Security: Phishing Attacks

Last Modified on 04/20/2022 2:11 pm CDT

Phishing is the act of attempting to acquire important, personal information such as passwords or credit card numbers by pretending to be a legitimate source. A common way to accomplish this sort of attack is via phishing emails. There has been an influx of phishing email attacks against university users, making knowledge about phishing attacks and password security incredibly important for UW-Eau Claire faculty, staff, and students.

Topics

- What Happens if Your Account is Compromised?
- Identifying Phishing Emails
- Important Notes to Remember
- LTS Anti-Phishing Campaign

View this commercial created by LTS, advertising the dangers of phishing attacks and how to guard against them.

What Happens if Your Account is Compromised?

When a hacker is provided with your password via a phishing attack, he or she has access to all your personal information on record with UW-Eau Claire. This means a hacker could do the following (and more):

- View personal information, such as your Social Security Number and address.
- Send out phishing attacks from your email account to other UWEC users and your personal contacts.
- Change your personal information.

If you use the same password for other accounts (e.g. online bank account, Facebook, etc.), hackers would have access to all those accounts as well. This also means that if another of your accounts is compromised, hackers have access to your UWEC account as well. **Therefore, it is strongly advised that your UW-Eau Claire account password be unique.**

Identifying Phishing Emails

Phishing emails tend to have a similar look and feel. Once you learn to identify them, it is usually pretty easy to differentiate them from legitimate emails. Below you will see some common characteristics of phishing emails as well as information regarding how to use these characteristics to identify an email as a phishing attack.

Also, view this annotated phishing email example that points out frequent characteristics of phishing emails.

- **"Click Here" to confirm your personal information or upgrade your account.**
  You will often see the words "Click Here" (or something similar) in the email, with the text being linked to an outside source. If you hover over the linked text, the URL will appear. If the URL is unknown to you and/or looks suspicious, do not click the link.
- **The text creates a sense of urgency.**
  Often the "click here to upgrade" text, as mentioned in the bullet point above, will be followed by a threat or a warning indicating that your account will be deleted if you do not act quickly. This is designed by hackers to push you to act quickly instead of thinking about what you are doing. Take a step back and evaluate the email before falling prey to this tactic.
- **The email is signed "Help Desk" or "IT Support."**
  Signing an email in this fashion is a common way for hackers to convince users that the message is coming from your technology support team. However, examine the "from" email to see if it comes from *helpdesk@uwec.edu*. Most of this time, the "from" email will not have the *@uwec.edu* domain. If it does come from a UWEC email, that likely means that user's account was compromised and is sending out spam.
- **Poor grammar and misspellings exist throughout the text.**
  While the grammar and spelling of companies and organizations may not always be perfect, legitimate emails will likely look and sound professional. Many phishing emails, on the other hand, frequently misspell words, have extreme punctuation errors, use run-on sentences, or use unprofessional fonts and/or font colors.
- **Mismatched name and email address.**
  Many Phishing attempts work because they make you think that the email originates from someone you know or work with. A simple check is to make sure that the email address matches the email address that you typically use for that person. An easy give away is if the email does not match the person’s company. For instance, the display text may say “James Schmidt” but the actual email’s domain, the portion to the right of the “@” sign, is not an

actual university email address. Most of the time, Phishing emails originate with a “from” email address that will not have the @uwec.edu domain. For example, the following email address is an example of a phishing email address:

