Think Before You Scan: QR Code & Online Safety

What are QR Codes?

QR (Quick Response) codes are images that store website links. When scanned, your phone automatically opens the link which can be safe or dangerous depending on where it goes.

Why Random QR Codes Can Be Dangerous

Cybercriminals sometimes place fake or tampered QR codes in public places or send them through
messages. This is called Quishing (QR + Phishing).

Common Risks:

1. Fake Login Page: Steals your username/password.
2. Payment Scams: Sends money to attackers.
3. Malware Downloads: Installs harmful apps.
4. Redirect Tricks: Sends you through multiple hidden sites.

How to Spot a Suspicious QR Code:

1. The QR code is a sticker on top of something else.
2. It asks for personal info (SSN, password, credit card).
3. The website address looks misspelled.
4. The link does not start with https://

How to Check a QR Code Safely:

1. Use your phone's built-in camera.
2. Tap and hold to preview the URL before opening.
3. Ask yourself: Do I recognize this website?
4. If unsure, don't scan. Search the site manually.

Safe Online Habits:

1. Use unique passwords or a password manager.
2. Turn on Multi-Factor Authentication (MFA).
3. Keep your phone and apps updated.
4. Be skeptical of urgent messages.

Key Takeaway:

QR codes are not the threat it's where they lead. Always preview, verify, and think before you scan.

Sources:

Microsoft Security Blog QR-code phishing is growing
https://www.microsoft.com/en-us/security/blog/2024/11/04/how-microsoft-defender-for-office-365-innovated-to-address-qr-code-phishing-attacks/
Kaspersky What is "quishing" (QR phishing)?
https://www.kaspersky.com/resource-center/definitions/what-is-quishing
Norton (Gen) What is quishing? How to spot it
https://us.norton.com/blog/online-scams/quishing
WIRED How to not get hacked by a QR code
https://www.wired.com/story/how-to-qr-code-hacks-avoid