



ОСТОРОЖНО: МОШЕННИКИ!



Вам звонят из банка и просят сообщить персональные данные или информацию о карте/счете — **ВНИМАТЕЛЬНО!** ЭТО МОГУТ БЫТЬ МОШЕННИКИ!

Мошенники с помощью специальных технологий могут сделать так, что на экране вашего телефона высветится официальный номер банка.

Они могут обратиться к вам по имени-отчеству и поговорить секретные сведения о карте или счете. Например, чтобы оставить персонализированное сообщение.

В ЧЕМ ОПАСНОСТЬ И ЧТО ДЕЛАТЬ?

Узнав важную информацию, преступник может украсть ваши деньги.

- Не говорите и не вводите ПИН-код, трехзначный код, с обратной стороны карты, или парольный пароль на СМС.
- Не набирайте на телефоне номера комбинаций и не переходите по ссылкам.
- Положите трубку. Позвоните в банк по официальному номеру — он есть на сайте или обратной стороне карты.
- Самостоятельно наберите номер на клавиатуре телефона. Не переключайте обрешетку экрана, вы можете снова попасть к мошенникам.



ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ



1. Звоните в Банк России
Наберите номер вручную. Телефон горячей линии указан на обратной стороне карты и на официальном сайте Банка.

Позвонив на номер, с которого пришел звонок или сообщение, вы рискуете снова попасть к мошенникам.



2. Сосредоточьтесь
Если банк выдает государственную транзакцию, он приостановит ее на срок до двух суток.

У вас есть 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.



3. Не говорите никому секретные коды
Если вас убеждают предоставить или ввести СМС/СМС-код на обратной стороне карты, ПИН-код или код на СМС — это мошенник!

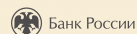
Назвать кодовые слова можно, только если вы сами звоните на горячую линию Банка.

Позвоните о том, как защититься от обмана и финансовых мошенников, читайте на сайте fincult.info



Контактный центр Банка России:
8 800 300-30-00
(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:
www.cbr.ru/reception



ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА



1. НА ВАС ВЫХОДИТ САМИ

Аферисты могут представиться службой безопасности Банка, налоговой, прокуратурой.

Любой неожиданный звонок, СМС или письмо — повод насторожиться.



2. РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность.



3. НА ВАС ДАВЯТ

Аферисты хотят принуждать, чтобы у вас не было времени все обдумать.



4. ГОВОРЯТ О ДЕНЕГАХ

Предлагают деньги, сбережения, получить компенсацию или вложиться в инвестиционный проект.



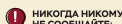
5. ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Мошенники пытаются узнать реквизиты карты, пароли и коды из Банковских уведомлений.



ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты.



НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на обратной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовые слова
- персональные данные



Как защитить свои финансы, читайте на fincult.info



СМС, МЕССЕНДЖЕРЫ, СОЦСЕТИ



Вам пришло СМС от банка с информацией:

- о заблокированном платеже или карте;
- о выигрыше;
- об ошибочном переводе на ваш банковский счет или мобильный телефон с просьбой вернуть деньги.

— Что делать?



НЕ ПЕРЕХОДИТЕ ПО ССЫЛКЕ И НЕ ПЕРЕЗВАНИВАЙТЕ!

Проверьте информацию, позвонив в банк по номеру, который указан на вашей банковской карте.



Знакомый в соцсетях просит дать в долг или перевести деньги на лечение.

— Что делать?



НЕ ПЕРЕВОДИТЕ ДЕНЕГ ИЛИ СРАЗУ!

Позвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страница взломана.

Контактный центр Банка России

8 800 300-30-00
(бесплатно для звонков из регионов России)

+7 499 300-30-00
(в соответствии с тарифами вашего оператора)

300
(бесплатно для звонков с мобильных телефонов)

Все представленные номера доступны для звонков круглосуточно

Банк России не совершает исходящих звонков с указанных номеров

fincult.info
только читать! ПОДЛЕЖИТ ЗАЩИТЕ



ОСТОРОЖНО: МОШЕННИКИ!

НИКОГДА НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ ЛЮДЯМ ТРЕХЗНАЧНЫЙ КОД НА ОБВОРОТЕ КАРТЫ, PIN-КОД И ПАРОЛИ ИЗ СМС



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО



Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Сравнивают данные карты.

— Что делать?



СРАЗУ ПОЛОЖИТЕ ТРУБКУ — ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.



Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

— Что делать?



НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят сообщить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.



Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

— Что делать?



ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прервите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.



На сайтах с объявлением («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

— Что делать?



НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлением.



Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

— Что делать?



ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надписи **https://** и **«замочек»** в адресной строке браузера.



ИНТЕРНЕТ



Предлагают вложить деньги на очень выгодных условиях.

— Что делать?



ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.