

РАЗБОР

Мы так привыкли к QR-кодам, что забываем: с их помощью мошенники умеют обманывать пользователей.

Как сканировать такие коды безопасно? Инструкция «Медузы»

06:29, 2 июня 2024 · Источник: Meduza

[Ссылка на материал](#)

Это PDF-версия материала, опубликованного на «Медузе». Вы можете отправить этот файл в любом мессенджере или по электронной почте вашим близким в России, особенно тем, кто не умеет обходить блокировки. Вы можете также распечатать этот текст и показать его тем, кто не пользуется интернетом.

«Медуза» признана «нежелательной» организацией на территории РФ, поэтому, пожалуйста, будьте осторожны и делитесь нашими материалами только с теми, кому доверяете.

Подробнее о «нежелательном» статусе.

Самый удобный способ читать «Медузу» без VPN — это скачать наше приложение. Оно работает в России, несмотря на блокировку, и это абсолютно безопасно. Версия для iOS и для Android.

Приложение на Android также можно скачать по прямой ссылке. Устанавливайте приложение не только себе, но и близким!

QR-коды стали частью нашей повседневной жизни благодаря своему удобству и универсальности. Они встречаются повсюду, от рекламных материалов и упаковок продуктов до меню в ресторанах и билетов на мероприятия. С помощью QR-кодов мы можем быстро получить доступ к информации, загрузить приложения, оплатить покупки и многое другое. Но их плюсы оценили не только обычные пользователи, но и злоумышленники. «Медуза» объясняет, в чем заключается основная угроза пользования QR-кодами — и как можно ей противостоять.

В чем опасность QR-кодов?

Главная угроза — это quishing, то есть фишинг с помощью QR-кодов. Жертва сканирует QR-код, который перенаправляет ее на мошеннический сайт, предлагает залогиниться. В итоге злоумышленники получают доступ к учетной записи жертвы. Пользователи часто менее осторожны при сканировании QR-кодов, считают их безопасными или не задумываются об этом риске.

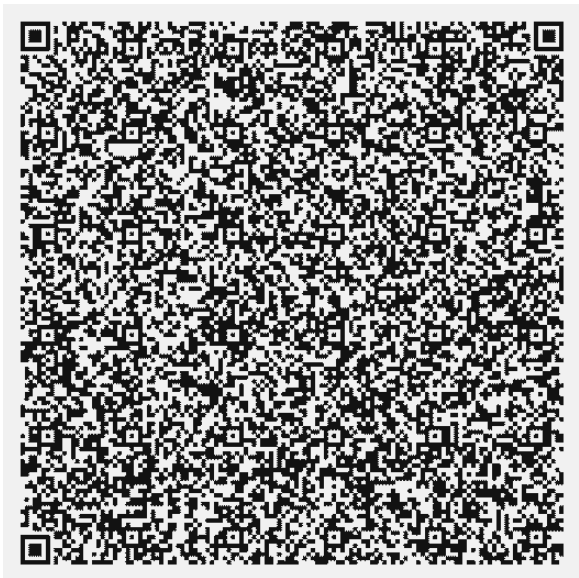
Злоумышленники стали рассылать такие QR-коды через электронную почту, так как это позволяет обойти традиционные методы защиты от фишинга. Их сложнее

анализировать автоматическими системами безопасности. Это затрудняет обнаружение и блокировку мошеннических QR-кодов.

Таким же образом можно рассылать и ссылки на вредоносные приложения со спрятанными внутри вирусами или троянами⁽¹⁾. Чтобы устройство оказалось заражено, пользователь должен их скачать и установить. В QR-код можно записывать не только текстовые строки, но и двоичный код. При этом разместить вирус в самом QR-коде вряд ли получится.

Вредоносная программа должна быть очень компактной, а в QR-код может уместиться всего 2953 байта двоичного кода. А вирус надо не только записать, но и каким-то образом заставить сканер QR-кода его запустить.

В 2020 году разработчик Мэтью К. С. Вонг сумел уместить в QR-коде игру «змейка» в виде исполняемого файла. Но для запуска его надо не только отсканировать, но и сохранить в виде exe-файла, перенести в Windows (если сканировать QR-код на телефоне), а потом еще и запустить там. Функционирующую таким образом вредоносную программу назвали бы «албанским вирусом» (он просит пользователя самостоятельно удалить все файлы и разослать себя другим жертвам).



