Банки зафиксировали новый сценарий телефонного мошенничества с применением методов социальной инженерии.

Мошенники обзванивают клиентов под видом службы поддержки сотовых операторов и сообщают якобы о взломе личного кабинета абонента или телефона.

Злоумышленники просят набрать на телефоне специальную USSD-команду, состоящую из комбинации цифр и символов, которая вводится при звонке, и номера телефона — это нужно якобы для предотвращения распространения личных данных. Таким образом, абонент самостоятельно меняет настройки своей сим-карты и устанавливает переадресацию СМС и звонков на номер мошенника.

Затем абоненту снова могут позвонить и сообщить об устранении проблемы со взломом, а в реальности злоумышленники получают коды из сообщений и могут похитить деньги со счетов в банке, получив доступ в личный кабинет банка.

Проявляйте бдительность и при малейшем сомнении прекратите разговор, который кажется Вам подозрительным.