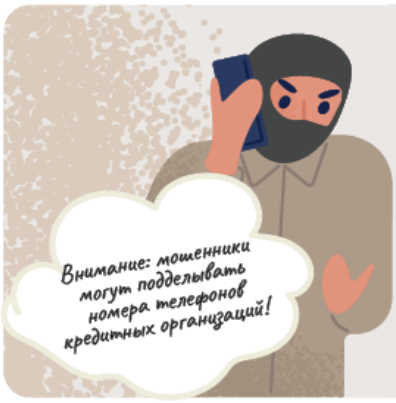
БАНК РОССИИ
ФИНЦЕРТ

Осторожно: мошенники

Коллеги! Во время самоизоляции вырос спрос на удаленные услуги – вместе с этим мошенники стали активнее работать с информационными технологиями. Пожалуйста, будьте бдительны и не поддавайтесь на их уловки!

Телефонное мошенничество



Мне позвонили из «службы безопасности банка» и сообщили о заблокированном переводе.

Что делать?

Положите трубку и позвоните по телефону, который указан на вашей банковской карте. Важно: набирайте номер вручную!

Мне позвонили и сказали, что я выиграл (-а) в лотерею или розыгрыше призов / могу получить бесплатную путевку, льготы или выплаты...

Что делать?

Скорее всего, вы разговариваете с мошенниками! Возможно, вас попросят совершить платеж под каким-то предлогом, сообщить персональные данные или данные банковской карты. Не продолжайте разговор, не сообщайте преступникам личную информацию!

Мне позвонили и сказали, что мой близкий человек попал в беду, просят перевести деньги...

Что делать?

Не продолжайте разговор, попытайтесь дозвониться до близкого человека самостоятельно!

БАНК РОССИИ
ФИНЦЕРТ

Интернет

Я прочитал в Интернете, что можно разместить средства с гарантированной высокой доходностью (гораздо выше по сравнению с условиями в финансовых организациях, получивших лицензию Банка России)

Что делать?

Не поддавайтесь на подобные уловки, в большинстве случаев это обман: так мошенники пытаются получить ваши накопления или персональные данные. Информацию о наличии лицензии Банка России у финансовой организации можно проверить на официальном сайте www.cbr.ru/finorg

На сайтах с объявлениями (Avito, Youla и т.п.) предлагают товары и услуги по заниженным ценам...

Что делать?

За привлекательными ценами часто прячутся мошенники. Не соглашайтесь на предоплату, пользуйтесь услугой «безопасная сделка», которая доступна на сайте с объявлениями. Не сообщайте секретные данные банковской карты. Не переходите по ссылкам под предлогом «ссылки для оплаты товара» или «ссылки на транспортную компанию».

Неизвестные интернет-магазины предлагают товары по низким ценам (гораздо ниже рыночных)...

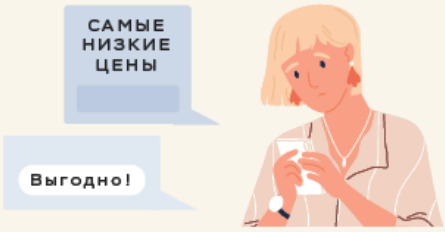
Что делать?

Не совершайте предоплату: проверьте среднюю цену на товар, рейтинг и отзывы о продавце.

Предлагают поучаствовать в онлайн-опросе за деньги или какой-то товар...

Что делать?

Цель таких предложений - данные вашей банковской карты и средства на ней. Злоумышленники просят оплатить комиссию за перевод суммы вознаграждения, например, «перевести 250 руб., чтобы получить 100 000 руб.». Это обман, будьте бдительны и не принимайте участие в подобных опросах!



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

Что делать?

Пользуйтесь только проверенными ресурсами. Мошенники часто завлекают потенциальные жертвы отсутствием комиссий и привлекательными условиями.

БАНК РОССИИ
ФИНЦЕРТ

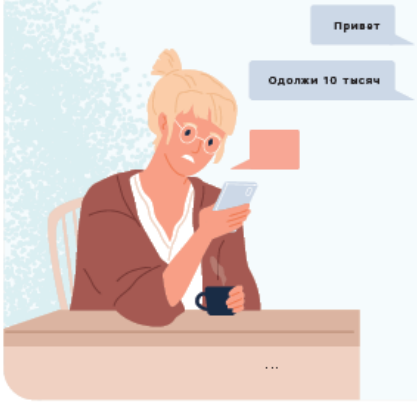
СМС, мессенджеры, соцсети

Мне пришла СМС от «банка» с информацией:
- **о заблокированном платеже;**
- **о выигрыше в лотерею;**
- **об ошибочном переводе на мой банковский счет**

или счет мобильного телефона с просьбой вернуть деньги.

Что делать?

- Не перезванивайте по номеру, указанному в сообщении. Обратитесь в ваш банк по номеру, который указан на оборотной стороне карты. Наберите его вручную!
- Не делайте того, о чем вас просят в сообщении.
- Не переходите по ссылке в сообщении.



Мой знакомый написал мне в соцсети:
просит дать в долг или перевести
средства на лечение

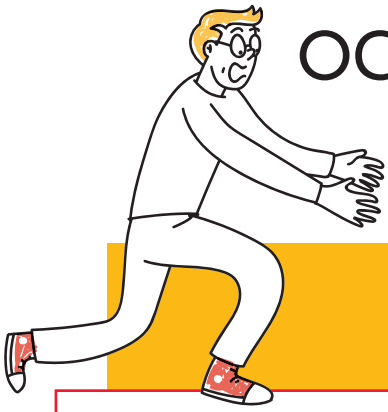
Аккаунт вашего знакомого могли взломать. Часто мошенники используют информацию о сборе средств, заменяя платежные реквизиты на свои.

Что делать?

Перезвоните этому человеку, чтобы выяснить ситуацию.

Тщательно проверяйте информацию, указанную в этой «просьбе о помощи», не совершайте импульсивных действий. Например, задайте вопрос, ответ на который не может знать мошенник.

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 пришел звонок или сообщение, вы рискуете снова попасть к мошенникам.

2 Сосредоточьтесь

Если банк выявит подозрительную транзакцию, он приостановит ее на срок до двух суток.

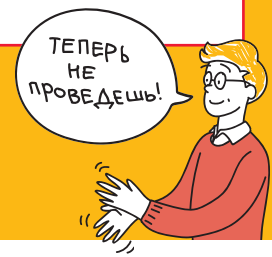
У вас есть 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.

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!

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

Подробнее о том, как защититься от киберкраж 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