ГОРЕЦКИЙ РОВД ПРЕДУПРЕЖДАЕТ:

В настоящее время отмечается значительный рост преступлений, связанных с хищением денежных средств с банковских счетов граждан, с использованием реквизитов банковских карт, привязанных к ним и личных данных граждан.

Одним из условий, способствующих совершению такого рода преступлений, является беспечность граждан. Как правило, злоумышленник осуществляет телефонный звонок на мобильный номер гражданина, у которого намеревается похитить денежные средства с банковской карты, при этом используется номер, код которого указывает на его принадлежность к оператору иностранного государства, например Литва, Латвия и других. В ходе состоявшегося разговора злоумышленник представляется работником службы безопасности банковского учреждения и сообщает, что с банковской карты его собеседника совершен (совершается) перевод денежных средств другому гражданину, при этом может указать вымышленные данные получателя перевода. Так же он сообщает, что для отмены данной операции необходимо предоставить номер банковской карты (в некоторых случаях злоумышленник может его сообщить сам) идентификационный номер паспорта, коды подтверждения содержащиеся в СМС-сообщениях поступивших на Ваш телефон после передачи номера банковской карты либо же идентификационного номера паспорта. Получив вышеуказанные сведенья, злоумышленник совершает хищение денежных средств с Вашей банковской карты.

Так же злоумышленник с целью хищения денежных средств проводит мониторинг различных интернет-сайтов, например «kufar.by» и иных. Обнаружив «свежее» объявление о продаже имущества инициирует переписку с использованием какого-либо мессенджера, например «Viber», при этом злоумышленник ведет переписку с номера, указывающего на его принадлежность к оператору иностранного государства, например Литва, Латвия и других. В ходе переписки злоумышленник может предоставить электронный чек, якобы об оплате покупки либо же ее доставки в виде ссылки, либо же ссылку на фишинговый либо вишинговый сайт, к примеру «kufar.cc», «kufar.co» и иные. **НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕЛЬЗЯ ПЕРЕХОДИТЬ ПО ДАННЫМ ССЫЛКАМ.** Перейдя по данной ссылке, Вы вводите там реквизиты своей банковской карты, якобы для оплаты товара либо подтверждения платежа и иными предлогами, после чего у Вас с банковской карты похищаются денежные средства.

Что бы не стать жертвой злоумышленника следует соблюдать следующие правила:

1. Ни при каких обстоятельствах не передавать реквизиты своих банковских карт, паспортные данные, а так же коды, содержащиеся в СМС-сообщениях, полученных от банковских учреждений посторонним лицам. Запомните! Работники банка никогда не будут спрашивать у Вас вышеуказанные данные по мобильному телефону.
2. В случае поступления Вам аналогичного звонка немедленно прекращать разговор с мошенником.
3. При использовании интернет-сайтов для покупки/продажи вещей не вести переписку в мессенджерах. **ВАЖНО!** Не переходить по ссылкам,

предоставленным Вашим собеседником в ходе переписки и ни в коем случае не вводить там реквизиты своей банковской карты.

4. Не выкладывать в публичный доступ в сети Интернет данные своих банковских карт, номер мобильного телефона, а так же иные паспортные данные.

Соблюдая вышеуказанные правила Вы никогда не станете жертвой злоумышленника, что так же Вам позволит сохранить Ваши денежные средства.