FBI FLASH

ACTIONABLE CYBER INTELLIGENCE

08 JANUARY 2026

FLASH Number
AC-000001-MW

North Korean Kimsuky Actors Leverage Malicious QR Codes in Spearphishing Campaigns Targeting U.S. Entities

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to alert NGOs, think tanks, academia, and other foreign policy experts with a nexus to North Korea of evolving tactics employed by the North Korean state-sponsored cyber threat group Kimsuky and to provide mitigation recommendations. As of 2025, Kimsuky actors have targeted think tanks, academic institutions, and both U.S. and foreign government entities with embedded malicious Quick Response (QR) codes in spearphishing campaigns. This type of spearphishing attack is referred to as *Quishing*.

Quishing (QR Code Phishing) is a phishing technique in which adversaries embed malicious URLs inside QR codes to force victims to pivot from their corporate endpoint to a mobile device, bypassing traditional email security controls. Tracked by MITRE ATT&CK as [T1660], Quishing campaigns commonly deliver QR images as email attachments or embedded graphics, evading URL inspection, rewriting, and sandboxing. After scanning, victims are routed through attacker-controlled redirectors that collect device and identity attributes such as user-agent, OS, IP address, locale, and screen size [T1598 / T1589] in order to selectively present mobile-optimized credential harvesting pages [T1056.003] impersonating Microsoft 365, Okta, or VPN portals.

Quishing operations frequently end with session token theft and replay [T1550.004], enabling attackers to bypass multi-factor authentication [T1550.004] and hijack cloud identities without triggering typical “MFA failed” alerts. Adversaries then establish persistence in the organization [T1098] and propagate secondary spearphishing from the compromised mailbox [T1566]. Because the compromise path originates on unmanaged mobile devices outside normal Endpoint Detection and Response (EDR) and network inspection boundaries, Quishing is now considered a high-confidence, MFA-resilient identity intrusion vector in enterprise environments.

The FBI strongly urges potentially targeted organizations to review and implement the mitigation strategies outlined in the “Recommendations” section below to reduce exposure to this emerging spearphishing technique.

Threat

The FBI identified Kimsuky actors deploying malicious QR codes as a part of targeted spearphishing campaigns:

- In May 2025, Kimsuky actors spoofing a foreign advisor sent an email requesting insight from a think tank leader regarding recent developments on the Korean Peninsula. The email provided a QR code to scan for access to a questionnaire.
- Later that month, Kimsuky actors spoofing an embassy employee sent an email requesting input from a senior fellow at a think tank regarding North Korean human rights issues. The email contained a QR code that purported to provide access to a secure drive.
- Also in May 2025, Kimsuky cyber actors spoofing a think tank employee sent an email with a QR code that, when scanned, would take the targeted individual to Kimsuky infrastructure designed to conduct malicious activity.
- In June 2025, Kimsuky actors sent a strategic advisory firm a spearphishing email inviting recipients to a non-existent conference. The email contained a QR code that directed the user to a registration landing page with a button to register. The registration button took visitors to a fake Google account login page, where users could input their login credentials for harvesting [T1056.003].

MITRE ATT&CK: Quishing Attack Lifecycle

Phase	ATT&CK
Email delivery with QR image	T1660 / T1566.002
Mobile fingerprinting	T1598 / T1589
Credential harvesting page	T1056.003
Session token theft	T1550.004
MFA bypass	T1550.004
Account persistence / manipulation	T1098
Lateral phishing from victim mailbox	T1566

Recommendations

The FBI recommends organizations adopt a multi-layered security strategy to address the unique risks posed by QR code-based spearphishing. These mitigations parallel best practices highlighted in prior notifications and are tailored for the QR code threat vector.

Organizational Strategies:

- Educate employees on the risks associated with scanning unsolicited QR codes, regardless of their source (email, letter, flyer, packaging).
- Implement training programs to help users recognize social engineering tactics involving QR codes, including urgent calls to action and impersonation of trusted entities.
- Advise staff to verify QR code sources through secondary means (such as contacting the sender directly), especially before entering login credentials or downloading files.
- Establish clear protocols for reporting suspicious QR codes or related phishing attempts.
- Deploy mobile device management (MDM) or endpoint security solutions capable of analyzing QR-linked URLs before permitting access to web resources.
- Require phishing-resistant MFA for all remote access and sensitive systems.
- Log and monitor all credential entry and network activity following QR code scans, to identify anomalies or possible compromises.
- Enforce strong password policies across all services, with specific attention to length, uniqueness, and secure storage.
- Review access privileges according to the principle of least privilege and regularly audit for unused or excessive account permissions.
- Regularly update anti-virus and anti-malware tools, and patch known vulnerabilities on devices used to scan QR codes.
- Maintain liaison relationships with the FBI Field Office in your region to receive updates and report malicious activity at www.fbi.gov/contact-us/field-offices.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This FLASH was coordinated with DHS/CISA and is marked TLP:CLEAR. The information in this product may be shared without restriction. Information is subject to standard copyright rules.

Your feedback regarding this product is critical.

Please take a moment to complete the survey at the link below. Input can be submitted anonymously and should be specific to your experience with our written products.

https://www.ic3.gov/PIFSurvey

This survey is for feedback on contact and value only. Reporting of technical information regarding FLASH reports must be submitted through your local FBI field office.