

## **Avoiding Cyber Threats that are attached to Emails:**

- 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.
- Keep software up to date - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- Trust your instincts - If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.
- 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.
- Consider creating separate accounts on your computer - Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.