

-----Original Message-----

From: CSITE <csite@rbi.org.in>

Sent: 18 May 2020 19:33

Subject: [Spam] ALERT: "SPOOFED EMAIL CONTAINING Suspicious Attachment :New Neft/Rtgs Procedure for Covid-19"

Importance: High

[External Email] You have received this email from an external source. Please exercise extreme caution while opening any attachment or link given in this e-mail.

Sir/ Madam,

A spoofed email from nefthelpdesknc@rbi[.]org [SEE ".IN" MISSING] is being getting circulated apparently containing malicious attachment. The email received (without the attachment is given below). Preliminary analysis of the attachment is as follows:

- * Suspicious Mail originated from nefthelpdesknc@rbi[.]org
- * File attachment: RESERVE BANK MANDATE.mht
- * Contains Malware : Heur.AdvMLB
- * Getting downloaded from site: [https://harryhiggins[.]com/]https://harryhiggins[.]com/
- * Hash value of malware: E966FEBB60685769C6914FB2B18D750FCA278E6FA57852524CD9CBEC2FA6FFE

Supervised Entities are advised to exercise caution while handling any email with COVID-19 related subject lines, attachments, or hyperlinks in emails, content related to or payment ecosystem, etc. Necessary instructions as per our earlier advisories, circulars and alerts shall be followed to secure from phishing/spear phishing types of attacks.

*****SPOOFED EMAIL BEGIN*****

----- Original Message -----

From: RBI <nefthelpdesknc@rbi.org>

Date: May 18, 2020 10:51:59 AM

Subject: New Neft/Rtgs Procedure for Covid-19

To: undisclosed-recipients; ;

Dear Sir/Madam,

Please find enclosed a file containing new banking mandate for Outward Neft/Rtgs.

Shri P. Vijaya Kumar
Chief General Manager
Department of Corporate Services
Reserve Bank of India
7th Floor, Main Building,
Shahid Bhagat Singh Road,
Fort, Mumbai-400 071.

*****SPOOFED EMAIL END*****

Regards,

Sarath CK
AGM
Cyber Security& IT Risk (CSITE) Group
Department of Supervision, CO
Reserve Bank of India

Caution: The Reserve Bank of India never sends mails, SMSs or makes calls asking for personal information such as your bank account details, passwords, etc. It never keeps or offers funds to anyone. Please do not respond in any manner to such offers, however official or attractive they may look.

Notice: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, any dissemination, use, review, distribution, printing or copying of the information contained in this e-mail message and/or attachments to it are strictly prohibited. If you have received this email by error, please notify us by return e-mail or telephone and immediately and permanently delete the message and any attachments. The recipient should check this email and any attachments for the presence of viruses. The Reserve Bank of India accepts no liability for any damage caused by any virus transmitted by this email.