

ЦИФРОВАЯ БЕЗОПАСНОСТЬ И МОШЕННИКИ · QR-КОДЫ

Поддельный QR-код: как не потерять деньги и что делать, если уже оплатили

Закон № 161-ФЗ о национальной платёжной системе ст. 9 · Закон № 218-ФЗ о кредитных историях (самозапрет на кредиты) · ГК РФ ст. 1102 · УК РФ ст. 159, 159.3 · УПК РФ ст. 141, 144 · Актуально на октябрь 2026

Как пользоваться этим листом

Мошенники клеят свой QR-код поверх настоящего: на самокатах, парковках, счетах в кафе, флаерах. Код ведёт на поддельную страницу оплаты или ставит вредное приложение. Сверху — как не попасться. Ниже — что делать в первый час, если деньги ушли.

Как не попасться

- ✓ **Самокат, парковку, такси открывайте из приложения** **НЕ КАМЕРОЙ**
Сервисы аренды сканируют код через своё приложение. Если камера телефона открыла сайт и просит номер карты — это подделка.
- ✓ **Смотрите адрес сайта до ввода данных** **АДРЕС**
Лишние буквы, дефисы, цифры, необычная зона вместо привычной — закройте страницу. Значок замка ничего не доказывает: он есть и у мошенников.
- ✓ **Проверяйте получателя в СБП** **СБП**
При оплате по QR-коду банк показывает название получателя. Не совпадает с кафе или сервисом — не платите.
- ! **Наклейка поверх наклейки** **ПРИЗНАК**
Неровный край, код наклеен на код, другой цвет — повод не сканировать.
- ! **Код предлагает скачать приложение** **ПРИЗНАК**
Ставьте приложения только из официального магазина. Файл по ссылке из QR-кода может читать СМС с кодами банка.
- ✗ **Никому не называйте коды из СМС** **ПРАВИЛО**
Ни «поддержке», ни «банку», ни «оператору самоката».

Если уже ввели данные или оплатили

- 1 **Сразу заблокируйте карту**
В приложении банка или по номеру с обратной стороны карты. Смените пароль от банка, если вводили его.

- 2 Сообщите банку об операции без вашего согласия**
Не позже дня, следующего за днём, когда банк уведомил вас об операции (ч. 11 ст. 9 закона № 161-ФЗ). Письменно, через приложение или в отделении. Сохраните номер обращения.
- 3 Удалите приложение, если ставили**
Отключите телефон от интернета. Банку скажите, что было вредное приложение.
- 4 Заявление в полицию**
О мошенничестве (ст. 159, 159.3 УК). Приложите выписку, скриншоты, фото QR-кода и место, где он висел. Возьмите талон-уведомление о приёме заявления.
- 5 Поставьте самозапрет на кредиты**
Через Госуслуги, если мошенники могли получить паспортные данные или доступ к банку. Снять запрет можно в любой момент.

Вернёт ли банк

- ✓ Списали без вашего подтверждения** СТ. 9 161-ФЗ
Вы сообщили банку вовремя, а банк не выполнил своих обязанностей по защите — требуйте вернуть деньги. Отказ банка можно обжаловать финансовому уполномоченному и в суде.
- ! Вы сами ввели карту и код из СМС** СЛОЖНЕЕ
Банк считает, что операцию подтвердили вы. Требование к банку слабое. Основной путь — уголовное дело и иск к получателю денег о возврате неосновательного обогащения.
- ! Оспорить покупку через платёжную систему** НЕ ЗАКОН
Опротестование операции по карте — правило платёжной системы, а не право по закону. Попросите банк об этом в том же обращении, но не рассчитывайте только на него.

Чего не делать

- ✗ Не ждите до утра — первые часы решают, успеют ли перевести деньги дальше.
- ✗ Не звоните по номерам из СМС и с поддельной страницы — только по номеру на карте.
- ✗ Не платите «службе возврата денег»: это вторая волна того же мошенничества.

КОДОВОЕ СЛОВО

самокат

Напишите его боту @labpravabot — пришлём этот лист и разберём вашу ситуацию.
Телефон +7 (499) 390-60-21 · labprav.ru

Оплатили по чужому QR-коду? Напишите в Telegram @labpravabot, когда и как ушли деньги и что ответил банк, — скажем, что требовать от банка и как подать заявление в полицию.

Нужен разбор вашего случая: письменная консультация юриста — правовая позиция, перечень документов и план действий по шагам. Заключение остаётся у вас. Запись по телефону +7 (499) 390-60-21.