Learning and Technology Services
Supporting Technology to Improve Learning

Scam #1

In general, phishing emails will ask you to provide your username and password to "verify" or "update" your account. **LTS will never ask you for your password or other personal information**; that is private information that you should not share with anyone else. **REMEMBER**, if you are unsure if an email is legitimate, contact the LTS Help Desk!

Note the **sentence structure** and **punctuation errors**. While valid UWEC business emails may not be flawless, they will certainly be better constructed and proofread than this.

Note that the "From" email is a **non-UWEC email address**. Sometimes the name can be deceiving; be sure to look at the actual email address.

From: University IT Service Desk [noreply@info.edu]
Sent: Sunday, June 16, 2013 8:59 PM
Subject: Dear Student/Staff Email User

Institution account routine, this has been made mandatory for all users.Due to the IP Security upgrades we have reason to believe that your webmail account was accessed by a third party. You are advice to re-validate this account To avoid loosing access to your account. Failure to do this you will have your account suspended . Protecting your account is our primary concern. to proceed with the account re-validation and admin assistance Click: ITS-SUPPORT

Text such as this creates a **sense of urgency** in a viewer's mind, often causing him or her to act first and ask questions later. Be wary of anything that tries to prompt you into immediate action.

Hover over the link with the cursor. Does the URL seem suspicious and/or un-connected with UWEC? In this case, it was https://adobeformscentral.com... In general, this is a good sign that it is not a legitimate email.
