ВНИМАНИЕ! МОШЕННИКИ!

В настоящее время нарушения граждан от хищений с использованием информационно-коммуникационных технологий продолжает оставаться крайне актуальной.

Уголовно-правовая статистики и практика правоохранительных органов показывает увеличение роста мошенничества хищений с использованием информационно-коммуникационных технологий.

Зачастую «кибер-мошенники» осуществляют звонки гражданам, представляются сотрудниками банков, называют их по имени, отчеству, путем сложных речевых оборотов, тревожным голосом просят сообщить данные банковских карт (кодовый номер карты, секретные слова, PIN-коды и т.п.) для предотвращения якобы незаконного, несогласованного с владельцем карты, перевода денежных средств и их списания, оформления кредита и т.п. Пользуясь данной ситуацией, указывая срочность предотвращения незаконного посягательства, удаленным доступом получают данные к личному кабинету клиента банка, осуществляют перевод денежных средств без ведома собственника. При этом, как правило, преступники используют программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка. Зачастую введенные в заблуждение граждане сами переводят денежные средства на счета, указанные мошенниками.

В связи с обширным развитием социальных сетей, распространенные хищения осуществляются с использованием социальных платформ «Инстаграмм», «ВКонтакте», «Телеграмм». Злоумышленники, дублируют официальные аккаунты продавцов, от их имени предлагают товарную продукцию, а также в ряде случаев предлагают перейти по ссылкам, на которые указывает лжепродавец с аналогичными товарными продуктами. В последующем гражданами оплачивается товарный продукт по подставной карте злоумышленника, после чего такое лицо не предоставляет оплаченный товар и не выходит на связь.

Нельзя не отметить, что, преступники, используя базы данных компаний мобильной связи, массово рассылают SMS-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру». Преобладающее число граждан, пренебрегая своими денежными средствами, не уделяя должного внимания и времени, перезванивают по указанному в SMS-сообщении номеру, вместо того, чтобы обратиться лично в ближайшее отделение своего банка для проверки поступившей информации. А в ходе разговора злоумышленники могут завладеть информацией о банковских реквизитах, в том числе о PIN-коде, после чего осуществить незаконное списание денежных средств.

Для недопущения наступления таких последствий необходимо соблюдать компьютерную гигиену. Владельцев банковских карт быть бдительными и осторожными, никогда не сообщать посторонним лицам данные карты, персональные данные и коды, присланные в СМС. В любых подозрительных ситуациях нужно в кротчайшие сроки обращаться лично в ближайшие отделение

банка, выдавший карту. При совершении покупок в онлайн- магазинах, проверять достоверную информацию о продавцах.

В случаях, если совершаются или совершены мошеннические действия, необходимо обратиться лично с заявлением о преступлении в МО МВД России «Ремонтненский» или подразделения МВД России, либо по телефону горячей линии. За мошенничество с использованием электронных средств предусмотрена уголовная ответственность по статье 159.3 Уголовного кодекса РФ. За мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошеннических действий, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы до шести лет.