



Банк России

Правила безопасности от финансового мошенничества



Банк России

Финансовое кибермошенничество — это одна из самых распространенных и опасных форм преступлений в современном мире. Оно может нанести серьезный ущерб не только отдельным гражданам и организациям, но и всей экономике страны.

Кибермошенники похитили у кузбасовцев почти **2 млрд.** рублей
в 2025 году!

Проблема стоит очень остро!
Какие современные схемы кибермошенничества существуют и как им противостоять?



Банк России

Современные схемы кибермошенничества и как им противостоять?

Звонок из банка, на вас берут кредит, необходимо перевести деньги на безопасный или специальный счёт

Звонок из полиции, Следственного Комитета, ФСБ: просят помочь задержать мошенников и не разглашать информацию. Игнорирование требований грозит вам уголовной ответственностью.

Звонят или пишут в мессенджерах руководители

Родственник в беде (попал в ДТП, совершил хищение, оказался в больнице)

Звонки в мессенджерах с логотипом Госуслуг

Звонят, сообщают о необходимости заменить СИМ-карту

Предлагают инвестировать под гарантированно высокий процент

Взламывают Ватсап с просьбой о финансовой помощи

С карты списаны деньги за покупку, которую вы не совершали

Предлагают получить компенсацию за приобретенные ранее лекарства

Поздравляем! Вы стали победителем!

Поступает сообщение от Федеральной налоговой службы

Подменивают голос через нейросеть

Предлагают проверить подлинность банкнот или обменять на новые банкноты

Под видом Центрального банка предлагают выгодно разместить деньги на счете

Сообщают о замене СНИЛС

Размещают объявления на подъездах о задолженности или смене чипов

Знакомства в интернете

Фальшивые кадровые агентства

Судебные приставы присылают письма

Фальшивые QR-коды на электросамокатах

Сообщают о положенных социальных выплатах

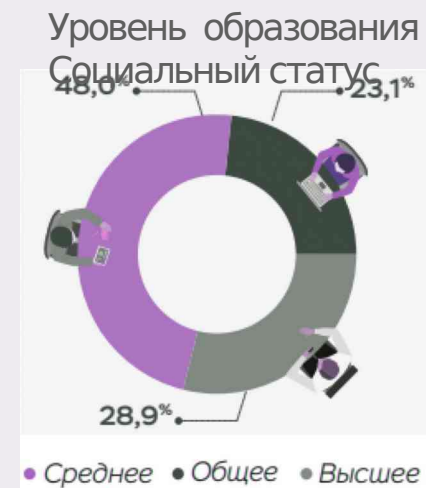
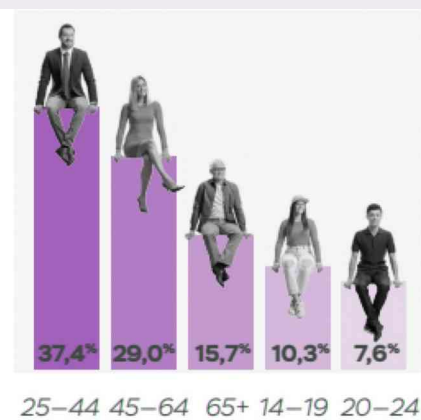
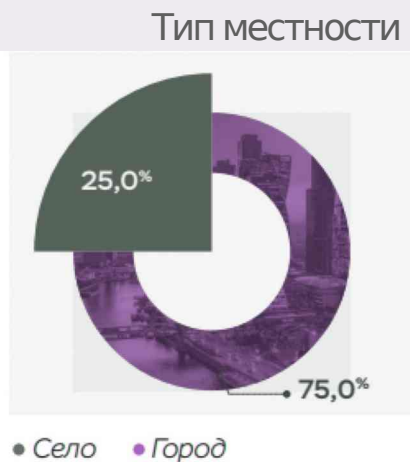
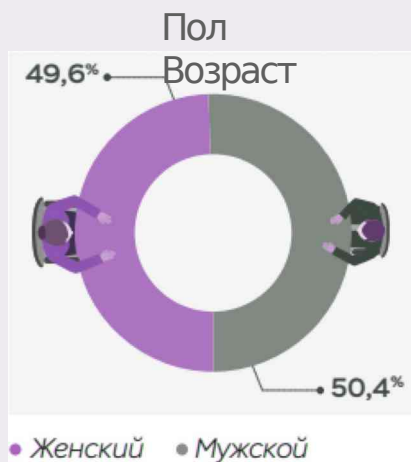
Предлагают счетчики, медицинские приборы, массажеры

