EC No. 85 / DoS -08 /2021

NB. DoS.HO. CSITE/ 227 / CS-01/2021-22 27 April, 2021

The Chairman and Managing Director/ Chief Executive Officers
All Regional Rural Banks / All State Co-operative Banks/
All District Co-operative Banks

Madam/Dear Sir,

Strengthening the controls of payment ecosystem between Sponsor Banks and RRBs/RCBs/UCB(s) as a corporate customer

Please refer to our circular EC.No.32 and 33 /DoS-07/ dated 06 February 2020 on Comprehensive Cyber Security Framework and circular No.315/DoS-31/2019 dated 10 December 2019 on domain email wherein Regional Rural Banks (RRBs) and Rural Co-operative Banks (RCBs) were advised, inter alia, to implement bank specific email domains within three months of the issue of the circular. However, it has been observed that many RRBs and RCBs have still not complied with this requirement as on date.

2. To specifically address the concern observed as above as well as risks associated with the payment ecosystem, RRBs / RCBs who may be serving as sponsor banks (for effecting payment transactions-fund transfers and/or providing internet banking services) for other RRBs/RCBs/UCBs are advised the following:

(a) Ensure to obtain confirmation from the RRB(s)/RCB(s)/UCB(s), that they have reconciled the transactions initiated by them (at least on a daily basis). In case the RRB/RCB/UCB does not provide confirmation, based on its risk assessment, the sponsor bank may consider putting its services on hold till confirmation is received from the RRB/RCB/UCB.

(b) Not to entertain email communication from the RRB(s)/RCB(s)/UCB(s) to whom they are providing sponsor bank services, if the email is originating from a domain other than that of the bank (e.g. gmail, rediff). If the RRB(s)/RCB(s)/UCB(s) have not complied with the requirement, the sponsor

bank may, based on its risk assessment, consider to keep their services on hold with the RRB(s)/RCB(s)/UCB(s). However, in case RRB(s)/RCB(s)/UCB(s) have not complied with the said requirement by April 30, 2021, the sponsor bank may put their services (which necessarily require email id for functioning) on hold till they have complied with the requirement.

3. We also enclose a copy of the Advisory No. UCB_1/2021 dated 24 February 2021 issued by RBI.

4. Please acknowledge receipt to our Regional Office concerned

Yours faithfully

(K. S. Raghupathi)
Chief General Manager

Encl: As above

पर्यवेक्षण विभाग, केंद्रीय कार्यालय
साइबर सुरक्षा और सूचना प्रौद्योगिकी जोखिम (CSITE) समूह
Department of Supervision, Central Office
Cyber Security & IT Risk (CSITE) Group

CONFIDENTIAL

Advisory No. UCB_1/ 2021 **Dated: February 24, 2021**

Un-authorized Fraudulent Transactions at Co-operative banks

It has been brought to our notice about un-authorized fraudulent transactions put through at an UCB. The fraudulent transactions were put through Host-to-Host mechanism provided by the sponsor bank for performing RTGS/NEFT transactions to its UCB corporate customers.

2. Following are the Modus-Operandi and Root Cause Analysis:

The attacker gained access of a system in the UCB's network and from there gained access to the toolkit from the server hosting the H2H application.

The attacker copied the H2H toolkit onto the secondary system, passed the fraudulent transactions. It was also observed that 2FA was not available to put through the transactions.

3. Major deficiencies observed from recent incidents occurred in UCBs:

- The affected UCB's server had an open internet connection and the internet usage was not monitored, server drives and folders were shared over the network and server had open USB ports for data transfer.
- Multiple remote desktop sharing applications were identified to have been installed on the server.
- Server access password was shared between UCB's employees.
- Periodic password change policy for the imaged server had not been implemented by UCB.
- There was a potentially malicious executable in the affected server which reportedly provided backdoor access to the attackers. It was connecting to a foreign IP address.
- Non-encrypted URLs of SMS services were observed which were used by UCB for sharing bank account updates with their customers

Instructions to be followed

4. A reference is invited to the Advisory 1/2019 dated May 9, 2019 on "Protection of Network/End-hosts for secure payment ecosystem" as well as Advisory no. UCB_1/ 2020 dated August 18, 2020 on "Un-authorized Fraudulent Transactions at Co-operative bank". It is reiterated that controls mentioned in the advisory ibid are to be strictly adhered to in respect of end point security, email security, network security and robust authentication mechanism.

5. A reference is also invited to “Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach” circular dated December 31, 2019. UCBs are advised to comply with the controls, as applicable (depending upon the level) expeditiously.

6. Based on the risk assessment, UCBs acting as sponsor banks may also consider implementing additional controls over and above the prescribed controls at transaction authorisation, transaction file upload, cross verification with its sub-members etc.

7. UCBs that are using dongle for digitally signing the transactions are advised to plug in the dongle only during the time of signing the transactions digitally and secure the PIN/ password to access the dongle. The dongle, otherwise, should be in safe custody of the owner of the digital signing certificate and not left unattended at the terminal/H2H client etc.

8. UCBs shall ensure to reconcile the transactions put through the sponsor bank **mandatorily on a daily basis and preferably more than once a day** to identify unauthorised transactions, if any and mitigate the risk.

9. IOCs in respect of above-mentioned incident are given below for securing the ecosystem:

Filename: music.exe

IP: 51(.)77(.)167(.)122

****