Using Caution with Email Attachments

While email attachments are a popular and convenient way to send documents, they are also a common source of viruses. Use caution when opening attachments, even if they appear to have been sent by someone you know.

Why can email attachments be dangerous?

Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- Email is easily circulated - Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email—they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.

- Email programs try to address all users' needs - Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.

- Email programs offer many "user-friendly" features - Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

What steps can you take to protect yourself and others in your address book?

- **Be wary of unsolicited attachments, even from people you know** - Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

- **Save and scan any attachments before opening them** - If you have to open an attachment before you can verify the source, take the following steps:

  1. Be sure the signatures in your anti-virus software are up to date Save the file to your computer or a disk
  2. Manually scan the file using your anti-virus software
  3. Open the file

- **Turn off the option to automatically download attachments** - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.