Предлагают поменять деньги на цифровые рубли



Банк России

Где злоумышленники ищут жертву и кто наиболее подвержен обману?





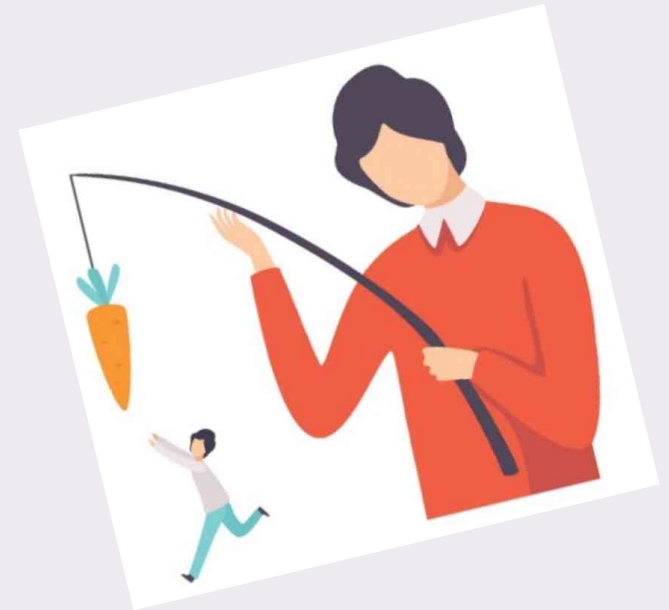
Банк России

Самые распространенные способы финансового мошенничества:



1. Мошенничество с банковскими картами. Социальная инженерия, телефонное мошенничество.
2. Мошенничество в Интернете: ссылки и письма.
3. Финансовые пирамиды.

Не путайте с индивидуальными предложениями, поступающими от специалистов финансовых организаций!

