Abnormal

CISO Guide to QR Code Attacks

Responding to the Latest Evolution in Phishing

The Rising Threat of QR Code Attacks

298,878

Number of phishing victims in 2023.

FBI IC3 Internet Crime Report

90%

Percentage of QR code attacks that are credential phishing attempts.

Abnormal Security

Phishing emails have been a favorite tool of bad actors for more than 30 years. By posing as trusted entities and fabricating a sense of urgency, attackers have been able to manipulate countless recipients into divulging sensitive information like login credentials or bank account details.

In the nascency of email, bad actors had two distinct advantages with phishing attacks. First, early email platforms were not developed with security as a priority, leading to a lack of built-in tools for detecting and preventing phishing attacks. Attackers also had the luxury of end-user naivete, as recipients had no reason to doubt the authenticity of the sender's claimed identity. However, with advancements in email security and heightened user awareness, cybercriminals have had to innovate their strategies to evade detection and maintain the efficacy of their attacks.

QR code phishing, the newest iteration of phishing, is the latest in a long line of malicious initiatives designed by enterprising attackers to evade organizational security measures and deceive end users. In QR code attacks, also known as quishing, threat actors utilize social engineering to trick targets into interacting with a malicious QR code that is linked to a phishing page.

It's true that, in terms of total losses, phishing falls in the bottom quarter of all attack types tracked by the FBI IC3. But phishing is frequently just the first step in a variety of crimes and is often used more as a "foot in the door" technique rather than the end goal. Thus, stopping quishing emails before they reach employee inboxes is essential to avoid costly consequences.

01

Why Cybercriminals Exploit QR Codes for Phishing

The history of phishing is characterized by opportunistic threat actors capitalizing on innovations in communication that have led to an increasingly interconnected world. For example, spear phishing, a more targeted form of phishing that began to emerge at the turn of the millennium, became a viable option when bad actors realized they could make their attacks more personalized (and more convincing) by harvesting the wealth of data available online.

Similarly, the rise of voice phishing (vishing) and SMS phishing (smishing)—two attack strategies that started gaining prominence in the 2010s—was facilitated by the pervasiveness of cell phones and the popularity of texting. And now, in the 2020s, we have QR code phishing.

The Evolution of Phishing Attacks

The precipitous rise of bad actors using malicious QR codes to steal sensitive data is driven by multiple factors.

Ubiquity

Although QR code technology was invented in 1994, at no point pre-2020 did QR codes have the omnipresence they do now. We scan QR codes to view menus at restaurants, check in at appointments, and make contactless payments. As a result, receiving an email with a request to scan an embedded QR code to reset an expiring password or access business documents is unlikely to raise any red flags—and attackers know this.

Novelty

A pillar of cybersecurity awareness training is emphasizing to end users the importance of not clicking on links in emails they weren't expecting to receive. Utilizing QR codes accomplishes the same goal of redirecting targets to a phishing page but makes the circumstances just different enough that the message may not set off alarms for the target in the way a standard link-based phishing attack might.

Signal Scarcity

Threat actors recognize that replacing hyperlinks with QR codes in phishing attacks improves the likelihood of the message bypassing legacy email security solutions. Unlike traditional email threats, quishing attacks contain minimal text content and no obvious URL, which significantly reduces the number of signals available for legacy security tools to analyze and use to detect an attack.

Mobile Device Vulnerability

If a target engages with a link-based phishing attack, all interactions with malicious elements occur on their laptop, within the purview of the organization and its security controls. Using a QR code, on the other hand, moves the attack to the target's mobile device, which lacks the lateral protection and posture management available in a cloud-based business environment.

