Ведь пользователь добровольно скачивает легальную программу, которая открывает мошеннику удаленный доступ к его устройству. В итоге злоумышленник, по сути, действует руками владельца телефона.

Мошенники могут использовать технологию подмены номера, так что у пользователя на телефоне отражается официальный номер банка. Злоумышленник может перечислить человеку последние операции по его карте, назвать его адрес и другую личную информацию. Все эти сведения мошенники получают из баз данных, которые покупают на черном рынке.

### **Как защитить свои счета от мошенников?**

- Если вам звонит сотрудник банка и сообщает об угрозе мошенничества, положите трубку и перезвоните в банк. Номер телефона (он указан на вашей карте и на официальном сайте банка) лучше набрать вручную: если звонили мошенники, обратный звонок может соединить вас с ними же.
- Никому не сообщайте личные данные, реквизиты карты и секретную информацию: секретное слово, SVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Банк может не вернуть вам деньги, если выяснится, что вы сами сообщили мошенникам секретные данные.
- Не скачивайте сторонние приложения на свой телефон по просьбе незнакомцев.
- Установите антивирусы на все гаджеты, которыми пользуетесь.