E.g. James C. Schmidt <jschmidt.uwec.edu@my.com>

Important Notes to Remember

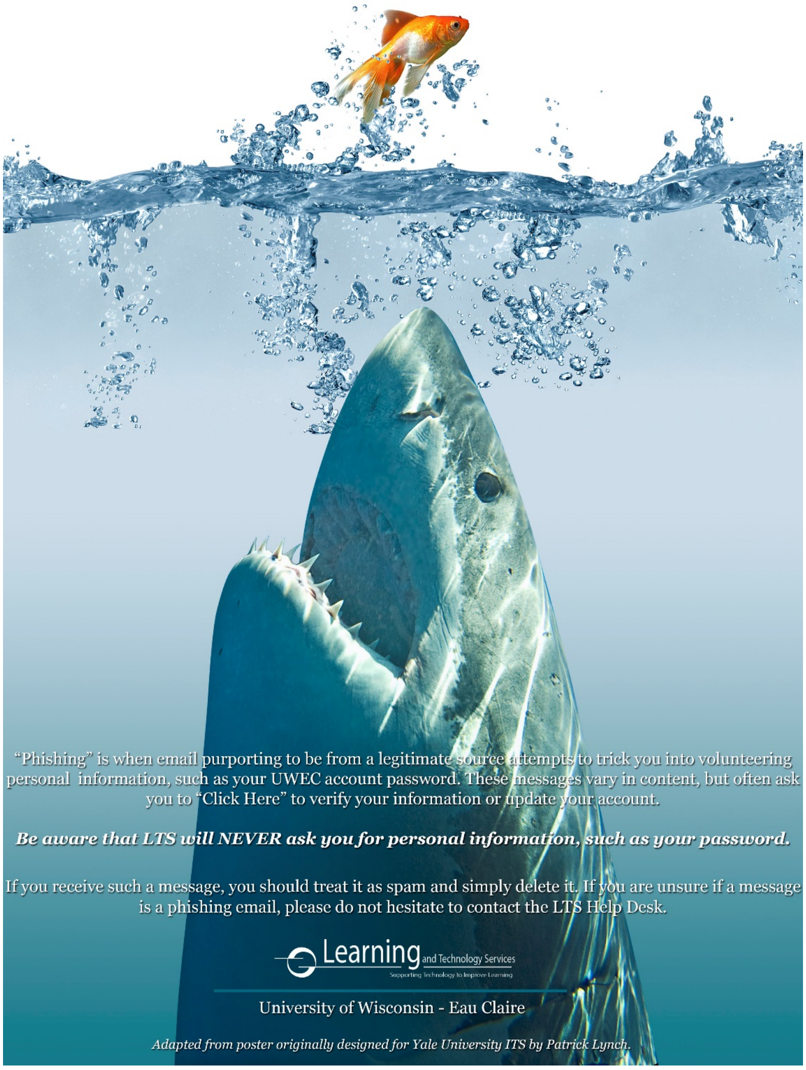
In the end, there are several key points that you need to remember to keep your information safe:

- **Do not share you password with anyone.** LTS will *never* ask you for your password, nor should any other legitimate organization. That is personal information that should *stay* personal. Do not even share your password with friends or family members.
- **If it sounds suspicious or too good to be true, it probably is.** Some phishing emails present untrue scenarios, such as claiming that you have inherited a large sum of money. Others that ask for your password or personal information are simply suspicious. Read all your emails with a discerning eye.
- **If you receive an email and are unsure of whether or not it is a phishing attempt, contact the LTS Help Desk.** The Help Desk can be reached via phone at 715-836-5711, or forward the questionable email to the Help Desk, along with your questions, at helpdesk@uwec.edu.

LTS Anti-Phishing Campaign

Below is the main poster used in the LTS anti-phishing campaign. This poster (among others) is displayed around campus in every general access lab.

In phishing, *you* are the fish.



"Phishing" is when email purporting to be from a legitimate source attempts to trick you into volunteering personal information, such as your UWEC account password. These messages vary in content, but often ask you to "Click Here" to verify your information or update your account.

Be aware that LTS will NEVER ask you for personal information, such as your password.

If you receive such a message, you should treat it as spam and simply delete it. If you are unsure if a message is a phishing email, please do not hesitate to contact the LTS Help Desk.

Learning and Technology Services
Supporting Technology to Improve Learning

University of Wisconsin - Eau Claire

Adapted from poster originally designed for Yale University ITS by Patrick Lynch.

University of Wisconsin-Eau Claire