Think Twice Before Scanning That QR Code

You have probably noticed that Quick Response — QR — codes are everywhere these days, on the tables at restaurants, on posters, print and electronic advertising, and even during TV programming and commercials.

By training your smartphone camera on one, you'll get a prompt to click to open a web page, typically one for the company behind the QR code. But now, even these are prone to misuse.

The FBI recently issued a warning, stating that criminals are using tampered codes to redirect customers to malicious sites and hack their financial and login information. They can send the code through e-mail as promotion codes.

They also may paste the tampered code on the original one, such as parking meters, flyers, or a restaurant table where the original code would bring up the menu.

These crimes can do serious damage to your finances and credit history. According to the FBI, criminals are using malicious QR codes in two ways:

- When scanned, the code takes you to an imposter phishing website trying to trick you into logging in, hoping that you will use an existing username and password, or share other personal or banking information.
  The QR code releases malicious code — such as malware, ransomware and trojans — onto your phone, allowing criminals to track information from your phone and even lock you out of the device and only releasing it if you pay up.
- The QR code can compose pre-written e-mails and send them from your account. These e-mails are often new phishing e-mails aimed at getting your contacts to open and click on malicious links. Scammers can also program the codes to open payment sites and follow social media accounts.

Worse, QR codes are easy to create with a number of free online tools. This makes the codes easy for businesses to use — but it's also easy for scammers to take advantage of them.

Prevention

The first step in prevention is being able to identify a potentially dangerous QR code. According to cyber security firm Aura, the most common scams are:

- QR code scams on parking meters and other contactless payments.
- QR codes sent in phishing e-mails (failed payments, credential phishing, etc.).
- Tampered QR codes in restaurants.
- Fake QR codes sent through the mail (surveys, sweepstakes, etc.).

- QR codes on unexpected package deliveries.
- QR codes at sham COVID-19 testing centers.
- QR codes sent over social media (hacked accounts).
- Cryptocurrency QR code scams.
- Fake QR code scanner apps that download malware.

Rather than avoid QR codes entirely, learn how to identify the common signs indicating that you're dealing with a fraudulent QR code.

Aura recommends the following to avoid becoming a victim of QR code fraud:

Look for signs of tampering — Scammers may print their own QR code stickers and paste them over legitimate ones. Check to see if the code is on a sticker above another one, or if there are signs it has been tampered with.

Preview the URL before following the QR code — The little box that opens up when you scan a QR code will include text identifying the site to which it will direct you. Check whether the URL seems safe, or with your waiter if you're at a restaurant. Beware of an URL that doesn't look complete or if you can't read it.

Check the site for signs it's not legit — There are often signs that you've landed on a phishing site: words are misspelled or the text has typos or odd grammar that is clearly not written by a native English speaker. The design may be shoddy and the images low resolution.

Additionally, the URL may be unsecure (secure sites start with https: and will display a padlock icon). Be wary of sites that start with http:.

Exercise caution with QR codes in public places — These codes may have been placed there by a scammer. You may want to completely avoid scanning these codes to be safe, especially if it's for a product or deal that seems too good to be true.

Avoid opening QR codes in e-mails or regular mail — This is usually a bad idea. If you do want to click on the code, try to reach the company first and check the legitimacy.

###