Как Узнать, Безопасен Ли QR-Код, Прежде Чем Открыть Его (Руководство по Квишингу)

Квишинг — это фишинг через QR-коды. Узнайте о тревожных сигналах перед сканированием и о том, что проверить перед нажатием 'Открыть'.

Автор: Lubor Šimůnek · Опубликовано: August 23, 2026 · Безопасность

Онлайн-версия: https://appstoryo.com/ru/blog/qr-code-safe-quishing-guide



Что такое квишинг?

Квишинг — это фишинг с использованием QR-кодов. Злоумышленник создаёт код, который после сканирования перенаправляет пользователя на вредоносный сайт, предназначенный для кражи учётных данных, установки вредоносного ПО или отображения поддельной платёжной страницы. Термин объединяет 'QR' и 'phishing', а угроза стремительно распространяется, поскольку люди доверяют QR-кодам почти автоматически.

Почему QR-коды представляют особую опасность

С обычной ссылкой можно навести курсор и прочитать URL перед нажатием. С QR-кодом вы не видите цель до момента его декодирования сканером — а многие приложения камеры мгновенно открывают браузер, не показывая адрес. Этого мгновения достаточно, чтобы вредоносный сайт начал отслеживать ваше устройство.

QR-коды также полностью обходят спам-фильтры: фильтры ищут подозрительный текст или известные вредоносные URL, однако изображение QR-кода выглядит совершенно безобидно. Именно поэтому фишинговые письма всё чаще заменяют гиперссылки QR-кодами, особенно в атаках на сотрудников компаний.

В реальной жизни квишинг встречается в виде наклеек поверх легитимных кодов на парковочных автоматах, поддельных меню ресторанов, фиктивных уведомлений о посылках в почтовых ящиках и поддельных общественных зарядных станций с предложением 'отсканировать для оплаты'.

Предупреждающие признаки ДО сканирования

- **Наклейка поверх оригинального кода.** QR-наклейка, приклеенная поверх другого кода, — классическая подмена. Осторожно поднимите угол: если отклеивается, не сканируйте.
- **Язык срочности на незнакомом флаере.** 'Сканируйте сейчас, чтобы получить приз' или 'Ваша посылка задержана — отсканируйте для переноса доставки' — это тактики психологического давления.
- **Нежелательное письмо или сообщение.** Неожиданное сообщение от банка, службы доставки или госоргана, где QR-код является основным призывом к действию, — весомый тревожный сигнал.

Что проверить ПОСЛЕ сканирования и ДО открытия

- **Соответствует ли домен ожиданиям?** Если вы сканировали QR-код в банке, URL должен находиться на официальном домене.
- **Это сократитель ссылок?** Сервисы bit.ly или tinyurl.com скрывают настоящий адрес назначения. Воспользуйтесь сервисом расширения URL, чтобы узнать реальный адрес до перехода.
- **Домены с ошибками или подделки.** Обращайте внимание на paypa1.com (цифра 1 вместо буквы L) или g00gle.com (нули вместо буквы O). Внимательно читайте каждый символ.
- **Подозрительные поддомены.** login.secure.amazon-dostavka-ru.com выглядит законно, но настоящий домен — amazon-dostavka-ru.com, а не amazon.com.

Как помогает QR Code Reader Without Ads

QR Code Reader Without Ads отображает полный URL-адрес до открытия чего-либо, давая вам время проверить ссылку перед действием. Если адрес кажется подозрительным, просто не нажимайте 'Открыть'. Приложение хранит историю сканирований локально на вашем устройстве, не собирает данные и не показывает рекламу. Найдите его в App Store или Google Play, введя 'QR Code Reader Without Ads'.

Скачайте QR Code Reader Without Ads бесплатно для iOS или Android — без рекламы, без слежки и полностью офлайн.

Как цитировать: Lubor Šimůnek (2026). *Как Узнать, Безопасен Ли QR-Код, Прежде Чем Открыть Его (Руководство по Квишингу)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/ru/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.