CS

CYBER SECURITY & YOU

APRIL 2023

LASERS

QR CODE AWARENESS

The popularity of Quick Response (QR) codes continues to rise. These square bar codes are easily scanned with a smartphone and are usually found in restaurant menus, TV commercials, and printed ads. It is a convenient way to access information from a phone, but it has also created new opportunities for cybercriminals to access your personal information.

Here are some tips to keep you safe when it comes to scanning QR codes:

>> Know where the code leads.

QR codes themselves are not malicious, but sometimes it's difficult to tell where a code will lead once it's scanned. The sites that QR codes open might obtain your data by using third-party companies. Sites can exploit financial information, expose social media account data (including contacts), gather geolocation data of the device, or even add unwanted contacts to trigger spear phishing attacks.

Before scanning a QR code, be sure there is a legitimate URL (web address) listed nearby. URLs can be malicious and may look similar to authentic URLs, so check carefully for misplaced punctuation or letters. Going straight to the website from a web browser by entering the address is always a better option. It may not be as convenient, but it is the best way to avoid being attacked.

Take a moment to read the privacy policy if one is provided with the QR code, but use caution as it is unlikely the privacy policy will list the "affiliates" they share your data with.

sources:

Infosec.com | washingtonpost.com | isaca.org
aarp.com | forbes.com

If you are using a QR code to verify an account, be sure the site is legitimate. For example, Microsoft will use this method when a person is setting up MFA for their account.

>> Beware of tampering.

If you receive a physical code to scan, make sure it has not been tampered with. Hackers will sometimes place a **sticker** on top of the code sending you to a malicious site.

>> Steer clear of open networks.

Avoid using QR codes provided to connect to **WiFi networks.** The code may contain authentication and credentials to an open network easily exposing your device to attacks.

>> Faster isn't always better.

A QR code may be provided as a quick way to download an app on a mobile device. Use caution when considering this as the app or even the link itself could be malicious. Instead, **use the app store** on the device.

Try it with your smartphone!

lasersonline.org

QUICK TIP

Most mobile devices can scan QR codes using the camera app that is provided.