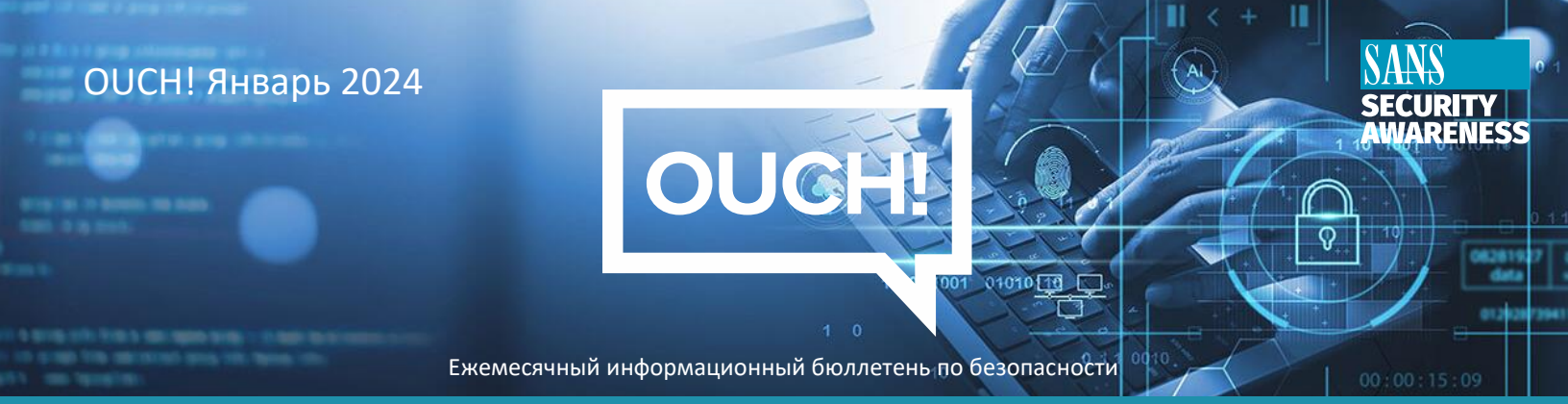
OUCH! Январь 2024



Ежемесячный информационный бюллетень по безопасности

QR-коды

Обзор

Вы когда-нибудь задумывались, что означают эти квадраты из точек или полос, называемые «QR-кодами»? Скорее всего, вы видели их размещенными на веб-сайтах, на плакатах, в качестве мобильных билетов или на столиках в ресторанах. Как это работает и есть ли риски, о которых вам следует беспокоиться? Давайте выясним.

QR-код, указывающий на сайт SANS OUCH.

Как работают QR-коды?

QR-код расшифровывается как «Код быстрого ответа» и представляет собой машиночитаемый код, обычно состоящий из матрицы черных и белых квадратов (они также могут быть других цветов и содержать фоновые изображения). Эти квадраты можно легко создать с помощью генераторов QR-кодов, и они используются для кодирования такой информации, как URL-адреса веб-сайтов, контактная информация электронной почты или другие типы данных. Думайте о QR-кодах как о штрих-кодах, но более универсальных. Большинство камер мобильных устройств распознают и декодируют информацию, закодированную в QR-коде. Другими словами, когда вы пытаетесь сфотографировать QR-код с помощью камеры вашего устройства, оно декодирует QR-код и спросит вас, хотите ли вы действовать в соответствии с содержащейся в нем информацией, например открыть ссылку на веб-сайт.

В чем опасность?

QR-коды могут быть трудными для интерпретации людьми, что облегчает киберзлоумышленникам кодирование информации, которая может быть вредоносной, Например, QR-код может отправить вас на вредоносный веб-сайт, который пытается получить вашу личную информацию, например пароли или номера кредитных карт, или, возможно, даже попытаться установить вредоносное ПО на ваше устройство. Кроме того, QR-коды могут выполнять дополнительные действия, такие как добавление контакта в список контактов или составление электронного письма от вашего имени. QR-код сам по себе не представляет угрозы; однако информация или действие, которые он вызывает, могут быть таковыми.

Например, вы находитесь в городе или, возможно, в аэропорту, и на стене висит плакат, рекламирующий продукт, который вас интересует. На плакате есть QR-код, который можно использовать для быстрого получения дополнительной информации. Чего вы не осознаете, так это того, что кто-то закрыл QR-код плаката наклейкой с другим QR-кодом. Когда смотришь на плакат, доверяешь ему, не осознавая, что QR-код на плакате подменил преступник. Когда вы сканируете QR-код, чтобы узнать больше о продукте, вы перенаправляетесь на веб-сайт, контролируемый преступником.

Итак, что вам нужно делать?

- Будьте осторожны, прежде чем доверять и сканировать QR-код. Сначала спросите себя: Можно ли доверять источнику? Доверяете ли вы плакату, ресторану или веб-сайту, на котором указан QR-код? Если кто-то оставил на вашей машине рекламный проспект с QR-кодом, можете ли вы ему доверять?
- После того, как вы отсканируете QR-код, ваше устройство спросит вас, хотите ли вы действовать на основе прочитанной информации. Например, если QR-код является ссылкой на веб-сайт, прежде чем перейти на него, ваше устройство спросит вас, хотите ли вы посетить этот сайт. Уделите время просмотру призыва к действию или самой ссылки и убедитесь, что вам удобно ее посещать.
- Убедитесь, что ваши мобильные устройства всегда обновлены и на них установлена последняя версия операционной системы. Это гарантирует наличие новейших функций безопасности. Самый простой способ сделать это — включить автоматические обновления.
- Для декодирования QR-кодов не нужно устанавливать специальные мобильные приложения, достаточно просто использовать встроенную камеру вашего устройства. Если веб-сайт требует загрузки специализированного приложения для сканирования QR-кодов, скорее всего, это подделка.
- Подумайте дважды, прежде чем предоставлять конфиденциальную или личную информацию любому веб-сайту, на который вы зашли с помощью общедоступного QR-кода.

QR-коды — это удобный способ получить доступ ко всей новой информации и возможностям. Выполнив несколько простых шагов, вы сможете максимально эффективно и безопасно использовать их.

Приглашенный редактор

Абдулмаджид АльАбдулхади — консультант по системам ИТ/ОТ в Saudi Aramco с более чем 27-летним опытом работы. Он является сертифицированным аудитором информационных систем (CISA) и сертифицированным менеджером по информационной безопасности (CISM) с патентом на кибербезопасность, выданным патентным ведомством США (10 693 906).

Ресурсы

Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Вишинг - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing/
Защита ваших мобильных устройств: https://www.sans.org/newsletters/ouch/securing-mobile-devices/

Роман Полаков