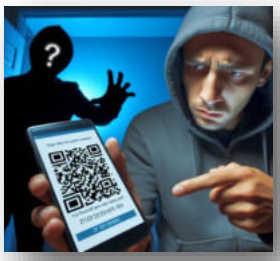
Newsletter Date
16-Dec-2024

Vol I Issue 7

# Cybersecurity Digest

Bi-Weekly Update by
the CISO Section of Meghalaya Rural Bank



QR Code Scam

Inside this issue:




## Quishing Scam: The new Cybercriminal Tool

**Quishing**, or QR phishing, is a cybersecurity threat in which attackers use QR codes to redirect victims to malicious websites or prompt them to download harmful content. The goal of this attack is to steal sensitive information, such as passwords, financial data, or personally identifiable information (PII), and use that information for other purposes, such as identity theft, financial fraud, or ransomware.

This type of phishing often bypasses conventional defenses like secure email gateways. Notably, QR codes in emails are perceived by many secure email gateways as meaningless images, making the users vulnerable to specific forms of phishing attacks. QR codes can also be presented to intended victims in a number of other ways.

QR codes, or Quick Response codes, are two-dimensional barcodes that can be scanned easily with a camera or a code reader application. The main component of a QR code is data storage. QR codes have the capability to store significant amounts of information including URLs, product details, or contact information. Scanning technology allows smartphone cameras or code readers to easily and quickly access the website to which the URL points.

In a quishing attack, the attackers create a QR code and link it to a malicious website. Typically, the attacker will embed the QR code in phishing emails, social media, printed flyers, or physical objects, and use social engineering techniques to entice the victims. For example, victims might receive an email urging them to access an encrypted voice message via a QR code for a chance to win a cash prize.

Upon using their phones to scan the QR code, victims are directed to the malicious site. The site may prompt victims to enter private information, such as login information, financial details, or personal information. In the example above, the site may request the user's name, email, address, date of birth, or account login information.

Once this sensitive information is captured, attackers can exploit it for various malicious purposes, including identity theft, financial fraud, or ransomware.

## Scareware

A scareware is a cyberattack tactic that scares people into visiting spoofed or infected websites or downloading malicious software (malware). Scareware can come in the form of pop-up ads that appear on a user's computer or spread through spam email attacks.

A scareware attack is often launched through pop-ups that appear on a user's screen, warning them that their computer or files have been infected and then offering a solution. This social engineering tactic aims to scare people into paying for software that purportedly provides a quick fix to the "problem." However, rather than fix an issue, scareware actually contains malware programmed to steal the user's personal data from their device.

# Zero Trust Model


Zero Trust is a network security strategy based on the philosophy that no person or device inside or outside of an organization's network should be granted access to connect to IT systems or workloads unless it is explicitly deemed necessary. In short, it means zero implicit trust.

In 2010, Forrester Research analyst John Kindervag proposed a solution he termed "Zero Trust."

It was a shift from the strategy of "trust but verify" to "never trust, always verify." In the Zero Trust model, no user or device is trusted to access a resource until their identity and authorization are verified. This process applies to those normally inside a private network, like an employee on a company computer working remotely from home or on their mobile device while at a conference across the world. It also applies to every person or endpoint outside of that network. It makes no difference if you have accessed the network before or how many times — your identity is not trusted until verified again. The idea is that you should assume every machine, user, and server to be untrusted until proven otherwise.

# UPI Fraud Prevention

- Beware of fraudulent calls or messages from individuals posing as bank representatives. Verify the authenticity of unknown numbers using apps like Truecaller, and refrain from responding or providing any personal information.
- Avoid sharing your UPI PIN, password or OTP (One-Time Password) with anyone, including bank representatives. Legitimate bank representatives will never ask for such information over phone calls, emails or text messages
- Avoid using public or unsecured networks that can be easily accessed by hackers.
- Do not disable push notifications and transaction alerts on your UPI apps.
- Never leave your bank account unattended.
- When conducting UPI transactions, ensure that you are using a secure and trusted Wi-Fi network.
- Regularly update your UPI apps to the latest version available. Software updates often include security enhancements that can protect you from potential vulnerabilities.
- Keep a close eye on your UPI account activity and transaction history. If you notice any unauthorised or suspicious transactions, immediately contact your bank and report the issue.