02

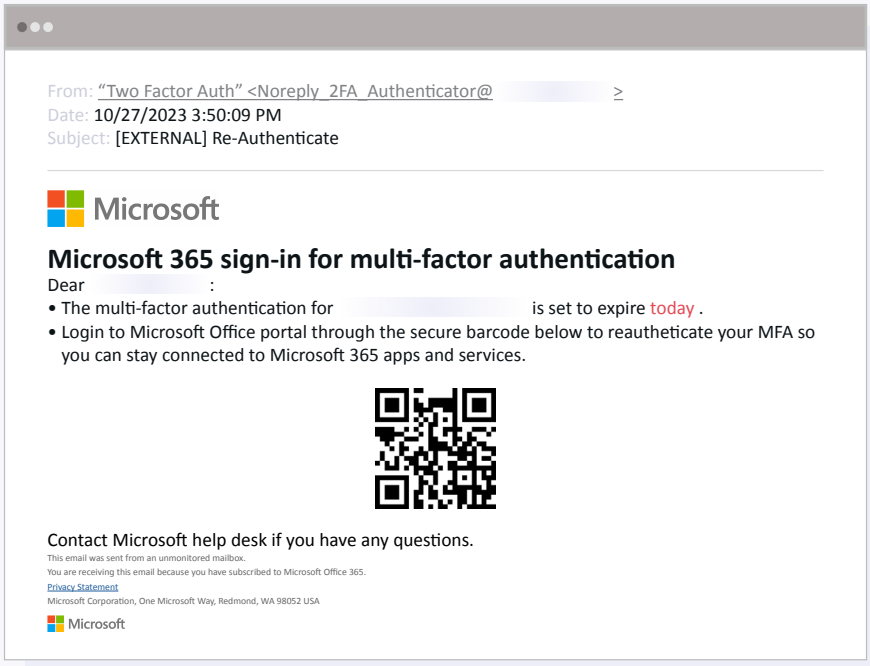
How Threat Actors Use Malicious QR Codes in Phishing Attacks

While malicious QR codes sent via email can be used for a variety of purposes, they are primarily utilized for credential phishing. Indeed, 90% of QR code attacks detected by Abnormal are credential phishing attacks.

In quishing attacks, the QR code is linked to what appears to be a legitimate website (often an emulation of a Google or Microsoft login page) with a prompt to enter login credentials or other sensitive details. Unfortunately, any information provided can then be used by the perpetrator to compromise the target's account and launch additional attacks.

Multi-Factor Authentication (MFA) Activation

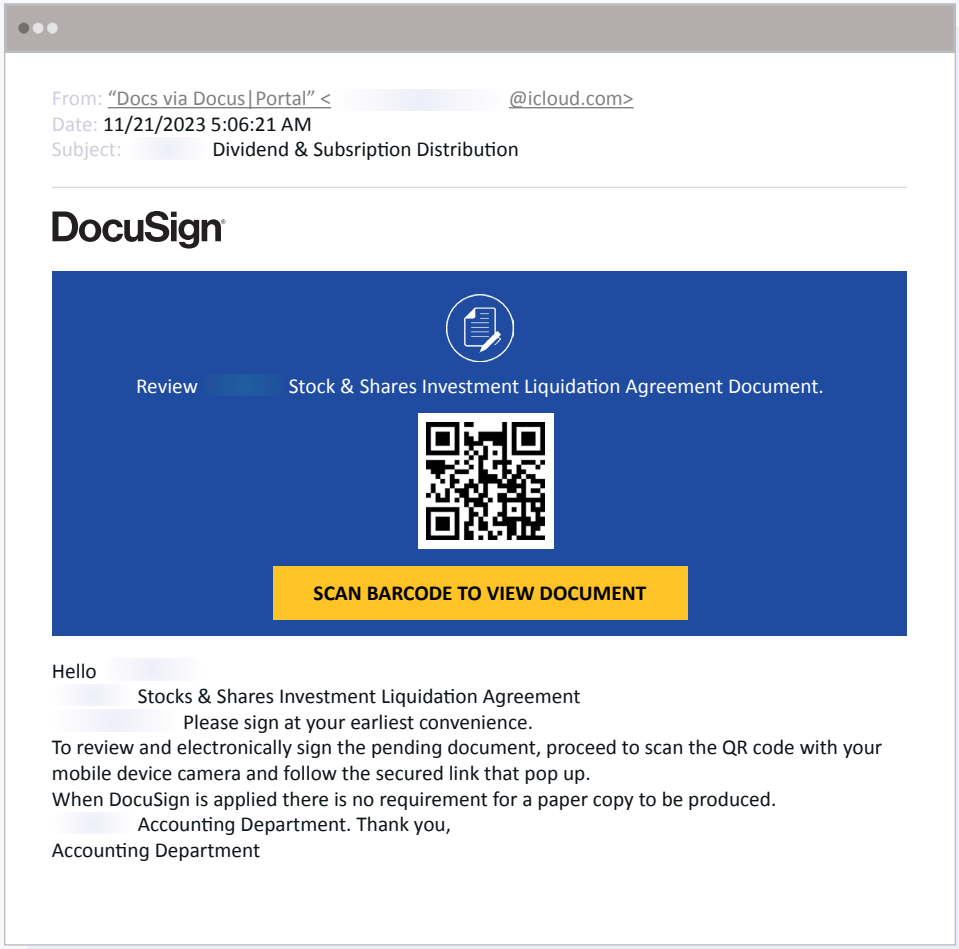
In approximately 27% of all quishing attacks, threat actors send fraudulent notices related to multi-factor authentication (MFA)—as shown in the real-world example of a quishing attack below.



