

Practicing Safe E-mail

(Or, how to read your e-mail without getting a virus!)

Attachments

- Do not open attachments!
- Don't view them.
- Don't save them.
- Do not configure your e-mail software to automatically open attachments. If your email program automatically opens attachments, change it!

If you get an attachment by e-mail:

- Contact the person who sent you the attachment to verify that they actually sent it. Ask the sender what the attachment is.
- If in doubt, contact a professional —your network administrator or Internet service Provider (ISP). Do not send them a copy; just tell them the sender, date, and name of the attachment.
- Run an anti-virus product. UF currently has a site license for McAfee VirusScan. You can download McAfee VirusScan from <http://www.software.ufl.edu/mcafee>, then click on "Desktop Protection". You will need to provide your GatorLink userid and password.
- If all else fails, forward the message with the attachment to virus@SecurityAdvice.com. They will investigate and let you know what they find.



Sending Email (and Possibly Attachments) Safely

1. Send the recipient a message to let them know that you are about to send an attachment.
2. Avoid sending executable files as attachments, such as Word documents with macros.
3. Send Rich Text Format (RTF) files instead (File-->Save As-->RTF).
4. Using an anti-virus product, scan the file before you attach it. (see instructions about downloading McAfee VirusScan above)

For More Information:

Viruses

<http://www.datafellows.com/virus-info/virus-news>
<http://vil.nai.com/villib/alpha.asp>

Hoaxes:

<http://www.datafellows.com/virus-info/hoax>
<http://vil.mcafeesecurity.com/vil/hoaxes.asp>

