

Phishing/Email Scams

What is Phishing?

Phishing is the use of email, text messages, or fraudulent Web sites to attempt to gain personal information such as: driver's license and Social Security numbers, credit card account numbers, login names, birthdates and passwords. Often you will be asked to click on a link to verify personal information.

How Can Phishing Cause Problems?

If you respond to a phishing attempt, you might end up sharing confidential information that can potentially be used to access your accounts or steal your identity.

How to Recognize E-mail Phishing Scams

Phishing attempts can be very clever and will often appear to be legitimate. Phishing "red flags" include:

- Email messages from senders who have an unusual or strange-looking From or Reply To address – Ex: ref_3792mutating@jobssearch.co.uk
- The message says that your account has been suspended or will be cancelled, your account information needs to be verified/confirmed/updated, or there is some other problem with your account. (eBay, PayPal, Amazon are commonly mentioned)
- You get a message stating that you have won a prize, and to claim it you must go to a certain Website and fill out a form.
- The message urges you to take immediate action.
- The message is not addressed to you personally. (Ex: Dear PayPal Customer)
- There are misspelled words or grammatical errors.
- When you rest your mouse pointer over the link in a message, the link in the pop-up doesn't match the printed text.
- You are directed to click on a link to a Website with strange random characters or numbers in the URL—especially if they are near the front of the Web address.

Ex: <http://085.183.14.80/service.citibank.com>

How to Protect Yourself from Scams

- Avoid opening emails or attachments from unknown senders; just delete them without opening. Note that viewing an email in Outlook's preview pane is not the same as opening it.
- Use common sense. If an email doesn't look right, don't respond to it.
- Keep Internet browser and operating system updated with latest security patches.
- When sending secure information, be sure you are on an encrypted site (closed padlock in status bar in browser window and **https** in the URL.)
- Adjust email spam filters as needed to keep out spam emails as much as possible.
- Avoid clicking on a link within an email unless you're absolutely sure it is from a valid source.

- Avoid responding to emails or text messages from unknown senders.
- Avoid clicking on a link to Unsubscribe from an email list; by doing so, you will be confirming to spammers that your email address is valid and active.

Information That Should Never Be Shared Via Email:

- Passwords
- Login names
- Email addresses
- Social Security number
- Driver's license number
- Bank account numbers
- PIN numbers
- Street address
- Personal telephone numbers
- Birthdates

*Note: Central IT will **never** ask you for confidential information via email.*

How to Report Phishing Emails In UW Colleges and UW-Extension

Should you have any questions or concerns about Phishing and Email Scams, or if you think you have been the victim of one, please contact Diane Nora at 608-263-5043 or diane.nora@uwex.uwc.edu , or the Service Center at 888-UWEXUWC (262-5034).

Additional Resources:

UW-Madison Anti-Phishing Video
<http://www.cio.wisc.edu/security/video.aspx>

UW –Madison Tips for Avoiding Phishing Scams Brochure
<http://www.cio.wisc.edu/security/docs/phishingBrochure.pdf>

Special thanks to the DoIT office at the University of Madison for granting permission to use and adapt some of the content on their Phishing/Email Scams site: <http://www.cio.wisc.edu/security/scams.aspx>