ПОЛИЦИЯ ИНФОРМИРУЕТ О МОШЕННИЧЕСКИХ СХЕМАХ С БАНКОВСКИМИ КАРТАМИ

Сотрудники МУ МВД России «Энгельсское» призывают жителей города и района быть бдительными и рассказывают, к каким методам прибегают злоумышленники, чтобы опустошить банковские карты граждан.

1) **Мошенник представляется работником банка.** Клиенту поступает звонок или SMS от неизвестного человека, который выдает себя за сотрудника службы безопасности банка. Он говорит, что зафиксирована попытка списания денег со счета клиента, выясняет данные карты и коды подтверждения, чтобы якобы спасти средства, но на самом деле списывает деньги со счета.
2) **Мошенник предлагает воспользоваться программами удаленного доступа**. Жертве звонит «представитель службы безопасности банка» и сообщает, что на устройстве клиента обнаружен вирус, необходимо скачать антивирус и сканировать гаджет. Во время сканирования устройство будто бы нельзя использовать, так как вирус может распространиться дальше. В действительности клиент скачивает программу удаленного доступа, а во время «проверки» мошенники получают доступ к мобильному банкингу и выводят средства.
3) **Безопасный счет**. Человеку также поступает звонок от «службы безопасности». Злоумышленник говорит, что произошла утечка данных, в ней замешаны сотрудники. Необходимо снять деньги через безопасный банкомат банка-партнера и перевести их на специальный страховочный счет.

   Другой вариант этой схемы: преступники предлагают сразу перевести деньги на счет, не снимая их в банкомате. За причиненные неудобства клиенту полагается вознаграждение. Мошенники просят не отключать телефонную связь во время операций. Предупреждают, что «банк» не несет ответственность за сохранность денег по условиям обслуживания счета: если их не снять, они могут пропасть.
4) **Автоматическая голосовая служба банка**. Лже-сотрудник банка оповещает клиента, что будто бы был зафиксирован вход в личный кабинет из другого города или страны. В рамках мер по безопасности необходимо назвать номер карты для идентификации. Мошенники предупреждают, что сейчас поступит код по SMS, но его никому нельзя называть. После чего переключают на голосовую службу. Клиент доверяет голосу робота и вводит код в тональном режиме. Мошенники меняют пароль и логин в его личном кабинете и выводят деньги.

Уважаемые граждане! Будьте бдительны и осторожны. Обо всех фактах мошенничества сообщайте в ближайший отдел полиции или по телефону «02» («102» – с мобильного).