ПРОКУРОР РАЗЪЯСНЯЕТ: Информация по телефонному мошенничеству

В последнее время наиболее распространенным видом мошенничества стало мошенничество в сфере информационно-телекоммуникационных технологий или компьютерной информации. По данным Генпрокуратуры РФ, на них приходится около 70% всех хищений, совершенных путем обмана или злоупотребления доверием. При этом более 42,7% мошенничеств совершалось с использованием средств мобильной связи. Также Генпрокуратура РФ констатировала значительное увеличение числа краж, совершенных с банковского счета или в отношении электронных денежных средств: за прошедший год зарегистрировано увеличение таких преступных посягательств более, чем на 44%, в сравнении с аналогичным периодом 2019 года.

Представленные данные свидетельствуют о том, что мошенничество по телефону становится одним из наиболее простых способов получения несанкционированного доступа к банковской информации граждан. Мошенники для совершения звонков чаще всего используют номера, которые стали доступными вследствие утечки персональных данных, например, из баз с номерами мобильных телефонов, ФИО и других сведений о субъекте персональных данных.

Владея такими данными, становится удобнее применять метод социальной инженерии, то есть психологическое манипулирование для выполнения необходимых для мошенничества операций или раскрытия конфиденциальной информации. Например, информация о наименовании оператора связи, которым пользуется абонент, поможет мошеннику с наибольшей долей вероятности расположить собеседника к раскрытию конфиденциальной информации, если он представится сотрудником компании оператора.

Действия телефонных мошенников квалифицируются по статье 159 Уголовного кодекса Российской Федерации как мошенничество, то есть умышленные действия, направленные на хищение чужого имущества путем обмана или злоупотребления доверием. Противодействие такому виду мошенничества осуществляется государственными органами не только с помощью регистрации и расследования уголовных преступлений, но и путем информирования граждан о потенциальной опасности.

Информирование о превентивных методах борьбы осуществляют заинтересованные в безопасности клиентов органы, например, банки. Так, Сбербанк осведомляет клиентов об отсутствии необходимости в совершении операций по инструкциям звонящего, так как все операции для защиты сотрудник банка выполняет самостоятельно, а такие данные, как коды безопасности с обратной стороны карты (CVV/CVC), логин от СберБанк Онлайн, коды из СМС, номер банковской карты, сотрудник банка самостоятельно просить не будет.

Со стороны потенциальных жертв лучшим способом избежать уловок телефонных мошенников является осведомленность о том, какие схемы существуют. Стоит помнить о том, что злоумышленники научились подменять телефонные номера, с которых осуществляется вызов. Также следует иметь в виду, что современные технологии умеют подделывать голос и видео на высоком уровне.

Идеальным способом защиты выступает прекращение разговора с собеседником, личность которого вызывает подозрение. Так, например, для противодействия мошенническим действиям предлагается не совершать операции по инструкциям, полученным в результате телефонного разговора. В случае сомнений в добросовестности звонящего, лучше завершить звонок и перезвонить по номеру телефона банка или мобильного оператора (в зависимости от того, кем представился звонящий). При этом следует помнить, что ни сотрудники банка, ни другие третьи лица не могут запрашивать важную конфиденциальную информацию по телефону, в связи с чем, звонки с соответствующей просьбой вероятнее всего являются мошенническими.

При поступлении подозрительного звонка или СМС рекомендуется незамедлительно обращаться по номеру 8-800-222-74-47 или в полицию по номеру 02/102 и не реагировать на просьбы мошенников.