



Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

- Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;
- Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;
- Под надуманными предложениями просят сообщить PIN-код банковской карты, содержащиеся на ней данные;
- Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

- Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;
- Сотрудник банка может запросить у клиента только контрольное слово, ФИО;
- При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;
- Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;
- При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

- Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;
- Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;
- Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону **02** (со стационарных телефонов) или **102** (с мобильных средств связи) или в дежурную часть территориального органа внутренни



Памятка безопасности при онлайн-покупке товаров и онлайн-оплате услуг

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

Злоумышленники:

- Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем;
- Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина;
- Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен;
- После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

- неоправданно низкая цена на товар;
- электронная почта или мессенджеры в качестве способов коммуникации;
- оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;
- обязательная предоплата, зачастую более половины стоимости товара;
- отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт;
- сомнительный интернет-адрес.

Запомните!

- Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;
- Самый безопасный способ оплаты - после получения заказа;
- Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предложениями (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки).

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону **02** (со стационарных телефонов) или **102** (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.



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 страницей 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 предложениями.



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!

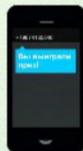


БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

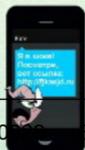
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

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, и отправляют SMS-сообщения по ссылкам.

ЭЛЕКТРОННЫЙ
ТАТАРСТАН



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ



Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке



Вам позвонили/прислали SMS «из банка» с неизвестного номера



- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы

Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»



Вы заподозрили интернет-продавца в недобросовестности



- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после
- Никогда не переводить незнакомым лицам

61/10926

**ЭЛЕКТРОННЫЙ
ТАТАРСТАН**



ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?

ТЕЛЕФОН



Представляются сотрудниками банка, сообщают, что совершен перевод денег с вашего счета



ПРЕРВАТЬ РАЗГОВОР

НАБРАТЬ НОМЕР ВАШЕГО БАНКА

Под видом близкого родственника, попавшего в беду, просят деньги за решение проблемы



ПРЕРВАТЬ РАЗГОВОР

НАБРАТЬ ЭТОМУ РОДСТВЕННИКУ

Предлагают товар и просят сообщить домашний адрес для доставки



ПРЕРВАТЬ РАЗГОВОР

НЕ СООБЩАТЬ СВОИ ДАННЫЕ

ИНТЕРНЕТ



Покупка вами товаров



ОПЛАТА ТОЛЬКО ПРИ ПОЛУЧЕНИИ: ПОЛУЧИЛ ТОВАР-ЗАПЛАТИЛ ДЕНЬГИ

Продажа ваших товаров



НЕ СООБЩАТЬ ПОКУПАТЕЛЯМ СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ

ДОМА



К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников



НЕ ОТКРЫВАТЬ ДВЕРЬ

НАБРАТЬ НОМЕР БЛИЗКОГО ЧЕЛОВЕКА, СОСЕДЕЙ



МВД Татарстана предупреждает:

Если вам звонят и сообщают:



Совершен перевод денег с
вашего счета



Нужно срочно блокировать счет



К вашему счёту получили доступ
мошенники или совершены другие
действия со счётом

Номер банка



Секретный код

ЗАПОМНИТЕ!

ВСЕ МОШЕННИЧЕСКИЕ ОПЕРАЦИИ

БАНК БЛОКИРУЕТ САМОСТОЯТЕЛЬНО

БЕЗ ЗВОНКА КЛИЕНТУ



Телефоны для связи с полицией:

**ПРЕРВАТЬ
РАЗГОВОР!**

**НАБРАТЬ
НОМЕР БАНКА**

**02
112**



Мошенничество с использованием сайтов-дублеров благотворительных организаций

В сети интернет регулярно размещаются объявления от лица благотворительных организаций, детских домов, хосписов, приютов и др. с просьбой о материальной помощи.

Злоумышленники:

- Создают сайт-дублер, являющийся точной копией оригинального;
- Меняют реквизиты для перечисления денежных средств.

Запомните!

Прежде чем помочь какой-либо организации:

- Позвоните по телефону в указанную организацию;
- Уточните номер расчетного счета, либо посетите ее лично;
- Убедитесь в достоверности размещенной информации.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону **02** (со стационарных телефонов) или **102** (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.