UCSB Cybersecurity Tip - Back to School Cybersecurity

This was posted by the UCSB Information Security Site with regards to Back to School Cybersecurity

https://security.ucsb.edu/news/ucsb-cybersecurity-tip-back-school-cybersecurity

As a reminder to everyone (Students, Staff and Faculty) Cybersecurity does rest upon the user.

Scammers are always finding new ways to get around Spam Filters with regards to email, so it is best best to follow the recommendations:

<table>
<thead>
<tr>
<th>Excerpt from the UCSB Cyber Security Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>The best way to avoid scams is to approach all unexpected messages, offers, and phone calls with a healthy skepticism. Helpful habits include:</td>
</tr>
</tbody>
</table>

1. Always think twice before clicking on links or opening attachments, even if they look like they are from someone you know. If you are not sure, contact the sender by a method you know is legitimate to confirm they sent it.
2. Verify requests for private information. Remember, con artists know how to fake their identity.
3. Protect your passwords. Make them long and strong, never reveal them to anyone, and use different passwords for different accounts. Also, use multi-factor authentication (MFA) where possible.

Also, Researchers,

Please be sure to read our section on Security here.

We have several articles on how to secure a Windows and Linux computer that you may want to do when having a computer on the Campus Network.