**Профилактика преступлений, совершаемых в сфере информационно-коммуникационных технологий или с использованием компьютерной информации**

Случаи совершения преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий получают все большее распространение.

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

Чтобы не стать жертвой злоумышленников необходимо помнить 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. Никому не сообщайте код подтверждения операции из СМС. При сомнительных звонках следует прервать телефонный разговор и перезвонить в банк, клиентом которого Вы являетесь.

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, преступник, 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.

Разъясняем, что при совершении в отношении вас любых мошеннических действий вам необходимо обратиться в правоохранительные органы.