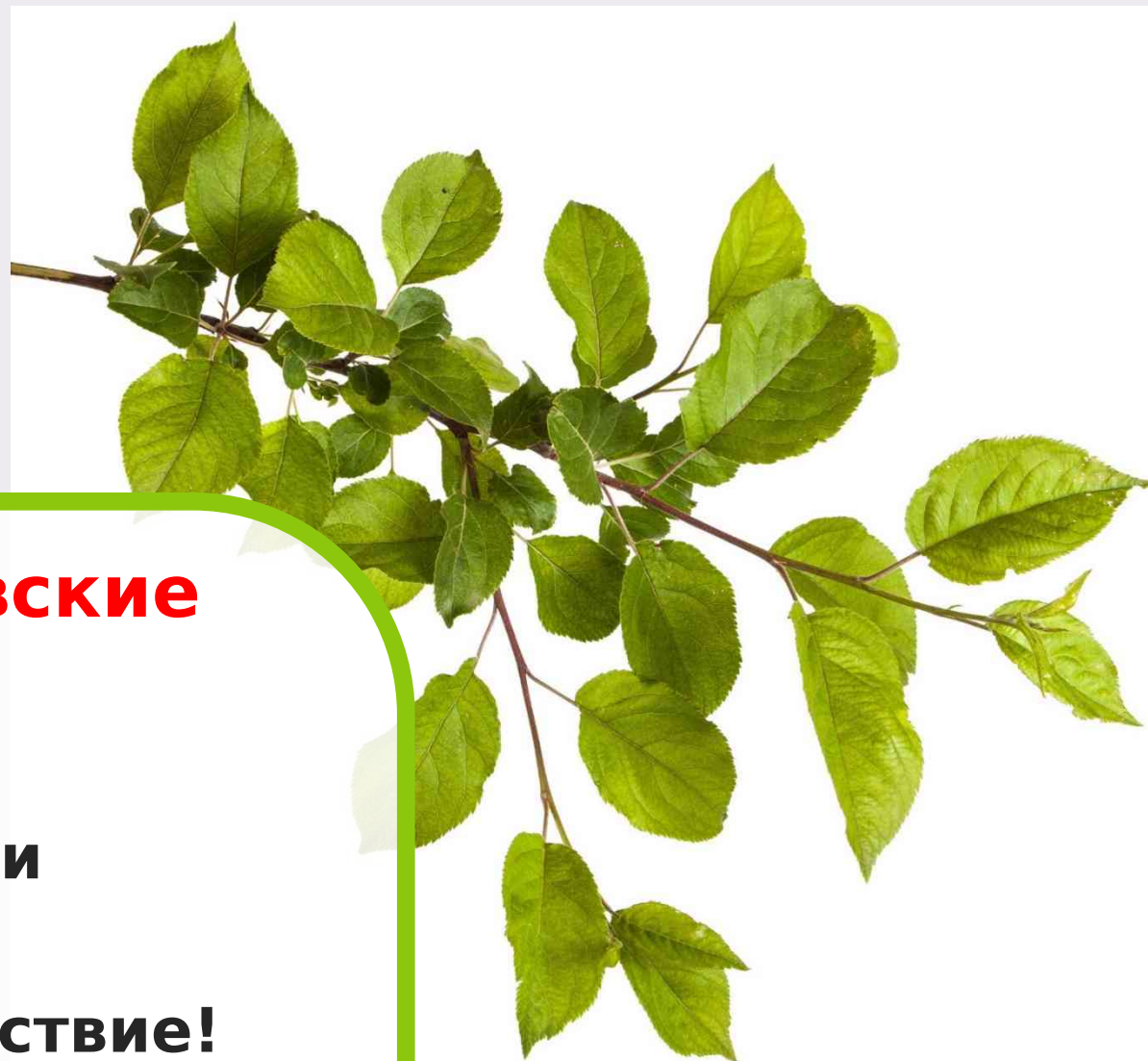




Банк России

1.1. Платежные банковские карты

**Не экономьте на SMS-уведомлениях о платежах и переводах с вашей карты
- это малая цена за спокойствие!**





Банк России

Безопасное использование банковских карт.

Банкомат

- ✓ Проверьте, нет ли посторонних устройств
- ✓ Банкоматы внутри отделения банка безопаснее
- ✓ Не пользуйтесь банкоматами в режиме ожидания
- ✓ Прикрывайте рукой вводимый PIN-код
- ✓ Сохраняйте квитанцию



Банк России



**Банк обязан по вашему
требованию незамедлительно
заблокировать утерянную карту!**
ЛАЙФХАК – занесите в
телефонную книжку смартфона
номер банка, выпустившего Вашу
платежную карту!!!



Банк России

Чтобы украсть деньги, мошенникам надо узнать:

- ✓ номер вашей карты
- ✓ имя и фамилию владельца
- ✓ срок действия
- ✓ PIN – код
- ✓ код проверки подлинности карты
- ✓ одноразовый пароль (sms-сообщение для подтверждения платежа)

Ваша персональная информация

Мошенник может снять все деньги с карты

Мошенник может оплачивать вашей картой свои покупки в интернете

Мошенник может войти в интернет-банк и получить доступ к вашим счетам



Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ?



