UTech Security Awareness Bulletin – Avoid Being a Victim of a Phishing Scam

Phishing is the act of sending an e-mail to a user falsely claiming to be another trusted user or company in an attempt to steal their credentials. The e-mail can contain a link to a fake website that asks the user to enter personal information such as username, password, credit card number, etc. There are several signs you should look for to identify a phishing e-mail:

1. Any e-mail asking for your name, birth date, social security number, e-mail username, e-mail password, or any other type of personal information, no matter who the e-mail appears to be from, is almost certainly a scam. California University of Pennsylvania and most other businesses do not send unsolicited e-mail requesting personal or financial information.
2. E-mails that are poorly worded, have typos, or have phrases such as "this is not a joke" or "forward this message to your friends" are generally scam e-mails.
3. Phishing mail often includes official-looking logos and other identifying information taken directly from legitimate websites, and it may include convincing details about your personal information that scammers found on your social networking pages.
4. A few phrases to look for if you think an e-mail message is a phishing scam are:
   1. "Verify your account."
   2. "If you don't respond within 48 hours, your account will be closed."
   3. "You have won the lottery."

How to avoid being a victim:

1. Verify the URL (web address) of a website before clicking on a link. Malicious websites may look identical to a legitimate site, but the URL may use a variation of spelling or a different name.
2. Don't send sensitive information over the Internet before checking a website's security.
3. Do not reveal personal or financial information, and do not respond to e-mail solicitations for this information. This includes following links sent in e-mail.
4. Never respond to suspicious e-mails or click on links inside suspicious messages.