Lookout

Mobile Threat of the Month

May 2026

QR Code (Quishing) Attacks Increase In Prevalence

Microsoft Threat Intelligence's Q1 2026 Email Threat Landscape analysis reports an unprecedented 146% surge in QR code phishing ("quishing") attacks against business environments. Malicious QR traffic skyrocketed from 7.6 million attacks in January to 18.7 million monthly attacks by April 2026.

Why QR Code Attacks Are On The Rise

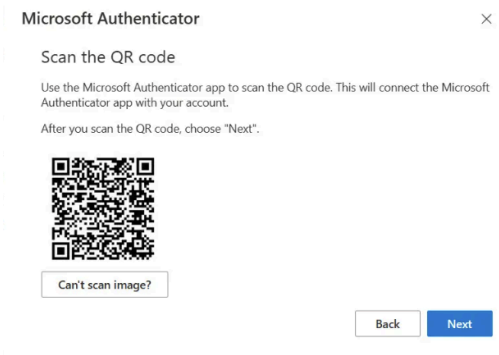
1. Using a mobile device camera rather than clicking a link on a computer moves the interaction away from secured laptops to an unprotected mobile device.

2. A QR code is a binary image meaning security tools cannot "read" or click a link hidden inside an image file or embedded in a standard PDF attachment.

3. These attacks are designed to trick employees to carry out Multi-Factor Authentication (MFA) resets, leading to lucrative company data compromise.

Financial & Business Impact

Pervasive Enterprise Access: A single targeted campaign mimicking a Microsoft Authenticator QR code login page successfully delivered over 1.2 million quishing emails, breaching defenses across 53,000 distinct organizations globally.

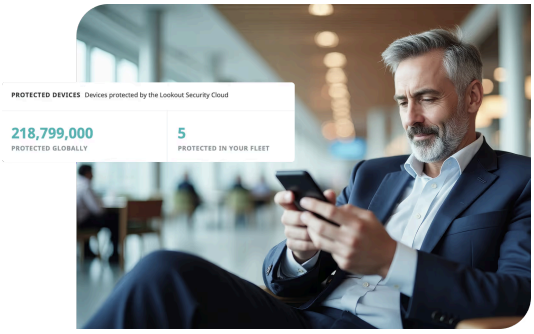


Elevated Executive Risk: Corporate executives and C-suite leaders are 40 times more likely to be targeted with high-urgency quishing attempts, drastically increasing the likelihood of high-privilege compromise.

Data Exfiltration: Stolen session tokens are used by attackers to authenticate as valid corporate users, initiating rapid automated data-scraping across cloud environments.

Lookout Mobile Security

Organizations must recognize that a mobile device's camera is now a viable corporate attack surface. Through this growing threat vector users are being navigated to harmful, untrusted or fake login webpages much more frequently.



Using threat telemetry gathered from hundreds of millions of mobile devices and apps globally, Lookout Mobile Security instantly detects and blocks connection to these sites before the employee can see the login prompt.

Modern quishing campaigns generate unique, randomized, and short-lived links to escape blocklists so instead of relying solely on static blacklists, Lookout Phishing AI analyzes the destination web page in real-time. It evaluates behavioral indicators and intent-based clues, (such as looking for rapid redirection patterns or unauthorized mimics of enterprise login portals like Microsoft 365 or Okta), to detect and neutralize these attacks.