



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, 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](https://fincult.info)



Финансовая  
культура



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 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](https://fincult.info)



Финансовая  
культура



Банк России

# 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)



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?

#### 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?

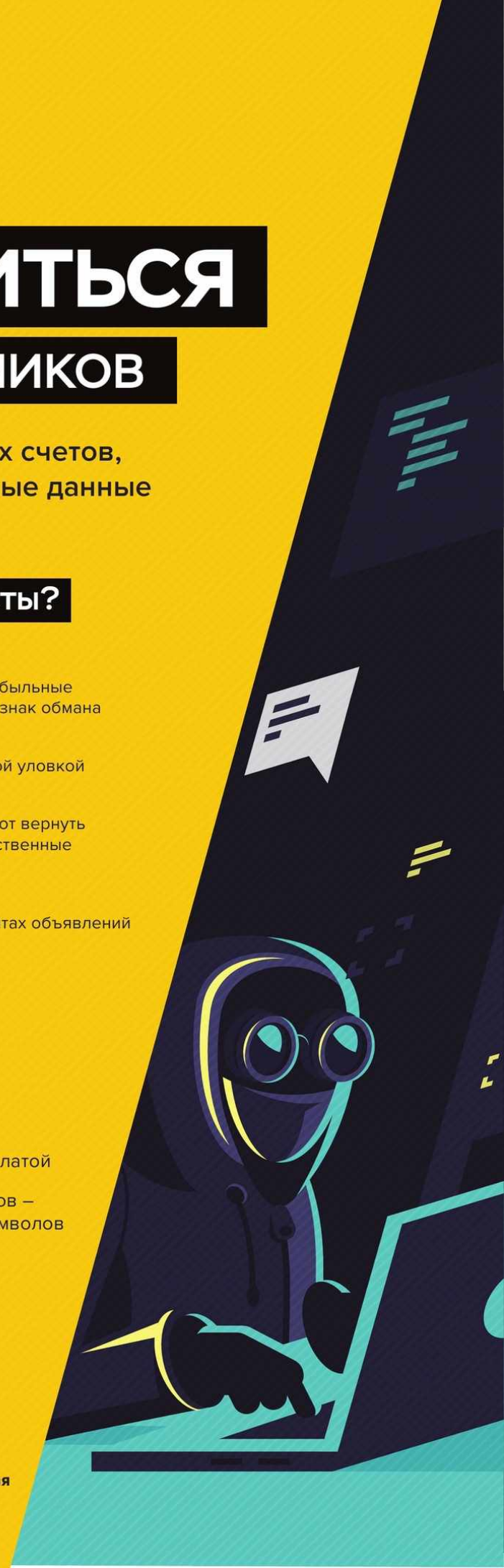
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на [fincult.info](http://fincult.info)



Финансовая культура



# Как не стать жертвой мошенников, покупая товары в интернете

## Признаки потенциально опасного интернет-магазина



1

### Низкая цена

Стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова «каждый», «количество ограничено», «спешите купить» и т.д.



2

### Отсутствие курьерской доставки и самовывоза

В этом случае нередко приходится вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.



3

### Отсутствие контактной информации и сведений о продавце

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует почитать отзывы в интернете.



4

### Подтверждение личности продавца посредством направления покупателю скана его паспорта

Документ, особенно отсканированный, легко подделать.



5

### Отсутствие истории у продавца или магазина

Потенциально опасными являются страницы, зарегистрированные пару дней назад.



6

### Неточности и несоответствия в описании товаров

Желательно почитать описание такого же товара на других сайтах.



7

### Чрезмерная настойчивость продавцов и менеджеров

Если представитель продавца начинает торопить с оформлением заказа или его оплатой, стоит отказаться от покупки. Мошенники часто используют временной фактор, чтобы нельзя было оценить все нюансы сделки.

БЫСТРЕЕ!!



8

### Требование предоплаты продавцом

Особенно должно насторожить предложение перевести деньги через анонимные платежные системы, электронные деньги, банковским переводом на карту частного лица. В таком случае нет гарантий возврата или получения товара.

## Ошибки самого покупателя



Недостаточных знаний об особенностях заказываемого товара; не совпадает размерный ряд, не подходит фасон и т.д.



Невнимательности при оформлении заказа



Поспешности

Потребитель вправе отказаться от покупки, совершенной в интернете, в течение семи дней после получения товара, при этом оплатив обратную доставку товара

Стоит помнить: желательно заранее изучить отзывы о магазине или продавце, посмотреть характеристики товаров на других сайтах, провести замеры, внимательно оформить заказ