



**МИНИСТЕРСТВО ЦИФРОВОГО  
РАЗВИТИЯ И СВЯЗИ  
ИРКУТСКОЙ ОБЛАСТИ**

664027, г. Иркутск, ул. Ленина, д. 1а  
тел./факс. (3952) 24-02-63  
e-mail: digital@govirk.ru

Главам муниципальных  
образований

на № 24.08.2022 № 02-65-1522/22  
от \_\_\_\_\_

О совместной работе по повышению  
уровня финансовой киберграмотности  
населения Иркутской области

Уважаемые коллеги!

В целях проведения совместной работы, направленной на повышение уровня финансовой киберграмотности населения и противодействия мошенничеству, направляю справочные материалы (разработанные сектором киберграмотности и образовательных инициатив Департамента информационной безопасности Банка России) для ознакомления и дальнейшего их размещения на официальных страницах в сети «Интернет», а также для рассылки в подведомственные учреждения и размещения на стендах организаций.

Видеоматериалы для ознакомления доступны по ссылке:  
<https://disk.yandex.ru/d/ju-52sM455e19g>.

Приложение: на 12 л. в 1 экз.

Министр цифрового развития и  
связи Иркутской области

И.А. Рыморенко

ДОКУМЕНТ ПОДПИСАН  
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 5A400952C14EC1718FD311395272D1FC  
Владелец **Рыморенко Игорь Александрович**  
Действителен с 30.03.2022 по 23.06.2023

Н.Э. Сорокин  
+7 (3952) 24-01-58

# Работающий способ защитить от мошенников деньги на карте



Банк России



Финансовая  
культура



# С 1 октября 2022 года вы можете ограничивать операции в онлайн-банке

Мошенники не смогут оформить на вас кредит и похитить все деньги с вашей карты, даже если получат к ней доступ.



# Какие услуги можно ограничить?

- Запретить онлайн-кредиты
- Ограничить максимальную сумму одной онлайн-операции – например, не больше 10 тысяч рублей
- Установить лимит трат на сутки, неделю, месяц или любой другой период времени
- Отказаться от всех видов банковских онлайн-услуг



# Запрет на онлайн-кредиты

При установленном запрете мошенникам не удастся оформить онлайн-кредит на ваше имя и оставить вас с долгами.

Если вы сами захотите взять онлайн-кредит, то сможете отменить запрет в любое время. После получения кредита можно будет подключить запрет снова.



# Лимит трат – для одной операции или на время

Лимит денежных трат – способ минимизировать возможные потери, если карта или ее данные попадут к мошенникам. Они не смогут увести со счета больше той суммы, которую вы установите.

Узнайте, какие типы лимитов есть в вашем банке, и выберите подходящий для себя – суточный, месячный, для интернет-покупок и др.



# Как установить такие ограничения?

Некоторые банки позволяют настроить самоограничения прямо в онлайн-приложении, другие – только по письменному заявлению в офисе.

Уточните, как это можно сделать в вашем банке.

Отменить запрет или изменить его параметры можно в любое время без ограничений.



# Не теряйте бдительность!

Даже при установленных ограничениях будьте осторожны и держите в секрете ваши личные и платежные данные.





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 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](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?

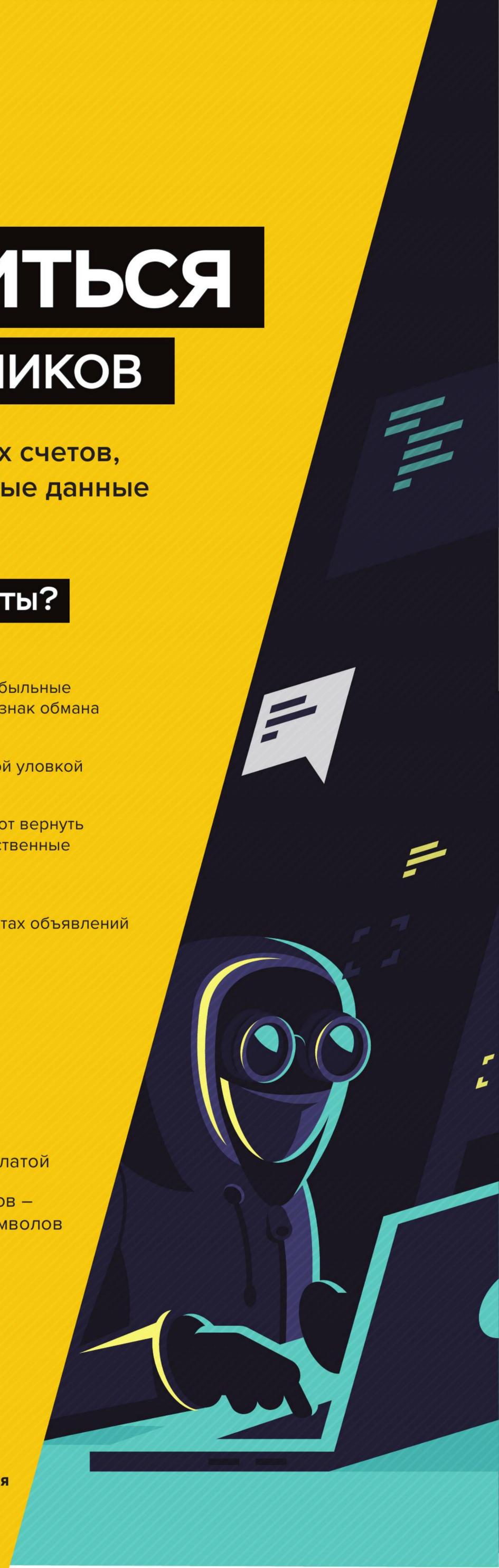
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам 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





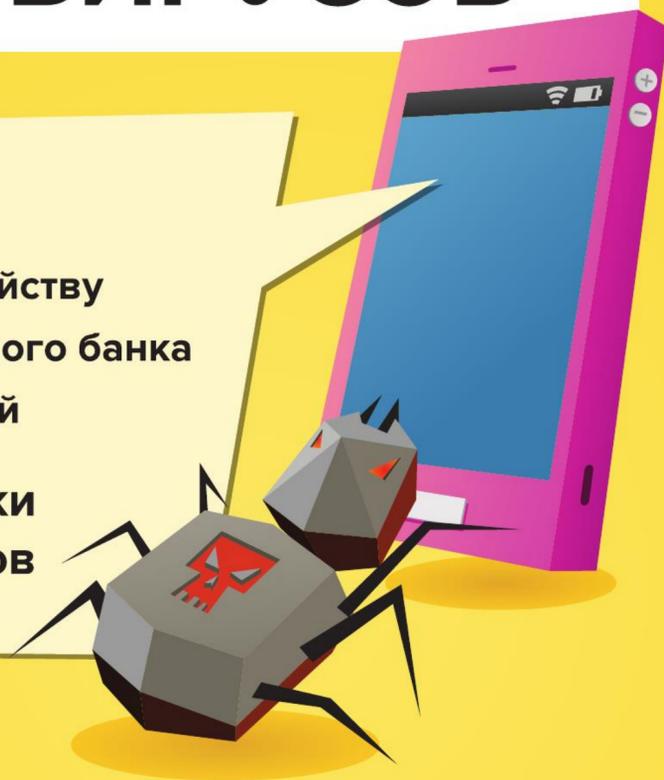
Банк России

# 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 вылечить гаджет
- Перевыпустите карты, смените логин и пароль 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 общедоступных Wi-Fi-сетей



Подробнее о защите гаджетов  
читайте на [fincult.info](http://fincult.info)



Финансовая  
культура