QR Code Scams – Stay Safe When Scanning

Cayenne Hot Tips!

How are these tips useful?

QR codes are now used everywhere — restaurants, parking, invoices, emails, and posters.
Scammers exploit this by replacing legitimate QR codes with malicious ones that redirect users to fake websites.
Once scanned, these codes can:

- Steal login credentials
- Install malware
- Redirect to fake payment pages
- Capture personal or company information

Unlike email links, QR codes hide the destination, making them harder to detect.

Do you have any questions?

If you have any questions, please feel free to reach out to us at Support@cayennecorp.com.

If you have any suggestions on the next tip topic you would like to would like to see, please let us know.

We highly value your input and would greatly appreciate any feedback. Whether it's a suggestion for improvement, or a specific tip you found particularly useful, your opinion matters to us.

Have a great day!

Be Careful Where You Scan QR Codes

Why:

QR codes in public places can be easily tampered with or replaced.

Benefit:

Reduces the risk of being redirected to malicious websites.

How:

- Avoid scanning QR codes on:
- Posters in public places
- Parking meters
- Stickers placed over original codes
- If possible, use a **known official website instead of scanning**

Check the Link Before Opening It

Why:

QR codes often redirect to a hidden URL.

Benefit:

Helps identify suspicious or fake websites before interacting with them.

How:

- After scanning, **do not open immediately**
- Preview the URL and check:
- Spelling errors (e.g., “micros0ft.com”)
- Strange domains
- Missing HTTPS (no padlock icon)

Here is a QR Code example

Extra Caution With QR Codes in Emails

Why:

Attackers now use QR codes in phishing emails to bypass security filters.

Benefit:

Reduces risk of phishing attacks.

How:

- Treat QR codes in emails the same as suspicious links
- Do not scan codes from unknown or unexpected senders
- Verify with the sender before scanning

Never Enter Credentials/Payment Info From a QR Code

Why:

Many QR scams lead to fake login or payment pages.

Benefit:

Prevents credential theft and financial fraud.

How:

- Do NOT enter:
- Email passwords
- Banking details
- MFA/verification codes
- Instead:
- Go directly to the official website manually

Use Your Device's Buil-in Security

Why: Modern devices include protections against malicious websites.

Benefit: Adds an extra layer of defence.

How:

- Keep your phone updated
- Use built-in browser protections (Safe Browsing, etc.)
- Avoid installing apps directly from QR codes

Bottom Line

QR codes are convenient, but they can also be used to hide malicious links and scams.

By following these steps, you can:

- Avoid phishing attacks
- Protect your credentials
- Prevent financial fraud
- Reduce security risks

If something feels off — don't scan it.

If you'd like to discuss this further or need assistance with any of the points mentioned here, we're here to help. Please email us at Support@cayennecorp.com