



MEMORANDUM

Ref : JL/PA/PA/CO/001/19
Date : 24 October 2019
To : All students, staff and business associates
Re : Spam / Phishing emails

Dear all

It is unfortunate that TMC has recently become a victim of a Business Email Compromise (BEC) scam. A few of TMC’s email accounts have been affected. We have reported this to the Singapore Computer Emergency Response Team (SingCERT) and actions have been taken to scan the computers to ensure that there is no malware in our system.

The scammers use spoof TMC email accounts to send out mass emails with malicious attachment. The email content may look like a legitimate ongoing discussion. An example is shown below.

From: Student Services studentservices@tmc.edu.sg <ventas@sevendeya.net>
To: student@gmail.com
Attachment: Message.doc

Hi

Please find enclosed notice.

Kindest Regards

Do not open the attachment

Scammer’s email address, pretending to be StudentServices@tmc.edu.sg

Please be vigilant by taking the following steps to protect your computers:

- Always check the email header to ensure that the email comes from a legitimate source
- Do not open any files or links in any suspicious email
- Delete the email if it is a spam
- Install anti-virus software

If you are unsure whether an email from TMC is a spam email, you may contact your course administrator (for students) or info@tmc.edu.sg (for others) for assistance.

Regards

John Lee

John Lee
CEO
TMC Academy