The cybercriminal attempts to compel the target to scan the malicious QR code by claiming that their MFA method is expiring that day and needs to be reauthenticated. Because most modern professionals rely heavily on mobile devices, losing access to Microsoft 365 applications can significantly inhibit their ability to do their job—which means they'd be highly motivated to act quickly.

Shared Document Notification

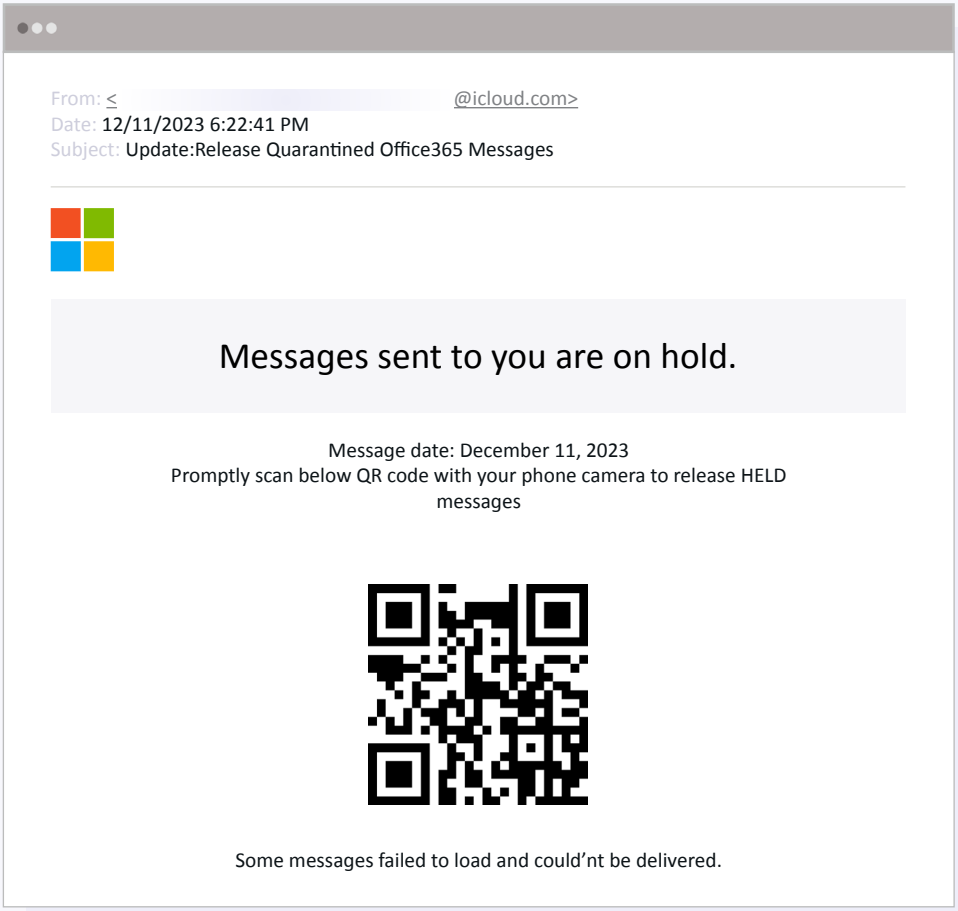
The second most popular strategy, used in approximately 21% of all QR code attacks, is to send targets fake notifications of a shared document. In this example, the attacker informs the target their signature is required on a pending document and claims they can view and sign the document by scanning the included QR code.



