How To Avoid Malicious QR Codes

Closely Inspect URLs

Most often, your device will display a clickable link when you scan a QR code. Make sure to closely inspect the link to ensure that it's directing you to a legitimate website. If the URL looks suspicious or doesn't align with what you expected, don't click! QR codes are commonly used to direct victims to malicious websites.

Remain Skeptical

Criminals have been known to replace legitimate QR codes with malicious ones. This allows them to easily defraud people out of money or steal confidential information. As such, it's generally best to avoid QR codes in public areas, and remain especially skeptical of any that you receive at random via email.

Use the Default Scanner

Most modern phones allow you to use the default camera app to scan QR codes, while others have a built-in QR app. Stick with these default options and avoid downloading any third-party QR scanners, which have been known to be malicious and vulnerable to exploits.

Think Before You Scan

If you're unsure if a QR code is safe, don't scan. Use alternative methods to accomplish whatever you need the QR code for, such as typing the web address or website name directly into a browser. Also, remember that QR code phishing can occur both online (such as codes sent via email or social media) and offline (such as the parking lot example). Always think before you scan!

As a general rule of technology, any time something is made to be quicker and easier, criminals will find a way to leverage it. QR codes are a perfect example of this, and that's why it's important to always prioritize security over convenience.