**Заблокируйте
карту**



**Сообщите
в банк**

в мобильном приложении банка звонком на
горячую линию банка личным обращением в
отделение банка



**Напишите
заявление в
полицию**

при личном обращении
в ближайший отдел ОВД



Сразу же



**В течение
суток**



**Как можно
скорее**



Банк России



1.2. Социальная инженерия (телефон, SMS)

Телефонное и СМС-мошенничество

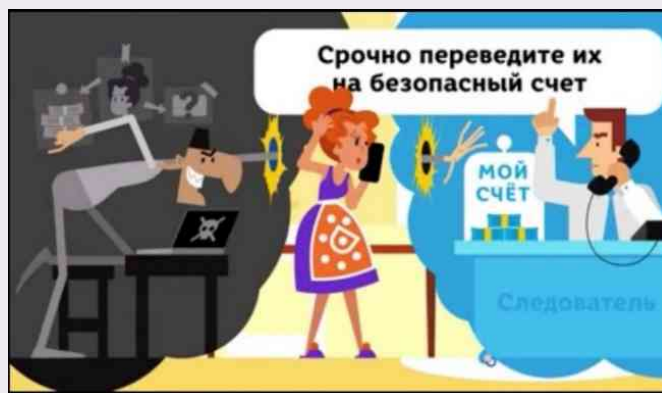
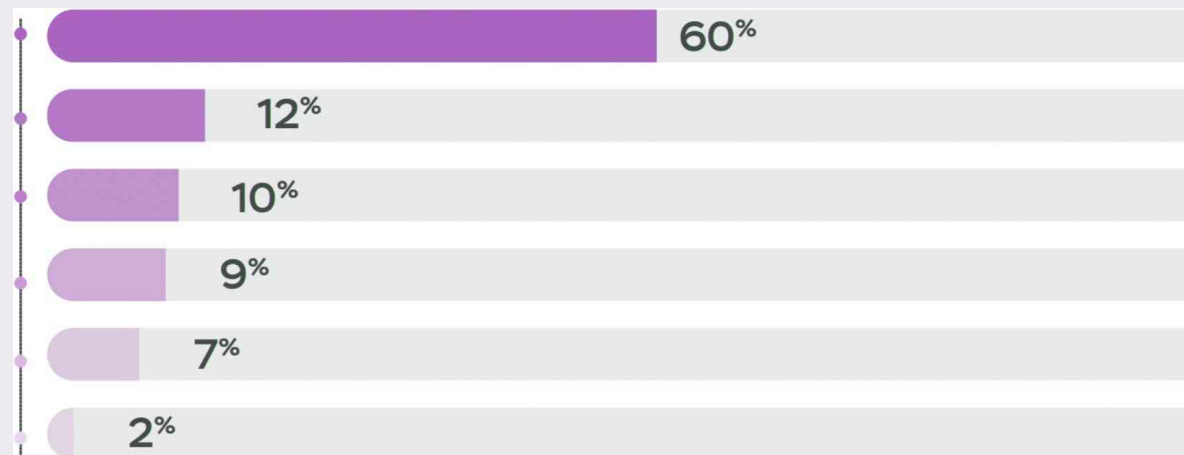
Мессенджеры

Социальные сети

Электронные письма

Поддельные сайты (фишинг)

Поддельные приложения банков





Банк России

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – ЗЛО

- 1 Обман или злоупотребление доверием
- 2 Психологическое давление
- 3 Манипулирование



 Под влиянием социальной инженерии жертва добровольно расстаётся с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств



Банк России

ФОРМУЛА УСПЕХА МОШЕННИКОВ



+



+



+



эффект
неожиданности

яркие
эмоции

психологическое
давление, паника

актуальная
тема

Увы, мы готовы сделать **ВСЁ**,
что просят от нас мошенники !!!



Банк России

ТЕЛЕФОННЫЕ МОШЕННИКИ



ЛЖЕСОТРУДНИК
ЦЕНТРОБАНКА
(Банка России)

По вашей карте зафиксирована сомнительная операция.
Для сохранности денег вам нужно перевести их на безопасный
счет в Центробанке.
Высылаю удостоверение

- По вашей карте пытаются перевести деньги...
- Ваша карта заблокирована...
- По карте зафиксирована подозрительная операция...



