

Forum:[Hack Forums](#)

Thread: [The Hidden Risk of "Quishing" or QR Code Phishing in 2025](#)

JoseMar - March 15, 2025, 7:14 am

The Hidden Risk of "Quishing"
or QR Code Phishing in 2025

QR codes have become essential for rapidly exchanging information or payments and navigating websites in the current digital era 2025. Still, there is also a downside: QR code phishing, often known as "quishing." It is a cyber threat that exploits our trust in these so-called useful little squares.

How Quishing Works:

Hackers develop fraudulent QR codes that direct visitors (the one who scans it) to fake, cloned websites or initiate software downloads, i.e., directly downloading something onto the mobile device.

These QR codes can be distributed through multiple methods, such as: emails
social networks
printed materials or stick stickers over authentic QR codes in public locations.

The Deception Process: Deceptive Redirection: Scanning a malicious QR code takes you to a convincing but fake website.

Information Theft: You are prompted to provide sensitive information about yourself, such as login credentials or bank details.

Malware Attack: Sometimes, scanning the code can download malware or another virus, endangering your mobile device in most cases.

The FBI has detected an increase in 2025 regarding this issue using QR codes and crypto ATMs, i.e., victims are tricked into using these ATMs to send money in crypto, which is then transferred to the creator's crypto wallet of the fake QR code.

Quishing attacks have targeted various industries, such as: energy,
manufacturing, insurance,
technology,

Financial services. These attacks are usually made in trusted domains, and ingenious tactics are used to prevent detection.

Risks Once a Hacker-Made QR Code is Scanned: Personal Data Theft: Your sensitive information could very likely be stolen.

Financial Fraud: Direct financial theft or fraud may occur in your name once your data is stolen.

Malware Infection: Devices and networks can be hacked with malware that your antivirus may not detect.

Trust Issues: The growing problem of squishing can weaken trust in QR codes, making them less effective for legitimate use.

How to Stay Safe: Always Be Cautious: Always verify the source before scanning a QR code.

Check URLs: Ensure the URL matches the intended destination, and do not click before verifying the URL.

Use Secure Scanners: Some QR code scanning applications offer additional security capabilities, which is very good to use.

Implement MFA: Add an extra layer of protection to your accounts with multi-factor authentication.

Monitor Campaigns: Businesses should check their QR code campaigns for any signs of

tampering.

Don't forget to stay safe!?

Additional sources to explore: You can also search directly on Google for more information:

<https://sosafe-awareness.com/glossary/quishing/>

<https://cybersecuritynews.com/gr-code-phishing/>

<https://www.nospamproxy.de/en/quishing-phishing-with-qr-codes/>

tkboom - March 15, 2025, 7:20 am

It would be horrible if someone did that.

Bastille - March 15, 2025, 7:23 am

Thanks for this thread, nowadays we see QR codes everywhere, even at restaurants on the tables to get the menu, those ones could be easy targets as their websites are usually easy to clone, could make a typosquatting domain, and boom.

This involves placing the fraudulent QR code on the table tho, and as we all know, the closer you're from the target, the riskier it is.