QR Code Safety

There's a catch to these convenient codes that can put your data at risk. Here's everything you need to know to protect yourself.

Know the Risks

Cybercriminals can use QR codes to lead unsuspecting users to malicious destinations, such as phishing websites or bogus apps. These can steal your payment information, download malware on your device that compromises your data, or even lead to a ransomware demand.

Check the Source

Always verify the source of the QR code. Scan codes only from trusted entities, like official websites, apps, or physical products. If the source looks sketchy—a QR code sticker placed over the original, for instance—avoid it.

Verify the URL

Examine the URL the QR code leads to before clicking it to ensure that it's legitimate. Is it an 'https' website, indicating a secure gateway? Even then it could lead to a malicious destination. Always confirm the site's spelling is legit. Any deviations are red flags.

Use a Trusted QR Code Scanner

Use a reputable QR code scanner app or your smartphone's built-in scanner, usually it's camera app, to minimize the risk.

Be Cautious with Personal Information

Don't share sensitive personal information through QR codes unless you're sure they're legitimate.

Analyze Permissions

Review the permissions requested by the website or app linked to the QR code. Be cautious if they request excessive access to your device. Taking the extra time to do this up front can prevent trouble later.

Keep Software Updated

Regularly update your smartphone's operating system and apps to patch security vulnerabilities.

New Term Alert: **Quishing**

When scammers use QR codes to target unsuspecting victims, it's called "Quishing." Learn more in this Barracuda blogpost.

Barracuda®

Your journey, secured.