QR PHISHING:
HOW TO PREVENT THEM

QR phishing is a type of phishing attack that uses QR codes to trick victims into revealing sensitive information or downloading malware. Scammers may use QR codes in emails, text messages, social media, public places, or even approach people directly to scan them. To protect yourself, be suspicious of unsolicited QR codes, check the URL before scanning, use a QR code scanner app, keep your software up to date, be wary of QR codes in public places, don't scan QR codes from unknown people, and if unsure, don't scan it.

STEPS TO PREVENT:

BE WARY OF UNSOLICITED QR CODES

Scammers may send them in emails, text messages, or social media. If you don't recognize the sender or the message, don't scan the code.

CONFIRM TRUSTED SOURCES

If you receive a QR code from a company you know and trust, contact them directly to confirm its legitimacy before scanning.

SPOT PHISHING HALLMARKS

Be wary of QR codes that create a sense of urgency, appeal to your emotions, or have poor grammar

REVIEW QR CODE URLS CAREFULLY

Make sure the URL matches the website you expect to visit before scanning.

BE WARY OF PERSONAL INFO REQUESTS

Don't give out sensitive information, such as login credentials or credit card numbers, to a website you reached through a QR code.

FOR MORE INFO, EMAIL US AT:
cyberaware@purdue.edu