Information Technology
Office of the CIO

AUB
American University of Beirut
الجامعة الأميركية في بيروت

March 24, 2016

Dear AUBnet Users,

Over the past few days, we have seen an increase in the number of “ransomware” attacks on the AUB community. The ransomware is typically sent as an attachment to emails or downloaded from unscrupulous websites. The ransomware encrypts all your computer data and the damage from these threats is often irreversible.

Despite our efforts in capturing these emails before they get to you, the attackers are continuously changing their techniques, and some emails will inadvertently get through .

To ensure your and AUB’s data safety, please pay extra attention to all emails you get, and make sure you follow these simple guidelines:

- Double check the “From” field on all emails you get before you open them.
- Do not open emails from people you do not recognize – even if the emails look official
- Do not download or open attachments from suspicious emails, or from people you did not expect attachments from.
- Do not click on any links in suspicious emails
- Do not forward such emails to anyone
- Do not download or install software from suspicious sites
- Delete suspicious emails from suspicious sources
- Make sure to regularly back up your critical data on a separate physical device

If in doubt, contact the helpdesk before opening the email or attachment

Should you have any concerns, please contact the IT Helpdesk (it.helpdesk@aub.edu.lb ).

Best regards,
Dr. Yousif Asfour
Chief Information Officer