INDIAN COUNCIL OF SOCIAL SCIENCE RESEARCH

(Computer Division)

No. F. ICSSR/CC/Security/2023-24/1

Dated: 10 May 2023

CIRCULAR

Subject: Phishing Awareness regarding emails sent in the Name of Highest Officials of ICSSR

We would like to bring to your attention a critical matter regarding the security of our organization's information and the potential risks associated with phishing emails. It has come to our notice that certain individuals are attempting to exploit our organization's credibility by sending fraudulent emails, falsely claiming to be from our highest-ranking officials.

Phishing is a malicious activity where scammers attempt to deceive recipients into revealing sensitive information, such as passwords, credit card numbers, or other personal details, by disguising themselves as trustworthy entities. These fraudulent emails often employ various tactics to manipulate recipients into taking actions that compromise the security of our organization's systems and data.

To combat this growing threat, we strongly urge all employees / members / beneficiaries to be vigilant and exercise caution when receiving emails, especially those appearing to be from top-level executives. It is essential to remember the following best practices:

- Verify the sender's email address: Carefully examine the email address of the sender. Phishing emails often use similar but slightly altered addresses that may not be immediately noticeable.
- Exercise caution with email content: Be wary of emails requesting sensitive information or urgent actions, especially if they seem unusual or out of character for the sender. Take the time to review such requests and verify their legitimacy before responding or clicking any links.
- Look for signs of phishing: Pay attention to grammatical errors, spelling mistakes, or generic salutations within the email. These can be indications of a phishing attempt.
- Avoid clicking on suspicious links or downloading attachments: Hover your mouse over links to reveal the actual URL before clicking. Ensure that the URL matches the expected destination. Additionally, refrain from downloading attachments from unknown or suspicious sources.

- Educate yourself: Familiarize yourself with the common characteristics and techniques used in phishing attacks. By staying informed, you can better protect yourself and the organization from potential threats.

By remaining alert, cautious, and well-informed, we can significantly reduce the risks associated with phishing attacks.

Thank you for your attention to this matter.

(Pushkar Pathak)
Systems Analyst

To:
All the employees of ICSSR
through their Divisional Heads
Website for uploading

Copy also to:
1. PS to Chairman
2. PS to Member Secretary