



# Мошенничество через QR-коды на улице: как не стать жертвой

В современном мире QR-коды стали неотъемлемой частью нашей повседневной жизни. От оплаты товаров до доступа к информации – их вездесущность делает их удобными, но также открывает двери для новых видов мошенничества. Эта презентация расскажет вам, как оставаться в безопасности.

# Что такое QR-код и почему он удобен?

QR-код (Quick Response Code) — это двухмерный штрихкод, разработанный в Японии. Он способен хранить большой объем информации и легко считывается камерой смартфона.

- **Мгновенный доступ:** Быстрый переход по ссылкам, загрузка приложений.
- **Бесконтактная оплата:** Широко используется для совершения платежей без физического контакта.
- **Распространенность:** Встречается в магазинах, ресторанах, на транспорте и в рекламе.





# Как мошенники используют QR-коды?

Удобство QR-кодов стало инструментом для злоумышленников. Они создают поддельные коды, которые внешне неотличимы от настоящих, но ведут к опасным последствиям.

## 1 Наклейки-обманки

Мошенники размещают свои QR-коды поверх настоящих на уличных плакатах, парковочных автоматах, меню кафе.

## 2 Фальшивые сайты

Сканирование такого кода перенаправляет жертву на фишинговый сайт, который выглядит как официальный.

## 3 Кража данных

На этих сайтах запрашиваются личные данные, пароли или информация о банковских картах.

## 4 Вредоносное ПО

В некоторых случаях QR-код может инициировать загрузку вредоносных приложений на ваше устройство.

# Пример мошенничества: фальшивые QR-коды на парковках



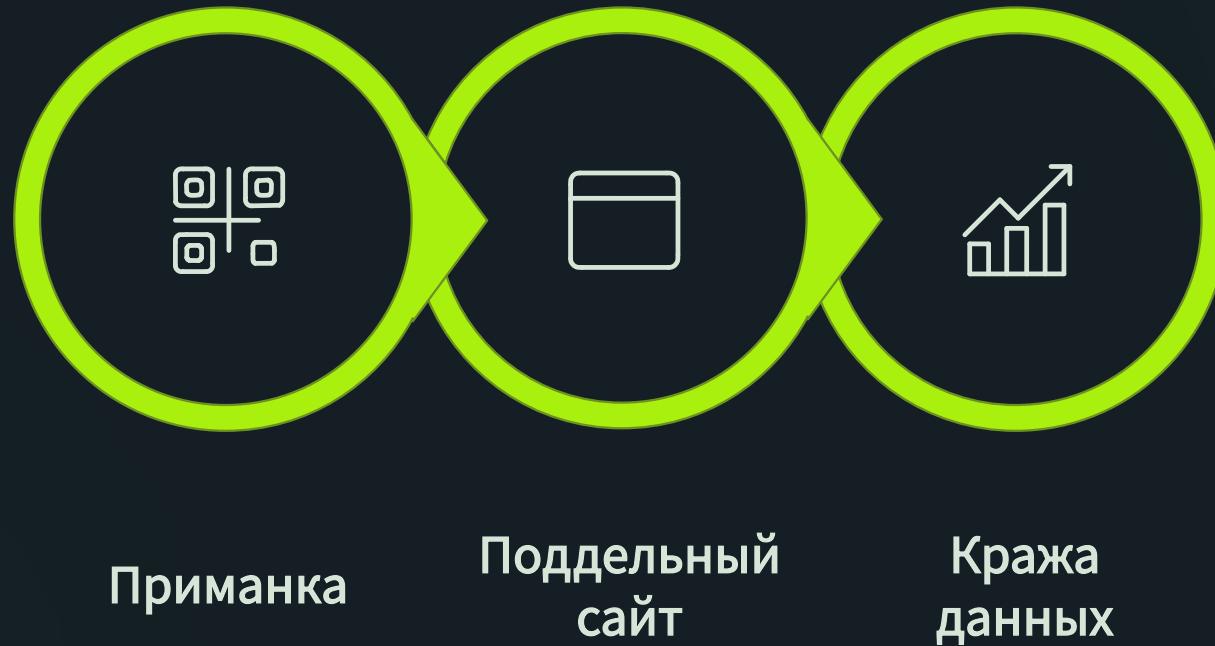
Остин, Сан-Антонио и другие города США

В крупных городах мошенники активно использовали поддельные QR-коды на парковочных счетчиках. Водители, спешащие оплатить парковку, сканировали эти коды.

