

Незнакомец неожиданно связывается с вами

1

Например, от имени банка, полиции, магазина. Способы могут быть разные — звонок, СМС или ссылка в мессенджере.

Общее у них одно — кто-то сам вышел на связь с вами. Значит ему что-то от вас нужно.



С вами говорят о деньгах



Основная задача мошенников — получить доступ к чужим деньгам.

Вам могут предложить:

- Перевести все деньги на «безопасный счет».
- Оплатить «страховку для получения кредита».
- «Очень выгодно» инвестировать свои сбережения.

И многое другое. Главное: речь всегда будет идти о деньгах.



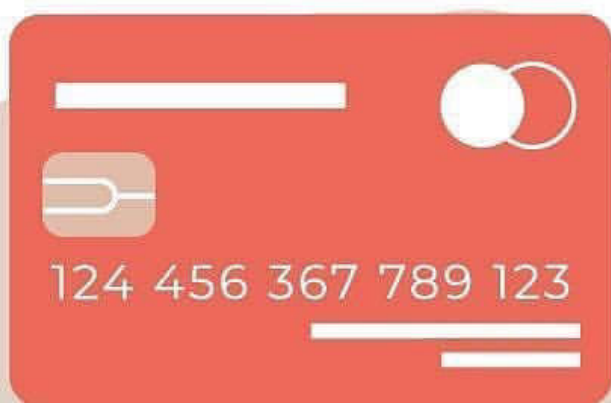
Вас просят сообщить данные



Обычным вора́м нужен ключ от квартиры, мошенникам — «ключ» от вашего счета:

- Срок действия карты и CVC-код.
- Логины и пароли к приложению банка или личному кабинету на сайте.
- Коды из банковских уведомлений.

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.



Назовите код из СМС

Сообщите 3-значный код на обратной стороне вашей карты



Вас выводят из равновесия



Мошенники стремятся вызвать у вас сильные эмоции – напугать или обрадовать.

Например, сообщают:
«Ваш онлайн-банк взломали!».

Злоумышленники хотят, чтобы вы растерялись и выдали любую информацию, лишь бы спасти деньги.

Еще вас могут обрадовать внезапным «выигрышем в лотерею». Взамен нужно лишь оплатить комиссию на сайте. С которого, конечно, мошенники уведут данные вашей карты.

Не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.

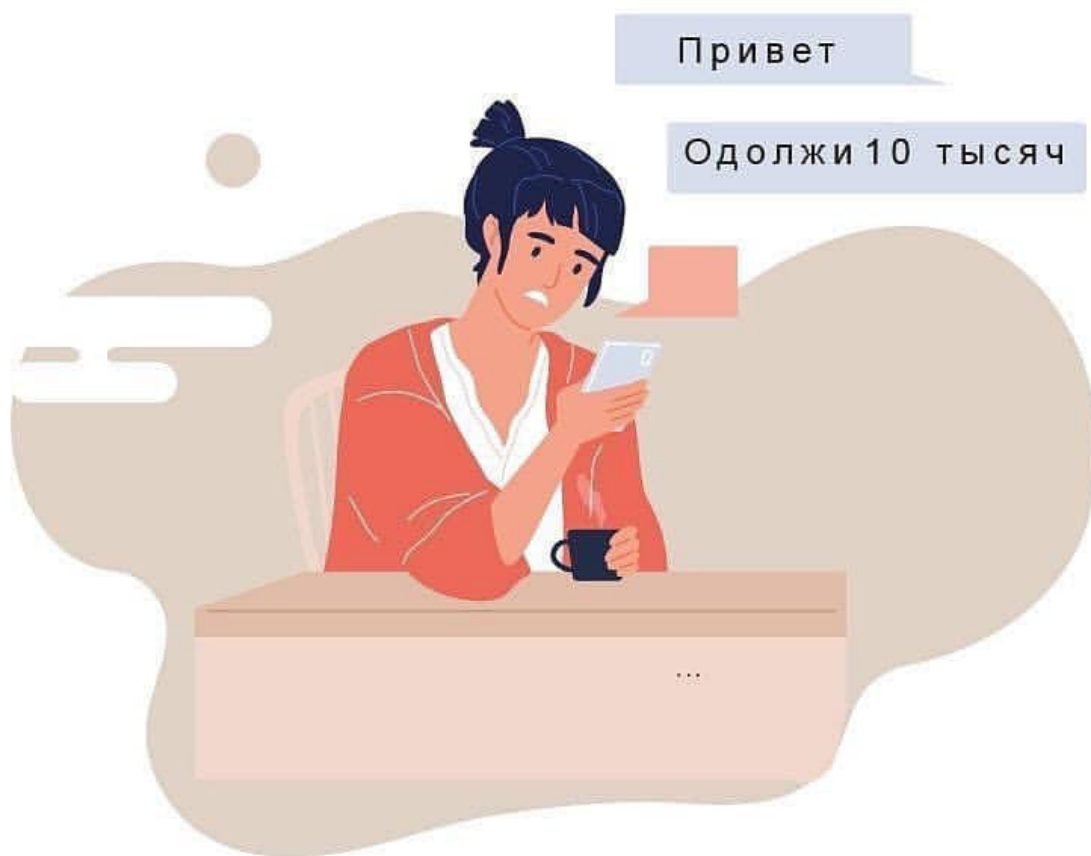


На вас давят:

5

- Торопят.
- Принуждают к чему-то.
- Ставят условия «сейчас или будет поздно».

Такие ситуации подозрительны.
Поэтому общение лучше прекратить сразу.





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 внутренних дел.



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 предлогами (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.



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.



МВД РОССИИ ПРЕДУПРЕЖДАЕТ

будьте бдительны! звоните **02** или **102**

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым

людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста!



НЕ ДОВЕРЯЙТЕ,

если Вам звонят и сообщают, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться.

Это ОБМАН!

СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ

Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!



Не подписывайте никакие документы!



Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам?

НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!