कम्प्यूटर सविधा,
एम्स, नई दिल्ली

दिनांक:

विषय:- फर्जी ईमेल एवं फ़िशिंग अटैक के संबंध में जागरूकता संबंधी।

कम्प्यूटर सुविधा, एम्स के संज्ञान में यह आया है कि फर्जी ईमेल द्वारा एम्स, नई दिल्ली के कुछ स्टाफ-सदस्यों एवं संकाय-सदस्यों को निशाना बनाया गया है। यह ईमेल वैध सरकारी संगठनों (जैसे:- दिल्ली पुलिस, गृह मंत्रालय आदि) सहित एम्स के संकाय-सदस्यों/स्टाफ-सदस्यों से प्राप्त हुए प्रतीत होते हैं। रोगियों को भी एम्स के संकाय-सदस्यों की ओर से अपॉइटमेंट/पुष्टि/धन आदि हेतु ईमेल प्राप्त हो रहे हैं। अत: यह सूचित किया जाता हैं कि इस प्रकार के फर्जी ईमेल वास्तव में विद्वेषपूर्ण फिशिंग योजना का हिस्सा होते हैं। इन ईमेलों को भेजने वाले फर्जी व्यक्ति संवेदनशील जानकारी को चुराने, वित्तीय धोखाधड़ी करने या आपकी वैयक्तिक सुरक्षा में सेंध लगाने का प्रयास कर सकते हैं।

इसे ध्यान में रखते हुए, सभी से अत्यधिक सतर्कता एवं निम्नलिखित सावधानियों का पालन करने का आग्रह किया जाता है:-

1. अपरिचित स्रोतों से आने वाले ईमेल से सावधान रहें।

- प्रेषक के ईमेल पते को ध्यानपूर्वक सत्यापित करें। यदि प्रेषक किसी मान्यता प्राप्त सरकारी एजेंसी या एम्स के संकाय-सदस्य/स्टाफ-सदस्य से प्राप्त प्रतीत होता है तो ईमेल पते में कुछ बदलाव दिखाई दे सकते हैं (उदाहरण:- आधिकारिक पते जैसे अक्षरों का इस्तेमाल करना)
- ईमेल में वर्तनी की त्रुटियों या फॉर्मेटिंग संबंधी समस्याओं की जांच करें। आमतौर पर आधिकारिक संप्रेषण अच्छी प्रकार से लिखे जाते हैं एवं उनमें इस प्रकार की त्रुटि नहीं होती है।
- किसी भी प्रकार के वित्तीय लेनदेन से पहले संबंधित व्यक्ति से प्रत्यक्ष रूप से पुष्टि करें।

2. संदिग्ध लिंक या अटैचमैंट पर क्लिक न करें

- अज्ञात या संदिग्ध स्रोतों से आने वाले लिकं पर कभी भी क्लिक न करें या अटैचमैंट को न खोलें, खासतौर पर यदि ईमेल में तत्काल कार्रवाई की मांग की गई हो या धमकी (जैसे:- जुर्माना, गिरफ्तारी आदि) दी गई हो।
- यदि कोई संदेह हो, तो आधिकारिक स्रोतों से सत्यापित संपर्क विवरण का प्रयोग कर सीधे कथित प्रेषक से संपर्क करें।

3. व्यक्तिगत जानकारी के अनुरोधों से सावधान रहें

- कभी भी ईमेल पर गोपनीय अथवा व्यक्तिगत जानकारी जैसे पासवार्ड, बैंक खाता विवरण या सोशल सिक्योरटी नम्बर साझा न करें, फिर चाहे ईमेल किसी आधिकारिक स्रोत से क्यों न प्राप्त हुआ हो।
- यदि ईमेल में किसी सरकारी निकाय अथवा विभाग से संबंधित होने का दावा किया जाता है तो उसे उनकी सत्यापित वेबसाइट पर सूचीबद्ध आधिकारिक सम्पर्क नंबर या ईमेल पते से क्रॉस-चेक करें।

4. संदिग्ध ईमेल की तुरंत रिपोर्ट करें

- यदि आपको कोई ऐसा संदिग्ध ईमेल प्राप्त होता है जिसके संबंध में आपको लगता है कि वह फिशिंग का प्रयास हो सकता है तो उसका जवाब न दें या उसे किसी को अग्रेषित न करें।
- यदि आपको लगता है कि आपकी संवेदनशील जानकारी से छेड़छाड़ हुई है तो कृपया अपने ईमेल का पासवार्ड तुरंत बदलें।
- आप इस प्रकार के संदिग्ध ईमेल की शिकायत https://cybercrime.gov.in पर कर सकते हैं अथवा साइबर अपराध की हेल्पलाइन नंबर 1930 पर सम्पर्क कर सकते हैं।

5. मल्टी-फैक्टर ओथेंटिकेशन (एमएफए) का इस्तेमाल करें

- सभी संकाय-सदस्यों एवं स्टाफ को विशेष रूप से सलाह दी जाती है कि आप सभी आधिकारिक संप्रेषण (आंतरिक एवं बाह्य) हेतु अपनी आधिकारिक ईमेल आईडी (aiims.gov.in) का इस्तेमाल करें। अपने व्यक्तिगत ईमेल अकांउट हेतु आप अनधिकृत एक्सेस के विरूद्ध अतिरिक्त सुरक्षा बढ़ाने के लिए मल्टी-फैक्टर ओथेंटिकेशन का इस्तेमाल कर सकते हैं।

