What is a Ransomware?

Ransomware is a serious security threat that has data-kidnapping capabilities. It limits access to files or system functions, or even renders systems totally useless. It then forces victims to pay a ransom to regain access to their files/systems. Ransomware are lately hitting MacOS in addition to Windows and Linux Machines.

How Serious? It is Real !! It is Close.

- 6 Mar 2016 Apple Macs hit by Ransomware 'for first time' – COMPUTERWORLD
- 26 Feb 2016 German Hospitals Hit with Ransomware – SC Magazine
- 6 Nov 2015 Ransomware Targets Linux Web Servers – ARSTECHNICA

How is AUB IT protecting you?

- Anti-Virus: Anti-virus is part of AUB standard image.
- Web-Filter: Basic filtering for most known malicious websites
- Email-Filtering: Basic filtering for most known malicious email content
- Patch Management: Patches are managed centrally and released on weekly basis (For Windows Machine only)
- Backup: Regular backup of the main enterprise solutions. End users’ X: drive is also subject to backup.

How Can you Protect Yourself? (Backup – Update – Verify – Notify)

You are the last and most important line of defense despite the best practice security measures put in place by IT.

- Protect yourself by following these four steps:
  - Backup your files regularly. Keep the backup copy separate from your machine.
  - Update your software regularly to protect yourself against any malware.
  - Verify the data source and be vigilant about suspicious-looking emails you receive, especially if they contain links or attachments.
  - Notify the IT Helpdesk if you suspect you have fallen victim of a malware by clicking a link or opening an attachment.

Contact IT Helpdesk

For More Details Contact the IT Helpdesk:

Email: IT.HELPDESK@AUB.EDU.LB Phone: 01350000 Ext: 2260
Or Visit us at : http://www.aub.edu.lb/it/Pages/index.aspx