



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ



ОМВД РОССИИ
ПО ХОХОЛЬСКОМУ РАЙОНУ
тел. 5(47371)41202, 41210

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 (с банка Вам ни когда не позвонят)
- 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 получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты



КАК РАСПОЗНАТЬ ТЕЛЕФОННОГО МОШЕННИКА

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

**ЕСЛИ ВАМ СООБЩИЛИ
ПО ТЕЛЕФОНУ, ЧТО:**

- ▶ ваша банковская карта заблокирована
- ▶ необходимо пополнить баланс неизвестного номера телефона...
- ▶ нужны деньги, чтобы спасти попавшего в беду родственника
- ▶ вы выиграли приз...
- ▶ вам полагается компенсация...



ПРЕКРАТИТЕ РАЗГОВОР

ПОМНИТЕ: это орудуют
телефонные мошенники!

ГУ МВД РОССИИ ПО ВОРОНЕЖСКОЙ ОБЛАСТИ

ВСЕГДА НА СВЯЗИ

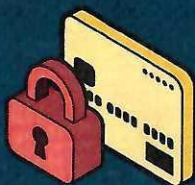
102 / 112



Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ



Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КODOBEE CЛOBO

называйте только сотруднику банка, когда сами звоните на горячую линию



Банк не компенсирует потери, если вы нарушили правила безопасного использования карты



Подробнее о правилах безопасности
читайте на fincult.info



Финансовая
культура



ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

МОШЕННИКИ:



Здравствуйте, Вера Петровна!
Я сотрудник БАНКА.

ЛОЖЬ

Добрый день! Я сотрудник
правоохранительных органов. Вы
приобрели некачественные БАДы,
за них Вам положена КОМПЕНСАЦИЯ
и мы ВЕРНЁМ деньги.

ЛОЖЬ



**ПРЕКРАТИТЕ
РАЗГОВОР**



СОВЕТ:

Убедитесь в том, что Вам звонили из банка,
перезвонив по НОМЕРУ, указанному на
ОБОРОТЕ Вашей БАНКОВСКОЙ КАРТЫ

ТАКЖЕ СТОИТ ЗНАТЬ:

**СМС
ИЗ БАНКА**



НИКОМУ
НЕ СООБЩАЙТЕ
СОДЕРЖИМОЕ
СМС-СООБЩЕНИЯ



НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ НА НОМЕРА
ТЕЛЕФОНОВ ИЗ СМС-СООБЩЕНИЙ
ТАКОГО ТИПА:

- ⚠ "МАМА, У МЕНЯ ПРОБЛЕМЫ, ПОПОЛНИ СЧЕТ"
- ⚠ "ВЫ ВЫИГРАЛИ ПРИЗ - ДЛЯ ЕГО ПОЛУЧЕНИЯ ОПЛАТИТЕ НАЛОГ"
- ⚠ "ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО ВАШЕМУ КРЕДИТУ. ТЕЛ: ..."



**ВСЁ-ТАКИ ПЕРЕВЕЛИ
ДЕНЬГИ МОШЕННИКАМ? -
СРОЧНО ЗВОНИТЕ
В БАНК!**

Сообщить о факте мошенничества:

02 / 102

со стационарного
телефона

с мобильного
телефона

либо обратиться в ближайший отдел полиции



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.



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.**

СОТРУДНИК БАНКА НИКОГДА НЕ ЗАПРОСИТ У ВАС:

данные банковской карты;

коды и пароли из СМС-сообщений,
поступающих из банка.



ЧТО ГОВОРЯТ МОШЕННИКИ?

...мы заметили подозрительную активность
на Вашем счету.
Для проверки Вам придет СМС-сообщение.
Продуктите мне код, присланный в нём.



**ОСТАНОВИСЬ!
НЕ СООБЩАЙ КОД!**

Сделки в соцсетях и
на торговых площадках



**НЕ ВНОСИТЕ
ПРЕДОПЛАТУ ЗА ТОВАР!**

**ВСТРЕЧАЙТЕСЬ
С ПРОДАВЦАМИ ЛИЧНО!**

САЙТЫ-БЛИЗНЕЦЫ или «ФИШИНГОВЫЕ» САЙТЫ

ОБРАЩАЙТЕ ВНИМАНИЕ
НА ПОДМЕНУ СИМВОЛОВ
В АДРЕСЕ САЙТА!

ПРИМЕР:

подлинный сайт
gosuslugi.ru

сайт мошенников
gosuslugi.ru



СДЕЛКИ НА БИРЖЕ

**ИГРАЕТЕ НА БИРЖЕ
И ВАМ ПРЕДЛАГАЮТ
БРОКЕРСКИЕ УСЛУГИ?**

- 1 Запрашивают удаленный доступ
к Вашему компьютеру
- 2 Просят установить неизвестное
Вам приложение
- 3 Просят данные к банковским
онлайн-сервисам

**ПРЕКРАТИТЕ
С НИМИ
РАЗГОВОР -
ЭТО АФЕРИСТЫ!**



Сообщить о факте мошенничества:

102 / 112

либо обратиться в
ближайший отдел полиции

