Email Attachments

Even if you consider yourself to be a knowledgeable user of the Internet and email programs like Microsoft Outlook, Outlook Express, Eudora, or Netscape, you might not always be aware of the ways that email can be used to affect your computer and how to prevent email attacks. Let's take a look at a few different attacks and the countermeasures that will keep you safe:

Viruses: Viruses and other types of malicious code are often spread as attachments to email messages. Before opening attachments, be sure you know where the attachment came from and what type of file it is. Many email viruses are known to exploit hidden file extensions. The files attached to these messages may appear to be harmless text, MPEG, AVI or other file types, but the file is actually malicious script or executable virus programs—.vbs, .exe, or .bat files, for example. Always read the entire file name before opening attachments.

Viruses and malicious code might be distributed in amusing or enticing programs, particularly around the holidays. It's always best to never run a program unless you know it to be made by a person or company that you trust. Also, don't send programs of unknown origin to your friends or family simply because they're funny -- they might contain a virus.

Spoofing: Advances in technology have allowed spammers and malcontents to actually impersonate another person's email address, also known as "spoofing." Email spoofing occurs when an email message looks as if it is from one person, usually someone you know, when it actually was sent from another source. Spoofing is often an attempt to trick you into opening an email attachment that contains a virus; remember that if you weren't expecting an attachment from someone, it is a good idea not to open it.

Social Engineering: Remember that while service providers like America Online may occasionally request that you change your password, they will **not** specify what you should change it to. Also, most legitimate service providers would **never** ask you to send any password information or file via email. If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately. Also, remember that a company will never actually send you a patch for a program via email.

Summary

The safest thing to do when you receive an attachment or file from someone that you're not expecting is to email back that person and ask him if he sent you a file. If he didn't, then delete it. If you receive an attachment from someone you don't recognize at all, don't even think twice and delete the file.