Protect Yourself from Phishing Scams

Be suspicious of requests for personal information.
A reputable organization will never ask you for personal information via email. If a message asks you for your: username and password, Social Security Number, credit card number or bank account number, delete it immediately.

Do not click on links.
Although the link may state it is taking you to a legitimate website, it will likely direct you to an unsecured site to collect your personal information. Also, by clicking on the link, malicious software such as viruses and spyware can be installed on your computer.

Compare the reply-to address.
Many times the reply-to address of a phishing message is a giveaway. Check if the reply-to matches the original sender’s address.

Check grammar and spelling.
Many of the phishing scams received by UWP users recently have contained obvious grammatical or spelling errors. Review the entire message.

Never call the phone number included in a phishing message.
If you have questions concerning the message, call the organization. But, use a phonebook or check your account statement to find customer support numbers. Never trust a phone number included in a suspicious message, even if the area code and/or exchange information is correct.

When in doubt, delete!

For more information:

OnGuard Online
www.onguardonline.gov

Phishing Scams, FDIC
http://www.fdic.gov/consumers/consumer/alerts/phishing.html

How Not to Get Hooked..., FTC
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Recognize phishing..., Microsoft
http://www.microsoft.com/protect/yourself/phishing/identify.mspx

OIT Help Desk
2311 Pioneer Student Center
608-342-1400
helpdesk@uwplatt.edu

ResNet
122 Royce Hall
608-342-1990
resnet@uwplatt.edu
What is Phishing?
Phishing is a type of email-based scam in which a message appearing to be from a legitimate source requests personal information. The information collected is then used for various fraudulent purposes including identity theft.

How to Identify Phishing
Phishing messages pose as being from a reputable source such as your employer, credit card company, or bank. The messages generate a tone of urgency to encourage you to reply in order to avoid severe consequences. A phishing email may say something like:

From: email-admin@uwplatt.edu
Subject: Account expiration
Due to updates to our email system, we need you to verify your account information. In order to avoid the suspension of your service, respond to this message with your username and password as soon as possible.

What if I Took the Bait?
If you feel you responded to a phishing scam, change the password of any compromised account immediately. Then, contact customer support. In the case of your UWP account, use the Password Self Service and contact the OIT Help Desk or ResNet.

I Received a Phishing Email. What Should I Do?
Delete! If you receive any email message asking for your username and password, delete the message. The Office of Information Technology, your bank, credit card company, etc will never ask you for your username, password and other personally identifiable information via email. Never respond to such messages.

What can Phishers do with My Information?
Once scammers have your information they can use it for a variety of purposes, affecting you and other users. With just your NetID and password, they have access to all of your UWP network resources including:

PASS and DataMart: If you have access to confidential information of others, the scammers have access too. It’s not just your personal information at risk.

Email: In addition to accessing your existing email, scammers can take over your email account to send spam, which places the @uwplatt.edu domain on blacklists of email providers such as Hotmail, Comcast, and AOL. Once on a provider’s blacklist, delivery of all @uwplatt.edu messages to that provider is halted, causing email issues for other users and creating additional work for our email system administrators.