

# ВНИМАНИЕ! МОШЕННИКИ!

## НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Будьте бдительны при совершении действий с банковскими картами и соблюдайте элементарные правила безопасности, чтобы не стать жертвой мошеннических действий.

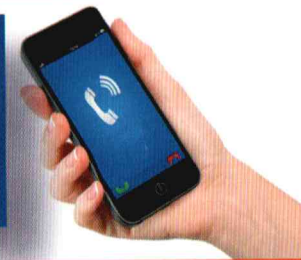
### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ



Вам поступил звонок (сообщение) о блокировке банковской карты или подозрительных операциях с деньгами – это МОШЕННИК. Прекратите разговор и позвоните на горячую линию банка.

### ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Вам позвонили от имени близкого человека, сообщили о несчастном случае и просят деньги – это Мошенник. Прекратите разговор и позвоните близкому человеку.



### ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

По Вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить смс-код, чтобы перевести деньги- это МОШЕННИК. Прекратите разговор и ни в коем случае не сообщайте код.

### УЧАСТИЕ В ОНЛАЙН БИРЖАХ И ТОРГАХ

Вам в сети «интернет» поступило заманчивое предложение приумножить свой капитал в онлайн биржах и бинарных аукционах, с доходностью в 100% и более за короткие сроки, обещают простой и быстрый вывод денег – это МОШЕННИКИ пытаются завладеть вашими деньгами под видом трейдеров. Прекратите общение и ни в коем случае не переводите деньги.

### СООБЩЕНИЕ В СОЦИАЛЬНОЙ СЕТИ

Ваш друг (родственник) пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные банковской карты, чтобы перечислить их Вам, это МОШЕННИКИ. Нужно сразу перезвонить другу (родственнику) по его телефону и выяснить обстоятельства.

В СЛУЧАЕ ХИЩЕНИЯ ВАШИХ ДЕНЕГ ИЛИ СОВЕРШЕНИЯ В ОТНОШЕНИИ ВАС МОШЕННИЧЕСКИХ ДЕЙСТВИЙ  
НЕМЕДЛЕННО ПОЗВОНИТЕ В ПОЛИЦИЮ ПО ТЕЛЕФОНУ «02» или «112»  
УМВД России по г. Туле

## 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

### КODOVOE 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](https://fincult.info)



Финансовая культура



# 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

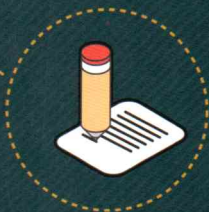


2

## 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





# 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**

ТЕПЕРЬ  
НЕ  
ПРОВЕДЕШЬ!



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**

# 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.





Банк России

# ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

## 5 ПРИЗНАКОВ ОБМАНА

### 1 НА ВАС ВЫХОДЯТ 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 всегда торопят, чтобы у вас не было времени все обдумать

### 4 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

### 5 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект



## **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 оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные



Как защитить свои финансы,  
читайте на [fincult.info](https://fincult.info)



**Финансовая  
культура**



Банк России

# КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

## Какие схемы используют аферисты?

### ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ

Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

### ЗАМАНИВАЮТ НА РАСПРОДАЖИ

Огромные скидки и низкие цены могут оказаться мошеннической уловкой

### СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

### МАСКИРУЮТСЯ

Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений





## Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на [fincult.info](http://fincult.info)



Финансовая  
культура





## КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций



### КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

- ! Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых



### КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты



## КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой



Подробнее о правилах кибергигиены читайте на [fincult.info](https://fincult.info)



**Финансовая  
культура**