TIR-20251029 Malicious QR Codes in the Workplace

10/29/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

QR codes have become standard in workplaces for everything from logins and invoices to employee resources and event check-ins. Unfortunately, that convenience has opened a new door for attackers. “Quishing”, which is phishing via QR codes, allows cybercriminals to move attacks from monitored corporate networks to personal mobile devices, where traditional security controls are often absent.

Recent investigations by the FBI, FINRA, and Google’s Threat Analysis Group have confirmed a sharp rise in quishing incidents. Attackers embed malicious QR codes in emails, PDFs, and even mailed packages. When scanned, these codes redirect users to fake login portals or malware-hosting sites. Because most employees scan with their personal phones, organizations often have little to no visibility into the compromise.

Groups such as ONNX Store, UNC5356 (CryptoChameleon), and TA571 have used quishing to steal credentials and gain access to enterprise systems. Beyond email campaigns, attackers are also tampering with physical QR codes, like those found on parking meters or menus, to trick users into giving up financial and personal data.

As QR codes continue to integrate into daily business operations, their abuse is

TIR SUMMARY

ASPIRE

The Threat

- Attackers now use everyday QR codes as phishing tools in workplace emails and materials.
- Quishing shifts attacks to personal phones, bypassing company security.
- Yes, those QR codes in the report were bait, and you scanned them anyway.

Tactics and Techniques

- Attackers hide QR codes in fake emails, PDFs, or printed materials that lead to phishing pages or malware.
- Some hijack real codes, like on posters or parking meters, replacing them with malicious stickers.
- The tactic exploits trust and routine; one quick scan can hand over credentials

Recent Attacks

- ONNX Store, UNC5356, and TA571 used quishing for Microsoft 365 and ransomware access.
- The LastPass “death verification” and FINRA PDF scams showed how convincing these look.
- Attackers now mix digital and physical delivery to stay undetected.

Lessons Learned

- QR codes are unseen links, treat them like suspicious emails.
- Include quishing and code tampering in security awareness training.
- And seriously, stop scanning random codes – even the ones with red stop signs.

expected to grow. Employees must learn to recognize malicious QR codes and verify URLs before scanning. Awareness and verification remain the most reliable defenses against this social engineering tactic.

What Are QR Codes?

A QR code, short for “Quick Response” code, is a two-dimensional barcode that can store large amounts of data (including URLs, text, payment information, and contact details) in a small grid of black and white squares. It was first developed in 1994 by Denso Wave, a subsidiary of Toyota, to track auto parts on production lines. The design allowed scanners to read information 10 times faster than traditional barcodes.

Image 1: QR Code Example

Over time, QR codes became a convenient bridge between the physical and digital worlds. They’re used for everything from opening menus and logging into websites to authenticating two-factor logins and sharing Wi-Fi credentials. The COVID-19 pandemic accelerated the use of QR codes. At the time touchless interaction was suddenly in demand, making QR codes common in offices, restaurants, healthcare facilities, and public buildings.

In the workplace, QR codes often appear in onboarding packets, HR portals, IT helpdesk tickets, training registration pages, and conference badges. They simplify access to resources and integrate easily into mobile-first business processes. Many organizations use them internally to connect employees to things they need, such as surveys and intranet pages. However, this convenience has introduced new risks. A QR code is essentially a link you can't see. When you scan it, your device immediately processes the encoded destination without the visible context a normal URL provides. This makes QR codes an easy disguise for malicious redirections. Attackers can create fake codes that redirect users to phishing portals or malware downloads.

Since mobile phones often lack enterprise-grade protection, this creates a blind spot for security teams. A compromised phone connected to corporate email or collaboration tools can expose entire environments. The growing dependency on BYOD (Bring Your Own Device) policies means attackers don't need to breach a company's network directly, they just need one employee to scan the wrong code.

QR codes alone aren't dangerous. The problem lies in how easily they can be weaponized. A single sticker over a legitimate QR code on a poster or invoice can reroute credentials and financial data directly to a threat actor's server. Organizations need to treat QR code scanning as cautiously as they do unfamiliar email links.

What is Quishing?

Quishing, a blend of "QR" and "phishing", is a social engineering tactic that uses malicious QR codes to trick users into giving up sensitive information or downloading malware. It's the most common QR-based attack employees are likely to encounter in the workplace, representing an evolution of traditional phishing designed to slip past filters and awareness training that catch suspicious links.

