

**ब्रिज एण्ड रूफ कंपनी इंडिया लिमिटेड**  
**BRIDGE AND ROOF COMPANY (INDIA) LIMITED**  
(भारत सरकार का एक उद्यम / A Government of India Enterprise)  
2/1, रसलस्ट्रीट कंकड़िया सेंटर, / Russel Street "Kankaria Centre"  
कोलकता / Kolkata – 700071

**ज्ञाप/MEMO**

प्रेषक/From :	General Manager (IT) Kolkata	सेवा में/To :	All Employee/ Offices
संदर्भ/Ref. :	BNR/IT/IS/MAIL/199	दिनांक/Date :	02-09-2024

**Sub: Advisory for Phishing mail.**

As per e-mail received from MHI (IT Cell) vide OM No. 11-B-12025/8(ii)/2024-IT Cell (28267) Dated 27<sup>th</sup> August, 2024 on the subject mentioned above, attaching herewith the e-mail communication where Cyber Security Group of NIC has shared an advisory of phishing mails.

In our ongoing efforts to ensure the security of our organization's digital environment, we would like to bring your attention to the growing threat of phishing emails. Phishing is a type of cyber-attack where malicious individuals attempt to deceive individuals/Organization into providing sensitive information, such as passwords or financial details, by pretending to be a legitimate entity.

Recently, it has been observed that email IDs have been receiving phishing mail from email ID "[deepakbhojwani@outlook.in](mailto:deepakbhojwani@outlook.in)".

In any case, if any of the recipients have clicked on the phishing link/downloaded attachment, we would request you to kindly advise the end user to take the following steps at their end.

1. The user needs to scan the systems from which the email id is accessed with an updated antivirus. If any malware is found, the devices have to be thoroughly cleansed, preferably by hard formatting.
2. Kindly ask user to change the password from a computer which is Virus/malware free.
3. Ask user to Get the machine scanned with latest patches of Anti-Virus on which users are accessing their mail and also get the OS updated with the latest patches.
4. Check whether any key logger is present in the system, if found must be removed by using anti-malware/anti-spyware tool available or by hard formatting of the system. Users are advised to leverage the free malware removal tools made available by CERT-In at [www.csk.gov.in](http://www.csk.gov.in)
5. The users need to ensure that the "REMEMBER PASSWORD" option isn't configured anywhere i.e. in the browser or in POP client i.e. outlook, thunder bird etc."

You are also requested to please do not share/ surrender any kind of personal information to the fraudsters. However, if you are used to getting any phishing mail or doubtful URL, please inform first to the undersigned only to take immediate action against such Cyber Crime.

You are once again requested to please use only the company email ID i.e. belong to bridgeroof.co.in domain for all official communications. Thank you for your attention to this important matter. Let's work together to keep our organization's information and systems secure.

Regards,



(Barun Kanti Das)

**GENERAL MANAGER (IT)**

CC: CMD

: D(F)

: D(PM)

: CVO



- For kind information please.

Encl:

1. Office memorandum note of MHI (IT Cell) vide OM No. 11-B-12025/8(ii)/2024-IT Cell (28267) Dated 27<sup>th</sup> August, 2024.

**By e-Mail / IMMEDIATE**

**No.11-B- 12025/8(ii)/2024-IT CELL (28267)**  
**Government of India**  
**(Bharat Sarkar)**  
**Ministry of Heavy Industries**  
**(Bhari Udyog Mantralay)**  
**(IT Cell)**

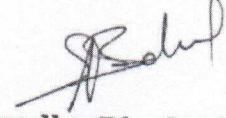
**Udyog Bhawan, New Delhi**  
**Dated : 27<sup>th</sup> August, 2024**

**OFFICE MEMORANDUM**

**Subject: Advisory of phishing mails - regarding.**

The undersigned is directed to refer to email dated 20.08.2024 from Deputy CISO of this Ministry on the subject mentioned above for information and immediate appropriate action.

Encl:- As above.



