DECEMBER 2023 VOL. 19

Security Matters
NEWSLETTER

SCAN WITH CAUTION. QUISHING ATTACKS ARE EVOLVING

Quick response codes (QR Codes) are nothing new. It has been around since the 90s as a way of tracking car parts during manufacturing. QR codes contain large amounts of data. This data, when scanned, directs users to a website, initiates a phone call, or downloads an application, among other possible functions. Today, we see them everywhere in restaurants, mass transportation, commercials, signs, walls, advertisements, etc. The pandemic fueled the usage of QR codes as organizations attempted to reduce transmission and follow protocols.

Many people know they need to be aware of phishy links and unknown attachments in emails. But thinking twice about scanning a QR code with our smartphone camera isn't second nature for most people. While QR codes do have their benefit, their rising popularity has also become the cybercriminals' arsenal of weapons - QR phishing attacks.

QR phishing or "quishing," works by directing victims who scan the QR code (typically using their smartphone) to malicious sites or links. There are numerous QR code phishing attacks occurring worldwide such as QR codes in phishing emails, malicious QR codes on banking app, fake parking tickets, parking meters, redeeming for free stuff, etc.

How Quishing can affect you?

- ✓ You might be redirected to a phishing website.
- ✓ It could be a malware attack.
- ✓ It might control your social media accounts.
- ✓ Attackers distribute malicious QR codes. These codes can be found in emails, websites, flyers, or even physical locations.
- ✓ Unsuspecting victims scan the codes. This action redirects them to malicious websites designed to steal credentials, install malware, compromise systems, or launch further attacks.

HOW TO PREVENT QUISHING?

1 **Think twice before scanning a QR code**

Don’t scan a QR code in an unexpected email or text message, especially if it urges immediate action.

2 **Analyze the source**

Check the QR code destination. Is the QR code included in a legitimate email, website, or location?

3 **Verify the URLs**

Check for any misspellings or grammatical errors. Ensure it’s a secure connection beginning with the “HTTPS”. If the URL has been shortened and there’s no way you can verity it, it’s better to stay away from it.

4 **Avoid stranger links**

Anonymous messages with phishing links or QR codes may redirect you to fake websites, prompt payments, or download malware to your device.

5 **Use built-in QR scanner**

Avoid using or downloading third-party apps to scan a QR code.

6 **Avoid scanning QR code in an email**

Legitimate companies will not send a QR code to verify your account.

7 **Updates Operating System and use anti-malware software**

Keep your Operating System and anti-malware updated. Protect your device and online accounts with strong passwords and enable two-factor or multi-factor authentication.

8 **Beware of QR codes received unexpectedly**

Especially a QR Code sent by a stranger to receive money. If you have scanned an unexpected QR code that required you to receive money, report the transaction to your bank and relevant authority immediately.

9 **Never enter sensitive information**

Don’t log in to accounts or provide personal details after scanning a QR code.

10 **Educate yourself about QR code before using them**

Keep yourself updated about the latest phishing tactics and educate others about quishing.

Related News

New Android update will enable apps to detect your screenshot activity

Taking a screenshot on your smartphone is no trivial matter. Depending on the case and the applications concerned, it can be subject to copyright or play a part in online harassment and piracy. A forthcoming update to Android 14 could lead to the restriction of users' ability to take screenshots.
Read more: https://bit.ly/45aF9iW

WhatsApp's new secret code feature lets users protect private chats with password

WhatsApp has launched a new Secret Code feature to help users protect sensitive conversations with a custom password on the messaging platform. The feature has been described as an "additional way to protect those chats and make them harder to find if someone has access to your phone or you share a phone with someone else."
Read more: https://bit.ly/47BjGB8

Scammers are hijacking Google forms and using a fake AI chatbot to steal money

Scammers have found another way to abuse a legitimate cloud service to deliver spam and phishing messages to people's inboxes. The attackers also deploy a fake AI chatbot in an attempt to steal people's cryptocurrency.
Read more: https://bit.ly/3RHSAmp

This crafty iPhone attack makes you think your phone is safe until it's hacked

Lockdown Mode, an iPhone feature introduced with iOS 16, is not an antivirus, does not detect malware, and cannot prevent malware from operating. Therefore, hackers can create a fake Lockdown Mode and run malware operating in the background unabated.
Read more: https://bit.ly/3Q6CJge

CyberSecurity Malaysia (CSM) warns of impersonation, scam activities on WhatsApp

CSM said there were fraudulent activities using WhatsApp, with the perpetrator posing as someone known to the victim before sending a link and asking the victim to click on it. The victim will subsequently lose access to their WhatsApp account once they click on the link.
Read more: https://bit.ly/3RHSAmp

Facebook Messenger gets end-to-end encryption by default and a slew of new features

Meta has officially begun to roll out support for end-to-end encryption (E2EE) in Messenger for personal calls and one-to-one personal messages by default. In addition to the encryption, you can now edit messages, send disappearing messages, hide your read receipt, so people can't see when you've read their message and there are some improvements to voice messaging.
Read more: https://bit.ly/3RHSAmp

Hackers spy iPhone users using malicious keyborad apps

A new method of keylogging using malicious keyboard apps has been discovered to affect iPhones, evading all Apple’s security detection procedures. Additionally, threat actors could also use this method to steal passwords, authentication codes, notes, private messages, etc.,
Read more: https://shorturl.at/mpqCT

PDRM and Whoscall is giving away 1 million premium accounts to help fight against scams

Polis DiRaja Malaysia (PDRM) is collaborating with Whoscall, powered by Gogolook, to combat the rising scam calls that are plaguing Malaysians. The collaboration saw PDRM and Whoscall giving away 1 million free Whoscall premium accounts to Malaysians as a safeguard against scam calls.
Read more: https://bit.ly/3RHSAmp

QR codes can steal money and install malware

Scanning a QR code can expose you to identity theft, according to the Federal Trade Commission. The technology helps retailers by giving them insights into customer behavior, such as by linking a QR code to a store loyalty program. Yet they can also give bad actors a stealthy tool for stealing consumers' personal information.
Read more: https://bit.ly/3RHSAmp

Decoding digital deals: beware of these common scams while shopping online

The flourishing ecommerce market has, sadly, opened the floodgates to an abundance of scams, posing significant challenges for both buyers and sellers. Indeed, payment frauds loom large, with scammers manipulating transactions through fake payment receipts or soliciting advance payments without fulfilling their end of the bargain.
Read more: https://bit.ly/3RHSAmp

Google's new tracking protection in Chrome blocks third-party cookies

Google has announced it will soon start winding down support for third-party cookies in its Chrome web browser. It’s a move designed to improve user privacy and stop websites from tracking you as you visit different URLs.
Read more: https://bit.ly/45aF9iW