Since the use of DocuSign is generally reserved for important and/or confidential documents, cybercriminals know posing as that company and claiming financial documents are in need of attention will likely convince the target to not think twice about scanning the QR code.

Quarantined Message Alert

While the most prevalent attack themes center on multifactor authentication and notices of shared documents, these certainly aren't the only tactics bad actors use in quishing attacks. Another recurring, albeit less common, strategy is sending targets an email claiming they have messages that have been quarantined by Microsoft 365, as in the following example.



By being deliberately vague about what types of messages are on hold, the hope is the target will be enticed to scan the QR code to find out more details.

03

Why QR Code Phishing Attacks Are Successful

Quishing emails, like other phishing attacks, rely on tactics that enable threat actors to bypass traditional email solutions and increase the appearance of legitimacy of their malicious messages to defraud employees.

Use of Social Engineering to Manufacture Urgency

Artificial urgency is a key component of QR code phishing attacks. To instill worry and spur action, quishing emails often claim the target is at risk of losing access to business-critical applications or that the target's immediate attention is required on time-sensitive documents. The goal is to circumvent the target's common sense and compel them to act quickly without first verifying the legitimacy of the email.

Impersonation of Trusted, Relevant Brands

While impersonating known individuals or brands is an essential aspect of all phishing attacks, threat actors who launch quishing attacks are more discerning about the entities they imitate. Because targets are directed to a site where they are generally asked to provide login credentials, attackers must impersonate brands that could reasonably prompt a user to enter their username and password without it being suspicious. This is why attackers primarily pose as brands like Microsoft and DocuSign in quishing emails.

Utilization of Legitimate Sender Domains

Attackers understand that to deceive targets they must first evade email security solutions. A common tactic in QR code phishing attacks is to send malicious emails from an iCloud address, as in the second and third examples above. Because iCloud.com is a legitimate sender domain, the emails pass SPF, DKIM, and DMARC checks. This improves the likelihood of a legacy security solution marking the email as safe and allowing the attack to be delivered to an employee's inbox.

04

How to Stop QR Code Phishing Attacks

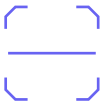
To counter these highly sophisticated social engineering attacks, organizations need the right email security platform. The next generation of email security includes:

API Architecture and Integrations

A solution that connects to Microsoft 365 and Google Workspace via an API and, in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more. More advanced solutions can also connect to other applications, including Slack, Okta, Zoom, and CrowdStrike, to understand identity and detect multi-channel attacks.

Behavioral Data Science Approach

The solution should use a fundamentally different approach that leverages behavioral data science and AI to profile and baseline known-good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious attachments or links, or unusual download requests.



Advanced QR Code Detection and Analysis

The solution should employ models specifically designed to determine when an email contains a QR code, whether that is in the body of the email or in image and PDF attachments. It should be able to parse the embedded link associated with the QR code, feed the extracted signals to an AI-native detection engine, and ingest that information alongside other signals to identify and remediate malicious activity.

Without each of these capabilities, QR code phishing attacks will continue to outpace security measures—making it even more difficult to prevent these attacks from reaching employees, creating financial loss, and causing reputational damage.

Conclusion

The emergence of malicious QR codes in phishing emails underscores one of the unfortunate truths of cybersecurity: if threat actors can determine how to exploit something fundamentally harmless for malicious purposes, they will.

Time and time again, cybercriminals have demonstrated their impressive ability to identify new ways to leverage everyday communication tools as mechanisms for deceiving employees into disclosing private information and completing fraudulent requests.

With each new development in the attack landscape, it becomes increasingly evident that legacy systems like secure email gateways (SEGs) are ill-equipped to defend against the evolving tactics of cybercriminals. Organizations must recognize the limitations of SEGs and invest in modern solutions that use AI-native detection engines to stop new and emerging threats like QR code phishing.

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages—all while providing visibility into configuration drifts across your environment. You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

Ready to Prevent QR Code Attacks?

Request a Demo →

See Your ROI →