**Что нужно знать,** **чтобы не стать жертвой мошенников**

С развитием технологий значительно возросла доля различных проявлений мошенничеств в телекоммуникационной среде, совершаемых посредством телефонных звонков и в сети «Интернет».

Оградить от мошенников в первую очередь способны знания, внимательность, здравомыслие и критическая оценка ситуации. По­может и знание типичных «схем» работы мошенников и соблюдение правил, изложенных в данной памятке.

**Среди способов хищения денежных средств с банковских карт можно выделить следующие «схемы»:**

**1)    СМС или звонок из банка о блокировке карты.**

Вам приходит сообщение о том, что банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации, либо дойти до ближайшего банкомата и следуя «подсказкам» оператора самостоятельно разблокировать карту.

**Как обезопасить себя.**

Не торопитесь немедленно выполнять требования лица, представившегося сотрудником банка. Свяжитесь со службой поддержки клиентов самостоятельно. Скорее всего, Вам сообщат, что никаких сбоев и блокировок не происходило.

**2)    Хищение денег с использованием «мобильного банка».**

Самый простой способ хищения денежных средств с использованием услуги «Мобильный банк» следующий: потерпевшим, при заключении договора, указывается абонентский номер, который подключается к «Мобильному банку». В дальнейшем, лицо перестает длительное время пользоваться данным абонентским номером по различным причинам, при этом не отключив от него услугу «Мобильный банк», после чего оператор сотовой связи перевыпускает сим-карту. Новый пользователь сим-карты продолжает получать СМС-сообщения об операциях по банковской карте и, соответственно, получает доступ к управлению счетом через «мобильный банк».

Другой способ – заражение телефона вирусом, который дает злоумышленнику доступ к управлению СМС-сообщениями потерпевшего и, соответственно, доступ к «мобильному банку». Как правило, заражение происходит при переходе по ссылке, полученной в СМС-сообщении или «мессенджере».

**Как обезопасить себя.**Своевременно уведомляйте банк о смене номера телефона, не открывайте с телефона сомнительные ссылки из сообщений, используйте антивирусные программы.

**Рекомендации по безопасному использованию банковских карт:**

* Никогда и никому не сообщайте ПИН-код Вашей карты и пароли из СМС-сообщений от банка. **Ни сотрудники банка, ни любой другой организации** не вправе требовать их. Относитесь к ПИН-коду и паролю из СМС как к ключам от сейфа с вашими средствами.
* Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете заблокировать счет в случае хищения или утери карты. Лучше всего этот код запомнить.
* При возникновении каких-либо подозрений в мошенничестве связывайтесь с клиентской поддержкой банка, номер телефона которой сохраните заранее.
* Оплачивайте покупки с использованием реквизитов банковской карты только в проверенных интернет-магазинах или кассах продажи билетов. Лучше всего завести для этих целей отдельную карту (либо получить виртуальную карту, уточните в банке такую возможность), на которую переводить средства исключительно для совершения покупки.
* С осторожностью относитесь к предоставлению реквизитов своей банковской карты посторонним лицам.