опасные разрешения: доступ и отправка SMS, доступ к сети «Интернет» и т.д.

Рекомендуется установление на телефон антивирусного программного обеспечения и своевременное его обновление.

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

При пользовании банковскими картами:

С целью избежания несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения какого-либо лица лично, по телефону, в сети «Интернет», через социальные сети или другим способом, которое под различными предлогами пытается узнать полные данные о вашей банковской карте: шестнадцатизначном номере, сроке действия, данных владельца, трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты и т.д. (паролях или другой персональной информации), будьте осторожны - это явные признаки противоправной деятельности. При любых сомнениях рекомендуется прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

Не следует прислушиваться к советам третьих лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обращаться к сотрудникам филиала банка или позвонить по телефонам, указанным на устройстве или на обратной стороне карты.

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).

В случае, если Вы стали жертвой мошенников обращайте в полицию по номеру 102

Прокуратура города Щекино

ПАМЯТКА

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Количество хищений у граждан, совершаемых с использованием информационно-коммуникационных технологий с каждым годом становиться все больше и больше.

ВАЖНО помнить, что мошенничества с использованием средств сотовой связи совершаются, в основном, путем сообщения гражданам заведомо ложной информации:

- под видом сотрудников полиции, о нарушении их близкими родственниками действующего законодательства, с целью передачи

потерпевшими денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившейся ситуации;

- о блокировке банковской карты путем рассылки SMS-сообщений, а так же о переводе денежных средств за покупку товара по объявлению и последующего информирования о необходимости дальнейшего введения ряда команд с банкомата;

- о возможности получения компенсации за ранее приобретенные некачественные товары или оказанные услуги, для чего необходимо перечислить определенный процент от полагающейся суммы;

- о сообщении Вам, якобы, из поликлиники или больницы, что у Вас или у Ваших родственников обнаружили страшный диагноз и чтобы вылечить болезнь необходимо перевести деньги за лекарства;

- получения СМС-сообщений с неизвестных номеров о выигранном призе, с просьбой положить деньги на телефон, или вернуть деньги, так как они были переведены ошибочно;

- с просьбой купить продукты или сделать заказ, доставить их по указанному адресу, а попутно перечислить денежные средства на телефон, с заверением, что деньги вернут по прибытию на адрес заказчика.

При этом мошенники стараются держать «жертву» всегда на связи, с целью исключения каких-либо действий с ее стороны.

Как понять обман:

- необходимо перезвонить на известные абонентские номера лицу, которым представляется злоумышленник, либо родственникам, с целью выяснения действительности произошедших событий;

- попросить звонящего назвать какие-либо данные лица, которым он представляется (Ф.И.О., дата рождения, место жительства, данные родственников, какие-либо факты из жизни и т.д.).

- никому нельзя сообщать реквизиты своей банковской карты, в том числе сотруднику банка, об этом всегда информируют банк при получении пароля к карте, в последствие необходимо лично обратиться в ближайшее отделение банка, с целью выяснения возникших проблем с банковской картой;

- различные компенсации выплачиваются гражданам только при их личном письменном обращении, никаких процентов за выплату компенсаций платить не надо;

- настоящий врач никогда не будет звонить Вам по телефону и сообщать о страшном диагнозе или просить перевести деньги за лекарства;

- в случае получения СМС-сообщений с неизвестных номеров, помните - это мошенники, человек не может выиграть приз, не участвуя в лотереях, родственники не будут Вам высылать СМС-сообщения с неизвестных номеров;

- если вы исполняете какое-либо поручение по телефону, доставляете заказы, не надо переводить деньги на незнакомые телефоны, сначала доставьте товар по назначению;

Как не стать жертвой мошенничества с банковскими картами

При использовании услуги «Мобильный банк»:

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением «Сбербанк Онлайн» следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» и/или «Сбербанк Онлайн».

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью отключения услуги «Мобильный банк» от старого номера и подключения на новый. Также необходимо помнить, что операторы сотовой связи, в случае длительного неиспользования номера, могут передать его другому абоненту, при этом услуга «Мобильный банк» останется подключенной.

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 необходимы программе. Если программе требуются излишние полномочия - это повод проявить настороженность. Обращайте внимание на такие