

[открыть](#)





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 или 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 http и знака закрытого замка

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 www.bankofrussia.ru



Финансовая культура



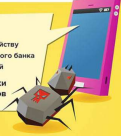
Банк России

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
- 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 использовали на устройстве
- Обратитесь в сервисный центр, чтобы выслать 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 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.bankofrussia.ru



Финансовая культура



Банк России

Обещают списать долги?

Проверь, что это не мошенники!



2 / 3



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?

ОБЫСЦАЮТ ЗОЛОТЫЕ ГОРЫ
 Обзвоны по телефону, сообщения в мессенджерах, рассылки по электронной почте. Прямые функции и переводы, обман

ЗАМАНИВАЮТ НА РАСПРОДАЖИ
 Ссылки на сайты, где можно купить товары по специальным ценам

СПЕКУЛИРУЮТ НА ВОЛНАХ СОБЫТИЙ
 Прогнозы, обещания обрести доход на биржевых торгах, обман, продажа за слишком редкие или предельно высокие государственные облигации

МАСКИРУЮТСЯ
 Подразывают рынок, продавая и покупая на популярном рынке облигаций

Как обезопасить свои деньги в интернете?

- 1 Избегать интернет- и телефонных обзвонов
- 2 Завести отдельную электронную карту для платежей в интернет и никогда не вносить деньги перед оплатой
- 3 Везде применять авторизацию картой и сайтах — не вводить логин/пароль/номер карты, если не уверены
- 4 Не переходить по ссылкам из незнакомых e-mail рассылок/сообщений
- 5 Никогда не сообщать свои персональные данные



Посетите в личном кабинете сайта на www.cbr.ru

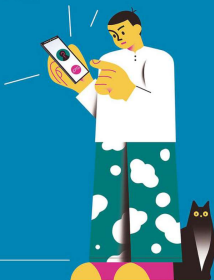


Банк России



Говорят про деньги?
Клади трубку и сам
перепроверяй
информацию!

 Банк России




Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

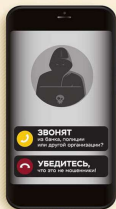
1 НА ВАС ВЫХОДЯТ САМИ

Адресаты могут представляться службой безопасности банка, налоговой, прокуратор.

Любой неожиданный звонок, СМС или текст — повод рассмотреть возможность обмана.

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ТРУТЯТ

Сильные эмоции могут спровоцировать беспечность.



3 НА ВАС ДАВЯТ

Адресаты хотят торговаться и вас не было времени вас обдумать.

4 ГОВОРЯТ О ОБИДАХ

Предлагают списать обиды, сообщить контактную информацию в анкетировательный проект.

5 ПРОСИТ СООБЩИТЬ ДАННЫЕ

Заполняют анкету, интересуют реквизитами карты, паролем и кодом из банковских уведомлений.

1 ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводов с вашей карты.



1 НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- персональные и банковские приложения и онлайн-банку
- название слова
- персональные данные



Как защитить свои финансы, читайте на finsovet.ru


Финансовое благополучие