CS-038 · Email Security

QR Code Phishing (Quishing)

Phishing that hides malicious links inside QR codes to bypass filters and reach mobile devices.

Executive Summary

QR code phishing, often called quishing, hides a malicious link inside a QR code so that scanning it takes the victim to a counterfeit website. Because the destination is encoded as an image rather than a clickable link, it can slip past email filters that scan text and URLs, and it moves the victim onto a mobile device where warning signs are harder to see. Quishing has become a common tactic in credential-theft campaigns.

What It Is

Quishing is a variant of phishing that swaps a visible, clickable link for a QR code. The attacker embeds the malicious destination in the code and presents it with a plausible reason to scan, such as viewing a document, resetting a password, or completing a verification. When the recipient scans the code with a phone, they are taken to a fake login or payment page that captures their information, or prompted to install something harmful. The technique exploits two shifts at once: many email filters do not fully analyze the link hidden inside an image, and scanning pushes the interaction to a personal mobile device that may lack corporate protections and makes the true web address hard to inspect.

Why It Matters

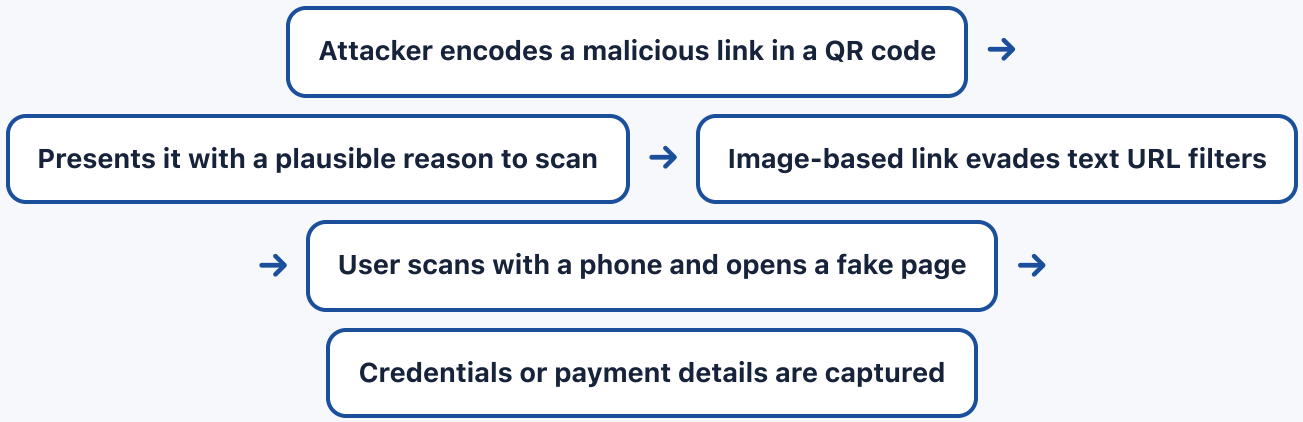
Quishing works because it defeats a common assumption that email security tools will catch bad links. A QR code is just an image to many filters, so a message that would be blocked with a visible URL can pass when the same URL is encoded. Scanning also moves the victim from a monitored corporate computer to a personal phone, outside many defenses and away from the visual cues, such as a full address bar, that help people spot fakes. Attackers place these codes

in emails, attachments, printed notices, and even physical stickers over legitimate codes. For organizations, quishing widens the phishing attack surface, and for professionals it is a reminder that defenses must account for images, mobile devices, and the physical world, not just text-based email links.

How It Works

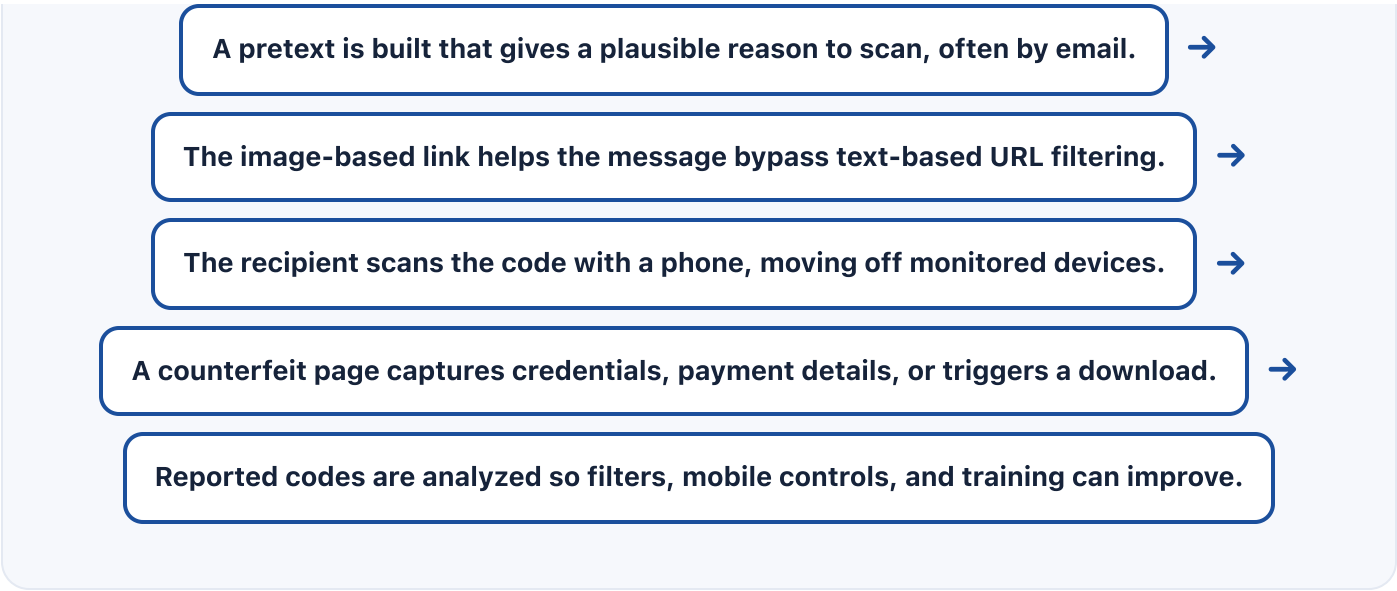
The attacker encodes a malicious link into a QR code and wraps it in a convincing pretext, often an email that claims a document, benefit, or account action requires scanning to proceed. Because the code is an image, text-based URL analysis may not flag it, so the message is more likely to reach the inbox. The recipient scans with a phone camera and is taken to a counterfeit page controlled by the attacker, where entered credentials or payment details are captured, or a malicious download begins. In physical settings, attackers may print codes on flyers or place stickers over genuine codes in public spaces. Defenses combine email tools that render and inspect embedded codes, mobile protections, and user habits such as previewing the decoded address and reaching services directly rather than through a scanned link.

