OUCH! January 2024

The Monthly Security Awareness Newsletter for You

QR Codes

Overview

Have you ever wondered what those squares of dots or bars called “QR codes” are all about? You most likely have seen them posted on websites, printed on posters, used as mobile tickets, or on restaurant tables. How do these work, and are there risks you should be worried about? Let’s find out.

QR code pointing to the SANS OUCH website.

How Do QR Codes Work?

QR code stands for “Quick-Response code” and is a machine-readable code usually consisting of a matrix of black and white squares (they can also come in other colors and contain background images). These squares can be easily created with QR code generators, and they’re used to encode information such as website URLs, email contact information, or other types of data. Think of QR codes like bar codes but more versatile. Most mobile device cameras recognize and decode the information coded in a QR code. In other words, when you try to take a picture of a QR code with your device’s camera, it will decode the QR code and ask you if you want to act on the information it contains, such as opening a link to a website.

What Is the Danger?

QR codes can be difficult for people to easily interpret, which makes it easier for cyber attackers to encode information that could be malicious or cause harm. For example, a QR code could send you to a malicious website that attempts to harvest your personal information, like passwords or credit card numbers, or perhaps even try to install malware on your device.

In addition, QR codes can take additional steps, such as adding a contact to your contacts list or composing an email on your behalf. The QR code by itself is not the threat; however, the information or action it triggers can be.

For example, let's say you are in the city or perhaps in an airport, and there is a poster on a wall promoting a product that interests you. The poster has a QR code you can use to quickly get more information. What you don't realize is that someone has covered the poster's QR code with a sticker of a different QR code. When you look at the poster you trust it, not realizing that the QR code on the poster has been replaced by a criminal. When you scan the QR code to learn more about the product, you are directed to a website controlled by the criminal to start an attack.

What Should I Do to be Safe?

- Be careful before trusting and scanning a QR code. First, ask yourself: Can you trust the source? Do you trust the poster, restaurant, or the website that is showing the QR code? If someone left a handout on your car with a QR code, can you believe it?
- Once you scan a QR code, your device will ask you if you want to act on the information it reads before it does anything. For example, if the QR code is a link to a website, your device will ask you if you want to visit the site before going to it. Take time to review the call to action or the link itself and ensure you feel comfortable visiting it.
- Confirm your mobile devices are always updated and running the latest version of its operating system. This ensures that it has the latest security features. The easiest way to do this is to enable automatic updates on your device.
- There is no need to install special mobile apps to decode QR codes, you should be able to simply use your device's built-in camera. If a website is requiring you to download a specialized QR scanning app, it is most likely counterfeit or fake.
- Think twice before providing confidential or personal information to any website that you reached via a publicly visible QR code.

QR codes are a convenient way to access all sorts of new information and capabilities. Taking a few simple steps can help you make the most of them, safely and securely.

Guest Editor

Abdulmajeed AlAbdulhadi is an IT/OT systems consultant in Saudi Aramco with more than 27 years of experience. He is a Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) with a granted cybersecurity patent by the US patent office (10,693,906).

Resources

Messaging / Smishing Attacks: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Vishing – Phone Call Attacks and Scams: https://www.sans.org/newsletters/ouch/vishing/
Securing Your Mobile Devices: https://www.sans.org/newsletters/ouch/securing-mobile-devices/