To help prevent Spam and Phishing, before opening any attachment or link, check these items:

- Verify the sender of the email
  - Look at the from email address, not the signature in the email.
  - Just because it appears to come from someone you know doesn't mean it is a safe email.
- Look for misspellings and grammar mistakes in the email (malicious emails will often, but not always, have misspellings and bad grammar).
- Don't click links in suspicious emails
  - Rather than clicking a link within an email or attachment, go to known sign in pages, such as mySWU to access SWU email.
  - If you are already signed into web-based SWU email, you will not be asked to enter your email credentials to access files within SWU email or Microsoft OneDrive.
  - Never enter your credentials on a page that is linked to from an email or attachment.
- Check for fake hyperlinks, (what is displayed is not always the website that the link takes you to).
  - Hovering over the link will display what the email links to, for example a link could be displayed in the email or attachment as www.microsoft.com but can take you to a phishing website that the spammer setup to look just like Microsoft's website.
  - Spammers can also setup fake websites with URLs that are very similar to real URLs, like having a common typo in the URL to make the URL look like it is the correct URL.
- Do not reply to suspicious emails to verify if they were intentionally sent.
  - When a malicious email is sent the bad guys have access to the account that sent the email, so they can reply to your email verifying that they send the email in question.
  - You can't trust a response that you receive if you question the legitimacy of an email.

If in doubt, delete the email or ask the Office of Information Technology by forwarding the email along with any questions to techsupport@swu.edu.