Architecture Diagram



Quishing encodes a malicious link as an image so it evades filters, then lands the victim on a fake page via a phone.

Visual Workflow



Common Attacks

- Emails with a QR code claiming a document or account action requires scanning
- QR codes inside attachments to further evade link inspection
- Physical stickers placed over legitimate codes on signs, flyers, or terminals
- Fake parking, payment, or benefits notices directing victims to scan and pay
- Codes that lead to counterfeit login pages harvesting corporate credentials

Common Mistakes

- Assuming email filters inspect links hidden inside QR code images
- Scanning codes from unexpected emails or unfamiliar physical locations
- Trusting a QR destination without previewing the decoded web address
- Overlooking mobile devices because they feel personal and separate from work
- Not training staff that QR codes can carry the same threats as links

Best Practices

- Use email security that renders and inspects links embedded in QR codes
- Preview the decoded address before opening it and confirm it is legitimate
- Reach services directly rather than through a scanned link for logins or payments
- Enforce multi-factor authentication so a captured password is not enough

- Protect mobile devices with management and up-to-date security
- Include QR code phishing in awareness training and simulations

Quick Checklist

- [x] Email gateway configured to inspect QR-embedded links where supported
- [x] Users trained to preview decoded QR destinations before proceeding
- [x] Policy to reach login and payment pages directly, not via scans
- [x] Multi-factor authentication enforced on key accounts
- [x] Mobile device management and updates protecting phones
- [x] Quishing included in awareness training and phishing simulations

Recommended Tools

Email security gateway
Detects and inspects links embedded inside QR code images where supported

Multi-factor authentication
Prevents account takeover when a quishing page captures a password

Mobile device management
Adds protection and control to the phones quishing targets

Security awareness platform
Trains and tests staff on QR code phishing scenarios

Industry Standards

NIST SP 800-177
Trustworthy email guidance relevant to filtering and authentication

NIST SP 800-124
Guidance on securing the mobile devices quishing targets

CIS Critical Security Controls
Email, authentication, and awareness safeguards that reduce quishing risk

Career Relevance

Quishing pushes phishing defense into images, mobile, and even the physical world. SOC analysts triage reported codes and related compromises, incident responders handle credential theft that starts with a scan, and security awareness leads teach staff that QR codes carry link risk. Security engineers tune email and mobile controls to inspect and contain these threats, while GRC analysts assess the widened attack surface. For the AI-Governance-Jobs.com audience, quishing is an emerging topic across security and governance roles.

Interview Questions

- What is quishing, and why does it evade many email filters?
- Why does moving the victim to a mobile device benefit the attacker?
- How would you defend an organization against QR code phishing?
- What user habits reduce the risk of malicious QR codes?
- How do physical QR code attacks differ from email-based ones?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | GIAC Security Essentials (GSEC)

Further Reading

- FTC: QR Codes May Be Scams
- CISA: Avoiding Social Engineering and Phishing Attacks
- NIST: Mobile Device Security

Key Takeaways

- Quishing hides malicious links inside QR code images.
- Image-based links can slip past filters that scan text and URLs.
- Scanning moves victims onto mobile devices with fewer defenses and cues.
- Preview decoded addresses and reach services directly, not via scans.

- Multi-factor authentication and mobile protection reduce the impact.

FAQ

Related Careers

RELATED ROLES

Soc Analyst

Security Awareness Lead

Incident Responder

Grc Analyst

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Security Essentials (GSEC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **QR Code Phishing (Quishing)**
3. Go deeper: Phishing
4. Go deeper: Smishing
5. Validate it: work toward **CompTIA Security+**

6. Find the role: browse current openings

RELATED SHEETS

CS-032 Phishing | CS-036 Smishing | CS-037 Vishing | CS-025 Multi-Factor Authentication (MFA) | CS-010 Cyber Hygiene