ИСТРИНСКАЯ ГОРОДСКАЯ ПРОКУРАТУРА ИНФОРМИРУЕТ

Преступления, связанные с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий

В последнее время в Российской Федерации участились случаи совершения преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий.

Распространены преступления в указанной сфере, связанные с хищением денежных средств граждан.

Одно из наиболее часто встречающихся подобных преступлений – хищение денежных средств со счетов граждан с использованием реквизитов банковских карт. Злоумышленники, как правило, получают такие реквизиты в телефонном разговоре.

Для того, чтобы не стать жертвой мошенников важно знать следующее. Сотрудники банка по телефону никогда не запрашивают реквизиты карты – ее номер, срок действия, трехзначный код на обороте. Если сотрудник банка по телефону просит совершить какие-либо операции с картой – это признак мошенничества. Не следует сообщать кому-либо код подтверждения операции из СМС. При сомнительных звонках необходимо положить трубку (прервать телефонное соединение) и перезвонить в колл-центр соответствующего банка (номер телефона всегда указан на оборотной стороне карты).

Хищение денежных средств может быть совершено также при совершении онлайн-покупок. При совершении онлайн-продажи товара для получения денег от покупателя достаточно сообщить только номер банковской карты. Если вас просят указать другие реквизиты (например, CVV-код) – это признак мошенничества.

Имеют место случаи мошенничества с использованием социальных сетей. Например, злоумышленник, обнаружив сохраненный логин и пароль от страницы гражданина в социальной сети, может без разрешения зайти на эту страницу, поменять логин, пароль и от имени гражданина осуществить рассылку друзьям (знакомым) последнего писем с просьбой об одолжении денежных средств. Лицу, получившему такое письмо, следует связаться с гражданином, от имени которого направлена просьба об одолжении денежных средств, и удостовериться в подлинности письма.

Кроме того, правоохранительными органами зафиксированы факты хищения денежных средств, совершенные с использованием мобильных приложений банков, установленных на телефонах, которые были утеряны их владельцами. Во избежание подобных случаев целесообразно устанавливать пароль на вход в мобильное приложение. В случае потери либо хищения мобильного телефона с установленным мобильным приложением, вход в которое не защищен паролем, незамедлительно свяжитесь с банком для блокирования операций с банковским счетом.

Разъясняем, что при совершении в отношении Вас любых мошеннических действий Вам необходимо обратиться в правоохранительные органы.