

Quishing: Think Before You Scan

Most people have been trained well to be cautious about suspicious links in emails, but QR codes can be even more of a risk. QR codes bypass many of our trained instincts and bad actors are increasingly using malicious QR codes in emails, texts, and even physical media to direct users to phishing sites to steal their credentials or confidential information. This is know as "quishing".



Where Did The QR Code Come From?

Is the code expected or from a source you trust? Does the accompanying messaging seem overly urgent or unusual to you? You should always verify the source is legitimate before scanning any QR code.

After Scanning the Code: Do More Verification

Once you have verified the source you will want to inspect the page that you are brought to. Does the domain name of the URL seem right? Is there odd wording or misspellings? If the URL seems odd, do not proceed.

Be Wary of Emailed Codes: Treat Them Like Links

Were you emailed a QR code? You should just think of them as links in any other email. Consider the source of the email first and if you feel something is off you can report the email as spam, or just delete it.

Did It Take You to a Login Page? STOP!

Be very cautious of the page. Close the page and open your own internet browser and find the login page independently. A fake login page that looks legitimate is a simple way for you to give away your login information.



<https://my.infotex.com/quishing-awareness-poster/>

Report Anything Suspicious: It Helps Everyone

If you are out in the world and are dealing with a physical QR code on a sign you should look for any irregularities or possible damage to the sign. You should report any such-noted problems to the staff of establishment.