Хищение денежных средств путем модификации компьютерной информации

Звонки из «службы безопасности» банковских учреждений и продажа имущества в сети Интернет стоила некоторым жителям г. Горки и Горецкого района в 2021 году денежных средств, находившихся у них на банковских счетах и соответственно явилось одним из главных уроков в их жизни… Как говорится, век живи- век учись!

Остановимся подробнее на том, как злоумышленники похищали денежные средства с использованием реквизитов банковских карт и персональных данных граждан (например: **идентификационный номер паспорта**).

Гражданину на мобильный телефон либо же в одном из мессенджеров (Viber, WhatsApp и др.) поступает звонок от неизвестного ему лица, которое представляется работником «службы безопасности» какого-либо банковского учреждения (Беларусбанк, Белагропромбанк и др.). В ходе вышеуказанного разговора работник «службы безопасности» сообщает своему собеседнику, что у него с банковской карты (при этом может назвать часть ее номера либо номер полностью) неизвестные лица пытаются осуществить перевод денежных средств и задают вопрос: совершает ли данную операцию ее владелец. Ошеломленный такой новостью собственник банковской карты поясняет работнику «службы безопасности», что он каких-либо переводов на данный момент не совершает. После этого работник «службы безопасности» сообщает, что он пришлет сейчас на телефон смс-сообщение с кодом, который необходим для отмены данного перевода. В течении нескольких секунд на мобильный телефон собственника банковской карты поступает сообщение от соответствующего банковского учреждения, содержащее код, однако вышеуказанный код не является отменой какого-либо перевода, а является подтверждением регистрации в системе «Интернет-банкинга». Собственник банковской карты сообщает данный код работнику «службы безопасности», после чего у него с банковского счета вышеуказанным работником «службы безопасности» похищаются все денежные средства и в течении нескольких минут переводятся за пределы Республики Беларусь.

Что касается реализации имущества в сети Интернет, то хищение денежных средств происходит следующим образом. Гражданин размещает на каком-либо интернет-сайте (зачастую kufar.by) объявление о продаже имущества, например пальто. Злоумышленник связывается с гражданином с использованием переписки на вышеуказанном интернет-сайте, либо же мессенджерах (Viber, WhatsApp и др.). В ходе переписки злоумышленник заверяет продавца, что он готов купить его имущество и сообщает, что он оплатил его стоимость на соответствующем интернет-сайте, после чего предоставляет продавцу ссылку на фишинговый сайт (примеры ссылок: https://kufar.uk/item.php?1119676514, https://kufar.li/item.php?1119676514, https://kufar.cc/item.php?1119676514 и иные; указанные ссылки являются примерными образцами) и поясняет, что ему необходимо перейти по вышеуказанной ссылке и на появившемся интернет-сайте ввести реквизиты своей банковской карты (номер, срок действия, CVC/CVV код), после чего продавцу будут зачислены на банковский счет денежные средства. На самом же деле каких-либо зачислений продавец не получает, так как введя на фишинговым сайте реквизиты банковской карты он просто передает злоумышленнику доступ к своему текущему (расчетному) банковскому счету и с вышеуказанного банковского счета злоумышленник похищает все имеющиеся денежные средства.

Что бы уберечь Ваши денежные средства от хищения злоумышленником, ни при каких обстоятельствах нельзя сообщать посторонним лицам (даже если они представляются работником банка) следующие данные:

1. Информацию с обеих сторон Вашей банковской платежной карты: номер, дату окончания действия, CVV/CVC код.
2. Сеансовые ключи из SMS-рассылки, коды на отдельной карте, выданной в банке, логин и пароль, иные цифровые или буквенные коды.
3. Паспортные данные.

Если подобные звонки Вам поступили, сразу же завершите разговор, обратитесь в контакт-центр банка, выпустившего карту, по номеру с официального сайта или указанному на вашей карте, сообщите официальному сотруднику банка о случившемся и далее следуйте его рекомендациям.

Помните! Безопасность Ваших денежных средств- в Ваших руках!

С уважением,
Старший оперуполномоченный группы
по противодействию киберпреступности
криминальной милиции Горецкого РОВД Александр Васильев