Don’t be a victim of Quishing

Published 10/15/2024 by Giuseppe Aloisi

Don’t be a victim of Quishing

Quishing, also known as **QR phishing**, is a cybersecurity threat in which attackers embed malicious content within QR codes and trick unsuspecting users into scanning them, leading them to fraudulent websites or installing malware on their devices. This method bypasses traditional security measures and allows cybercriminals to steal sensitive information or gain unauthorized access to devices.

As people increasingly use QR codes for various purposes, such as accessing menus or making payments, they may unknowingly scan these deceptive codes, putting their personal information at risk.

The versatility of QR codes, which can be scanned from both screens and paper, has led to their widespread adoption across various industries, including payment processing, marketing, and advertising. Today, QR codes are commonly found in public spaces like billboards and restaurants, as well as in digital communications such as emails, text messages, and social media.

There are two kinds of QR codes— **Static** and **Dynamic** QR codes. **Static QR codes** are fixed and cannot be altered once created. They don’t use a short URL. Instead, the information is encoded directly into the image. These QR codes are commonly used to advertise static information like a website URL and contact details. On another hand, **dynamic QR codes** are more flexible as the information they encode can be updated or changed without changing the code’s appearance. They contain a unique URL that directs users to a server where the information is stored. This flexibility poses high security risk, as scammers can exploit dynamic QR codes by altering their source to redirect users to malicious sites.

How can a quishing attack be detected and prevented?

To protect yourself from QR code fraud, it’s important to be vigilant and look for certain signs before scanning a QR code.

- **Unexpected or unsolicited QR codes**: Be cautious of QR codes that appear in unsolicited emails or messages, especially if they prompt you to take immediate action.
- **Lack of context or explanation:** Legitimate QR codes are usually accompanied by clear explanation of their purpose.
- **Suspicious Sender:** Do you recognize the sender, and is the email address correct? Check the sender’s email address or contact information for any sign of illegitimacy, such as misspelling or unusual domain names.
- **Urgency or pressure:** Does the tone or wording of the email seem off? Scammers often create a sense of urgency to prompt quick action. Be skeptical of messages that pressure you to scan a QR code immediately.
- **Verify the source:** If possible, verify the legitimacy of the QR code by contacting the supposed sender through official channels.
- **Be more cautious of publicly posted QR codes on posters:** Threat actors place malicious QR codes in public areas with the hopes that people passing by will scan them.
- **QR code scams on parking meters and other contactless payments:** One of the most common uses of QR codes is to enable customers to quickly pay for goods and services such as meals or parking. But any QR code placed in public offers a prime opportunity for scammers.
- **Use a secure QR code scanner:** Some QR code scanner apps offer security features that check the safety of the link before opening it. Consider such an app to add an extra layer of protection.