
	<p>रक्षा लेखा प्रधान नियंत्रक (मध्यकमान) 1 करियप्पा मार्ग, लखनऊ छावनी-226002 Principal Controller of Defence Accounts (Central Command) 1 Cariappa Road, Lucknow Cantt.- 226002 कार्यालय फोन सं.-0522-2451084/कार्यालय फ़ैक्स सं-0522-2453038 Office Phone No.-0522-2451084/Office Fax No.-0522-2453038 E.Mail- cda-luck@nic.in & pcdacedp.dad@gov.in</p>	 <p>आजादी अमृत महोत्सव</p>
---	---	---

Circular

No. IT&S/AN/174/Cyber Security/2023-24

Date: 17/07/2023

To,
The Officer-in-Charge
All sections of Main Office
All sub-offices
Under PCDA (CC) Lucknow

Sub:- Advisory – Safeguards against Malicious QR Codes.

Ref:- HQrs office circular no Mech/IT&S/810/Cyber Security dated 12/07/2023.

With reference to HQrs office circular cited under reference, an advisory is issued regarding “Safeguards against Malicious QR Codes”. A copy of the same is enclosed herewith for your information & to disseminate the guidelines to all concerned for strict compliance.

It is also requested to submit an action taken report to this office latest by 20/07/2023 at 03:00PM.

Encl: As above.

Copy to:

OA Cell (Local): for uploading on website.


Sr. Accounts Officer (IT&S)


Sr. Accounts Officer (IT&S)

“ हर काम देश के नाम ”

रक्षा लेखा महानियंत्रक



उलान बटारोड, पालम, दिल्ली छावनी-110010
Controller General of Defence Accounts
Ulan Batar Road, Palam, Delhi Cantt.- 110010
(IT&S Wing)

Phone: 011-25665586, 25665589, 25665763 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security

Circular

Date: 12/07/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)

Sub: Advisory - Safeguards against Malicious QR Codes.

Quick response (QR) codes are very fast, convenient, encrypted and interoperable method, being used for contactless registration and digital money transfer etc. It is crucial for individuals to be aware of potential threats and to adopt protective measures. Hence, all are requested to bring to the knowledge of all employees about the security concerns raised, measures and practices recommended below:

A. Common types of QR code based Attacks:

- **Phishing:** Malicious QR codes are used to redirect unsuspecting individuals to phishing websites masquerading as legitimate ones to steal sensitive information such as login credentials, credit card numbers or other personal data.
- **QR code Swaps:** Legitimate QR codes displayed at businesses are altered or tampered with to trick individuals into directing payment to threat actor's bank account instead of the intended recipient.
- **Malware Distribution/Infection:** Malicious QR codes are embedded with links that when scanned and accessed, lead to downloading and installation of malware onto the individual's device, potentially leading to unauthorized access, data breaches or other malicious activities.
- **Malicious Advertisements in QR code scanner applications:** Victims may come across advertisement banners assuming it is a part of the service that they had scanned for, victims click on the advertisement and are directed to a phishing site requesting for personal information and banking credentials. Individuals are advised to remain vigilant specially when using a third party QR code scanning application.

B. Safeguards:

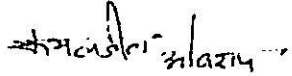
- **Be Vigilant:** Avoid scanning codes received via unsolicited text or whatsapp messages, emails, social media messaging platforms or from unknown entities.
- **Check QR codes prior to scanning:** Before scanning QR codes, carefully examine them for any signs of tampering or irregularities. Avoid scanning QR

codes if it appears to have been pasted over the original code or if there are design inconsistencies.

- **Check the Destination link before accessing the website:** Always check for misspelt domains, extra characters or unfamiliar addresses. If appears suspicious, don't access the website.
- **Verify Recipients of Digital payments through QR codes:** Always review the transaction details, amount, recipient's name and other information displayed on the payment application carefully before confirming the payment.
- **Update of Device's Software:** Regularly update your devices' operating system and applications to ensure that they contain the latest security patches and updates.
- **Refrain from downloading applications from QR codes:** Refrain from downloading applications from third party websites that the QR code links to. Mobile applications should be downloaded from official sources.
- **Be wary of attractive offers:** If the QR code leads to a website that solicits for personal information in exchange for attractive offers or handouts, extra vigilance should be exercised. When an offer is too good to be true, it is probably not.

2. This is for your information and dissemination please.

Jt. CGDA (IT&S) has seen.


(Kamaljit Oberoi)
SAO (IT&S)