OFFICE OF INFORMATION TECHNOLOGY

IT Alert!

Ransomware Alert

May 14,2017

Email Helpdesk

Dear AUB Users,
Following up on our previous Alert,experts are predicting that more ransomware cases may come to light on Monday, possibly on "a significant scale"

Despite the collective and collaborative efforts that the IT department is taking to secure our servers, networks and machines, the ransomware attacks still pose serious threat to all individuals.
Practice has shown that 100% security is impossible and that security is everyone's responsibility.
This is a reminder to pay extra attention and follow below steps:

- **Do not click on any links from suspicious emails.**
- **Do not open email from people you do not recognize – even if the emails look official**
- **Always double check the "from" field to make sure that the email is legitimate.**
- **Do not download or open attachments from suspicious emails (ending in extensions such as .SCR, .CAB, .EXE)**
- **Do not forward such emails to anyone**
- **Do not download or install software from suspicious sources**
- **Delete suspicious emails from suspicious sources**
- **Try to maintain continuous and regular data backups.**

Directly contact Helpdesk if you have any questions or notice anything suspicious on your machine.

Thank you,
Dr. Yousif Asfour
Chief Information Officer