

ОСТОРОЖНО! ЗВОНИТ МОШЕННИК:

БЛИЗКИЕ ПОПАЛИ В ДТП, НУЖНО ПЕРЕВЕСТИ ДЕНЬГИ
ПЕРЕЗВОНИТЕ БЛИЗКОМУ ЧЕЛОВЕКУ!

ВАШ СЧЕТ АРЕСТОВАН
НЕ СООБЩАЙТЕ ДАННЫЕ БАНКОВСКОЙ КАРТЫ!

ПОЗДРАВЛЯЕМ, ВЫ ПОБЕДИЛИ В КОНКУРСЕ!
НЕ УЧАСТВОВАЛИ – КЛАДИТЕ ТРУБКУ!

МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ РЕКЛАМЫ

НЕ ОСТАВЛЯЙТЕ ДАННЫЕ НА ПОДОЗРИТЕЛЬНЫХ САЙТАХ

ОТДЕЛЬНАЯ КАРТА ДЛЯ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

ИСПОЛЬЗУЙТЕ АНТИВИРУС

ТЕЛЕФОН ПОЛИЦИИ: 102

ЗАЩИТИ СВОИ УСТРОЙСТВА ОТ КИБЕРМОШЕННИКОВ

УСТАНОВИТЕ АНТИВИРУС

ОБНОВЛЯЙТЕ СИСТЕМУ

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ

СКАЧИВАЙТЕ ПРОВЕРЕННЫЕ ПРИЛОЖЕНИЯ

ТЕЛЕФОН ПОЛИЦИИ: 102

Банк России

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 подаст заявление, тем выше вероятность, что преступников поймает

КАК БЕЗОПАСИТЬ 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 пароли от онлайн-банка

КОДОВОЕ СЛОВО
называете только сотруднику банка, когда сами звоните на горячую линию

НЕ ПУБЛИКУЙТЕ
персональные данные в открытом доступе

УСТАНОВИТЕ
антивирусы на все устройства

Подпишитесь на правила безопасности платежей на [banki.ru](https://www.banki.ru)

Финансовая культура

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ
Аферисты могут представляться службой безопасности банка, налоговой, прокуратурой

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ
Слишком хорошие предложения притягивают бдительность

3 НА ВАС ДАВЯТ
Аферисты всегда просят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ
Предлагают деньги, оборудование, получить кредитацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ
Злоумышленники пытаются узнать данные карты, пароли и коды из банковских уведомлений

ЗВОНЯТ
из Банка России или другой организации?

УБЕДИТЕСЬ
что это не мошенники!

ВАЖНО!
Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершить переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- РПН-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовый слово
- персональные данные

Как защитить свои финансы, читайте на [banki.ru](https://www.banki.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, SMS, сообщений в соцсетях или мессенджерах, рекламе, объявлений о лотереях, распродажах, конкурсах от государства

❗ Хакеры часто взламывают чужие аккаунты, и фишинговые ссылки могут прийти даже от знакомых

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой символов
- В адресной строке нет титла и знака закладки сайта
- Дизайн скопирован некачественно, в текстах есть ошибки
- У сайта много 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 [banki.ru](https://www.banki.ru)

 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?

ОБЩАЮТ ЗОЛОТЫЕ ГОРЫ
Обещают огромные деньги, социальные выплаты или дорогостоящие медицинские услуги. Требуют быстрые действия – перевод денег

ЗАМАНЯЮТ НА РАСПРОДАЖИ
Отправляют смс-ки и сайты, где могут оказаться мошеннические сайты

СПЕКУЛИРУЮТ НА ТРЕНИИ СОБЫТИЯХ
Например, обещают обзор денег на предстоящие выборы, обещают вернуть деньги за невостановленные штрафы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Иногда имитируют роль продавца и покупают на популярных сайтах обмундирование

Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для покупок и платежей и используйте ее при покупке товаров и услуг
- 3 Всегда проверяйте адрес электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам из мессенджера – сразу удаляйте сообщения
- 5 Никогда не сообщайте свои персональные данные

 Подробнее о правилах безопасности читайте на [banki.ru](https://www.banki.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
- пересылает 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

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
- Переустановите 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 из мессенджера, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- Обновляйте операционную систему устройства
- Идентифицируйте общедоступный Wi-Fi-сигнал

 Подробнее о защите гаджета читайте на [banki.ru](https://www.banki.ru)

 Финансовая культура



[Аудиоролик киберпреступность](#)