Вместо официальной страницы оплаты они попадали на подставные сайты, где вводили данные своих банковских карт. Таким образом деньги списывались мошенниками, а парковка оставалась неоплаченной.

Общий ущерб от такого вида мошенничества исчисляется сотнями тысяч долларов.

# Как работает атака «квишинг» (QR-фишиング)?



«Квишинг» – это разновидность фишинга, где вместо вредоносных ссылок в электронной почте используются поддельные QR-коды. Эта схема может быть очень убедительной из-за быстроты и кажущейся надежности QR-кодов.

# Опасности после сканирования

1

## Кража личных данных

Мошенники получают доступ к вашим логинам, паролям, данным банковских карт, адресу, номеру телефона.

2

## Финансовые потери

Незаконное списание средств со счетов, оформление кредитов на ваше имя.

3

## Вредоносное ПО

Установка шпионских программ или вирусов, которые могут контролировать ваше устройство.

4

## Компрометация аккаунтов

Ваши социальные сети, электронная почта или мессенджеры могут быть использованы для рассылки спама или другого мошенничества.

# Как распознать мошеннический QR-код?

Будьте бдительны и внимательны к деталям!



## Признаки наклеек

Если QR-код выглядит как наклейка, приклеенная поверх другого, аккуратно потяните уголок. Часто мошенники просто заклеивают настоящие коды.



## Контекст и качество

Обращайте внимание на качество печати, орфографические ошибки, несоответствие дизайна официальным материалам. Подозрительные предложения или слишком заманчивые акции тоже повод задуматься.



## Проверяйте URL

После сканирования, но до перехода по ссылке, ваш телефон покажет URL. Убедитесь, что он начинается с `https://` и соответствует ожидаемому официальному адресу.

# Советы по безопасности при использовании QR-кодов



## Не торопитесь

Всегда проверяйте код на наличие признаков подделки, прежде чем сканировать.



## Используйте встроенный сканер

Сканеры, интегрированные в камеру телефона, часто имеют дополнительные функции безопасности.



## Ручной ввод URL

Если есть сомнения, лучше вручную ввести адрес сайта в браузере, чем рисковать.



## Обновляйте ПО

Регулярно обновляйте операционную систему и антивирус на своем смартфоне для максимальной защиты.



# Что делать, если вы стали жертвой?

Действуйте быстро, чтобы минимизировать ущерб!

01

## Свяжитесь с банком

Немедленно заблокируйте все скомпрометированные банковские карты и счета. Сообщите о мошеннической операции.

03

## Сообщите в полицию

Подайте заявление в правоохранительные органы (полицию, киберполицию) с подробным описанием произошедшего.

02

## Измените пароли

Срочно поменяйте пароли на всех важных онлайн-сервисах, особенно на тех, где вы использовали украденные данные.

04

## Проверьте устройство

Запустите полное сканирование антивирусом на вашем телефоне, чтобы убедиться в отсутствии вредоносного ПО.

# Итог: Будьте внимательны и защищайте себя!

QR-коды – это мощный и удобный инструмент, но, как и любая технология, они могут быть использованы во вред. Ваша осведомленность и внимательность – лучшая защита.

- **Думайте, прежде чем сканировать:** Проверяйте источник и контекст.
- **Безопасность прежде всего:** Ваш телефон и ваши данные – ваша ответственность.
- **Доверяй, но проверяй:** Всегда перепроверяйте URL-адреса.

