Рекомендуется установление на телефон антивирусного программного обеспечения и своевременное его обновление.
Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие поSMS/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 кого-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 случае, если имеются основания полагать, что в отношении Вас предпринимаются мошеннические действия, либо Вы уже стали жертвой мошенничества, необходимо незамедлительно обращаться в правоохранительные органы.

ТЕЛЕФОН ОМВД России по Колпашевскому району УМВД России по Томской области:

02 или 8(38254) 79206, 8(38254) 79286

Прокуратура Российской Федерации

ПРОКУРАТУРА ТОМСКОЙ ОБЛАСТИ

КОЛПАШЕВСКАЯ ГОРОДСКАЯ ПРОКУРАТУРА

ПАМЯТКА

о том, что каждому надо знать, чтоб не стать жертвой телефонного и интернет мошенничества

КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННОГО и ИНТЕРНЕТ МОШЕННИЧЕСТВА

ЦЕЛЬ МОШЕННИКА—заставить Вас передать свои денежные средства “добровольно”. Для того, чтобы не стать жертвой таких преступлений необходимо помнить о том, что преступники стараются максимально правдоподобно представить жизненную ситуацию и заставить Вас передать свои денежные средства “добровольно"

Сообщение-просьба о помощи

ПРИМЕР: На мобильный телефон, «якобы», от близкого человека поступает сообщение о необходимости срочного перевода определенной суммы на телефон, причину которого объяснят позже.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Объясните своим близким, что на SMS такого характера реагировать не стоит, для уточнения информации лучше созвониться с «якобы» нуждающимся в переводе денег лицом.

Телефонный номер-грабитель

ПРИМЕР: Вам поступает сообщение с просьбой перезвонить на определенный номер мобильного телефона. Например – помощь другу, изменение тарифов связи, проблема с банковской картой. При звонке Вас длительное время держат на связи, но не беседуют, а после отключения, оказывается, что со счёта списана крупная сумма.

МЕХАНИЗМ: Существуют сервисы с платным звонком, чаще всего это развлекательные, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

ЧТО ДЕЛАТЬ: Не звоните на незнакомые номера. Каждому пользователю мобильного телефона хотя бы раз в жизни поступало уведомление о рекламной акции, выигрыше в лотерею или проведению розыгрыша подарков с участием операторов связи, известных теле-радио каналов. Мошенники часто используют их для прикрытия своей деятельности, поздравляя Вас с выигрышем и предлагая сообщить код карты экспресс-оплаты, которые упростили процедуру зачисления денежных средств на счет, но одновременно и стали новым способом хищения денежных средств мошенниками.

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Мошенничеств с банковскими картами

Банковская карта – инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

ПРИМЕР: Вам приходит SMS-сообщение о том, что Ваша банковская карта заблокирована, а для получения подробной информации необходимо перезвонить на указанный в сообщении номер. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой и просят сообщить номер карты и ПИН-код для ее перерегистрации.

МЕХАНИЗМ: Как только Вы сообщите номер карты и код от нее - деньги будут сняты.

ЧТО ДЕЛАТЬ: Удостоверьтесь в правдивости информации в службе поддержки Вашего банка. **Не сообщайте свой ПИН-код никому.**

Меры безопасности:

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