FS-ISAC

CITIZENS BANK OF KANSAS

Security Tips Newsletter

February 2024 | Issue No. 7

Security is Everyone's Responsibility

Quishing, the New Phishing

Summary

QR codes seem to be everywhere. You may have scanned one to see the menu at a restaurant or pay for public parking. You may have used one on your phone to get into a concert or sporting event or to board a flight. There are countless other ways to use them, which explains their popularity. Unfortunately, scammers hide harmful links in QR codes to steal personal information. Here's what to know.

There are reports of scammers covering up QR codes on parking meters with a QR code of their own. And some crafty scammers might send you a QR code by text message or email and make up a reason for you to scan it. These are some of the ways they try to con you:

- *Lying and saying they couldn't deliver your package and you need to contact them to reschedule*
- *Pretending like there's a problem with your account and you need to confirm your information*
- *Lying and saying they noticed suspicious activity on your account, and you need to change your password*

These are all lies they tell you to create a sense of urgency. They want you to scan the QR code and open the URL without thinking about it. A scammer's QR code could take you to a spoofed site that looks real but isn't. And if you log in to the spoofed site, the scammers could steal any information you enter. Or the QR code could install malware that steals your information before you realize it.

Prevention Tips

How can you protect yourself?

- If you see a QR code in an unexpected place, inspect the URL before you open it. If it looks like a URL you recognize, make sure it's not spoofed — look for misspellings or a switched letter.
- Don't scan a QR code in an email or text message you weren't expecting — especially if it urges you to act immediately. If you think the message is legitimate, use a phone number or website you know is real to contact the company.
- Protect your phone and accounts. Update your phone's operating system to protect against hackers and protect your online accounts with strong passwords and multi-factor authentication.

If you realize you clicked or responded to a phishing email involving your [Institution] account, contact us immediately. You will need to change your passphrase. Additionally, you can report the incident to the FTC at ReportFraud.ftc.gov or the Internet Crime Center at www.ic3.gov. Please remember, that *security is everyone's responsibility*.