

# 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 ссылке из интернета или электронной почты, SMS, сообщений в соцсетях или мессенджерах, рекламе, объявлений о лотереях, распродажах, конкурсах или от коллег/друзей.

Закоры часто используют чужие аккаунты, а фишинговые сайты имеют привлекательный внешний вид.



## КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего (лицо другой компании)
- В адресной строке нет HTTPS и значок закрытого замка
- Дизайн (кнопки/ссылки неадекватные), в текстах есть опечатки
- 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 нулевую сумму прямо перед оплатой.

# 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 совершения и списания денег
- на месте в отделении банка

## 3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



Чем быстрее полиция получит заявление, тем выше вероятность, что преступника поймают

## КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

### НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее обратной стороне (CVV/CVC)
- пароли и коды на уведомлениях
- логины и пароли от сайтов Банка

### НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

### УСТАНОВИТЕ

антивирус на все устройства

### кодовое слово

используйте только сотруднику Банка, когда сами звоните на горячую линию



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

# 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?

- Всплывают уведомления или уведомления
- Само завершает работу приложения
- Появляются всплывающие окна
- Таргет объяв. реклама

## 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 таргет
- Переименуйте карты, замените логины и пароли от онлайн-банка и заново установите банковские приложения

## 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
- Настройка общедоступных Wi-Fi сетей



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

