Информация
по профилактике ИТТ-преступлений для граждан и сотрудников полиции

Способы совершения ИТТ преступлений:

Преступления, совершаемые с использованием пластиковых банковских карт путем набора пин – кода, либо бесконтактным способом (wi-fi).

Примеры:
1. гр. Н., обнаружив в общественном месте утерянную неизвестным лицом банковскую пластиковую карту (с возможностью оплаты без ввода пин –кода), совершил с ее помощью покупку на сумму 1 000 рублей.
2. Преступник совершил кражу сумки, в которой находились документы и банковская карта (с записанным в документах пин - кодом). После чего совершает снятие денежных средств с банковской карты через банкомат, либо совершает по карте покупки.

Меры по обеспечению безопасности банковской карты
1. необходимо принять более тщательные меры по обеспечению сохранности личных банковских карт, пин-коды к ним хранить отдельно.
2. позвонить на «горячую линию» своего банка (номер указывается на обратной стороне банковской карты).
3. лично обратиться в ближайшее отделение банка и позвонить в дежурную часть ОВД (102 или 112).

Преступления, при совершении которых преступник использует устройство с возможностью выхода в сеть «Интернет», где формируются:
1) сайт-двойник, визуально похожий на какой-либо известный официальный сайт.
2) при использовании специальных программ удаленного доступа – мошенники при общении с гражданами убеждают последних установить «антивирусы», «безопасные программы», которые на самом деле являются программами, позволяющими управлять устройством гражданина дистанционным способом, после чего похищают деньги, находящиеся на счету граждан («Rust Desk», «Team Viewer», «Any Desk»).

Пример: гр. Н. в социальной сети «N» увидела объявление о покупке товаров и услуг по выгодной цене. Далее гр. «Н» переводит денежные средства преступнику, который в дальнейшем перестает ей отвечать, при этом, объявление блокируется.

Действия граждан
1. Чтобы не попасть при оказании услуг на сайт-двойник, обращайтесь к проверенным ранее Интернет-ресурсам, либо знакомым, родственникам и другим лицам, которые могут подтвердить достоверность официального сайта.
2. При поступлении звонка и разговора с неизвестными лицами о деньгах – прекратить телефонный разговор и позвонить в дежурную часть ОВД (102 или 112).
3. Не переходить по неизвестным ссылкам.

Преступления, совершаемые с использованием сотового телефона, с которого преступник осуществляет звонок потерпевшему, и обманным путём вынуждает последнего перевести ему денежные средства. Данный способ может применяться для **краж** и **мошенничеств**.

Пример:
гр. Н. поступает телефонный звонок от преступника, который представляется сотрудником службы безопасности банка. В ходе телефонного разговора преступник сообщает потерпевшему о том, что его банковская карта заблокирована, и для сохранения денежных средств, находящихся на банковском счете, ему необходимо осуществить их перевод на «безопасный» счет. Потерпевший, боясь за свои сбережения, осуществляет перевод денежных средств преступнику.

Действия граждан
1. При поступлении звонка и разговора с неизвестными лицами о деньгах – прекратить телефонный разговор и позвонить в дежурную часть ОВД (102 или 112).
2. При общении с неустановленными лицами по сети Интернет – не передавать поступающие коды и персональные данные из SMS-сообщений.