FAB ALERT: QUISHING

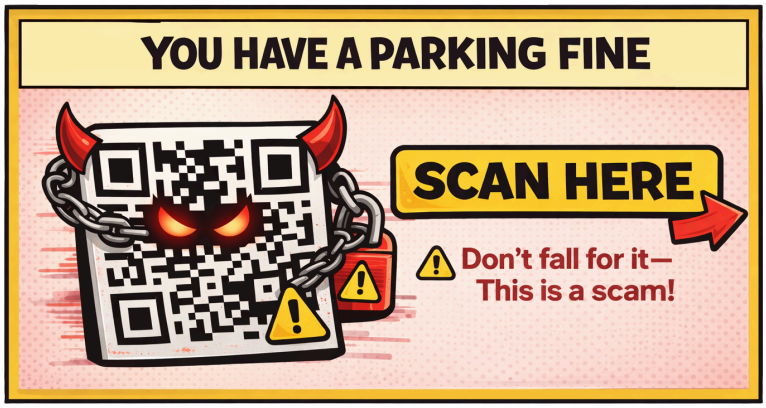
WHAT IS QUISHING?

Quishing (QR Code Phishing) is a rapidly growing fraud tactic where scammers use QR codes to direct victims to malicious websites designed to steal login credentials, financial information, or sensitive data.

These QR codes may appear in emails, text messages, or physical locations and often impersonate trusted organizations such as banks, Microsoft 365, or internal systems.

INTRODUCTION

Quishing attacks are evolving beyond traditional phishing by targeting mobile devices and bypassing standard email security controls.
In recent cases, attackers have used QR codes in place of links to avoid detection. Once scanned, users are redirected to fake login pages that closely mimic legitimate systems such as VPN portals or Microsoft 365.
These attacks are particularly dangerous because they can capture credentials and session tokens, enabling attackers to bypass multi-factor authentication (MFA) and gain unauthorized access without triggering alerts.



HOW DOES IT HAPPEN?

- **User Receives a Legitimate Looking Email**
  - Email includes a QR code for "secure access," document review, or authentication.
- **QR Code is Scanned on Mobile Device**
  - Bypasses traditional email security and link inspection tools.
- **Redirect to Fake Login Page**
  - Page mimics Microsoft 365, VPN, or authentication portals.
- **User Enters Credentials**
  - Credentials and session tokens are captured instantly.
- **Account Takeover Occurs**
  - Attackers gain access without triggering MFA alerts.
- **Fraud Activity Begins**
  - Used for wire fraud, BEC, identity theft, or internal access.

F-FRAUD
A-AML
B-BSA

FAB@GREENWICHFIRST.COM

FAB ALERT: QUISHING

QUISHING DETECTION: SIGNS TO LOOK OUT FOR

Unsolicited QR Codes
Unexpected emails or messages asking you to scan a code.

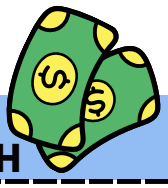
Urgency or Pressure
"Scan immediately," "Account access required," "Security alert."

Mobile-Based Login Requests
Prompts to authenticate or log in after scanning.

Generic or Unexpected Requests
Surveys, shared files, or MFA resets you didn't request.

External or Unverified Senders
Emails that appear legitimate but originate outside the organization.

PROTECT YOURSELF



THINK

Before scanning a QR code, ask yourself:
- Where did this come from?
- Who sent or posted it?

Be extra cautious with QR codes from:
- Untrusted emails or text messages
- Signs, posters, flyers, or public locations

If it's unexpected or creates urgency -> DO NOT SCAN

TREAT YOUR INFORMATION LIKE CASH

Your personal information is valuable:
- Social Security Number
- Credit/Debit Card Information
- Login Credentials

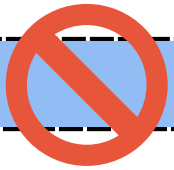
If a scammer gets it, they can:
- Steal your money
- Open accounts in your name to

Commit fraud without your knowledge

REPORT

If something feels suspicious:
- Contact the bank, company, or agency being impersonated
- Report it internally so we can **alert others and investigate**

Early reporting helps stop fraud before it spreads



BLOCK SPAM MESSAGES

Reduce exposure to scams:
- Call your carrier (dial 611)
- **Request:**
  - "Block all text messages sent as email"
  - "Block all multimedia messages sent as email"

You may also be able to enable these settings in your mobile account

F-FRAUD
A-AML
B-BSA

FAB@GREENWICHFIRST.COM