

Телефонное мошенничество – один из самых распространённых видов преступной деятельности в наше время.  
Делимся памятками, которые помогут не попасться на уловки мошенников.

#Безопасность #ДШИГречанинова #БанкРоссии

**Банк России**

**ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!**

**5 ПРИЗНАКОВ ОБМАНА**

- НА ВАС ВЫХОДЯТ САМИ**  
Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой. Любой неожиданный звонок, СМС или письмо – повод насторожиться.
- РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУТАЮТ**  
Сильные эмоции притупляют бдительность.
- НА ВАС ДАВЯТ**  
Аферисты всегда говорят, чтобы у вас не было времени все обдумать.
- ГОВОРЯТ О ДЕНЕГАХ**  
Предлагают спасти, собрать деньги, получить компенсацию или вложиться в инвестиционный проект.
- ПРОСЯТ СООБЩИТЬ ДАННЫЕ**  
Эмоциональному интересу рассказывать карты, пароли и коды из банковских уведомлений.

**ВАЖНО!**  
Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли и 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
- кодовые слова
- персональные данные

Как защитить свои финансы, читайте на [finrb.ru](https://finrb.ru)

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
- Торкает объектив камеры

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

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

**КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?**

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

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

Финансовая культура

**Банк России**

**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, в течение суток после сообщения о списании денег
  - на месте в отделении банка
- ОБРАТИТЬСЯ в полицию**
  - Чем больше людей поддуют заявления, тем выше вероятность, что преступников поймут

**КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?**

**НИКОМУ НЕ СООБЩАЙТЕ:**

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

**КОДОВОЕ СЛОВО**  
назначают только сотрудникам банка, когда сами звоните на горячую линию

**НЕ ПУБЛИКУЙТЕ** персональные данные в открытом доступе

**УСТАНОВИТЕ** антивирусы на все устройства

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на [finrb.ru](https://finrb.ru)

Финансовая культура



Банк России

### 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, рекламе, объявлений 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 знака закрытого замка
- Дизайн скопирован некачественно, в тексте 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 безопасности читайте на [www.bankofrussia.ru](https://www.bankofrussia.ru)

Финансовая культура



