Fake QR Code Scams

QR codes, or Quick Response Codes, are meant to serve as easy access to URL links and websites. Here are some examples of when one might use a QR code:

- Sitting at your favorite restaurant and there are no paper menus, the server asks that you please scan a QR Code that is stickered to the table
- In a museum, you walk up to an exhibition and scan the QR code to hear all about the dinosaurs
- Shopping online and see a QR code for 50% off your favorite shopping site
- Received an email with a "Scan me for a 'special event sale'" QR code
- Paid the parking meter with a QR code on a sign or in a parking garage
- Email from merchant stating your merchandise cannot be delivered, scan QR code to reschedule delivery

In each of these examples, the random QR codes you scan, especially those found in public and embedded on websites for use, can pose a risk to the health of your device. A fraudulent QR code could take you to a spoofed site that looks real but isn't. If you log in to the spoofed site, the scammers can easily steal any information you enter. The QR code could also install malware that steals your information before you realize it. Within minutes of scanning a fraudulent QR code, malware is installed, your device has been hacked, the funds in your Financial Institution's app have been transferred out of your account(s), and you are locked out.

Scammers are placing fraudulent QR code stickers over real codes found in public, and hacking into webpages to embed these fake codes. The problem is the naked eye can't detect which codes are genuine, and which are the work of scammers.

So, how can you protect yourself from these fake QR codes?

- **Consider the source of the QR code.** If it was broadcast on Channel 5 news this evening, it's probably a legit link. Is the QR code in a magazine on the page of a familiar company? Chances are, it's probably ok. What has been found to contain fake QR codes are flyers that are passed on the street or stored in the entry way of a restaurant. *Do not scan random QR codes found in places you wouldn't expect them.*

- **If you see an ad that seems tempting, go directly to the website of that merchant using a secure search engine,** search to see if that same deal can still be found, and can you make the purchase without scanning a QR code. When in doubt, always go directly to the website of that merchant or contact them directly to see if they have a valid QR code offer. *Avoid any message that gives a sense of urgency.*
- **Check physical pamphlets, flyers, papers, menus, message boards, etc. for a sticker overlay.** If you suspect multiple layers of the QR code, chances are a fraudster placed a fake code over the valid one. *Make sure no one has tampered with any code you plan to scan.*
- **Verify the sender of the QR code.** If you receive an SMS message or email with a QR code, visit that business's trusted site. *Call only phone numbers that are found on this trusted secure site.*
- **Look at the URL that the QR code is leading to.** Are there misspellings, or letters switched? Make sure the link isn't spoofed.
- **Keep your phone and devices' operating system up to date.** The FTC recommends keeping the OS as current as possible and having strong, multifactor authentication passwords in place. You should also consider getting antivirus software.

What to do if you suspect you fell victim to a QR code scam:

1. File a complaint online to the Federal Trade Commission, which has information on fake QR codes.
2. Secure your device to ensure no malware or virus remain
3. Contact any financial institute that may have compromised account information to secure your accounts. Add password access to any account possible and lock down your credit to ensure no fraudulent credit lines are obtained.