QR Code Phishing Emails: Early Detection | Proofpoint US

By October 04, 2023 Tim Bedard and Tyler Johnson

Published: 2023-10-03 · Archived: 2026-04-05 19:18:13 UTC

This blog post is part of a monthly series exploring the ever-evolving tactics of today's cyber criminals. Cybersecurity Stop of the Month focuses on the critical first steps in the attack chain—reconnaissance and initial compromise—in the context of email threats.

The series is designed to help you understand how to fortify your defenses to protect people and defend data against emerging threats in today's dynamic threat landscape.

The first two steps of the attack chain: reconnaissance and initial compromise.

In our past installments, we have covered supplier compromise, EvilProxy, SocGholish and e-signature phishing. All of these are examples of threats we regularly detect for our customers before they're delivered to users. In this post, we explore a recent detection of a phishing attack in which the URL was encoded into a QR code. We'll also explore the mechanisms employed by our AI-driven detection stack that ultimately prevented the email from reaching the inbox of its intended target.

The scenario

Phishing, especially credential phishing, is today's top threat. Bad actors constantly devise new methods and tools to gain authenticated access to users' accounts. This illicit entry often results in financial loss, data breaches and supplier account compromise that leads to further attacks.

We recently detected a phishing attack hidden behind a QR code at an agriculture company with more than 16,000 employees. Fortunately, our Aegis platform detected the threats and broke the attack chain.

In this scenario, a threat actor crafted a phishing lure purporting to contain completed documentation about the target's wages. Instead of including a link for the target to click, the bad actor created a QR code phishing email scam instructing the recipient to scan with their mobile phone's camera to review the documentation. Once scanned, a fake SharePoint login screen prompts the user to provide credentials.

QR Code phishing emails (quishing) represent a new and challenging threat. It moves the attack channel from the protected email environment to the user's mobile device, which is often less secure. With QR code phishing emails, the URL isn't exposed within the body of the email. This approach renders most email security scans

ineffective. What's more, decoding QR code phishing email scams using image recognition or optical character recognition (OCR) quickly becomes resource-intensive and difficult to scale.

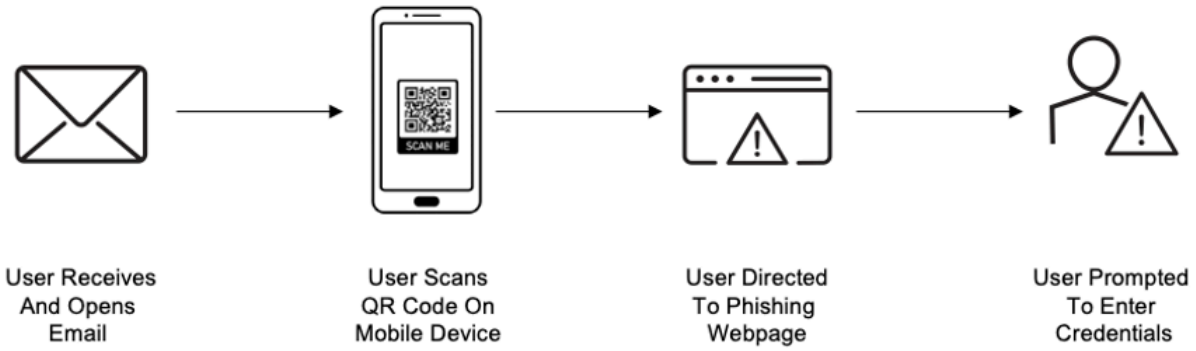
The Threat: How did the attack happen?

Here is a closer look at how the recent attack unfolded:

1. The deceptive message: An email claiming to contain employee payroll information sent from the organization's human resources department.

Malicious email blocked by Proofpoint before it was delivered to the user's mailbox. (Note: For safety, we replaced the malicious QR code with one linking to Proofpoint.com. The rest of the message is a redacted screenshot of the original.)

2. QR Code Attack Sequence: The recipient is instructed to scan the QR code with their mobile device.



Typical QR Code Attack Sequence for Phishing.

3. SharePoint phishing lure: Once the user decodes the URL, a fake SharePoint login screen tries to fool the recipient into entering credentials.

Decoded QR code redirecting to an example SharePoint phishing page.