QR-код с игрой «змейка»

То есть для успешной атаки надо не только уместить код в ограниченный размер двумерного штрихкода, но и найти такую уязвимость в сканере, которая бы его автоматически запустила.

С мошенническими QR-кодами можно встретиться не только в интернете, но и в реальной жизни. Злоумышленник может наклеить свой QR-код поверх реального в меню ресторана, на стенде в музее или на памятнике.

Что можно предпринять для защиты?

Не торопитесь

QR расшифровывается как «быстрый отклик» (quick response). Но ради безопасности лучше всего, наоборот, немного помедлить. Например, визуально сравнить адрес криптокошелька на сайте и в QR-коде, прежде чем переводить криптовалюту. Или вместо того, чтобы сразу переходить по адресу, распознанному сканером, можно проверить его с помощью сервиса VirusTotal, использующего десятки антивирусов для проверки файлов и ссылок на наличие вирусов, троянов, червей⁽²⁾ и других типов вредоносного программного обеспечения. Перед сканированием можно подойти и всмотреться в QR-код, размещенный на стенде, памятнике или другом объекте — чтобы проверить, не наклеен ли он поверх другого.

Используйте надежные сканеры QR-кодов

Во многих случаях достаточно использовать QR-сканер, встроенный в ваше мобильное приложение для съемки фото и видео. Если злоумышленники сумеют уговорить вас установить их собственное приложение для сканирования QR-кодов, то оно в теории может подменять не только ссылки, но и, например, адреса криптокошельков.

Даже если для работы с конкретным QR-кодом требуется установить отдельное приложение, всегда можно сначала отсканировать его стандартным сканером и посмотреть, что же там внутри. Скорее всего это будет текстовое

сообщение, какая-то ссылка или секретный код для двухфакторной аутентификации (то же — в виде ссылки, начинающейся с *otpauth://totp*). Лишь в редких случаях (вроде европейских «ковидных» QR-кодов) вы встретитесь с непонятным набором символов.

Для автоматической проверки ссылок через VirusTotal вы можете установить на свой телефон сканер QR-кодов компании Trend Micro (есть версии для андроидов и для айфонов).

Используйте пасски⁽³⁾ или ключи FIDO U2F⁽⁴⁾

Они гарантированно защитят вас от фишинговой атаки, даже если вы перейдете по подозрительной ссылке. USB-ключи с протоколом FIDO U2F (FIDO1) и пасски (FIDO2) не дадут злоумышленникам воспользоваться вашей неосмотрительностью, так как позволяют залогиниться только при использовании правильной ссылки.

Главная проблема заключается в том, что эти технологии поддерживают пока лишь небольшое количество сайтов.

Устали создавать и запоминать пароли? Возможно, скоро они не понадобятся вовсе: Apple, Google и Microsoft готовят для нас «беспарольное будущее» с помощью новой технологии. Вот как она работает (не идеально)

Что делать, если я параноик?

Можно научиться декодировать QR-коды вручную. В декабре 2023 года на хакерской конференции Chaos Communication Congress была представлена подробная инструкция, в теории позволяющая отказаться от сканеров в виде приложений.

Но в этом случае вам придется:

- научиться разбивать QR-код на сетку и выделять ключевые блоки;
- определять угловые маркеры для правильной ориентации двухмерного штрихкода и установления размера сетки;
- находить информацию об используемом формате и маске;
- извлекать данные, считывая оставшиеся черные и белые квадраты в нужной последовательности и накладывая на них определенную маску.

«Медуза»

(1) Троян

Вредоносная программа, которая маскируется под легальное программное обеспечение.

[Вернуться к тексту](#)

(2) Червь

Вредоносная программа, самостоятельно распространяющаяся через локальные и глобальные компьютерные сети.

[Вернуться к тексту](#)

(3) Пасски

Форма беспарольной аутентификации, использующей асимметричную криптографию. Вместо пароля при регистрации создается пара ключей: приватный остается на устройстве пользователя (аутентификаторе), а публичный передается на хранение сервису. Они же потом используются для аутентификации пользователя при входе в учетную запись.

[Вернуться к тексту](#)

(4) U2F

Открытый стандарт аутентификации, который использует один ключ для нескольких сервисов. Он упрощает и повышает уровень безопасности, обеспечиваемый двухфакторной аутентификацией, поскольку не требует установки драйверов или клиентского программного обеспечения.

[Вернуться к тексту](#)