Image 2: Malicious Quishing Email Example

A typical quishing attack begins with a fake email or PDF attachment containing a QR code, much like the one you just scanned above, **red warning sign and all**. The message might claim that your Microsoft 365 session has expired or that a document is waiting for approval. The QR code directs victims to a counterfeit login page that looks nearly identical to a legitimate portal. Once credentials are entered, the attacker gains full access.

What makes quishing so effective is its ability to bypass security defenses. Email filters can't easily detect malicious content within images, and the QR code's destination is only revealed after scanning. Furthermore, employees often scan codes using personal smartphones outside the company's network, leaving no trace in enterprise logs.

Like traditional phishing, quishing relies on urgency and trust. Messages often impersonate well-known services or internal departments, using convincing branding to lower suspicion. Because QR codes appear on common communications such as posters, invoices, parking meters, and meeting invites, users often don't question them. In recent years, quishing has grown rapidly. Studies show a more than 500% increase in QR code phishing incidents between 2023 and 2025. High-value targets such as executives and administrators are prime victims because their accounts provide direct access to sensitive systems. Attackers also exploit industries that rely heavily on mobile access, including finance, healthcare, energy, and construction.

The psychology behind quishing mirrors classic social engineering principles. Attackers exploit trust, curiosity, and convenience. The more familiar a QR code looks, whether on a branded document or a company sign, the more likely users are to scan it. Even cautious employees who avoid clicking suspicious links may fall for a QR code because they perceive it as harmless.

Quishing campaigns are also used for credential theft, business email compromise (BEC), and multi-factor authentication interception. Some Phishing-as-a-Service (PhaaS) operations, like ONNX Store, even sell ready-made QR phishing kits capable of deploying fake login portals and bypassing MFA tokens.

QR Code Hijacking

As an added twist to quishing, QR-code hijacking is when an attacker physically or digitally replaces a legitimate QR code with a malicious one. This includes sticker overlays on parking meters or flyers, a doctored PDF, or swapped codes on printed materials. It's not really its own category, just a delivery method that makes quishing harder to detect in physical or hybrid attacks.

Treat hijacked codes like suspicious links. Make sure you verify the source, inspect the expanded URL before authenticating, and assume any unexpected QR request that arrives off-channel (printed mail, a poster, or an unseen PDF) needs the same handling as a suspicious email.

Threat Actors Who Use Quishing in Attacks

While quishing started as a simple social engineering tactic, it has now become a tool used by both cybercriminals and state-linked groups. Threat actors view QR codes as an effective way to slip past email filters and endpoint protections by shifting the attack to mobile devices. Several well-known groups have adopted this method.

Below are some of the actors currently leveraging quishing in their operations, along with their regions of origin, motives, targeted industries, and the impact of their recent campaigns.

ONNX Store / Caffeine Operators (Likely Russia / Eastern Europe)

- **Overview -** ONNX Store is a Phishing-as-a-Service (PhaaS) platform believed to be a successor to Caffeine. Both have been used to conduct credential theft campaigns targeting Microsoft 365 environments.
- **Motives -** Financial gain through stolen credentials and resale on underground markets.
- **Targeted Industries -** Finance, legal, and professional services sectors.
- **Targeted Regions -** Primarily North America and Europe.
- **Last Known Attack -** FINRA reported that ONNX Store operators distributed PDF-based quishing emails impersonating Microsoft 365. Victims were redirected to fake login pages to harvest credentials and intercept MFA tokens. The fallout included unauthorized email forwarding, financial fraud attempts, and business email compromise events.

UNC5356 / CryptoChameleon (Believed to Operate from Eastern Europe)

- **Overview -** UNC5356, tracked by Google's Threat Analysis Group, is behind advanced phishing operations using fake cryptocurrency and password management portals. They are known for quishing campaigns against LastPass and major crypto exchanges.
- **Motives -** Credential theft for financial exploitation.

- **Targeted Industries -** Cryptocurrency, fintech, and consumer password managers.
- **Targeted Regions -** Global, with concentration in North America and Europe.
- **Last Known Attack -** October 2025 phishing emails impersonated LastPass death verification alerts containing QR codes that redirected users to a malicious recovery site. Compromised credentials allowed access to stored password vaults.

TA571 (Eastern Europe)

- **Overview -** TA571 is a prolific initial access broker that often delivers malware through phishing and quishing campaigns. They distribute payloads for ransomware affiliates.
- **Motives -** Profit through access resale and ransomware partnerships.
- **Targeted Industries -** Manufacturing, education, and healthcare.
- **Targeted Regions -** U.S., Canada, and the U.K.
- **Last Known Attack -** Used QR code attachments disguised as payment confirmation requests, leading to credential theft and secondary malware infections used by ransomware affiliates.

