Как не стать жертвой мошенничества с банковскими картами

Наибольшую массу от общего числа зарегистрированных краж с банковских карт граждан составляют хищения денежных средств путем массовой рассылки сообщений, содержащих ссылки, при переходе по которым осуществляется несанкционированное копирование специальной программы на Ваше мобильное устройство. Пользователь этого не замечает, так как его согласие на установку не запрашивается. Данная программа предназначена для выполнения действий по несанкционированному блокированию, модификации и копированию компьютерной информации и обеспечивает возможность удаленного доступа третьих лиц к Вашему устройству (в большинстве случаев – мобильному телефону или планшету). После этого злоумышленники осуществляют хищение денежных средств с банковских карт, при этом уведомления о списании денежных средств потерпевшим не поступают, так как блокируются вредоносной программой. Особо подвержены рискам гаджеты, с помощью которых используют «мобильные банки».

Одним из вариантов обезопасить себя от подобного рода преступлений является подключение услуги «мобильный банк» к абонентскому номеру, работающему на телефоне, не имеющем выход в сеть «Интернет» (резервный телефонный аппарат).

Также следует соблюдать следующие меры безопасности:

● *При использовании услуги «мобильный банк»:*

В случае потери мобильного телефона с подключенной услугой «мобильный банк» следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в контактный центр Банка для блокировки самой услуги.

При смене номера телефона, на который подключена услуга «мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью её отключения на старом абонентском номере и подключения на новый. Также необходимо помнить: если абонентский номер длительное время не используется владельцем, оператор связи может передать его другому абоненту. При этом предыдущий владелец о данной операции не уведомляется. В результате, услуга «мобильный банк» останется подключенной на номер, который принадлежит третьему лицу, и оно получает доступ к управлению Вашими финансами.

Не следует оставлять свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг другими лицами.

Не подключайте к услуге «мобильный банк» абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.

При установке на телефон дополнительных программ, необходимо обращать внимание на полномочия, которые Вы предоставляете программе. Обращайте внимание на такие опасные разрешения: доступ и отправка SMS, доступ к сети «Интернет» и т.д.

Рекомендуется установить на телефон антивирус и своевременно его обновлять.

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по SMS/MMS/электронной почте/мессенджерам, в том числе от имени Банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.

● *При пользовании банковскими картами:*

С целью исключения несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии.

В случае попыток третьих лиц лично, по телефону, в сети «Интернет», через социальные сети или другим способом, под различными предлогами узнать полные данные о вашей карте: номер, срок действия, данные владельца, трехзначный код проверки (на обратной стороне карты), пароли и т.д. - будьте осторожны - это признаки противоправной деятельности. Рекомендуется прекратить общение.

Во избежание использования карты другим лицом, следует хранить ПИН-код отдельно от карты, не писать ПИН-код на карте, не сообщать ПИН-код другим лицам (в том числе родственникам).