6. सोशल इंजीनियरिंग युक्तियों से सावधान रहें

- ये फर्जी व्यक्ति आपके परिचित नामों अथवा सहकर्मियों की आवाज की नकल करके आपका विश्वास जीतने का प्रयास कर सकते हैं। सहायता अथवा सूचना के लिए प्राप्त अनपेक्षित अनुरोधों से हमेशा सावधान रहें विशेषत: जब वे तत्काल या गुप्त मामलों से संबंधित हो।

7. अपने व्यक्तिगत एवं व्यावसायिक डेटा की सुरक्षा करें

- अपने डिवाइस एवं खातों की सुरक्षा के प्रति सचेत रहें तथा सार्वजनिक अथवा असुरक्षित नेटवर्क पर संवेदनशील कार्य-संबंधी सामग्री को एक्सेस करने से बचें।

प्रभारी-आचार्य
कम्प्यूटर सुविधा

प्रतिलिपि:

1. निदेशक, एम्स
2. संकायाध्यक्ष (शैक्षिक, अनुसंधान, परीक्षा)
3. अपर निदेशक (प्रशासन)
4. चिकित्सा अधीक्षक (एम्स)
5. सभी केंद्र प्रमुखगण/अध्यक्ष, एनसीआई, झज्जर
6. सभी विभागाध्यक्षगण
7. वरिष्ठ वित्त सलाहकार
8. श्री अमित भाटी, वरिष्ठ प्रोग्रामर, कम्प्यूटर सुविधा - इस सूचना को एम्स की वेबसाइट पर अपलोड करने तथा कंटेंट प्रोवाइडर के माध्यम से सभी संकाय-सदस्यों/स्टाफ-सदस्यों में परिचालित करने की व्यवस्था करें।

COMPUTER FACILITY,
AIIMS, New Delhi

Date: 30.12.2024

Subject: Awareness Regarding Fake Emails and Phishing Attacks

It has come to the attention of Computer Facility, AIIMS that some employees and faculty members of AIIMS, New Delhi, have been targeted by fraudulent emails. These emails appear to be from legitimate government organizations (such as Delhi Police, The Ministry of Home Affairs etc.) as well as AIIMS faculty members/staff. Patients are also getting emails on behalf of AIIMS faculty members for appointment/confirmation/money etc. It is to inform that such fraudulent emails are actually part of a malicious phishing scheme. The impersonators behind these emails may attempt to steal sensitive information, initiate financial fraud, or compromise your personal security.

In light of this, everyone is urged to exercise heightened vigilance and follow the below precautions:

1. Be Cautious with Emails from Unfamiliar Sources

- Verify the sender's email address carefully. Even if the sender appears to be from a recognized government agency or AIIMS faculty member/staff, the email address may be slightly altered (e.g., using characters that resemble official addresses).
- Check for spelling errors or formatting issues within the email body. Official communication is usually well-written and free of such mistakes.
- Confirm directly from the concerned person before any financial transaction.

2. Do Not Click on Suspicious Links or Attachments

- Never click on links or open attachments from unknown or suspicious sources, especially if the email demands urgent action or threatens consequences (e.g., fines, arrest, etc.).
- If in doubt, directly contact the supposed sender using verified contact details from official sources.

3. Beware of Requests for Personal Information

- Never share confidential or personal information such as passwords, bank account details, or social security numbers over email, even if the email seems to come from an official source.
- If an email claims to be from a government body or department, cross-check it with the official contact number or email address listed on their verified website.

4. Report Suspicious Emails Immediately

- If you receive a suspicious email that you believe may be part of a phishing attempt, do not respond or forward it to anyone.
- If you believe any sensitive information has been compromised, please take immediate steps to change your passwords.

- You may lodge complaints of such suspicious emails on https://cybercrime.gov.in or contact on cybercrime helpline no. 1930.

5. Enable Multi-Factor Authentication (MFA)

- It is strongly recommended that all faculty members and staff use their official email ID (aiims.gov.in) for all official communication (internal and external). For their personal email accounts, they may enable Multi-Factor Authentication to add an extra layer of protection against unauthorized access.

6. Be Aware of Social Engineering Tactics

- Impersonators may attempt to gain your trust by mimicking familiar names or office holders. Always be cautious of unsolicited requests for assistance or information, particularly when they involve urgent or secretive matters.

8. Protect Your Personal and Professional Data

- Be mindful of the security of your devices and accounts, and avoid accessing sensitive work-related content over public or unsecured networks.

Professor Incharge, CF

CC:

1. Director, AIIMS
2. Dean/s (Academic, Research, Examination)
3. Addl. Director (Administration)
4. Medical Superintendent (AIIMS)
5. Chief(s) of all Centers / Head, NCI, Jhajjar
6. Head(s) of all Departments
7. Sr. Financial Advisor
8. Mr. Amit Bhati, Sr. Programmer, CF- To arrange uploading of this advisory on AIIMS website and circulation to all faculty members/staff through content provider