NEED TO KNOW NEWSLETTER | DECEMBER 2023

Think before you scan

QR codes are becoming more and more common. They appear everywhere you look: gift cards, tickets, menus, advertisements, games, and more. The more popular they become, the more hackers want to exploit them.

This month's newsletter will cover how QR codes have become a security risk and what you can do to protect yourself.

About QR codes

The QR, or quick response, code was created in 1994 to track production parts. The code consists of tiny black-and-white squares. You use your phone to scan this special type of link, and it displays text, downloads information or takes you to a website.

The interaction is quick and easy but can also be dangerous. With a traditional link, you can see the address and know where you will be landing on the internet. With a QR code, you don't.

Risks

The key risk factor with QR codes stems from that hidden content. QR codes keep their message under wraps until scanned. That means that scanning a QR code could be the first step in a **malware** or **phishing attack.**

Hackers may place malicious codes over legitimate ones or place them in high-traffic areas, hoping to catch someone's curiosity. Behind the malicious code hides malware. Malware on your device can compromise your data and put you at risk of your accounts getting hacked.

Hackers have also been known to send phishing emails with QR codes in them. These types of emails can often bypass security measures put in place to stop unwanted phishing emails from getting into your mailbox. We've all been trained not to click phishy links, but we also shouldn't scan phishy codes!

QR codes can also insert contact information into your phone. A hacker's QR code may **create a new contact** that looks legitimate. Many people forget the exact contacts they enter into their phone, and hackers can reach you by pretending to be legitimate contacts.

Staying safe

First, **don't scan a QR code unless you absolutely must.** Free food and promotional offers are great, but they aren't enough to risk having your data stolen.

Second, **treat every QR code as suspicious.** You never know where a QR code leads or who posted it.

Third, **only scan QR codes from trusted sources.** Get QR codes from a company's official resources, like their website. If you receive the code on a business card from someone you know and trust, it's probably safe to scan. But if you receive the code on a flier from a stranger, don't trust it.

Oh no! I might have scanned a malicious QR code. What should I do?

- **Don't trust odd websites** — The website you land on might ask you for sensitive information like your username and password. Do not provide any information.
- **Don't make any online payments** — Infected devices may allow hackers to capture your financial information. Do not log into your bank or transfer any money.
- **Immediately close the website** — If you have found yourself on an unexpected or unrelated website after scanning a QR code, immediately close the browser.

Pro tip: Be proactive with mobile security. Keep your phone and apps up-to-date, only download apps from trusted vendors and stay vigilant with ongoing cybersecurity threats.

Avoid secret gift exchanges with strangers online

"Do you want to join a secret gift exchange with 36 other people? All you have to do is send one gift, and you will receive 36 gifts!" Hold on, slow down! This is a popular scam going around on social media sites. These scams collect your personal information — and sometimes, the information of your friends and relatives, too! Keep your gift-giving to the people and charities that you know.

E-TECH