

From: UTech Security

RE: UTech Security Awareness Bulletin - **How to Handle Suspicious Email**

There are good reasons to be suspicious of email. Some email messages could be phishing scams or carry viruses. Phishing is the act of sending an email to a user falsely claiming to be another trusted user or company in an attempt to steal their credentials.

Follow these guidelines to help protect yourself when suspicious email shows up in your Inbox:

1) Approach links in email messages with caution - Links in email messages can often take you to fake sites that encourage you to transmit personal or financial information to scammers. Some email messages contain links that download and install viruses when clicked.

Before you click a link, make sure to read the target address. If the message appears to come from your bank, but the target address isn't your bank, do not click the link.

2) Approach attachments in email messages with caution - Attachments might be viruses or spyware that download to your machine when you open the file. If you don't know who the attachment is from, or if you weren't expecting it, do not open the file.

3) Don't trust the sender information in email messages - Even if the message appears to come from a sender that you know and trust, use the same precautions that you would with any other message. Some mass emailing viruses infect computers and spread by sending to the infected person's contact list.

4) Don't trust offers that seem too good to be true.

5) Use up-to-date anti-virus software - Anti-virus software recognizes most known viruses and protects your computer against them, so you may be able to detect and remove the virus before it can do any damage.

6) Keep your computer current with the latest operating system and web browser updates and patches.