



ОСТОРОЖНО: МОШЕННИКИ! НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) sms-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!



БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель — узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «Финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».



ВИРУС В ТЕЛЕФОНЕ



Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не переходите по сомнительным ссылкам.

Вы получили sms-сообщение о том, что ваша банковская карта заблокирована или с вашей карты происходит списание денежных средств.



НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных sms. Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей банковской карты.

звонят и называют Вас по имени и отчеству, то есть они уже заранее подготовились к разговору и узнали определенную информацию о Вас. В большинстве случаев, аферисты просят своих собеседников не отключать сотовый телефон, быть с ними на связи. Далее они убеждают потерпевших зайти в мобильное приложение или прийти к ближайшему банкомату с целью совершения определенных денежных операций. Как правило, мошенники стали использовать номер телефона, в котором указан московский код города 8(495) или 8(499). Увидев на экране сотового телефона данную комбинацию цифр, граждане теряют бдительность и начинают вступать в диалог с аферистами.

Вы продаете или покупаете какой-либо товар по объявлениям, размещенным на интернет-сайтах, сдаёте или хотите арендовать жилье и для перевода денежных средств помимо номера банковской карты Вас просят назвать ещё ПИН-код, код безопасности (это три последние цифры, расположенные сзади банковской карты), а также пароли из телефонных sms-сообщений. Никогда и никому не сообщайте эти данные!



При продаже товара в Интернете не сообщайте данные карты потенциальному покупателю, просите расчёт наличными. Не приобретайте товары в сомнительных интернет-магазинах, это могут оказаться мошенники. Так, житель Белоярского района на сайте — двойнике решил приобрести снегоход стоимостью 700 тысяч рублей. Внес 100% оплату за транспортное средство, после чего менеджер компании перестал выходить на связь и сайт, на котором оформлялся заказ в настоящее время не существует.

Не перечисляйте денежные средства, не убедившись в надежности адреса!



С осторожностью относитесь к предложениям, обещающим более высокий процент возврата по кэшбэку!

Такая схема обмана все чаще стала появляться в полицейских сводках региона.

Неизвестные звонят и представляются банковскими работниками, предлагая оформить кэшбэк по банковским картам с каждой покупки при расчёте с помощью электронных средств платежа. При этом для возврата денег злоумышленники запрашивают помимо реквизитов карты иные конфиденциальные данные, которыми сотрудники банка обычно не интересуются. Таким образом, потерпевшие сами предоставляют доступ к управлению своими счетами.

В случае, если кто-то все же стал жертвой мошенников, нужно сразу же обратиться в банк и полицию с заявлением об отмене операций и возврате денежных средств.



Помните о том, что отдать персональные сведения о карте или кредитке посторонним — это всё равно, что подарить свой кошелек. Ни в коем случае не оставляйте карты без присмотра и не записывайте пин-код в доступных местах. Ни работники банка, выдавшего карту, ни обслуживающий персонал банкомата не вправе требовать таких данных.

Если вы храните на карте достаточно большую сумму, установите лимиты на одновременное снятие и на дневной оборот наличных. Будет полезным подключить SMS-оповещение к вашей карте. Услуга стоит недорого и поможет держать ваш электронный кошелек под контролем. Вы сразу же узнаете о том, что по вашей карте была совершена незаконная операция.

Одно из важных правил — никогда не сообщайте CVV2-код, указанный на оборотной стороне карты.



Чтобы не попасть на мошенничество «ВКонтакте» или «Одноклассники», желательно следовать нескольким простым правилам:

- уточните у адресата, от которого пришло странное сообщение, отправлял ли он вам его.
- Если он ничего не отправлял, не выполняйте никаких указаний из письма;
- старайтесь не добавлять «в друзья» незнакомых людей;
- не используйте очень простой пароль для входа на вашу страничку или сайт.