**Куда обратиться гражданину, если он стал жертвой информационных мошенников?**

Защита прав граждан, пострадавших от хищений, совершенных с использованием информационно-коммуникационных технологий, продолжает оставаться крайне актуальной.

Рассмотрим наиболее типичные способы их совершения.

Так, например, злоумышленники звонят гражданам, представляясь сотрудниками банков, называют их по имени, отчеству, просят сообщить данные банковских карт (номер карты, пароли, специальный код и т.п.) под предлогом предотвращения оформления нежелательного кредита либо несанкционированного списания денежных средств. При этом, получая персональные данные гражданина, мошенники с помощью удаленного доступа к личному кабинету клиента банка, осуществляют незаконный перевод денежных средств без согласия собственника. Как правило, преступники используют программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка. Бывает и так – введенные в заблуждение граждане сами переводят денежные средства на счета, указанные мошенниками.

Интернет-преступники, используя базы данных компаний мобильной связи, массово рассылают SMS-сообщения следующего характера: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру...». Большинство граждан вместо того, чтобы сразу обратиться в ближайший офис своего банка для проверки поступившей информации либо осуществить звонок в службу клиентской поддержки, перезванивают по указанному в SMS-сообщении номеру, в ходе разговора передают злоумышленникам информацию о банковских реквизитах, в том числе о PIN-коде, после чего и осуществляется незаконное списание денежных средств. Таким образом, денежные средства фактически выбывают из законного владения и собственник не имеет к ним доступа.

Не искоренены случаи, когда мошенники представляются родственниками либо знакомыми потерпевших, рассказывают, что попали в беду (стали виновником дорожно-транспортного происшествия, задержаны сотрудниками полиции, и им срочно требуются деньги на операцию) и просят срочно перевести денежные средства.

Неединичными являются факты мошенничества посредством сбыта через интернет-магазины техники, препаратов и лекарств, товаров и услуг по якобы льготным расценкам, а фактически по завышенной цене. В итоге потребитель либо не получает товар, либо получает, но совсем не тот, который ожидал.

Для защиты владельцев банковских карт необходима простая бдительность и осторожность граждан. Запомните, нельзя сообщать посторонним лицам данные своей банковской карты и персональные данные. Старайтесь не передавать третьим лицам свою банковскую карту, сотовый телефон, либо иные технические устройства; при поступлении звонков от лиц, представляющихся сотрудниками банка и предлагающих совершить какие-либо операции по карте или счету либо сообщить персональные данные, не спешите выполнять действия, навязываемые мошенником.

В случаях, если гражданин пострадал от мошеннических действий с банковскими картами либо в отношении него пытаются совершить мошенничество, то ему необходимо незамедлительно обратиться в банк, и сообщить, что списание денежных средств произошло против воли собственника, далее заблокировать карту, получить выписку о движении денежных средств по счету (по возможности), и обратиться с заявлением о преступлении в любой территориальный орган МВД России (подразделение полиции).

Прокурор Беловского района                                                             И.И. Зубков