ЛЖЕСОТРУДНИК
БАНКА



Банк России

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

- 1 Не отвечайте на звонки с незнакомых номеров
Прервите разговор,
- 2 если он касается финансовых вопросов
- 3 Не торопитесь принимать решение
- 4 Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам



- 5 Самостоятельно позвоните близкому человеку/ в банк/ в организацию
- 6 Не перезванивайте по незнакомым номерам



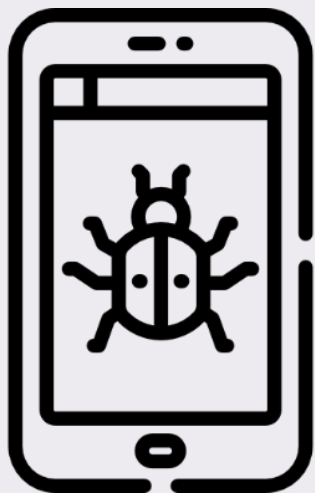
**Возьмите паузу
и спросите совета
у родных и друзей!**



Банк России

2. Мошенничество в Интернете - это подозрительные ссылки и письма

Защитим себя в Интернете:



- не открываем подозрительные письма, не доверяем сомнительным ссылкам;
- устанавливаем пароли – реально защищаемые пароли!
- а также устанавливаем **двухфакторную аутентификацию** на вход в ЛК на известных ресурсах!





Банк России

ПРИЗНАКИ ФИШИНГОВЫХ САЙТОВ

- Ошибки в адресе сайта
- Сайт состоит из 1 страницы (только для ввода данных)
- В адресной строке отсутствует замочек
- В названии сайта нет https
- Ошибки в тексте и дизайне
- Побуждают ввести свои личные / финансовые данные
- Предлагают скачать файл, установить программу



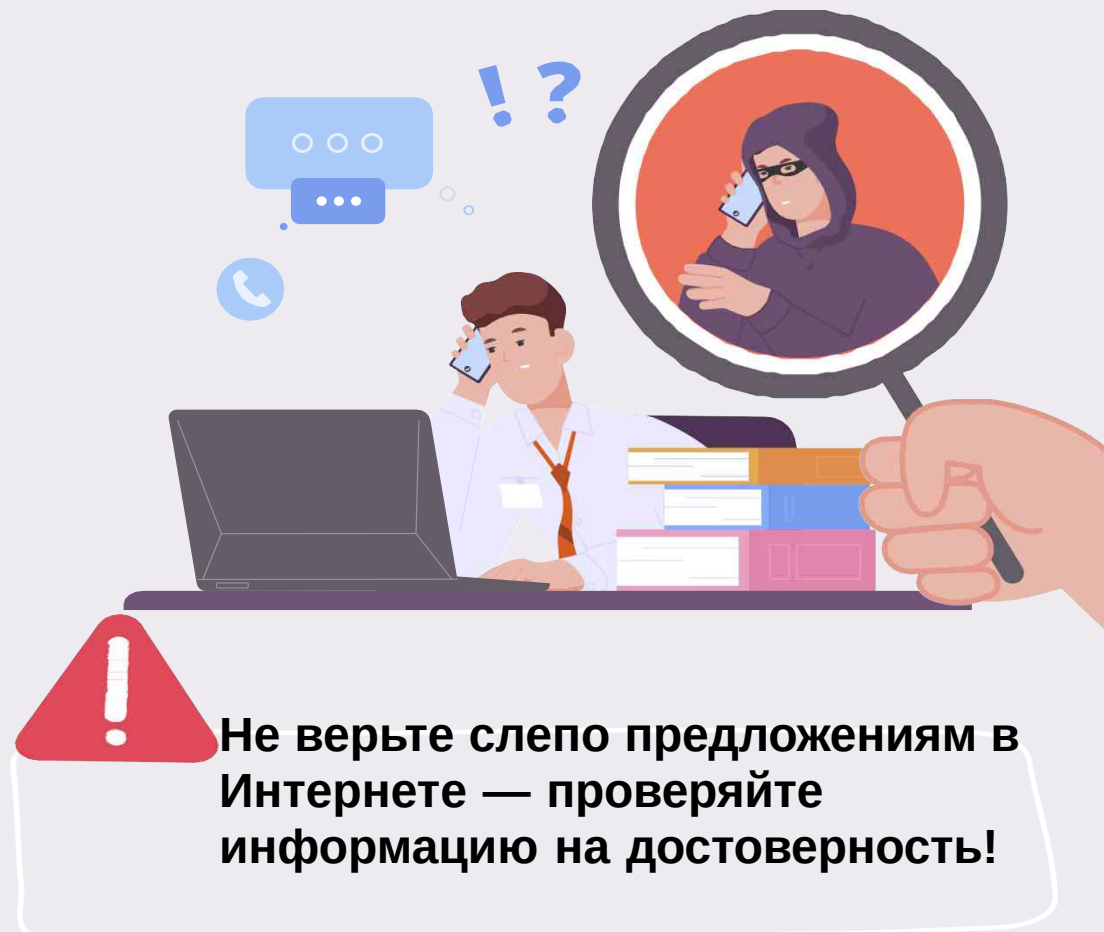
Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания!