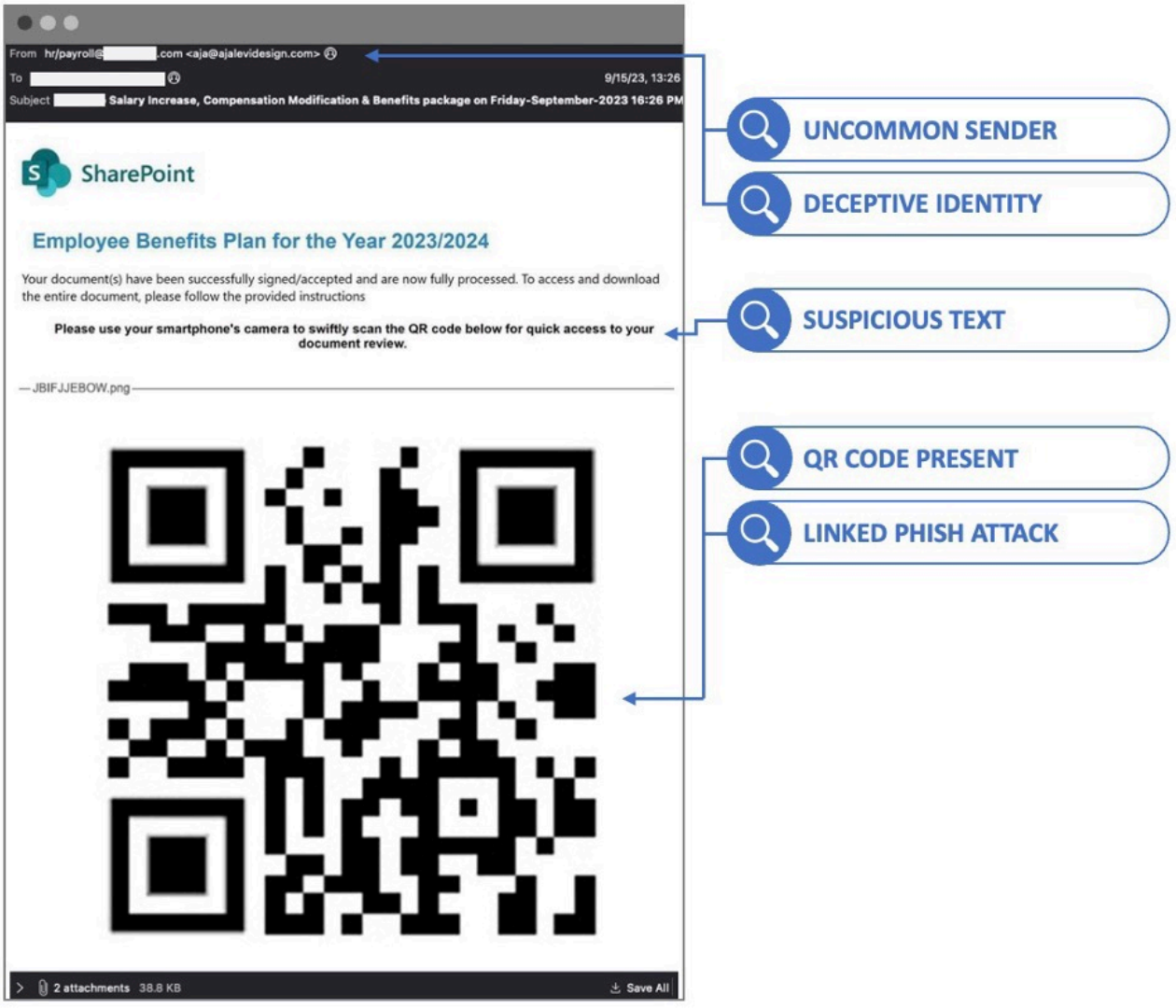
Detection: How did Proofpoint detect the attack?

QR Code phishing email scams are challenging to detect. First, the phishing URL isn't easy to extract and scan from the QR code. And most benign email signatures contain logos, links to social media outlets embedded within images and even QR codes pointing to legitimate websites. So the presence of a QR code by itself isn't a sure sign of phishing.

