Report on Patient Privacy Volume 23, Number 12. December 07, 2023 Security Checklist: Steps to Thwart QR Code-Based 'Quishing'

By Jane Anderson

The HHS Health Sector Cybersecurity Coordination Center (HC3) is warning that QR codes—short for "quick response"—are increasingly being used by bad actors in phishing attacks. These attacks, called "quishing attacks," most often are the initial step in a multistage cyberattack, HC3 said.

"QR codes are often inserted into e-mails for legitimate purposes," HC3 said.[1] "They can serve to replace traditional hyperlinks and be especially useful when the end user is utilizing a smartphone." However, they also can be abused as part of a cyberattack, the agency said. "The most common way QR codes are used for malicious purposes is to simply e-mail the user a QR code in a way presented as useful, but actually points the user towards a malicious site or initiates the download of malware."

Fundamentally, HC3 said, quishing is very similar to more traditional phishing, which tries to trick the user into clicking a malicious link. "The ability to trick a user into scanning a QR code is often based on false context; an email containing text and graphics falsely creating the impression that it is something the user would be interested in," the agency said.