Банк России

ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ В ИНТЕРНЕТЕ

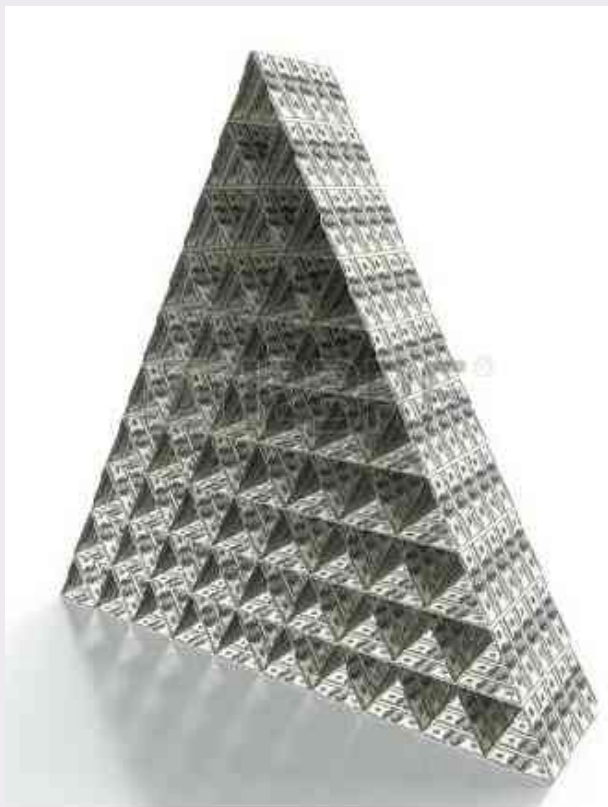
- Интернет-магазины и аукционы
- Восстановление кредитной истории
- Сообщение о крупном выигрыше или выплате от государства
- Заманчивое предложение о работе
- Льготные кредиты
- Туристические путевки со скидкой
- Сбор «пожертвований» для детей, больных, животных и др.
- Предложение вложиться в высокодоходные инвестиции





Банк России

3. Финансовые пирамиды



**Вам предлагают вложить деньги
под невероятно высокие проценты!**

Мошенническая схема получения
дохода, известная сотни лет

Финансы поступают за счет
постоянного привлечения новых
участников

Организаторы скрываются с
деньгами обманутых вкладчиков



Банк России

Признаки финансовых пирамид





Банк России

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ

- ✓ Не сообщайте никому личную и финансовую информацию (данные карты)
- ✓ Установите антивирусные программы на все свои гаджеты и регулярно обновляйте их
- ✓ Не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам
- ✓ Не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы

Заведите отдельную банковскую карту для покупок в Интернете



Будьте бдительны: не действуйте впопыхах и проверяйте информацию!



