Don't Get Phished!

Follow these tips and save yourself!

NEED HELP?
ATUS Help Desk
helpdesk@wwu.edu
360-650-3333
Haggard Hall 123

See examples:
https://atus.wwu.edu/security

Don't follow a login link that is not secure.

A good sign the link is secure is if it begins with https:// and if the web address is what you expect it to be—even when you hover over it.

Report phishing attempts to ATUS.

We will check to see how widespread the message is and make sure the remote site gets blocked.

Contact bank before following fake link.

When in doubt, don't follow the link and then go directly to your bank's website. If you received a legitimate link in an email, it's probably in your online banking inbox.

Don't share info via urgent emails.

Creating a sense of urgency is a scammer tactic. Be suspicious of emails asking you to take action quickly without verifying their authenticity.

Do not open unknown attachments.

Don't know the sender? Don't open! Even if you recognize the sender, verify they intended to send it to you before opening an attachment you were not expecting.

Create a strong password.

Strong passwords are harder to crack. They should be long and have numbers, special characters, and uppercase & lowercase letters.

Don't use same password for multiple services.

Your password(s) for WWU should be unique and not the same as those you use for other services like your social networks or your bank's login.

Realize links like wwu.edu.gq are not OK.

Some phishing attempts try to make it look like the link goes to a wwu.edu address. They are counting on you not reading the address carefully.

Ignore unsolicited job offers.

These are usually scams! Even some jobs you find on sites where legitimate jobs are posted might be scams. Research offers before you apply.

Recognize prize offers as too good to be true.

These are usually scams to acquire your password or personal info or install malware on your computer if you click the link. Resist the urge!

Do not fill in web form without verifying site.

Think about why you are receiving a request to complete a form, and delete it if you do not recognize the sender or the context.

Don't share login with friends.

By using your login, your friends might accidentally lock you out of your own account...or worse! You are responsible for anything done with your account.

Take time to think before acting.

Many phishing attempts try to create a sense of urgency so you will act before thinking.

Verify a URL before clicking it.

Use the mouse hover technique to check out each link. Links in Western email are converted to addresses with safelinks.protection... outlook.com