**(Anuradha Bhadwal)**  
**Under Secretary to the Govt. of India**  
**Tel. No.23063512**

**To**

- 1. All Divisions of MHI.**
- 2. PE-I to PE-XII/TSW Section (in r/o CPSEs) and HE&MT and AEI Divisions (in r/o ABs).**
- 3. e-Office Notice Board.**

---

**Fwd: Reg advisory of phishing mails**

---

**From :** Sandeep Kaviraj <sandeep.kaviraj@nic.in>  
**Subject :** Fwd: Reg advisory of phishing mails  
**To :** Sandeep Kaviraj <it-ic-cell-mhi@gov.in>

Tue, Aug 20, 2024 05:39 PM

---

**From:** "Amit Saxena" <amit.saxena@nic.in>

**To:** "Abhinav Gupta" <g.abhinav@gov.in>, "Rajeev Ranjan" <ranjan.rajeev75@gov.in>, "kamalkumarAssistantSectionOfficer" <kamal.koli@nic.in>, "Dhayalan Karuppannan" <dayal.spk@gov.in>, "Sandeep Kaviraj" <sandeep.kaviraj@nic.in>

**Cc:** "Rahul Kapoor" <jsupa-mohua@gov.in>, "P Palanivel" <ppalanivel.iss@gov.in>, "Dr Renuka Mishra" <ea.dhi@nic.in>, "amit saxena" <dciso-cstmhua@nic.in>, "amit saxena" <dciso-cstmhi@nic.in>, "amit saxena" <dciso-cstmmsme@nic.in>, "Pradeep Kumar Gupta" <pkgupta@nic.in>, "M. Ezhil Arasu" <arasu@nic.in>, "Vinay Agarwal" <vinay.agarwal@nic.in>, "Manoj Kumar Gupta" <mkg@nic.in>, "Rahul Meena" <rahul.meena17@nic.in>

**Sent:** Tuesday, August 20, 2024 1:59:12 PM

**Subject:** Reg advisory of phishing mails

Sir

You are requested to circulate the alert among the officials of ministry/department.

"It is observed that email IDs have been receiving phishing mail from email ID "[deepakbhajwani@outlook.in](mailto:deepakbhajwani@outlook.in)".

In any case, if any of the recipients have clicked on the phishing link/downloaded attachment, we would request you to kindly advise the end user to take the following steps at their end.

- 1) The user needs to scan the systems from which the email id is accessed with an updated antivirus. If any malware is found, the devices have to be thoroughly cleansed, preferably by hard formatting.
- 2) Kindly ask user to change the password from a computer which is Virus/malware free.
- 3) Ask user to Get the machine scanned with latest patches of Anti Virus on which users are accessing their mail and also get the OS updated with the latest patches.
- 4) Check whether any key logger is present in the system, if found must be removed by using anti-malware/anti-spyware tool available or by hard formatting of the system. Users are advised to leverage the free malware removal tools made available by CERT-In at [www.csk.gov.in](http://www.csk.gov.in)

5) The users need to ensure that the "REMEMBER PASSWORD" option isn't configured anywhere i.e in the browser or in POP client i.e outlook, thunder bird etc."

With Regards

(AMIT SAXENA)  
DyCISO MHI,MSME,MoHUA

**ब्रिज एण्ड रूफ कंपनी इंडिया लिमिटेड**  
**BRIDGE AND ROOF COMPANY (INDIA) LIMITED**

(भारत सरकार का एक उद्यम /A Government of India Enterprise)

2/1, रसलस्ट्रीट कंकड़िया सेंटर, / Russel Street "Kankaria Centre"

कोलकता / Kolkata – 700071

**ज्ञाप/MEMO**

प्रेषक/From :	General Manager (IT) Kolkata	सेवा में/To :	All Employee/ Offices
संदर्भ/Ref. :	BNR/IT/IS/DOMAIN/183	दिनांक/Date :	12-07-2024

**Sub: Company under threat of mimicking of Phishing Domain.**

Please refer our memo **BNR/IT/IS/DOMAIN/182** dated July 10<sup>th</sup>, 2024 on the subject of **mimicking of Phishing Domain**, where in, we had provided guidelines as how to recognize such phishing e-mails/ domains etc. and also alerted with sufficient points to do the needful action of receiving such phishing e-mails from phishing domain.

