what you need to know about

Microsoft QR Code Phishing Emails

Be on the lookout for phishing emails using QR codes. These codes are sent through email, SMS, or even printed and left in public places for an unsuspecting scan.

QR Codes and Phishing

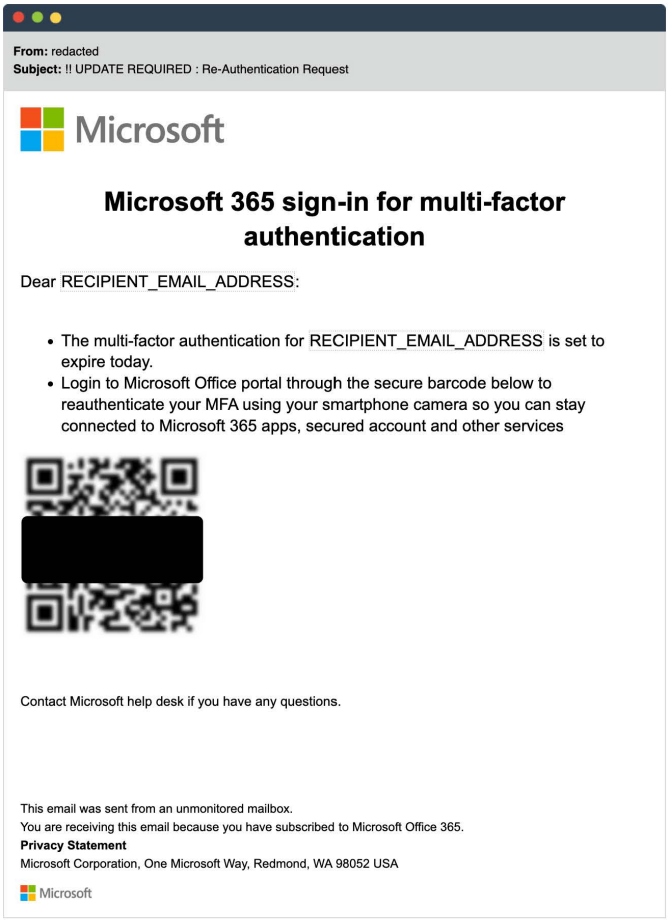
A QR code, short for Quick Response code, is a two-dimensional code that can store data such as messages, URLs, and contact information.

By concealing phishing links within a QR image, it has a higher likelihood of bypassing email filters to reach your inbox.

Microsoft Brand Impersonation

QR code phishing emails often impersonate Microsoft. If you scan the QR Code, it takes you to a fake Microsoft login page designed to steal your credentials.

See an example of this phishing email below.



From: redacted
Subject: !! UPDATE REQUIRED : Re-Authentication Request

Microsoft

Microsoft 365 sign-in for multi-factor authentication

Dear RECIPIENT_EMAIL_ADDRESS:

- The multi-factor authentication for RECIPIENT_EMAIL_ADDRESS is set to expire today.
- Login to Microsoft Office portal through the secure barcode below to reauthenticate your MFA using your smartphone camera so you can stay connected to Microsoft 365 apps, secured account and other services

Contact Microsoft help desk if you have any questions.

This email was sent from an unmonitored mailbox.
You are receiving this email because you have subscribed to Microsoft Office 365.
Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Microsoft

1. **Don't interact with unsolicited QR codes.**
   Think twice and don't scan QR codes unless you trust the source and were expecting it.

2. **Scrutinize all email requests.**
   Be on the lookout for popular phishing narratives like shared documents, overdue payments, order requests, invoices, and authentication requests.

3. **Always verify.**
   Phishing emails often use brands and images you recognize to create a sense of trust. Call the sender to verify the email is legitimate if anything looks unusual.

Report Phishing

Remember, you are the last line of defense against phishing.
If you receive a suspicious email, report it immediately.