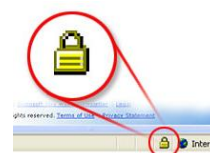


Do Not Get Reeled in by Phishing Email!!

What is phishing Email? The term comes from a variant of the word “fishing.” The nature of the Email is it appears to come from our Information Technology Department, AOL, on-line banks, eBay, Paypal – basically any account you may hold that has personal identity and password information. It is a criminally fraudulent process that attempts to get personal information from you if you respond to it. The Email message appears to come from a credible web site that you trust, but it is actually a scam to steal your personal information. Another ramification of this scam is it can hijack mail servers and other Otterbein systems and engage in malicious activity.

How do you recognize phishing Emails:

- The Emails may have official looking logos, and have phrases such as “Verify your account,” “If you do not respond in 48 hours, your account will be closed,” “Dear Valued Customer,” and /or “Click the link below to access your account.”
- The web addresses often contain numbered addresses instead of words. For example, the web link might be to an address such as <http://195.61.1.74/ebay/login.php>.
- Some phishing Emails use a slight misspelling of a web address, for example, <http://www.eboy.com/login.asp> (note the misspelling of eBay’s address).
- Some phishing Email fake web addresses. One way to verify that the web address is valid is to make sure the page is on a secured server (almost all major web sites use a secured log in). Look for a picture of a closed padlock in the status bar (for example in Internet Explorer). If you see this, the site is secure.
- If you’re still not sure about the validity of an Email, manually type in the address of the site requesting information. For example, if eBay needs something from you they will certainly make that request after you log in.



What to do if you get a phishing Email:

- Do not respond to the Email. Just delete it.
- If you click on a web address in a phishing Email, close the browser (going to a different address won’t necessarily protect you).
- Never respond to popup windows. Use the red “x” in the corner to close them and do not even trust the cancel button.

How do you prevent and avoid phishing schemes?

- Use Phishing filters in your browsers.
- Don’t post your Email address on web pages like MySpace, Facebook and other web pages.
- Never install software from unknown or untrusted sources or use file sharing for uploading and downloading files. (These are the worst offenders)
- Don’t trust any offers. If it sounds too good to be true, it is! It is very rare that any secure site will contact you via Email to request information from you in the first place!
- Above all, keep your computer protected with Windows Updates, Virus Protection and Spyware and Adware removers.