Recently, we have received one such communication from our Commercial department. Commercial Department against their **Tender no: BANDR/HO/71144/CIVIL-2/NRL/SILIGURI/NIT/04/R Dated 21/02/2024** asked for Earnest Money Deposit Security with a face value of Rs.20,35,000/- (Rupees Twenty Lakhs Thirty-Five Thousand only) in form of Bank Guarantee (BG) from respective bidders. Accordingly, the bidder submitted their bid along with BG documents. As a normal practice, Commercial Department sent a request e-mail on dated June 18<sup>th</sup>, 2024 with BG details to DCB bank to confirm if the BG is issued by them or not for the following bidder along with a copy to their Corporate office also.

Name of the Bidder	M/s. DEEP NIRMAN, OLD HASIMARA, PO- HASIMARA-735215, DIST- ALIPURDUAR, WEST BENGAL, PH- 9434740384, EMAIL- <a href="mailto:deepnirman3@gmail.com">deepnirman3@gmail.com</a> , <a href="mailto:rdpandey2@gmail.com">rdpandey2@gmail.com</a>
--------------------	--

Interestingly, they have noticed that they are getting such response from the concerned local bank which is a bit suspicious. Due to finalization of the tender on urgency, they repeatedly chased with mail documents to their Corporate Office and, finally the Corporate office of DCB bank confirmed the following:

**“We refer to your appended e-mail dated 06.07.2024 on the captioned subject and would like to inform that the email received by you from the email ID- [bm.shakespearesarani@dcbbank.com](mailto:bm.shakespearesarani@dcbbank.com) on 04.07.2024 is not genuine and not from our domain ID. The alphabet ‘a’ is inverted in it. We once again confirm that the attached guarantee dated 04.06.2024 for Rs. 20,35,000/- is not issued by DCB Bank Ltd, Shakespeare Sarani Branch and M/s Deep Nirman is not banking with DCB Bank Limited.”**

So, company is now under threat of such **mimicking of phishing domain**. Here, the bidder **M/s. Deep Nirman** used mimicking of **DCB bank domain** as follows:

Original Domain of DCB bank	<b>bm.shakespearesarani@dcbbank.com</b>
Mimicking Domain of DCB bank	<b>bm.shakespearesarani@dcbbank.com</b>

→ **Fraud**

Also, they did mimicking other different e-mails of DCB bank officials for communications as reflected are : Kolkata.tfu@dcbbank.com, anita.thakkar@dcbbank.com, tfmis@dcbbank.com, mandarn@dcbbank.com, yasiflakhani@dcbbank.com, where it has been noticed that M/s. Deep Nirman is a fraudster and as per guidelines of CERT-In, we had already raised complaint to the following authorities as per their directive for needful actions against them.

- IT Cell, MHI, Government of India
- To the authority of CERT-In, Government of India
- To the authority of National Critical Information Infrastructure Protection Centre

All are therefore requested to please be alert enough on **Phishing Domain** on day to day official activities & while using internet services and do needful for effective sanitize of your system and mitigate the potential risks associated with Phishing URLs/ Phishing Domains'.

Regards,



(Barun Kanti Das)

**GENERAL MANAGER (IT)**

CC: CMD  
: D(F)  
: D(PM)  
: CVO

- For kind information please.

Encl: 1. Memo **BNR/IT/IS/DOMAIN/182** dated July 10<sup>th</sup>, 2024.

