Phishing is a form of fraud or theft by deceit! Phishing takes the form of an individual(s) pretending to be a legitimate company or person in an email or other communication method in order to obtain your login credentials or sensitive personal information.

How Can I Avoid Getting Caught!

- Ignore and delete email messages asking you for your Northwest account credentials!
- Ignore and delete email messages asking you to click on a link to expand your mailbox size!
- Ignore and delete email messages asking you to click on a link to prevent your account from being closed!
- Ignore and delete email messages urging you to click on a link because the sender has been trying to reach you for a while!

Sense of Urgency - It’s a Red Flag

Most email scams try to generate a sense of urgency! They want you to act quickly and impulsively!

If an email is urging you do something immediately, this should send up a red flag! Take a step back, a deep breath, and look for the signs of a scam!

What are the Signs of a Scam?

Below are some signs you should look for when determining if an email might be a scam. Criminals are clever so even if an email includes an authentic-looking logo, it might be a phishing scam!

- Unsolicited emails that ask for personal information or urge you to click on a link
- Spelling and grammar mistakes
- Salutation addressed vaguely like “Dear Valued Customer” or “Dear Client”
- Threatening or urgent language like “dire consequences” and “account termination”
- Email address of sender looks odd

Will Northwest ever ask me to click on a link in an email to prevent my account from being closed or to increase my account size?

No!

Emails like those listed above are SCAMS and do NOT originate from Northwest! See Northwest Phish Tales:

www.nwmissouri.edu/compserv/ClientComputing/email/nw_phish_bowl.htm

Beware of Phishing! Don’t Get Caught!

Your Questions! Our Solutions!

Information Technology Help 660.562.1634

help@nwmissouri.edu
Hover over email links before you click!

Don’t ever assume a link will take you to a legitimate web site.

As a precaution hover over the link to see its full web address (URL).

To hover, simply place your mouse pointer over the link! **Do NOT click the link!** The actual web address should appear!

If the underlying link is **different** from what is being claimed, **don’t** click on the link!


Ctrl+Click to follow link

nwmissouri.edu Upgrade and complete

Be cautious of any link that doesn’t clearly indicate where it links!

From isn’t always reliable!

While the name of a sender might look legitimate, if you examine the email address critically it has a **From** address that doesn’t make sense or doesn’t match the domain where it really came from.

Example of an illegitimate Northwest address:

From: Bobby Bearcat <executive.server@aol.com>

Example of a legitimate Northwest address:

From: Bobby Bearcat <bobbyb@nwmissouri.edu>

Check Email Headers!

**From** and **Reply to** can be faked! You can view full email **headers** to try and determine where an email originated. You want to closely examine the received by and return-path details.

How do I check email headers?

In your Northwest Email (Office 365) do the following to see full email headers:

- Login to your Northwest Email
- Select a message in your Inbox
- In the preview pane, click on the small, black, down arrow next to **Reply all**
- A drop down menu will appear
- Click on **view message details**
- A window will open that essentially shows the complete journey of the email message

You clicked on a link or opened an attachment in a suspicious email!

**What do you do?**

**Action Steps:**

- Change your password immediately on a different computer (if possible)!
- Check forwarding and rules in your email
- Contact the **Northwest Technology Service** Center for help!

View real life Northwest phish tales here:

www.nwmissouri.edu/compserv/ClientComputing/email/nw_phish_bowl.htm