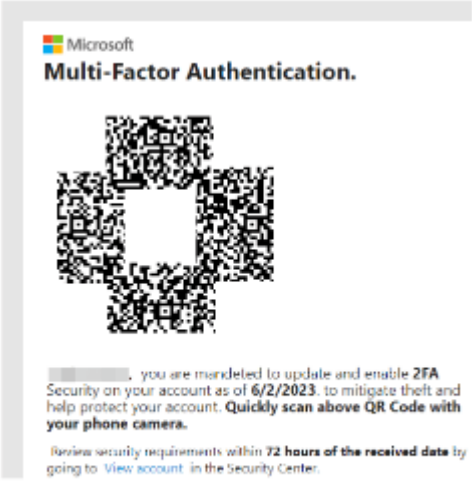
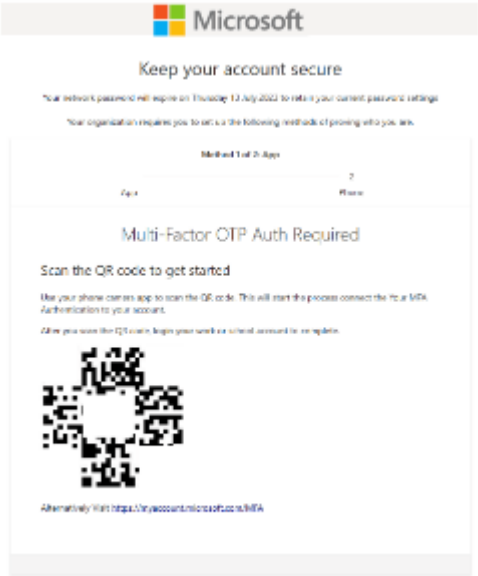
Malicious QR Codes Attacking the Energy Sector

Since May 2023, a large phishing campaign is utilizing Quick Response (QR) codes in an attempt to collect Microsoft credentials from victims. The emails masquerade as a Microsoft security notification with a QR code embedded inside a PNG image or a PDF attachment. This phishing campaign has been seen across multiple industries with the energy sector being the largest industry targeted. A U.S.-based energy company has been the primary target, receiving 29% of the emails pertaining to this phishing campaign. Other top industries targeted include manufacturing, insurance, technology, and financial services. Most of the QR codes send individuals to a Bing redirect URL, however other domains such as krxd[.]com (associated with the Salesforce application), and cf-ipfs[.]com (Cloudflare's Web3 services) have also been used. This phishing campaign marks a shift in threat actor tactics, as QR codes have traditionally not been used in phishing attacks.





(Source: TheRecord)

QR codes are less likely to be considered malicious by cybersecurity measures and victims as there are no typical indications of it being malicious, such as spelling errors or strange URLs. As phishing campaigns continue to evolve, awareness among employees and organizations is paramount. By understanding the tactics used by attackers, organizations can better equip themselves to detect and prevent these attacks. Encouraging a culture of skepticism can go a long way in thwarting phishing attacks.

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/
2. https://therecord.media/phishing-campaign-used-qr-codes-to-target-energy-firm