**ब्रिज एण्ड रूफ कंपनी इंडिया लिमिटेड**  
**BRIDGE AND ROOF COMPANY (INDIA) LIMITED**

(भारत सरकार का एक उद्यम /A Government of India Enterprise)

2/1, रसलस्ट्रीट कंकड़िया सेंटर, / Russel Street "Kankaria Centre"

कोलकता / Kolkata – 700071

**ज्ञाप/MEMO**

प्रेषक/From :	General Manager (IT) Kolkata	सेवा में/To :	All Employee/ Offices
संदर्भ/Ref. :	BNR/IT/IS/DOMAIN/182	दिनांक/Date :	10-07-2024

**Sub: Advisory for Phishing Domain mimicking Department of Defence.**

As per e-mail received from MHI (IT Cell) vide OM No. 11-B-12025/4/2023-IT Cell (26857) Dated 21<sup>st</sup> June, 2024 on the subject mentioned above, attaching herewith the document where in Cyber Security Group of NIC has shared an advisory on "Phishing Domain Mimicking Department of Defence".

An Internet **Domain** (Ex: bridgeroof.in, nic.in, gov.in etc) is an administrative structure for organizing, delivering and accessing services on the internet where **Phishing** is a type of fraud in which an attacker impersonates a reputable company or person in order to get sensitive information such as login credentials or account information etc. via e-mail or other channel.

Recently, it has been observed that phishing is found popular among cyber attackers & mimicking the domain of reputed organizations. It is therefore requested to all that while on day to day official activity in using internet services, please be alerted enough specially on domain aspect maintaining following points:

1. In case such a phishing mail is received, do not enter your email Login Credentials when redirected login prompt appears.
2. Delete these phishing emails from your inbox.
3. In case, you have already clicked the phishing URL
  - a) Take your device offline – Disable your internet connection.
  - b) Change your password - You need to change the passwords for any accounts that might have been hit in the cyber attack.
  - c) Change your passwords from a different device to ensure that the hacker can't access your new information.
  - d) Turn on multi-factor authentication for the account that might have been attacked.
  - e) Back up your files - To protect your data from the phishing attack, back up your files to an external hard drive or USB.
  - f) Scan your device with anti-virus software.
  - g) Update your Operating System, Web Browsers, and other Software with the latest security patches.

**ब्रिज एण्ड रूफ कंपनी इंडिया लिमिटेड**  
**BRIDGE AND ROOF COMPANY (INDIA) LIMITED**  
(भारत सरकार का एक उद्यम / A Government of India Enterprise)  
2/1, रसलस्ट्रीट कंकड़िया सेंटर, / Russel Street "Kankaria Centre"  
कोलकता / Kolkata – 700071

- h) Report suspicious message to your email service provider or undersigned mail address
- i) Avoid sharing personal information.

By following above steps, you can effectively sanitize your system and mitigate the potential risks associated with clicking on a phishing URL.

**Some ways to recognize a phishing email are given below:**

- a. Be suspicious of emails that claim you must click, call, or open an attachment immediately or urgently.
- b. If a mail received from unknown source, this may be a source of phishing.
- c. If an email message has obvious spelling or grammatical errors, it might be a scam. E.g. nlc.in where the first "i" has been replaced by "l", or gov.in, where the "o" has been replaced by a "0" (zero).
- d. Images of text used in place of text (in messages or on linked web pages) may be scam.
- e. Be cautious of links shortened by using Bit.Ly or other link shortening techniques.
- f. Be cautious on domain alphabet if any inverted one is used or not (Ex. b instead of b)

You are also requested to please do not share/ surrender any kind of personal information to the fraudsters. However if you are used to getting any phishing domain or doubtful URL, please inform first to the undersigned only to take immediate action against such Cyber Crime.

You are once again requested to please use only the company email ID i.e. belong to bridgeroof.co.in domain for all official communications and while accessing internet service, be mindful on proper domain of other also.

Regards,



(Barun Kanti Das)

**GENERAL MANAGER (IT)**

CC: CMD

: D(F)

: D(PM)

: CVO

- For kind information please.

- Encl: 1. E-mail communication from MHI, GOI  
2. Advisory & Resource Facilitation Note from NIC GOI.