ITS Communications

Algonquin College
Cybersecurity
Awareness Month
2024

Embedded Links and QR Codes in PDFs

Be on the lookout for malicious links and QR codes in PDF files. Threat actors are exploiting this trusted file type to deceive targets and bypass Secure Email Gateways (SEGs). QR codes have been especially popular, since they require you to use a mobile device, which typically doesn't have the same protections as your work computer.

If you click a link or scan a QR code, it will take you to a page to download malware or steal your credentials.

Before opening an attachment, ask yourself:

- Were you expecting it?
- Do you recognize the sender?
- Does the email have any indicators of a phish, like appeal to emotions or sense of urgency, strange formatting, or spelling/grammar mistakes?

Is there any reason that your company would use a QR code or URL embedded in a PDF instead of a link in the email?

Remember, you are the last line of defense against phishing.
IF YOU RECEIVE A SUSPICIOUS EMAIL, REPORT IT IMMEDIATELY.

Report Phishing

REAL EXAMPLES OF THIS THREAT BELOW