Email Security Best Practices

E-mail - so simple, so important Security

Email messages containing Spam, Phishing or those containing viruses as hoaxes are becoming more and more challenging to identify. Spammers and phishers are getting better everyday at making these messages look legitimate. However, these messages often fail on a number of counts. They usually contain bad spelling and/or grammatical mistakes. Also, some such emails ask for your personal information, namely username/password. You are of course strongly advised against replying to such emails. You should also inform IT Help Desk (helpdesk@uaeu.ac.ae).

Recognize Scam

Scam tactics are constantly changing and becoming increasingly sophisticated. If an email looks genuine, be careful and look for these warning flags

- The message is unsolicited and asks the user to update, confirm personal information.
- The message is labelled as urgent.
- The message has an unusual source address or and unusual reply-to address instead of "@uaeu.ac.ae" address.
- The web address does not have 's' after http://, indicating it is not a secure site.
- Opened-link does not match the given link in the email.

Phishing by Numbers

91% of cyber-attacks begin with spear phishing email.

94% of spear phishing emails use malicious file attachments.

Handling email Attachments

Be careful of all attachments and links:

- The most dangerous ways malware can be spread is via attachments and harmful links (Any attachment, especially .exe). Avoid clicking on links / attachments in unsolicited emails.
- Never open email attachments or links you don't recognize.
- Never respond to spam/phishing emails.
- Don't provide sensitive or personal information over email. Use email Encryption New Service (ask Help Desk for email Encryption), when sharing personal or confidential information.