Памятка по профилактике дистанционных мошенничеств и хищений денежных средств со счетов граждан

Дистанционное мошенничество, преимущественно, совершается следующими способами:

1. Потерпевшие под различными предлогами перечисляют денежные средства мошенникам.

2. Потерпевшие сообщают мошенникам реквизиты и пароли доступа к операциям по счету посредством поступившего им СМС-сообщения, что приводит к хищению денежных средств.

Участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Для разблокировки карты, абонента просят позвонить или отправить смс на короткий номер

Мошенники выступают в роли «сотрудников службы безопасности банков» и в ходе телефонного разговора получают информацию по банковской карте (номер банковской карты, а также CV-код).

Дальнейшим шагом является получение злоумышленниками разового пароля (в виде СМС-сообщения), который поступает на абонентский номер, привязанный к банковской карте. Держатель банковской карты сообщает разовый пароль мошенникам, тем самым предоставляет доступ к денежным средствам.

Уважаемые граждане, в целях пресечения и противодействия преступных намерений и действий мошенников, информируем Вас о том, что ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, тем более пароли от них.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов или продажи товара от частных лиц. При заказе товаров вас попросят внести предоплату, а потом продавец бесследно исчезает, либо присылает некачественный товар.

Если вы хотите купить товар по предоплате, поищите информацию о магазине либо продавце в сети Интернет, посмотрите, как долго он находится на рынке. При необходимости свяжитесь с администратором магазина и уточните информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц.

Следующий вид мошенничества - просьба в предоставлении денежных средств родственнику или знакомому, чаще всего через социальные сети, доступ к которым взламывается злоумышленниками. Мошенники могут представляться сотрудниками правоохранительных органов, знакомыми и даже вашими родственниками. Обязательно свяжитесь с теми, от чьего имени действуют незнакомцы, и убедитесь в правдивости информации.

Значительную распространённость имеют преступления, совершенные с использованием высоких технологий, то есть в сети Интернет, в том числе объявления о продаже и рассылка вирусных ссылок в социальных сетях. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Рекомендации гражданам:

1. Не диктовать пароли из смс-сообщений.

2. При поступлении подобного рода звонка, незамедлительно завершить разговор, и перезвонить по официальному телефону банка.

3. Не перечислять денежные средства по просьбам родственников и знакомых, полученных через социальные сети в личных сообщениях. Обязательно свяжитесь с теми, от чьего имени получены сообщения, и убедитесь в правдивости информации.

4. Никому не сообщать ПИН-код, CVC или CVV коды банковской карты.

5. В случае утери телефона незамедлительно сообщите в банк о приостановлении (блокировке) имеющихся на счетах сбережений.