Prof. M.N. Pursoqui Computer Centre
Aligarh Muslim University, Aligarh
Phone No. 0571-2700920 (Extn. 3850 & 3851)

R. No. 334 Hist.
Dated 16-5-17
Time

D.No. 512/CC

May 16, 2017

Office Memo

All Deans of Faculties/Dean Students Welfare
All Principals of Colleges
All Directors | Coordinators of Centre (through Coordinator-AMU Nodal Centre)
All Chairpersons of Department of Studies
All Concerned Heads of Offices / MICs / PRO
All Principals of Schools (through Director-DOSE)
All IT-Focal Points of AMU Campus | All Section-I/Cs-CC | Coordinator-IT-Helpdesk-CC

All University functionaries are requested to apprise all e-mail users of their respective department/office, to take necessary precautions to guard against attempt to phishing scams. Prescriptive guidance regarding the same is as follows:

Advisory for all E-mail Users (to guard against Phishing Attempts) at AMU

While checking incoming e-mails (be it institutional e-mail id of AMU or even personal e-mail id of users), all ICT-Users may sometimes be receiving fraudulent e-mails from cyber-criminals who often build a webpage or e-mail that mimics a trust worthy sender (like a department inside AMU like e-mail IDs appearing to be coming from VC/PVC/Registrar/FO/Deans/HoDs/Directors, or external entities like a bank or any GoI-dept.) and use it to deceive targeted users. Some of the targeted users end-up respooding to these requests that often ask them to "verify" or "update your account" or "failure to update your records will result in account suspension" etc.

Please remember that no credible organization to which you have provided your information will ever ask you to re-enter it, so do not fall for this trap. Mimicking of E-Mail Administrators , Network Administrator, Webmaster etc. are a common method of these cyber-criminals, by way of replicating the identity information in e-mails. Following precautions are strongly recommended for all the ICT-users of AMU Campus:

(1.) Be suspicious of any email with urgent requests asking you to fill a form or share personal financial information warning you of consequences if you do not respond within a fixed timeline. It could be a Phishing Attempt.

(2.) Whenever you receive any Phishing e-mail do not click on any embedded links and do not provide any information in response to such e-mails. Even if the email has official logos or text or even links to a legitimate website, it could easily be fraudulent.

(3.) Any email that asks for your personal or sensitive information should be seriously scoured and not trusted. Never give out your private/personal information, never send passwords, bank-account numbers etc. in e-mails to anyone.

(4.) Avoid filling out forms in email messages that ask for personal/financial information. Neither respond to it nor forward it to others.

(5.) Be wary of any unexpected attachments or links, even if it appears to be coming from people you know (listed on your contacts or saved in your address book).

(6.) In the event of any questions, comments or concerns, please connect with IT-Helpdesk through your respective IT-Focal Points who are in regular contact with concerned IT-Services teams of Computer Centre for prescriptive guidance on corrective and preventive measures, from time to time.

(7.) Above prescriptive guidance will be helpful for all ICT-Users of AMU Campus to be better prepared for preventing phishing scams.

16/05/17

Director

Copy to:

AR to VC's Secretariat | AR to PVC's Secretariat | PS to Registrar | PS to FO | PS to CoE | PS to Proctor |PS to DSW

circulate / Mr. Nadeem / Pass-ds.

Chairman
Department of History
A.M.U., Aligarh