

**КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ**

Чтобы добраться до ваших банковских счетов, мошенники ищут ваши персональные данные и реквизиты карт

**Какие схемы используют аферисты?**

- ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ**  
Обещают высокие проценты, социальные выплаты или сверхвысокий инвестиционный доход. Переходя быстрее, обманывают – переводят деньги.
- ЗАМАНИВАЮТ НА РАСПРОДАЖИ**  
Обещают продать товары или услуги по сниженной или нулевой цене.
- СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ**  
Например, объявляют ордерами на заработок валюты, обещают вернуть деньги за отмененные рейсы или предлагают покупать государственные облигации.
- МАСКИРУЮТСЯ**  
Рассказывают ольте продажи и покупки акций на популярных сайтах объявлений.

**Как обезопасить свои деньги в интернете?**

- 1 Установите антивирус и регулярно обновляйте его
- 2 Защищайте социальную сеть, банковскую карту или платежную систему и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адрес электронной почты и сайта – он всегда отличается от официального лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте рекламные сообщения
- 5 Никогда не сообщайте свои персональные данные

Подробнее о правилах кибербезопасности читайте на [www.fsb.ru](https://www.fsb.ru)

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 два капли воды похожи на сайты реальных организаций

**КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?**

По ссылке из интернета или электронной почты, SMS, сообщениям в соцсетях или мессенджерах, рекламе, объявлениям о лотереях, распродажах, конкурсах 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, и текст 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 перед оплатой

Подробнее о правилах кибербезопасности читайте на [www.fsb.ru](https://www.fsb.ru)

Финансовая культура

**КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ**

**ВИРУСЫ:**

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перезаписывают 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
- Появляются всплывающие окна
- Теряет объем памяти

**ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?**

- Позвоните в банк и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовались на устройстве
- Обратитесь в сервисный центр, чтобы выключить гаджет
- Перезагрузите карты, смените логины и пароли от онлайн-банка и заново установите финансовое приложение

**КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?**

- Используйте антивирус и регулярно его обновляйте
- Не переходите по ссылкам от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения только из проверенных источников
- Обновляйте операционную систему устройства
- Избегайте общественных Wi-Fi сетей

Подробнее о защите гаджетов читайте на [www.fsb.ru](https://www.fsb.ru)

Финансовая культура

Банк России | Министерство внутренних дел Российской Федерации | Федеральная прокуратура Российской Федерации

## ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

### 5 ПРИЗНАКОВ ОБМАНА



- НА ВАС ВЫХОДИТ САМИ**  
Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой.  
Любой неожиданный звонок, СМС или письмо — повод насторожиться.
- РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПОДАРОК**  
Сильные эмоции притупляют бдительность.
- НА ВАС ДАВЯТ**  
Аферисты всегда "торопят", чтобы у вас не было времени все обдумать.
- ГОВОРЯТ О ДЕНЬГАХ**  
Предлагают деньги соразмерно, получить компенсацию или вложиться в инвестиционный проект.
- ПРОСЯТ СООБЩИТЬ ДАННЫЕ**  
Злоумышленники интересуют реквизиты карты, логины и коды из банковских уведомлений.

**ВАЖНО!**  
Сотрудники банков и полиции НИКОГДА не запрашивают 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 [vostok.spb](#)

Финансовая культура

Банк России | Министерство внутренних дел Российской Федерации | Федеральная прокуратура Российской Федерации

## ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

- 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
- НАПИСАТЬ заявление о несогласии с операцией**
  - Заявление должно быть написано:
  - с помощью сотрудника, сообщивший о списании денег
  - на месте в отделении банка
- ОБРАТИТЬСЯ в полицию**
  - Чем больше людей подает заявление, тем выше вероятность, что преступника поймут.

### КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

**НИКОМУ НЕ СООБЩАЙТЕ:**

- сроки действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логины и пароль от онлайн-банка

**НЕ ПУБЛИКУЙТЕ** персональные данные в открытом доступе

**УСТАНОВИТЕ** антивирус 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 [vostok.spb](#)

Финансовая культура