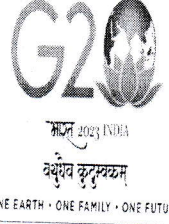कार्यालय ,रक्षा लेखा नियंत्रक
नं. 1स्टाफ रोड, सिकिंद्राबाद ,
Office of the Controller Of Defence Accounts
No.1 Staff Road, Secunderabad-500 009
(Tele/Fax:040-27843385-407 Fax: 040-27810499)
Email id: secdedpcda.dad@nic.in

सं./NO.ITS/5805/Gen.Corr/CyberSecurity

दिनांक/ Date: 14.07.2023

परिपत्र/CIRCULAR

(वेबसाइट के माध्यम से/Through Website)

सेवा में/To

1. र.ले.नि., आई.टी.एस.डी.सी., सिकंदराबाद/ The CDA, IT&SDC, Secunderabad
2. प्रभारी संयु.नि., वे.ले.का. (अ.श्रे) ई.एम.ई., सिकंदराबाद/ The Jt.CDA i/c, PAO(ORs)EME, Secunderabad
3. प्रभारी उप-नि., क्षे.ले.का. (थलसेना), विशाखापट्टणम्/ The DCDA i/c, AAO(Army), Visakhapatnam
4. वरिष्ठ उप-आई.एफ.ए.. आई.एफ.ए. (हैदराबाद/सिकंदराबाद)/ The Sr.Dy IFA, IFA Hyd/Sec'bad
5. प्रभारी उप-नि., वे.ले.का. (अ.श्रे) सेना आयुध कोर, सिकंदराबाद/ The DCDA i/c, PAO(ORs)AOC, Sec'bad
6. सभी व.ले.अ./ले.अ./कर्मचारी (स्थानीय)/ All SAOs/AOs/Staff(Local)
7. सिकंदराबाद/हैदराबाद/विशाखापट्टणम/तिरुपति/यद्दुमैलारम स्थित उप-कार्यालय/ All Sub-Offices in Sec'bad/Hyderabad/ Visakhapatnam/Tirupathi/Eddumailaram

विषय: परामर्शी - दुर्भावनापूर्ण QR कोड के विरुद्ध रक्षणोपाय ।
Sub: Advisory-Safeguards against Malicious QR Codes.

संदर्भ: मुख्यालय कार्यालय का दिनांक 12.07.2023 का पत्रांक Mech/IT&S/810/Cyber Security
Ref: HQrs Office letter No.Mech/IT&S/810/Cyber Security dated 12/07/2023.

*****

दुर्भावनापूर्ण QR कोड के विरुद्ध रक्षणोपाय से संबंधित परामर्शी सूचित करते हुए मुख्यालय के उपरोक्त पत्र की एक प्रति आपकी सूचना एवं अनुपालन के लिए संलग्न है ।   सभी अधिकारियों और कर्मचारियों से अनुरोध है कि वे दिए गए परामर्शों का पालन करें।

A copy of Hqrs letter containing Advisory-Safeguards against Malicious QR Code is enclosed for information and compliance. All the officers and staff are requested to follow the advisories given by the HQrs.

संलग्न: उपरोक्तानुसार
Encl: As above.

(के. गोपीचंद)
लेखा अधिकारी (आई.टी.)

रक्षा लेखा महानियंत्रक

उलान बटाररोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts
Ulan Batar Road, Palam, Delhi Cantt.- 110010

(IT&S Wing)

Phone: 011-25665586, 2566589, 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)