*In recognition of October being National Cyber Security Awareness Month, the Office of Safe and Secure Computing is bringing you tips to stay safe online. Our first weekly topic is email safety.*

*From phishing, to malicious attachments, to shady hyperlinks, email can be a dangerous place. Following these tips can help keep you safe when using email.*

 

**Always look at the “From” address**, which consists of 2 parts: the associated name and the actual address. Scrutinize both parts to see if anything looks suspicious.

* Does the email address end with another country code, such as **.ru** or **.cn** when you are not expecting to communicate with someone from another country?
* If the person is claiming to be from an organization, does their email address end with a domain name that matches the organization? For example, Tri-C emails end with **@tri-c.edu**

**Always consider the contex**t:

* Did you receive a message about receiving a package but are not expecting one?
* Would the organization the message appears to be from have the email address it was sent to? For example, you probably did not provide the IRS with your work email, and you probably did not sign up for online baking to your work email.
* Is the person sending an invoice for services/products that you did not order?
* Do you know the sender? If so does the message seem to be in character with him/her?

**Provocative messages** **should be examined closely before acting**.

*These type of messages are designed to elicit a quick response are more likely to be illicit.* *Example messages include:*

* Are these pictures really of you?!
	+ Fake bills for large amounts of money (Verizon wireless services, fake Amazon orders, etc.)
	+ Your Account will be deleted in 24 hours
	+ Unusual Activity Detected
	+ HR Salary Data.xlsx

If anything is unusual, **do not open attachments** or **click on any links.**

**Do not open attachments** and **do not follow links (URLs)** unless you are certain that everything is legitimate and you have a specific reason to do so.

* You can “hover the mouse cursor” over the URL link. In most cases, the browser will display at the bottom where the link REALLY goes to. If it looks unusual or does not match where it looks like it should go, **do not click the link**.