#289 Cybersecurity & QR Codes

Do you know that QR means Quick Response? QR codes were originally invented in 1994 by a subsidiary of Toyota to improve their manufacturing process. They were ahead of their time, long before smartphones. They were then adopted by marketing companies to al-

Microsoft

Microsoft 2FA Security Policy

Your Microsoft 2FA security Authenticator access expires soon.
To avoid being locked out of your email account, scan the QR code below with your phone.

This QR code expires ion the next 24 hours.

Note: This action is required immediately to avoid service interruption.

Thank you,
The Microsoft Account Team

Figure 1. QR code as an image within email body redirecting to a malicious website.

low mobile devices to quickly launch websites with a long and complicated addresses. Now, globally, and in particular Thailand QR codes are almost ubiquitous in terms of our daily financial exchanges, from major supermarkets to small shops along the soi. They're everywhere. This form of digital cash transaction is so convenient that several people I know don't carry cash around anymore. The latest phishing campaigns, known as Quishing, are now exploiting this general trend to using QR codes, so we need to be vigilant.

For example, would you know that this image was a quishing email? More recently QR codes have been used as part of massive global phishing campaigns. According to Microsoft, approximately 1.5 million QR code phishing emails are blocked per day. Scanning a malicious QR code can take you to a website that can harvest the usernames and passwords of your bank account and other sensitive data. Also, phishing emails are becoming much more difficult to identify. The prevalence of A.I. has made it much easier for the phishing emails to appear genuine. There are no longer spelling or grammatical errors. In addition, they use A.I. to create sophisticated campaigns to target demographics within society that may be susceptible to this type of cybersecurity attack.
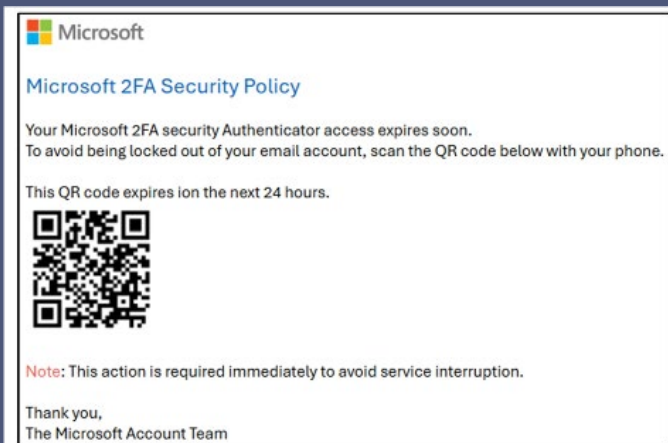
If you suspect the email is a phishing for data, do not click on any links or open attachments. Report it as phishing within your email client first, then delete it. Do not forward to anyone else. If you're not sure, take a screenshot and contact helpdesk@patana.ac.th. Reporting it as phishing will help to block further emails being sent to members of our community. This is a collective responsibility we have within our community to keep us safe.

You can keep up to date on the latest phishing campaigns here.

Stay safe.

Brian Taylor

Vice Principal, Technology for Learning