

Распространенные виды мошенничества

Рассказываем про разные виды мошенничества и объясняем, как их можно избежать.

Ложное SMS о блокировке банковской карты

Свернуть ^

Примеры текстов мошеннических рассылок:

- «Ваша банк.карта заблокирована!Инф.тел.8(902)294-52-89.»;
- «Заявка на перевод 9000 руб. с Вашей карты принята. Инф: 89925254984»;
- «Ваша банковская карта заблокирована.Информация по номеру 79022944761.ЦБ/РФ».

Ситуация:

Получено SMS о блокировке банковской карты, с указанием номера для связи. Позвонив, можно получить инструкцию о разблокировке. Ее выполнение приведет к краже средств с банковской карты.

Выход:

Получив SMS из банка, не нужно перезванивать по указанным там номерам. Необходимо найти номер банка в открытых источниках (на официальном сайте, в договоре на услуги данного банка) и воспользоваться именно им. Обычно, банки указывают круглосуточные бесплатные номера на самой карте.

Родственники в беде

Свернуть ^

Примеры текстов остановленных мошеннических рассылок:

- «Мама, пополни счет номер 79646190450, не звони, потом все объясню»;
- «мам, срочно положи 2500 р. на 79605920943, позже объясню, выручи»;
- «Привет это Света, положи мне на этот номер 100 рублей, завтра приеду отдам».

Ситуация:

Получено SMS якобы от близкого родственника о критической ситуации и с просьбой срочно пополнить указанный номера телефона. Выполнение просьбы приведет к переводу денег мошенникам.

Выход:

Прежде всего, необходимо позвонить «попавшему в беду» родственнику или тем, кто может быть рядом с ним, и выяснить, все ли с ним в порядке.

Подписка на незнакомые развлекательные сервисы

Свернуть ^

Ситуация:

Регулярно начали поступать SMS от некоего развлекательного сервиса, на который вы не подписывались.

Выход:

Наберите USSD-команду *189#

На ваш номер придет SMS со списком активных подписок и командами по их отключению.

Чтобы обезопасить себя от интернет-подписок в будущем, наберите *931#.

Поступление «ошибочного» платежа

Свернуть ^

Ситуация:

Получено SMS о пополнении баланса телефона на небольшую сумму. Через несколько минут с неизвестного номера приходит SMS с просьбой вернуть ошибочно зачисленные деньги. Выполнение просьбы ведет к переводу средств мошенникам, а «SMS о пополнении» оказывается обманом.

Выход:

Не переводить деньги на неизвестные номера. Возврат платежей производится оператором сотовой связи.

Использование мобильного банка

Свернуть ^

Ситуация:

Утрачен телефон, номер которого был привязан к банковской карте.

Выход:

Нужно срочно заблокировать или отключить мобильный банк, чтобы предотвратить возможную кражу средств злоумышленниками.

Ситуация:

Изменился телефонный номер, что привело к утрате доступа к мобильному банку.

Выход:

Обратитесь в банк, который выпустил вашу карту.

Ссылка на скачивание MMS, фотографии или открытки

Свернуть ^

Примеры текстов остановленных мошеннических рассылок:

«У вас новое ммс от номера 9198453322. Смотрите информацию на сайте <http://ru4.ru/2tf>»;
«Приколись с этого приложения:) <http://goo.gl/Q3WR>»;
«Мое фото [htt://ru4.ru/2tf](http://ru4.ru/2tf). Алена».

Ситуация:

Получено SMS с интригующей ссылкой. При переходе по ссылке загружается фотография нейтрального характера, а параллельно скачивается вредоносное ПО. В числе возможных последствий - кража средств со счета телефона и привязанной к номеру банковской карты.

Выход:

Не переходить по ссылкам внутри SMS сообщений, полученных из неизвестных источников. Если избежать этого не удалось, нужно проверить телефон на наличие вирусов. [Пользователям ОС Android](#) в этом поможет приложение «[Mobile Security Tele2](#)».

Просьба «закинуть денег на счет»

Свернуть ^

Ситуация:

Мошенники представляются сотрудниками государственных учреждений и делают заказы на доставку товара или оказание услуг в своем офисе на крупные суммы. По пути в указанный офис работников просят выполнить несколько мелких просьб, среди которых пополнение счета указанного номера, с обещанием возврата средств в офисе. Выполнение просьбы ведет к переводу средств мошенникам, а «офис» оказывается обманом.

Выход:

Не переводить деньги на неизвестные номера. Вернуть обратно переведенные деньги будет практически невозможно.

Выигрыш ценного приза

Свернуть ^

Примеры текстов остановленных мошеннических рассылок:

«внимание! ваш платеж через терминал призовой. Приз авто - мазда 5 (819000руб)
потребности по тел +79042225123 Компания евротелефон»;
«Ваш номер обладатель Шевролет Авео. Инфо по номеру 79469903954»;
«Pozdravlaem vash nomer obladatael avto Chevrolet AVEO inf.8(846)990-39-54 www.kapella-63.ru».

Ситуация:

Получено SMS о выигрыше приза с указанием номера для связи. Позвонив, можно узнать условия получения приза, среди которых оплата государственной пошлины. Инструкцию по оплате «пошлины» мошенники также предоставляют. Ее выполнение приведет к переводу денег мошенникам.

Выход:

При получении такого SMS не нужно торопиться звонить по указанному номеру. Необходимо убедиться, что заявленная компания-организатор действительно проводит эту акцию. Получить справку всегда можно на официальном сайте компании или по контактными данным в открытых источниках.