Банк России

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ



Самостоятельно звоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка



Установите двухфакторный способ аутентификации – например, логин и пароль + подтверждающий код из СМС



Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой



Будьте бдительны: не действуйте впопыхах и проверяйте информацию!



Банк России

ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИКАМ: МЕРЫ БАНКА РОССИИ



Обмен
информацией
с МВД России



Самоограничение
онлайн-операций



Отключение
каналов ДБО
дропам



Новый порядок
возврата
похищенных
денежных
средств



Период
охлаждения



Официальный
сайт Банка России
cbr.ru



Информация
доступным языком
fincult.info



Курсы для
инвесторов
любого уровня
school.moex.com/



Официальный портал
о социально-экономической
ситуации в России
obyasnyem.rf



Официальный сайт
Ассоциации развития
финансовой грамотности
fincubator.ru



Персональный
навигатор
по финансам
moifinansy.rf

Кто предупрежден - тот вооружен!

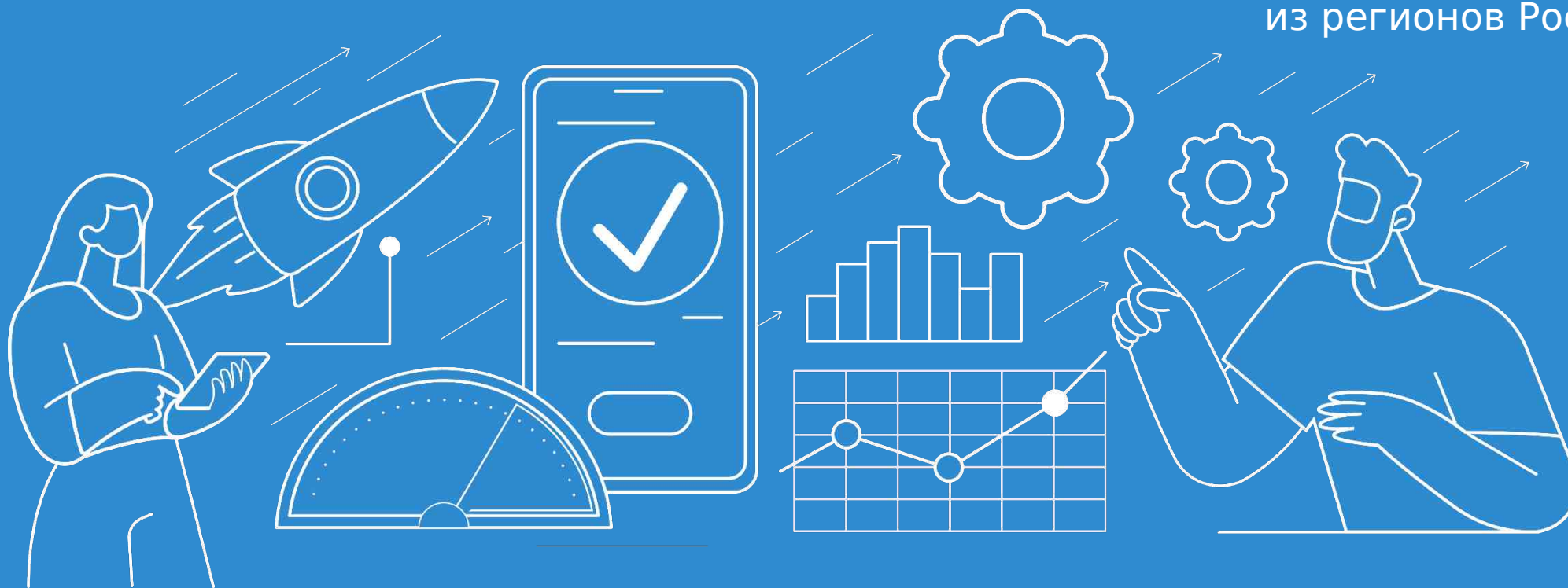


Банк России

Контактный центр Банка Рос

8-800-300-30-00

(для бесплатных звонков
из регионов России)



СПАСИБО ЗА ВНИМАНИЕ!