Прокурор разъясняет: Новые способы дистанционного мошенничества

С каждым годом увеличивается количество преступлений в сфере информационно-телекоммуникационных технологий. Под влиянием злоумышленников доверчивые люди начали оформлять кредиты на большие суммы и переводить деньги мошенникам.

Для введения 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 правоохранительного органа или банка.

Появились новые сценарии мошенничества.

Мошенники представляются службой поддержки сотовых операторов, сообщают о взломе личного кабинета или телефона, затем просят набрать определенную комбинацию цифр и символов, таким образом меняя настройки сим-карты и устанавливая переадресацию смс-сообщений и звонков на номер злоумышленника. Получая информацию из сообщений, преступники открывают доступ к счетам и совершают операции по списанию денежных средств.

Все больше распространяется способ мошенничества, при котором в социальных сетях и на сайтах мошенники размещают объявления о продаже каких-либо вещей: одежды, мобильных телефонов, наушников и др.

Далее, потенциальному покупателю предлагается воспользоваться опцией «безопасная сделка», в связи с чем ему направляется ссылка, которая оказывается фишинговой, и при введении реквизитов банковской карты происходит списание находящихся на счете денежных средств.

В зоне риска находятся также граждане, которые дают объявления о купле-продаже. Им звонят мошенники, вводят в заблуждение о намерении приобрести товар и под этим предлогом узнают сведения о банковских счетах, с которых осуществляется хищение.

Жертвы преступлений, к сожалению, зачастую сообщают злоумышленникам необходимые сведения для списания денег со счетов либо самостоятельно переводят деньги, действуя по инструкции.

Чтобы не стать жертвой преступников, необходимо запомнить и соблюдать следующие правила:

– не сообщать никому, в том числе лицам, представившимися сотрудниками банковских организаций, данные банковских карт, а также сведения из смс-сообщений для входа в онлайн-банк или совершения финансовой операции;

– не осуществлять поспешные переводы денежных средств, лицам, представившимся родственниками, без проверки данной информации;

– не загружать на мобильные устройства приложения и программы из непроверенных источников;

– приобретать товары только на официальных сайтах организаций;

- проявлять бдительность при осуществлении онлайн-покупок, не переходить для покупок по ссылкам.

Если доверившись злоумышленнику сообщили данные своих банковских карт и другую значимую информацию, необходимо незамедлительно позвонить либо посетить банковскую организацию, где у открыты счета, установить блокировку на совершение банковских операций и обратиться в правоохранительные органы.

Прокурор Сосновского района М.А. Абакаров