

**АДМИНИСТРАЦИЯ КРАСНОДАРСКОГО КРАЯ**

## **Онлайн мошенники**



# 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 кибергиены читайте на [fincult.info](http://fincult.info)



Финансовая культура



## 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  
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**  
ПОРА УЗНАТЬ ПРО ДЕНЬГИ ВСЕ



Банк России



**ОСТОРОЖНО:  
МОШЕННИКИ!**

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

# 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 кибергиены читайте на [fincult.info](http://fincult.info)



Финансовая  
культура

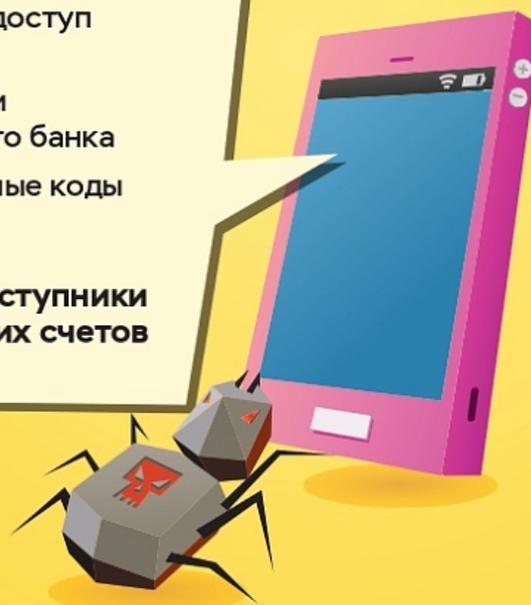


Банк России

## КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

- ВИРУСЫ:**
- открывают удаленный доступ к вашему устройству
  - крадут логины и пароли от онлайн- и мобильного банка
  - перехватывают секретные коды из сообщений

**Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов**



### КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

Выгодные ставки  
всем заемщикам?

Обещают  
кредит  
без справок  
и проверок?

Гарантируют  
одобрение даже  
с плохой кредитной  
историей?

## Будьте бдительны!

За выгодными  
условиями часто  
скрываются мошенники!



Проверьте на сайте Банка России,  
законно ли работает компания:



◀ Есть ли  
у нее  
лицензия?

[cbr.ru/fmp\\_check/](https://cbr.ru/fmp_check/)



◀ Нет ли  
организации  
в списке  
нелегалов?

[cbr.ru/inside/warning-list/](https://cbr.ru/inside/warning-list/)



# 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.



# 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

## 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

### КОДОВОЕ СЛОВО

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](http://fincult.info)



Финансовая  
культура

# 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 ГОВОРЯТ О ДЕНЬГАХ**

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

**5 ПРОСЯТ СООБЩИТЬ  
ДАнные**

Злоумышленников интересуют 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 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](http://fincult.info)

# КАК РАСПОЗНАТЬ ФИНАНСОВУЮ ПИРАМИДУ



**Финансовая пирамида – это мошеннический проект, который имитирует выгодные инвестиции.**

**Вас призывают вложить деньги в фиктивный бизнес и агитируют приводить друзей и родственников.**

В результате можно потерять не только деньги, но и доверие своих близких.





## **лифлет-мошенники**

[лифлет\\_мошенник...](#)

## **Фишинг**

[Фишинг.pdf](#)

## **Вирус**

[Вирус.pdf](#)

## **Нелегалы**

[Нелегалы.PDF](#)

## **Онлайн-мошенник**

[Онлайн-мошенник...](#)

## **Подменные номера**

[Подменные номер...](#)

## **С карты украли**

---

[С карты украли....](#)

## **Телефонные мошенники**

[Телефонные моше...](#)

## **Финансовые пирамиды**

[Финансовые пира...](#)

## **Документы**

liflet\_moshenniki.pdf

pdf, 1.9 МБ

[Скачать](#)

Fishing.pdf

pdf, 3.2 МБ

[Скачать](#)

Virus.pdf

pdf, 69.85 КБ

[Скачать](#)

Nelegaly.PDF

PDF, 584.98 КБ

[Скачать](#)

Onlajjn\_moshennik.pdf

pdf, 3.14 МБ

[Скачать](#)

Podmennye\_nomera\_listovka\_PRESS.pdf

---

pdf, 196.68 КБ

[Скачать](#)

S\_karty\_ukrali.pdf

pdf, 3.38 МБ

[Скачать](#)

Telefonnye\_moshenniki.pdf

pdf, 3.06 МБ

[Скачать](#)

Finansovye\_piramidy.pdf

pdf, 1.57 МБ

[Скачать](#)

Дата публикации: 06.09.2023

Теги: [Финансовая грамотность](#), [МВД](#).

[-----](#)  
Копировать ссылку

[Предыдущая новость](#) [К списку новостей](#) [Следующая новость](#)