Phishing Checklist

Have you received an e-mail, supposedly from Computer Services, requesting your password or prompting you to click on a hyperlink to help fix a problem? Beware! It might be a phishing attempt.

Use this check list to help determine if it bogus or not.

- ☐ **Is it from Cuesta?**
  Does the address in the "From" field end in "…cuesta.edu"?
- ☐ **Is it addressed to you?**
  Is the name in "To" field yours (as opposed to blank or addressed to something like "undisclosed-recipients")?
- ☐ **Does "Cuesta" appear *anywhere* in the message text?**
- ☐ **If there's a link, does it point to a "…cuesta.edu" site?**
  If you hover the mouse pointer without clicking over the hyperlink, does the displayed web address contain "cuesta.edu"?

If you **checked all** the boxes, then the email is probably **safe**.
However, if **2 or more** of the boxes are **blank**, then the e-mail is highly suspect and may be a **phishing attempt**.

Remember, Computer Services will ***never*** ask for your **password** via e-mail.

If in doubt, please contact Computer Services at x3248.