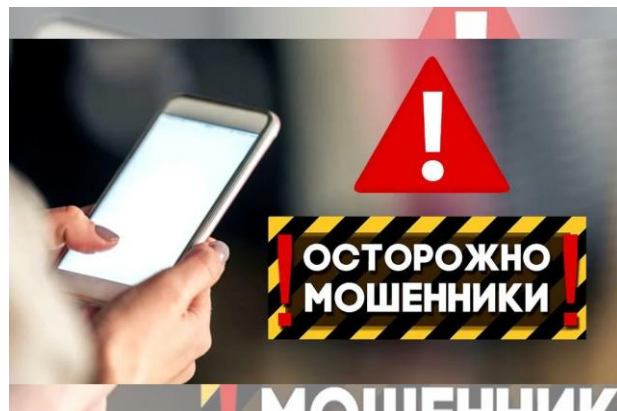




Прокуратура г. Стрежевого
Томской области

ПРЕДУПРЕЖДАЕТ



Основные схемы IT и телефонного мошенничества:

Ошибочный перевод средств

ПРИМЕР:

Вам приходит SMS-сообщение о поступлении денежных средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат. Сразу после этого поступает звонок или SMS о том, что на Ваш счет ошибочно переведены деньги, которые просят вернуть обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите деньги, после чего такая же сумма списывается с Вашего счёта.

МЕХАНИЗМ:

Чтобы во второй раз списать сумму с Вашего счёта, мошенник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер.

То есть первый раз Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

ЧТО ДЕЛАТЬ:

Предложите звонящему использовать для возврата денег чек из терминала.

Если в ответ сообщат о его утрате, скорее всего, с Вами общается мошенник, просьбы которого выполнять не следует.



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. Реклама таких сервисов всегда информирует о том, что звонок платный. 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 счёт, но одновременно и стали новым способом хищения денежных средств мошенниками.

МОШЕННИЧЕСТВО 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.

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ:

ПИН-код необходимо запомнить и не хранить его рядом с картой, например, в кошельке, сумке, мобильном телефоне. Так, в случае утраты или хищения карты, Вы успеете обезопасить свой счёт, заблокировав ее.

Если Вам позвонили из какой-либо организации или Вы получили письмо по электронной почте с просьбой сообщить реквизиты карты и ПИН-код по различным причинам, то не спешите ее выполнять. Позвоните в службу поддержки банка и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям его сотрудника.

Номер телефона службы помощи банка должен быть в списке контактов Вашего мобильного телефона.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения или охраной, например, в государственных учреждениях, банках, крупных торговых центрах.

При возможности посещения банка старайтесь не использовать карту в уличных банкоматах.

Обращайте внимание на картоприемник и клавиатуру банкомата. Они не должны быть оборудованы какими-либо дополнительными устройствами.

Все действия с пластиковой картой в ресторанах, кафе, магазинах, супермаркетах и других местах должны происходить в Вашем присутствии.



*Прокуратура г. Стрежевого Томской области
636785, г. Стрежевой, ул. Кедровая, 71
Тел.: 8 (382-59) 3-68-62*