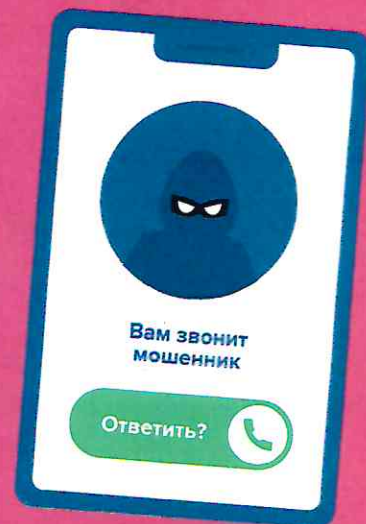


# Осторожно: телефонное мошенничество

Звонят из банка, полиции или другой организации? Просят перевести деньги на безопасный счет или назвать данные карты, пароли из банковских уведомлений, персональные данные? Это мошенники.



## Как обезопасить свои деньги?

Положите трубку и перепроверьте информацию. По любым операциям с картами и банковским счетом звоните в свой банк сами. Вручную наберите номер банка, указанный на обороте карты или на его официальном сайте. Только там вам прояснят ситуацию.

Обратите внимание на признаки, которые помогут быстро распознать мошенников:

### На вас выходят сами.

Аферисты могут представиться кем угодно: службой безопасности банка, налоговой, прокуратурой. Но они всегда иницируют общение сами. Если вы получили подозрительный звонок, СМС или письмо – насторожитесь.

### Просят сообщить данные.

Мошенники любыми способами пытаются выманить секретные данные карты, включая срок действия и три цифры с оборота, а также пароли и коды из банковских уведомлений. Настоящий сотрудник банка никогда ими не интересуется.

### С вами говорят о деньгах.

Схемы обмана почти всегда связаны с финансами: вам обещают золотые горы, предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно вложиться» (на самом деле – в финансовую пирамиду).

### На вас давят.

Аферисты всегда торопят, чтобы у вас не было времени обдумать ситуацию. Провоцируют сильные эмоции, стараясь сбить с толку. Например, сообщают: «Ваш онлайн-банк взломали!», чтобы вы от растерянности и волнения безоговорочно следовали их инструкциям, лишь бы спасти свои деньги.

Не всегда при общении с аферистом вы заметите все пять признаков мошенничества. Но в любой ситуации стоит проявить бдительность.







# КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

## ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ  
БАНКОВ НИКОГДА НЕ ЗВОНЯТ  
КЛИЕНТАМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ  
ОБ ИМЕЮЩИХСЯ ПРОБЛЕМАХ,  
СВЯЗАННЫХ С КАРТАМИ!



Не следуйте инструкциям звонивших и не отвечайте на задаваемые вопросы, а просто положите трубку!



Проверить информацию можно, позвонив  
в контактный колл-центр банка по  
телефону, указанному на задней стороне  
вашей банковской карты

Никогда и никому не сообщайте данные своей банковской  
карты (ПИН-код, код безопасности, пароли и др.)

Знайте, что мошенники уже  
могут располагать некоторой  
информацией о Ваших  
персональных данных!  
Будьте внимательны!



Знайте, что СМС - это Ваша электронная подпись!  
Озвучивая СМС-код мошенникам, Вы даете право  
злоумышленникам совершать любые действия с Вашими  
**деньгами!**



# Как не попасться на уловки мошенников



Чтобы обезопасить свои деньги от злоумышленников, придерживайтесь главных принципов кибербезопасности:

**1**

## Держите в секрете конфиденциальные данные

Никому не сообщайте полные реквизиты карты, включая срок ее действия и три цифры с оборота, а также пароли и коды из банковских уведомлений. Ими интересуются только мошенники.

**2**

## Не спешите выполнять инструкции незнакомцев

Не переходите по ссылкам неизвестных отправителей, не переводите деньги по первому требованию (даже если вас об этом просит друг или родственник – возможно, это мошенники, взломавшие их аккаунты). Не перезванивайте на неизвестные номера и не вводите данные карты на подозрительных сайтах.

**3**

## Перепроверяйте информацию

Получили внезапный тревожный звонок «из банка»? Не верьте собеседнику на слово. Чтобы прояснить ситуацию, положите трубку и вручную наберите номер банка, указанный на вашей карте или на его официальном сайте.

**4**

## Защищайте данные на своих устройствах

Установите антивирус на все гаджеты, которыми пользуетесь, и не забывайте его обновлять. Ставьте надежные пароли на вход в аккаунты, к которым привязана ваша банковская карта. Используйте биометрическую разблокировку для телефона – мошенники не смогут ее подделать, если вы потеряете устройство.



Банк России



Финансовая культура

Узнай больше на [fincult.info](http://fincult.info)

