COMPUTER FACILITY

ALL INDIA INSTITUTE OF MEDICAL SCIENCES

Date: 24.05.2021

SUBJECT: DO'S AND DON'TS FOR PREVENTION OF PHISHING ATTACKS AT AIIMS, NEW DELHI

It has been observed that there has been an increase in the Email spoofing/Phishing attacks at AIIMS, New Delhi. Therefore, it is important to be cautious and understand Email Spoofing and Phishing:

Email spoofing is the creation of email messages with a forged sender address to trick users into thinking a message came from a legitimate person or entity they either know or can trust, which most users take at face value. The purpose of email spoofing is spam and **phishing attacks** to breach security of systems or to steal sensitive information of users.

Phishing attack is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

How does a spoofed email message look like?

In the above email, the impostor is posing as Director, AIIMS with the forged email ID *managingdirectormail555@gmail.com* and is trying to deceive the receiver of the email (*picf@aiims.edu*) into thinking that the above message came from Director, AIIMS.

In the recent past, there have been multiple instances of such spoofed email messages at AIIMS, New Delhi. **It is the user's responsibility to check the authenticity of the sender's email ID & not to respond to the emails that look suspicious or that asks for your personal information like credit card/debit card/aadhar card/ bank details etc.**

The following Do's and Don'ts may be useful in the prevention of such attacks:

Do's

- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.
- Look for the sender email ID before you enter/give away any personal information.
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do confirm if it is legitimate or not.
- Do use a separate email accounts for things like online shopping, personal etc.

Don'ts

- Don't reply to an e-mail or pop-up message that asks for personal or financial information.
- Don't email personal or financial information i.e. credit card or other sensitive information via. email.
- Don't open e-mail that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try another means.
- Don't open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.
- Don't use AIIMS email address for personal things.
- Don't open any spam email.

If you are a recipient of spoofed email(s) as elaborated on pre-page, it is to inform you that Computer Facility, AIIMS facilitates reporting of such matters to CERT-In (nodal agency of the Govt. of India to deal with cyber security threats) for further necessary action. In such cases, you may contact Mr.Amit Bhati, Sr. Programmer, Computer Facility (nodal officer for IT Security) on 011-26593570 or 7428377001.

However, if your personal information has been compromised or if you are a victim of fraudulent financial transaction as a result of phishing attack, you are also advised to report such matters to Security Department, AIIMS as legal action such as lodging FIR with the law enforcement agency etc. (if required) needs to be taken either by the Security Department, AIIMS or the concerned person himself/herself.

24/05/21.

**Professor Incharge,
Computer Facility**

To,

- Mrs. Ankita Saini, Programmer, Computer Facility – to upload the Do's and Don'ts in Notice Section on AIIMS website.

CC:

- Director, AIIMS, New Delhi – For information
- DDA, AIIMS – For information