# QR Code Scams

QR codes have become an important part of our everyday life, making tasks like checking menus or accessing websites more convenient. However, there's a darker side to QR codes – scammers can exploit them to deceive you. Here's a breakdown of QR code scams and some practical tips on how you can protect yourself.

## What Are QR Code Scams?

**QR code scams involve malicious QR codes that lead you to fake websites, apps, or actions. Scammers design these codes to steal your sensitive data, infect your device with malware, or trick you into sending money to someone you don't know.**

## How to Protect Yourself:

**Scan Wisely:** Only scan QR codes from sources you trust. Avoid scanning codes from random websites, flyers, or emails. When possible, verify the source of the QR code. If it's from a reputable company or a trusted source, it's probably safe. If you aren't absolutely sure it's safe, think twice before scanning. Remember if something feels off or too good to be true, it probably is. Trust your instincts.

**Use a QR Scanner App:** Download a reliable QR code scanner app from your device's app store. These apps often have built-in security features to detect malicious codes.

**Beware of Shortened URLs:** If a QR code leads to a shortened URL, use a URL expander service to reveal the full link before visiting the site.

**Review Permissions:** When a QR code prompts you to download an app, review the permissions it requests. If it asks for unnecessary access to your data, reconsider installing it.

**Keep your Software Updated:** Regularly update your devices operating systems and apps. These updates often include security patches to help protect you from vulnerabilities, including those associated with QR code scams.

**Avoid Personal Information Sharing:** Be cautious when QR codes lead you to a request for personal or financial information. Legitimate sources don't usually request this information via QR codes.