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, позвоните 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 ДЕНЬГИ СРАЗУ!

Перезвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страницу взломали.

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
всё о финансах по-взрослому

Банк России

ОСТОРОЖНО: МОШЕННИКИ!

НИКОГДА
НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ ЛЮДЯМ ТРЕХЗНАЧНЫЙ КОД НА ОБОРОТЕ 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. Спрашивают 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 совершить 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. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

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.

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

— Что делать?

НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

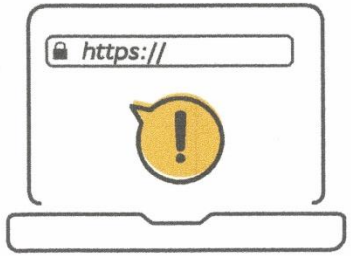
Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.

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 надпись **https://** и **«замочек»** в адресной строке браузера.



ОСТОРОЖНО: МОШЕННИКИ!

Вам звонят из банка и просят сообщить персональные данные или информацию о карте/счете – БУДЬТЕ БДИТЕЛЬНЫ, ЭТО МОГУТ БЫТЬ МОШЕННИКИ!

Злоумышленники 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 попросить секретные сведения о карте или счете. Например, чтобы остановить подозрительную операцию.

В ЧЕМ ОПАСНОСТЬ И ЧТО ДЕЛАТЬ?

Узнав нужную информацию, преступник может украсть ваши деньги.

- Не говорите и не вводите ПИН-код, трехзначный код с обратной стороны карты, или одноразовый пароль из СМС.
- Не набирайте на телефоне никаких 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 перезванивайте обратным звонком, вы можете снова попасть к мошенникам.

ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ

1 Звоните в банк сами

Набирайте номер вручную. Телефон горячей линии указан на обратной стороне карты и на официальном сайте банка.

Перезванивая на номер, с которого пришли звонок или сообщение, вы рискуете снова попасть к мошенникам.

2 Сосредоточьтесь

Если банк выявит подозрительную 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 продиктовать или ввести CVC/CVV-код на обратной стороне карты, пин-код или коды из СМС — это мошенники!

Назвать кодовое слово можно, только если вы сами звоните на горячую линию банка.

Подробнее о том, как защититься от кибератак и финансовых мошенников, читайте на сайте fincult.info

Банк России

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

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