QR Code Awareness

Cybercriminals are exploiting the growing use of QR codes to target unsuspecting users. They count on people scanning QR codes without checking their legitimacy first.

For example, a scammer might replace a legitimate QR code on a parking meter with a malicious one, tricking you into entering your credit card details on a fake website. Or they might swap the QR code on a restaurant table with one that downloads malware onto your device instead of showing the menu.

Follow these tips to stay safe while scanning:

Use Built-In Scanners

Most mobile devices have a built-in QR code scanner through the camera app. If your device doesn't, only download trusted scanning apps from official app stores.

Check for Tampering

Cybercriminals can easily print fake QR codes as stickers and place them over real ones. If something seems off, ask an employee to verify the code before scanning.

Preview the Link

Always preview the URL before clicking. Look out for misspellings or strange characters in the web address. When in doubt, don't click.

Be Cautious with Personal Information

Never enter sensitive details like passwords or credit card numbers unless you're certain the website is legitimate and belongs to the intended business.