Malicious QR Code Red Flags

Malicious QR codes can look legitimate, but they often carry subtle signs of tampering. Whether in an email, text, or posted in a public space, small details usually give them away.

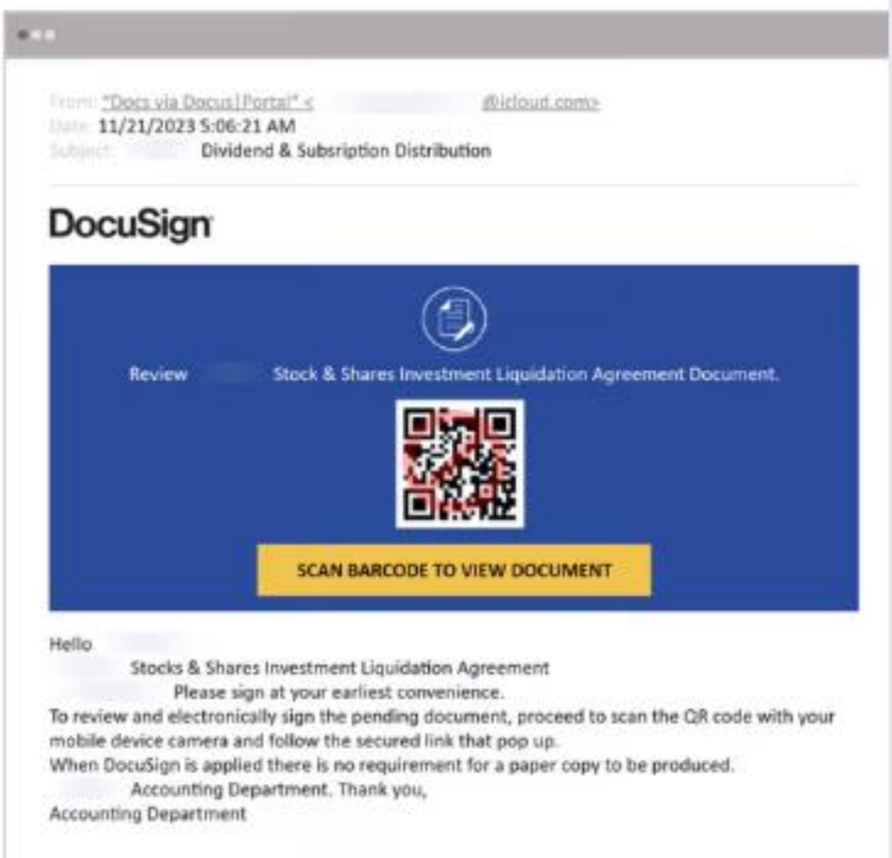
Email and Text Message Red Flags:

- QR codes sent unexpectedly or from unknown senders.
- Messages claiming account expiration, payment failure, or document access.
- Urgent or fear-based language such as “act now” or “verify immediately.”
- Attachments containing QR codes in PDF or image files.
- QR codes linking to shortened URLs or domains with spelling errors.

Public Red Flags:

- QR codes placed on top of existing posters, meters, or signage.
- Stickers that appear misaligned, faded, or inconsistent with branding.
- Codes placed in odd or low-traffic locations, such as restrooms or parking lots.
- Flyers or conference badges with unverified or generic QR codes.
- Any QR code offering free items, prizes, or gift cards.

Image 3: Malicious QR Code Phishing Attack Resembling a DocuSign Notice



Source: [Abnormal.ai]

Think Before You Scan

Verifying a QR code before scanning is one of the easiest ways to prevent phishing or malware attacks. You skipped that step again with the one above — even with the big red stop sign staring back at you. Consider that your reminder to **stop scanning random codes without thinking twice.**

Many of these codes are designed to look trustworthy, often using familiar company logos or messages that create a false sense of urgency. Taking a few seconds to examine a QR code can prevent credential theft or device compromise. Users should get into the habit of inspecting codes closely and confirming the source every time. The steps below outline practical ways to check a QR code before trusting it.

