Microsoft Security

Protect against QR code phishing with Microsoft Defender for Office 365

Over the past year, QR code phishing campaigns have become the fastest growing type of email-based attack, and account for nearly [20% of all phishing emails](). These attacks embed QR code images linked to malicious content directly into the body of an email, and often entice unwitting users with seemingly genuine prompts, like a password reset or a two-factor authentication request.

Embedded images like QR codes are normally unreadable by conventional threat detection tools during mail flow, as they can only scan images once rendered (i.e. when the email is actually opened by an end-user). This makes detecting these types of attacks more difficult than other phishing emails.

What is a QR code?

A QR code (short for "Quick Response code") is a two-dimensional barcode that can be scanned using a smartphone or other mobile device equipped with a camera. QR codes can contain various types of information, such as website URLs, contact information, product details, and more. They are most commonly used for taking users to websites, files, or applications. The easiest way to think about a QR code is to treat it just as you would a URL.

For example, when this QR code is scanned it will redirect you to the **Defender for Office 365 product page**.

How Defender for Office 365 detects QR code phishing

Given the urgency and complexity of this issue, here's what you need to know about how Microsoft Security is responding to this rising threat, and how organizations can proactively protect themselves from QR code phishing.

Image detection capabilities

With new advanced image extraction capabilities, Defender for Office 365 and Exchange Online Protection can determine if a QR code links to malicious content during email flow. It does this by extracting URL metadata from a QR code and feeding that signal into our established and industry leading URL threat protection and filtering database (i.e. using internal and external sources of reputation). The URL is also sent to an isolated sandbox environment to be securely opened and detonated if need be. Altogether, this feature's capabilities can proactively identify and block QR code phishing attacks before they get a chance to reach an end-user's inbox.

Multiple contextual threat signals and heuristics

Defender for Office 365 and Exchange Online Protection have a long-established precedent of combining multiple contextual signals together for enhanced detection of malicious messages of all types, and this effective methodology is now being utilized to respond to the QR code phishing threat. QR codes are now a new signal being fed into our machine- learning-powered detection models in addition to other signals, including sender intelligence, message headers, and recipient details, to identify relationships between them and produce highly accurate predictions of QR code phishing attacks.

Furthermore, foundational to Defender for Office 365 and Exchange Online Protection is the flexibility to quickly deploy new heuristics rules, which is critical for mitigating malicious email campaigns like QR code phishing, as their tactics and methodologies can evolve on a day-to-day basis. Deploying new heuristics has been one of our most immediate actions we've taken as a fast response to this situation and has already been used extensively to identify attack patterns and proactively block QR code phishing campaigns.

End-user training and vigilance

At Microsoft, we know firsthand that end-users are the first line of defense against any type of email-based threat, and this is particularly true for QR code phishing attacks. Defender for Office 365 customers will soon be able to use Attack Simulation Training to equip their end-users with the knowledge to be vigilant about QR code phishing through simulations of real-world attacks. This training can help users recognize the signs of QR code phishing attacks, such as identifying suspicious senders, anomalous email body content, and other important factors, and teach them how to respond appropriately. Private Preview for QR code-based simulations is slated for CY24Q1, and interested customers can join our Customer Connection Program for early access.

Unparalleled scale of QR code phishing blocked by Microsoft Defender for Office 365

Microsoft Defender for Office 365 image detection technology has significantly disrupted QR code phishing attacks, compelling attackers to alter their strategies between Q4 2023 and Q1 2024. This shift in tactics is evident in the substantial decrease in daily phishing emails intercepted by our system, dropping from three million in December to just 179,000 by March.

Blocked **~1.5M** QR code phishing emails per day by heuristics rules	Blocked **96%+** of blocked QR code phishing emails were enterprise	Blocked **~179k** QR code phishing emails per day by image detection
Scanned **150M** unique URLs from QR codes weekly	Blocked **18M+** unique QR code phishing emails weekly	Scanned **200M** unique URLs from emails weekly

Learn more about Defender for Office 365

Visit our website »

Get started with a free trial »

- › See how SecOps can hunt for QR code AiTM phishing and user compromise
- › Use modules to train your users to be more resilient against QR code phishing
- › Protect your organization against QR code phishing
- › Hunting and responding to QR code-based phishing attacks with Defender for Office 365