

IT@UC

INFORMATION SECURITY

Email Safety

Unsafe computing can corrupt your files, expose the contents of your internal drive to strangers, cause other computers to become compromised, and so much more. This document provides recommendations to follow to protect the yourself when using email.

Using safe email practices helps you:

- Protect your inbox
- Protect your computer
- Protect your privacy
- Protect your friends and neighbors

Here are recommendations you should follow to protect yourself when using email.

1. Screen messages before viewing them, and delete anything that appears suspicious.
 - a. **Carefully examine your list of unopened messages.**

Do any of them come from people or addresses you don't recognize? Do the subject lines have words with too many spaces, or long random numbers? Do they seem too good to be true, or somehow odd? If so, it's probably best to just delete the message along with any attachments.
 - b. **Wait! Don't open that email yet...**

If a message has attachments don't open it unless you know the sender and are expecting the attachment.
 - c. **Don't be fooled.**

Most computer worms (a kind of malicious program) spread themselves via email by spoofing addresses found in the infected computer's address book and sending copies of itself to other addresses in the address book. ***It is very likely that an infected message can appear to come from someone you know.*** Many of these messages will use vague or generic subject lines like "Re: " or "Hi." Others will try to look like they come from a technical support service, or even from Microsoft. Be careful about opening these.

2. Handle Attachments Safely.

a. Don't open attachments unless you are absolutely sure about what they are and who they came from.

Even attachments that were sent directly to you by a known sender might contain malicious code.

b. Be especially careful with MS Word & Excel files.

When opening Microsoft Word or Excel attachments containing macros, always select the "Disable Macros" option if you are not sure if there should be a macro.

c. Beware of Dangerous File Types!

Some file types have been deemed unsafe by Microsoft. Most of these file types are executable or exploitable and are considered unsafe to send and receive as email attachments.

d. Windows Users - Make Extensions Visible

Some malicious attachments will "pose" as a harmless file type like digital image by including that file type extension in its name. You might get an attachment called "hawaii.jpg" and think it's a picture from your friend's vacation. But it might actually be a .pif file, one of the exploitable file types. This can happen because Windows does not display file extensions by default, so a .pif file named "hawaii.jpg.pif" will appear as "hawaii.jpg"

4. Don't Unsubscribe.

Spammers often include an "unsubscribe from this list" link in their messages. This makes them appear more responsible and reputable, but they often use this as a way to confirm your email address so they can send you more spam or sell your email address to other spammers. If you don't want it, mark it as junk and delete it.

5. Be a Good Internet Citizen.

a. Don't use your email in ways that will contribute to the problem.

b. Don't send unsolicited email and attachments.

c. Don't forward chain letters.

d. Don't respond to or participate in email hoaxes.

e. Don't send attachments which use the "unsafe" file types.

f. Use a "disposable" email account (a free account from yahoo or hotmail) for online shopping and posting to off-campus online discussion boards.