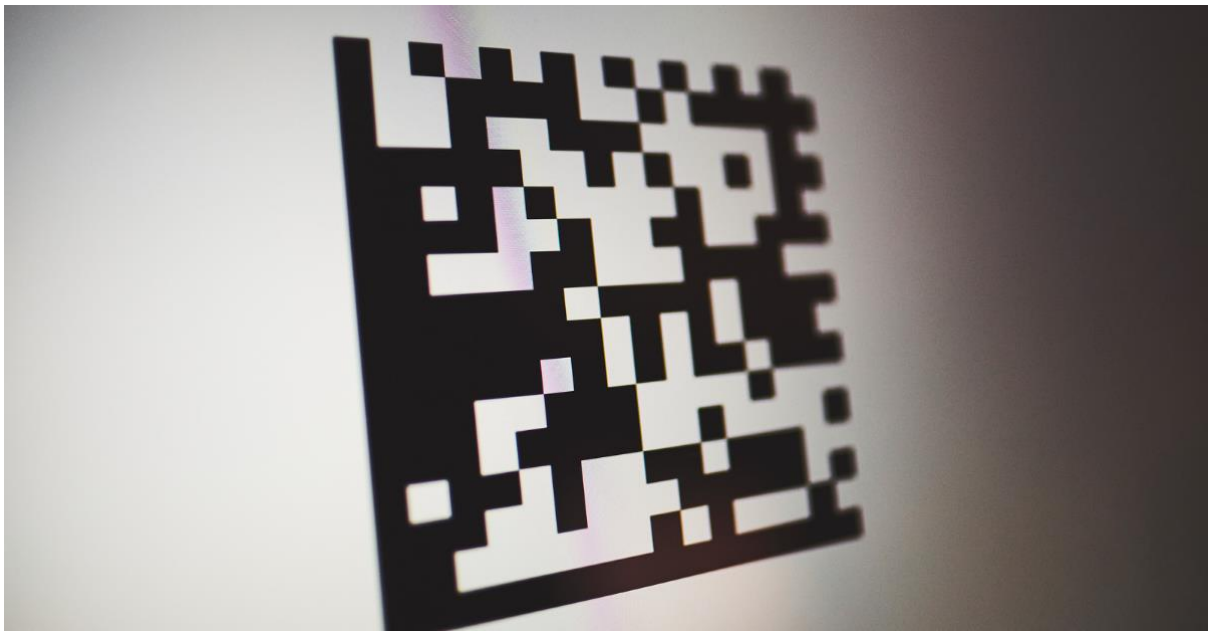
The Rising Threat of Quishing: How QR Code Phishing Is Evolving



QR code phishing, commonly known as “quishing,” has rapidly emerged as one of the fastest-growing cyber threats facing individuals and organizations today. As QR codes become increasingly common in everyday life—from restaurant menus and parking meters to mobile payments and workplace systems—cybercriminals are exploiting the trust and convenience associated with them to launch sophisticated phishing attacks.

In a quishing attack, malicious QR codes are embedded in emails, advertisements, PDFs, public posters, or even placed over legitimate QR codes in public spaces. Once scanned, users are redirected to fake websites designed to steal credentials, financial information, or install malware such as ransomware and spyware. Unlike traditional phishing links, QR codes conceal the destination URL, making it more difficult for users to identify malicious activity before it is too late.

Cybercriminals are increasingly impersonating trusted brands such as Microsoft, Adobe, HR departments, and financial institutions to pressure users into urgent actions like password resets, payroll updates, or account verification. Security researchers have also identified advanced techniques such as split QR codes and nested QR codes, which help attackers bypass traditional email security filters.

Why Quishing Is So Effective

- QR codes are widely trusted and commonly used in daily activities.
- Hidden URLs prevent users from easily verifying website legitimacy.
- Attackers create urgency through fake security alerts or exclusive offers.
- Mobile devices often lack the same security protections as corporate systems.

- QR codes can bypass traditional email security tools because they are image-based.

Common Quishing Attack Methods

- Fake QR codes placed over legitimate posters, kiosks, or parking meters.
- QR codes embedded in phishing emails or malicious PDF attachments.
- Fraudulent payment requests impersonating utility companies or government agencies.
- Fake HR or payroll notifications requesting employees to update information.
- Social media advertisements containing malicious QR codes linked to malware downloads.

Signs of a Quishing Attack

- Tampered, damaged, or suspicious-looking QR codes.
- Requests for passwords, banking details, or sensitive information after scanning.
- URLs containing unusual characters or unfamiliar domain names.
- QR codes promising unrealistic discounts, rewards, or prizes.
- Requests for excessive device permissions or software downloads.

Risks and Impact

- Credential theft and account takeovers (ATOs).
- Financial fraud and unauthorized transactions.
- Malware infections including ransomware and spyware.
- Data breaches affecting healthcare, finance, education, and enterprise sectors.
- Operational disruption, reputational damage, and regulatory penalties.

Key Recommendations for End Users

- Verify QR codes before scanning, especially in public spaces.
- Avoid scanning QR codes from unsolicited emails or text messages.
- Use trusted QR scanning apps that preview URLs before opening links.
- Carefully inspect website addresses after scanning.
- Never provide sensitive information without verifying the source.

- Be cautious of urgent messages, unexpected payment requests, or unrealistic offers.
- Keep mobile devices and security software updated regularly.
- Report suspicious QR codes or phishing attempts to the relevant authorities or IT teams.

Key Recommendations for IT Professionals

- Deploy advanced email security tools with QR code and OCR scanning capabilities.
- Implement multifactor authentication (MFA) using biometrics or hardware tokens.
- Conduct regular employee awareness and quishing simulation training.
- Strengthen email authentication using SPF, DKIM, and DMARC protocols.
- Use AI-powered monitoring tools to detect suspicious QR-related activity in real time.
- Continuously update incident response procedures to address quishing scenarios.
- Establish verification procedures for sensitive requests involving QR codes.
- Monitor for account takeover attempts and suspicious login behavior.
- Educate employees about advanced evasion tactics such as split and nested QR codes.

As QR code usage continues to expand globally, cybersecurity awareness must evolve alongside it. Quishing is no longer an emerging threat—it is now a mainstream attack method that requires constant vigilance, proactive security measures, and shared responsibility across both personal and professional environments.

Source: **The University of Tennessee, Knoxville, Trend Micro**