Милиция Гродненщины предупреждает!

На территории области фиксируется рост хищений денежных средств, совершенных с использованием реквизитов банковских карточек, полученных злоумышленниками в ходе беседы по мобильному телефону от самих потерпевших. Злоумышленники, представляясь представителями службы безопасности банковских учреждений, входят в доверие граждан, и, получая необходимые реквизиты доступа к карт-счетам, совершают хищения денежных средств.

Под реквизитами карт-счета необходимо понимать:

16-значный номер карты, срок действия, имя владельца (эти данные указаны на лицевой стороне карты), обычно 3-значный С VC-код с обратной стороны карты, код подтверждения транзакции 3D-Secure (может задаваться пользователем либо формироваться процессинговым центром и направляться на мобильный номер владельца карты посредством SMS или push-уведомления);

логин и пароль доступа к системе дистанционного банковского обслуживания (интернет-банкинга), а также код подтверждения доступа с карты кодов либо динамический код, направленный на мобильный номер владельца карты посредством SMS или push-уведомления.

Наличие у третьих лиц указанной выше информации позволяет им совершать расходные операции в сети Интернет, например перевод средств на другие карты, приобретение электронных денег, оплату товаров и услуг в пределах баланса карточки. Доступ в интернет-банкинг позволяет распоряжаться депозитами клиента и оформлять заявки на получение кредитов.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем, либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства с использованием действующего в Беларуси принципа нулевой ответственности пользователей банковских карточек.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем можно предложить пользователям в любой ситуации не терять бдительность. В случае поступления сомнительных звонков от представителей банков, не передавайте им никаких реквизитов доступа к карт-счетам, логинов и паролей доступа к системе дистанционного банковского обслуживания (интернет-банкинга), даже если они называют Ваши анкетные данные, либо другую малоизвестную о Вас информацию. В случае поступления таких звонков, незамедлительно обратитесь в службу безопасности обслуживающего Вас банка и убедитесь в целостности карт-счетов.

Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!

УУР КМ УВД Гродненского облисполкома

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

** Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).*

*** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.