Spotting Spam/Scam E-mail

Always check that

✓ The e-mail address has the correct company domain
  o (ex: UCF e-mail will come be a “ucf.edu” address)
✓ Spelling, grammar and capitalization are correct
✓ No sensitive information is asked for in a reply back to the e-mail
✓ The e-mail is personalized with your name/information
  o Spammers are getting smarter about this, but it is still a good way to spot some spam
✓ There is a specific sender or department (that exists!)
  o Most UCF e-mail will have a person or department listed. You can look them up on the UCF Phonebook: http://phonebook.ucf.edu

Scam 1: Your Account is in Trouble!

Scammers want to scare you into clicking a link or replying with sensitive information. Often they write that your account will be deleted or your access blocked.

1. **Is it asking for personal or account information? SPAM.** UCF will never ask for you to reply with personal or account information. No legitimate company will ask you to send that kind information in an e-mail.
2. **Is e-mail address different than the company domain? SPAM.** Often the sender’s address won’t even match the company they are claiming to represent. UCF messages will come from UCF e-mail addresses ending in the ucf.edu domain. (ex: ucfstaff@listserv.cc.ucf.edu or servicedesk@ucf.edu)

Important: Never click a link or call a number provided in an unsolicited e-mail. Always open a web browser and go to the official site to get a phone number or find an e-mail address.

Example 1: This e-mail threatens “permanent deactivation” of your e-mail account if you don’t reply with your account information.

Not a UCF e-mail address.
UCF will never ask for this kind of information in an e-mail.
Not a UCF department, no UCF contact information provided.
Scam 2: Faking It

Many scammers will try to make the e-mail look as legitimate as possible. They may copy the style and graphics. If you are in doubt, open a new browser, go to the actual company website. From there you can check your account or use the contact information and then verify what is going on.

- Never call a number provided in a spam e-mail
- Never click the links provided in a spam e-mail

Example 1: This e-mail is trying to look like it came from Facebook.

Example 2: This e-mail is pretending to be from a bank.