ОБРАТИТЕ ВНИМАНИЕ!!!

«Злоумышленники похищают денежные средства с банковских  
карт жителей г. Горки и Горецкого района»

За второе полугодие 2020 года (июль-декабрь) отмечен значительный рост преступлений, связанных с хищением денежных средств с банковских счетов граждан, с использованием реквизитов банковских карт, привязанных к ним и личных данных граждан. Всего за 6 месяцев 2020 года злоумышленниками было совершено более 40 преступлений, жертвами которых стали жители г. Горки и Горецкого района.

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 злоумышленнику номера банковской карты либо же идентификационного номера паспорта. Получив вышеуказанные сведения, злоумышленник совершает хищение денежных средств с банковского счета своего собеседника, который добровольно сообщил ему вышеуказанные личные данные либо реквизиты 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 сайт, к примеру: «kufar.ee», «kufar.co» и иные. **НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕЛЬЗЯ ПЕРЕХОДИТЬ ПО ДАННЫМ ССЫЛКАМ.** Перейдя по данной ссылке, гражданин вводит на нем реквизиты своей банковской карты, якобы для оплаты товара либо подтверждения платежа и иными предлогами, после чего у него с банковской карты похищаются денежные средства.

С третьей декады декабря 2020 года актуальность приобрел так же способ хищения денежных средств с банковских карт с использованием программ удаленного доступа, таких как «AnyDesk», «Team Viewer» и иных. Рассмотрим

на конкретном Примере! Злоумышленник связывается с жертвой зачастую путем мессенджера «Viber» и иных. В ходе разговора злоумышленник убеждает жертву в том, что он является работником банка и под предлогом защиты банковского счета от посторонних посягательств рекомендует установить на мобильный телефон из приложения «Play Market» либо «Арр Store» программу удаленного доступа: «AnyDesk», «Team Viewer» и иные. После установки жертвой вышеуказанной программы злоумышленник просит сообщить код идентификации данной программы, который отображается при входе в нее. Заполучив данный код, злоумышленник осуществляет удаленный доступ к устройству жертвы (мобильному телефону) и с использованием приложения М- Банкинг похищает путем перевода все имеющиеся у жертвы денежные средства.

Чтобы не стать жертвой злоумышленника следует соблюдать следующие правила:

1. Ни при каких обстоятельствах не передавать реквизиты своих банковских карт, паспортные данные, а также 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 И НИ ПОД КАКИМИ**

**ЛИБО ПРЕДЛОГАМИ НЕ ПЕРЕХОДИТ ПО ПРЕДОСТАВЛЕННЫМ СОБЕСЕДНИКОМ ССЫЛКАМ, В ТОМ ЧИСЛЕ ДЛЯ ПОЛУЧЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ! ЭТО ВАЖНО!**

1. Не выкладывать в публичный доступ/не вводить на каких-либо сайтах (в том числе появившихся после перехода по ссылке, предоставленной покупателем Вашего имущества) в сети Интернет данные своих банковских карт, номер мобильного телефона, а также иные паспортные данные.
2. Не устанавливать на свои устройства программы удаленного доступа типа «AnyDesk», «Team Viewer». До установки любой программы установите ее назначение с использованием поисковых сервисов в сети Интернет.

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

Старший оперуполномоченный

группы по противодействию киберпреступности

криминальной милиции Горецкого РОВД Александр Васильев