Spam

Email spam is email that you did not ask to be sent to you. Spam is similar to the bulk rate "junk mail" that is delivered by the post office. There are many ads with some scams and chain letters mixed in. Email spam is more dangerous though because clicking the links, opening attachments, or providing information back to the spammers can compromise your computer or your identity.

Due to the number of complaints we receive regarding spam, we strongly encourage everyone to take the appropriate measures described below.

Spotting Spam

Before opening an email:

Check the subject line. Many spam messages are easy to spot based on the subject line. Don't even open them, just delete.

Look at the sender's email address.

- UCF email will come from a @ucf.edu address.
- If it is spam, delete it.

In the message, check for:

Correct spelling, grammar and contact information. Spam will likely contain misspellings, incorrect grammar, and false contact information. UCF email should include verifiable contact information. Verify the contact information using the online UCF Phonebook www.phonebook.ucf.edu.

Threats. Malicious spam often makes a threat and then asks you to provide sensitive information.

- A common threat: "Your account will be terminated/has been locked, give us your username and password for the account." UCF will never ask for your information in this manner. This kind of email is a **phishing attempt**.

You can **report spam** here: junk@office365.microsoft.com

Phishing

If you believe you have inadvertently submitted information to a phishing site, then **contact your department's IT staff or DSC immediately**. If you do not have an IT team, please contact the UCF Police Department, the Security Incident Response Team (sirt@ucf.edu) and refer to the Federal Trade Commission identity theft website: http://www.consumer.gov/idtheft.

Phishing is the act of convincing someone to surrender their private information (e.g. bank account number, Social Security number, passwords) which can then be used to commit identity theft. Often phishing is done as spam email formatted to look like official communication from banks, eBay, or other organizations including UCF.

Phishing messages typically contain a threat that an account will be disabled if the recipient does not re-enter or update their information. The recipient is then asked to click a bogus web link or reply to the email and provide personal information.

You can **report phishing** messages to Microsoft here: phish@office365.microsoft.com

Protect Yourself

Legitimate businesses do not solicit user account information through email. **Delete all phishing email that you receive**.

- **Do not click on links in a phishing spam.**
- **Do not reply to a phishing spam.**
- **Contact the company directly.**

Do not use any contact information listed in a spam.

Open a web browser and go directly to the site (if you know the address) or search for the company site.

Check the institution's website for more information on phishing attacks.

If you have any questions regarding any of these computer threats, contact your department's IT staff. If you don't have an IT team, contact the UCF Service Desk at (407) 823-5117.

Learn more about Spotting Spam and how to identify phishing attacks.

Handling Spam

Do not open any attachments. Turn off the preview feature for your email client to prevent it automatically opening an infected file or running a malicious script.

Do not click on any links. Links go to infected sites or fake ones that capture your username and password. If you want to check out a site, open a browser and search for the actual company on the web.

Do not respond to spam, report it! Do not send a reply email or click the "remove me" link. Instead, report the spam to:

- junk@office365.microsoft.com – Alert Microsoft of junk or spam email to help filter out any unwanted messages in the future.
- the sender's ISP – use our Reporting Spam PDF to have the offending mailbox shutdown.

Is it threatening? If you feel the spam is malicious or a threat contact:

- SIRT@ucf.edu– forward the email as an attachment.
- University Police at (407) 823-5555 if you are harassed via e-mail and feel as if your personal safety has been threatened.

Delete!

UCF has multiple filters to block spam from arriving in your inbox, unfortunately no filter can be 100% effective. The easiest way to handle spam is to delete it.

Preventing Spam

When purchasing or signing up for services on the Internet, do not provide your UCF email address.

TIP: Sites with a checkbox to "Do not share this address" may not honor your request.