Universities and their computers are targets for hackers. The bad guys want your computer for malicious or inappropriate activity and/or to steal your sensitive data.

To help reduce the risk of identity theft and unauthorized access to your computer:

- Be suspicious of any unexpected attachments to an email or other social media tools. When in doubt, verify the attachment with the sender before opening it.
- Never install an application unless you know exactly what it does and what company created it. Malicious code is often hidden in seemingly simple and basic apps. You should only install apps for which your school has a valid license.
- Be suspicious of unexpected phishing emails:
  - Is the email “From:” address appropriate? If the email appears to be coming from the University, does the “From:” address use our University.edu address?
  - Do not click on suspicious or unknown links. If the message has a URL link, use the mouse hover trick to determine the ultimate destination of the link. Without clicking, hover your mouse pointer over the URL and a box will appear with the actual destination of the link. For phones and tablets, place your finger on the link and hold until the box pops up.
  - Does the content of the message contain unusual spelling and grammar errors?
  - Is there contact information for any questions? Again, if the email appears to be from the University, is there a contact number that begins with our University phone exchange or an email address that contains our University.edu address?
- Do not be fooled by emails that want you to provide any personal information including your ID and password.
- Don’t use the same password for all of your accounts – especially for any account used to access sensitive information (e.g. online banking, etc.).
- Change your password often.
- Don’t use an easy-to-guess password such as pet/relative names, or dictionary words.
- If possible, include special characters (#*!&%), numeric, and both upper/lower case letters in your passwords.
- Don’t post your password on or near your monitor or anywhere others can find it.