Before You Scan QR Codes:

- Hover your phone's camera before scanning to preview the destination URL.
- Confirm the domain matches the legitimate company website.
- Manually visit the organization's official site instead of scanning.
- Inspect for stickers placed over printed codes.
- Avoid scanning QR codes in unsolicited emails or texts.
- Use QR scanner apps that display safety ratings or warnings (Scam Shield QR Reader, Safe QR Scanner & Generator – iOS, etc.).
- Check that the website begins with HTTPS and includes valid certificates.
- Report suspicious QR codes to your manager and IT team immediately.
- Do not authorize downloads or grant permissions prompted by the QR code.
- When in doubt, verify directly with the sender or department before scanning.

RESPONDING TO A MALICIOUS QR CODE SCAN (ASPIRE'S RECOMMENDATIONS)

Even the most cautious user can make the mistake of scanning a malicious QR code. Once that happens, quick action can mean the difference between a contained incident and a full compromise. Quishing and QR code hijacking attacks often redirect users to credential harvesting sites or trigger malware downloads, so it is important to respond immediately and logically. The steps below outline what organizations should do right after scanning a suspicious or known malicious QR code.

- <u>Disconnect</u> from all networks immediately to prevent further communication with the attacker's server.
- <u>Do not continue interacting</u> with any website or prompt opened by the QR code and close all related browser tabs or apps.
- <u>Run a full malware scan</u> using mobile or endpoint security software to detect potential infections.
- <u>Change all passwords</u> used after scanning, starting with email, banking, and work accounts.
- <u>End active sessions</u> on devices and apps to block attackers from maintaining unauthorized access.
- <u>Review authentication logs</u> for unusual login attempts, unfamiliar devices, or logins from new geographic locations.
- <u>Enable stronger MFA</u> methods that do not rely on QR codes, such as app-based tokens or hardware keys.
- <u>Report the incident</u> to your organization's IT or security team, or if personal, to the FBI's Internet Crime Complaint Center (IC3.gov).
- <u>Monitor financial and online accounts</u> closely for suspicious activity over the following weeks.

- Consider resetting or reimaging the device if signs of compromise persist or malware is confirmed.

Conclusion

QR codes have become a normal part of daily business, but their convenience has turned into a weapon for attackers. Quishing has emerged as a modern form of phishing that preys on employee trust and routine. While most users know not to click strange links, many still scan QR codes without hesitation, unaware that they can be just as dangerous. Threat groups like ONNX Store, UNC5356, and TA571 have taken advantage of this gap, using QR codes to steal credentials and infiltrate networks.

Preventing these attacks takes more than technology, it requires awareness and user education. Organizations should train employees to verify QR codes before scanning and treat every code as a potential threat. Email filters and mobile device policies should evolve to detect malicious QR content, but education remains the strongest defense.

MITRE MAP

Initial Access	T1566.002 – Phishing: Spearphishing Link T1189 - Drive-By Compromise
Execution	T1204.001 - User Execution: Malicious Link
Credential Access	T1056.003 - Input Capture: Web Forms
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols
Exfiltration	T1041 - Exfiltration Over Web Services

Aspire Protects

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

QR Code Security Guide | Information Security

QR Code Hijacking

What is quishing? | Cloudflare

What is Quishing (QR Phishing)? - Check Point Software

Evolution of Sophisticated Phishing Tactics: The QR Code Phenomenon

Four Risks and Solutions When Using QR Codes

Scan with Caution: The Light and Dark Sides of QR Codes - Blackpoint

Weaponized QR Code Powers New Quishing Attack Targeting Microsoft Users

New QR Code-Based Quishing Attack Targets Microsoft Users

Phishers try out 'split' QR codes

How QR code attacks work and how to protect yourself - Help Net Security

New PoisonSeed Attack Let Attackers Trick Users into Scanning a QR Code with an MFA Authenticator

"Quishing" - The Emerging Threat of Fake QR Codes | Tripwire

Quishing attacks 101: how QR codes are exploited | authentic8

10 Real-Life Quishing Attack Examples - Keepnet

FINRA Cyber Alert – ONNX Store Purportedly Targeting Firms in Quishing Attacks | FINRA.org

Hackers are targeting Signal with new QR code-linked cyberattack | TechRadar

Beware the QR code trap - how 'quishing' threatens your business

How to protect against QR code phishing attacks | SC Media

FBI Report: Attackers Are Sending Physical Packages with Malicious QR Codes

The QR Code Threat Hiding in Plain Sight: Why Quishing is Every Business's Nightmare

[QR Code Scams: Protect Yourself with Tips & Best Practices in 2023]

[Staying Safe With Qr Codes]

[Is that QR code actually a scam? Here's what to know about 'quishing' before you scan | CBC News]

[ONNX Store: Phishing-as-a-Service Platform Targeting Financial Institution]

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.