Have you noticed the increase of phishing attacks with realistic context?  Hackers use typical business scenarios against the employees of targeted organizations.   Sometimes the phishing emails use familiar logos, common entities, or formatting.  Other times phishing attacks incorporate your name or other familiar information.  All of this is disturbing. How can you identify and defend against such attacks?  Here’s a short list to keep handy.

1. Check the email address.  Extensions for Campus entities should be “@csusb.edu”.  If a third party is involved go to step 2
2. Verify the context with phone calls or independent research.  Call the responsible department or look up information either online or through associates.  But never use links or content from the phishing email.
3. Hover over links to decipher the URL.  If that isn’t possible due then open a browser and search for the URL or manually type it.

If you accidentally click the URL of a phishing email then do the following:

1. Discontinue use of that machine and contact the Technology Support Center (TSC) x77677.  They will assess your machine for malware.
2. Use a different machine to change the passwords to any program open when you clicked the link.
3. Forward as an attachment the phishing email to abuse@csusb.edu.  This assists in identifying and fighting potential phishing email.
4. Consider using multifactor authentication.

For more information on phishing please refer to this CSUSB ITS Knowledge Base article on Phishing Awareness.  <https://www.csusb.edu/its/support/knowledge-base/36096>

To protect yourself against identity theft check out this other CSUSB ITS Knowledge Base article on Control Identity Theft.  <https://www.csusb.edu/its/support/knowledge-base/33236>

As always, let’s stay cyber safe!

Regards,

 ---

Michelle Behne

**Information Security Analyst**

Information Security & Emerging Technologies

Information Technology Services Division

909.537.7262

 ---

*Disclaimer: This e-mail message is for the sole use of the intended recipient(s) and may contain confidential and privileged information protected from disclosure.  If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.  If you have received this communication in error, please notify us immediately by replying to the message and deleting it from your computer.*