ВИШИНГ
как основной способ хищения денежных средств с банковских счетов

За два месяца 2021 года в отношении жителей г. Горки и Горецкого района совершено 14 фактов хищения денежных средств с банковских счетов граждан с использованием способа, получившего название «вишинг».

Вишинг- это один из методов интернет-мошенничества, связанный с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, к примеру), под различными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим банковским счетом/платежной картой.

Остановимся более конкретно на использовании данного способа для хищения денежных средств с банковских счетов. Злоумышленник связывается со своей будущей жертвой посредством мессенджера «Viber» либо же посредством звонка на мобильный телефон. В ходе состоявшегося разговора злоумышленник представляется зачастую работником банка и сообщает будущей жертве, что у нее пытаются похитить денежные средства с банковского счета путем перевода гражданину А. В свою очередь, для отмены данного перевода злоумышленник просит сообщить ему номер банковской карты либо же идентификационный номер паспорта. Заполучив данные сведенья, злоумышленник с их использованием осуществляет регистрацию в системе дистанционного банковского обслуживания соответствующего банка, после чего на мобильный телефон жертвы поступают в виде смс-сообщений сессионные коды, необходимые злоумышленнику для подтверждения регистрации. Заполучив данные коды, к примеру под предлогом отмены перевода денежных средств гражданину А., злоумышленник имеет возможность распорядиться денежными средствами жертвы, в том числе перевести их на банковские счета иностранных государств.

Что бы не стать жертвой злоумышленника и сохранить денежные средства на Вашем банковском счету, необходимо помнить следующее:

1. Ни при каких обстоятельствах не передавать реквизиты своих банковских карт, паспортные данные, а так же сессионные 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. 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.

Запомните! Денежные средства с банковского счета не могут пропасть «сами по себе». Если Вы никому не сообщите свои личные данные и

конфиденциальные сведенья, указанные на банковской карте (ее номер, срок действия, CVV/CVC код), а так же сессионные коды, Ваши денежные средства будут в сохранности и никто их похитить не сможет.

Ваша безопасность- в Ваших руках!

С уважением,
Первый заместитель начальника Горецкого РОВД-
начальник криминальной милиции Сергей Питяков