What is Quishing? How to prevent a Quishing attack?

What is a Quishing attack? How does this form of attack work and what can you do to protect yourself from being targeted?

What is a Quishing attack? How does this form of attack work and what can you do to protect yourself from being targeted? Let's find out how Squishing puts your device and data at risk.

What is Quishing?

Quishing, also known as QR code phishing, is a phishing technique involving QR codes to trick potential victims. Similar to other types of phishing attacks, the goal is to steal sensitive information, install malware on your device, or get you to visit a website.

Malicious individuals relying on QR codes have become increasingly common, especially during the pandemic, as people have become accustomed to using them.

How does Quishing work?

First, hackers plan their attack by creating a QR code that looks harmless. There are many online tools for generating QR codes, and you can even generate QR codes on your Android phone.

QR codes can redirect you to wrong payment gateways, malicious links or infected document archives. Hackers place malicious QR codes in places where victims can scan them to achieve their goals, such as restaurants, malls, parks, and airports. So, QR codes placed on fake posters, flyers and advertisements in public places could be concealing a phishing attack.

How can Quishing affect you?

Because hackers use QR codes, you may not realize you're the victim of a Quishing attack until it's too late. So you should know how Quishing can affect you.

1. You may be redirected to a phishing website

A scanned QR code can take you to a website designed to closely resemble the content you expect. In this way, hackers convince you to provide personal information such as phone number, email or credit card number.

2. It could be a malware attack

QR codes can also store content such as malware, ransomware or even Trojans. This software can be configured to automatically download and install on your device as soon as you scan a QR code. Hackers can install new software on your device, steal personal information, or track your activities.

3. It can control your social media accounts

Besides installing malware on your device, scanning QR codes can cause you to lose control of your social media accounts. For example, scanning a QR code can set up software to send emails from your account or message people on social media platforms like Instagram, WhatsApp, etc.

How to prevent Quishing attacks?

Not scanning any QR codes might be a bit excessive. However, there are some ways to protect yourself from Quishing.

1. Preview the URL

Before accessing the QR code's landing page, your device will preview the link. If the URL has been shortened and there's no way you can tell what the destination is, you're better off staying away from it.

Also, check the security protocol as most secure websites use the HTTPS protocol instead of HTTP.

2. Check the destination of the QR code

If you've visited the website, see the URL. If you notice any misspelled words, bad language, or low-resolution images, the site is most likely a scam. Additionally, if the site's content creates a sense of urgency or even requires immediate action, it's better to leave the site.

3. Use your built-in QR scanner

When in a hurry, you can download a third-party app to scan QR codes or find a scanning tool online. However, these tools can be developed and used by hackers to carry out a Quishing attack. To avoid that, you should use the QR scanner built into your phone's camera.