We employ an advanced blend of signals and layers of analysis to distinguish between weaponized and benign QR codes. We analyze and profile:

- The sender
- The sender's patterns
- The relationship of the sender and recipient based on past communication

Those clues help identify suspicious senders and whether they are acting in a way that deviates from an established profile. In this example, our systems had never before seen this sender communicate to this organization or recipient. Our platform proactively identified this new threat.



Signals our Aegis platform used to condemn the message as a threat.

By itself, uncommon sender patterns are a weak basis for condemning the message. Using patterns alone can result in falsely classifying a benign message as bad. That's often the case with email security tools that try to address threats post-delivery.

To reduce the number of false positives, we combine a multitude of signals to extract the theme nature and metonym of the email's content. (A metonym is a word or phrase used to represent something else, such as "the crown" for British royalty. This kind of analysis enables our platform to infer the sender's intent no matter what words the sender uses to phrase it.) We analyze the sender's email history along with a linguistic and semantic

analysis of the email's body. Using this approach, our platform identified language that revealed the email was asking the recipient to take action—in this case, to scan a QR code with their mobile device.

Outside of the behavioral and language analysis, we also detected deception tactics within the headers of the message. Even when passing email authentication, bad actors try to spoof trusted entities or other employees. In this case, the bad actors crafted the email headers to appear to be from the employer's HR and payroll team. This tactic is meant to foster the recipient's trust.

AI-driven machine learning and behavioral AI play a pivotal role in our ability to detect all kinds of threats. Here, our detection engines caught this threat based on message-level indicators.

But we went a step further—and deeper—by analyzing the QR code. By using the OCR and image recognition technology in our detection engines, we scanned and condemned malicious URLs hidden within the QR code itself. We extract both URLs and text to ensure that any messages that *should* be delivered *are* delivered and those that shouldn't be are blocked or remediated.

Remediation: What are the lessons learned?

To safeguard against threats such as QR-code scams, phishing, and other socially engineered threats, we recommend the following:

- **User education:** Your employees and customers are your first line of defense. Make sure they get security awareness education about all types of phishing attacks. Topics should include deceptive emails and fake login pages. This can greatly reduce their chances of being a victim.
- **Account takeover protection:** A good cloud security platform can identify account takeover (ATO) attacks and prevent unauthorized access to your sensitive cloud resources. This security control should cover both initial- and post-compromise activities. And it should let your security team get a closer look into which services and applications are being abused by attackers. Make sure to look for a solution that automates remediation. This reduces attackers' dwell time and keeps damages to a minimum.
- **Supply chain protection:** Defend your organization from emails sent from potentially compromised vendors and partners. Proofpoint Supplier Threat Protection uses advanced AI and the latest threat intelligence to detect the supplier accounts that have been compromised and prioritize any that should be investigated.
- **Multifactor authentication (MFA):** Strong authentication measures such as MFA can boost to your security posture. But MFA is no silver bullet; a growing number of attacks shows how traditional MFA approaches can fail. That's why cloud-based ATO automated tools, which can promptly remediate these types of incident, are critical.
- **Pre-delivery email security:** Preventing and blocking messages is the only sure way to keep users safe. Why is this so important? Because nearly 1 in 7 malicious URLs are clicked on in less than one minute, according to our research. Your organization needs a cybersecurity solution that uses a both machine learning and advanced threat detection to identify and stop these threats, such as the Proofpoint Aegis threat protection platform. Post-delivery email security tools claim to detect these threats. But even when they do, they do so later in the attack chain—after the threat is already in users' inboxes. A post-delivery approach exposes users and your organization to threats until it is remediated from the inbox.

Break the attack chain with Proofpoint

Bad actors continue to find new and creative methods to skirt existing security solutions. QR code phishing email scams are just the latest reminder of the critical need for multi-layered and robust cybersecurity measures. In today's world of sophisticated cyber threats, organizations must be vigilant and proactive in protecting themselves and their customers.

To stay ahead of these evolving dangers, you need a comprehensive approach to protecting against threats targeting your people. Pre-delivery detection and protection combined with post-delivery automated remediation and user awareness are essential. Unlike post-delivery email security tools, we stop attacks farther up the attack chain, *before* messages get delivered to the inbox.

To learn how to protect yourself against threats like SaaS app phishing, download our e-book, *The Definitive Email Cybersecurity Strategy Guide*.
