The Internet is a great place, and a dangerous place. We've all likely been forced to deal with malware, viruses and other Internet woes. The greatest risk for infections is via the web and email. Being prepared with basic antivirus and anti-malware, enabled firewall and a few simple rules goes a long way to preventing the Internet blues.

Your first line of defense is antivirus and anti-malware software, along with a good firewall will help prevent and remove any infections on your computer. As a consultant, I usually recommend Trend Micro antivirus and MalwareBytes (free version) together to prevent and eliminate malicious software. These will eliminate and prevent most, but not all problems online.

A simple rule while browsing online is to first visit only sites you know and trust. Frequently review the URL to make sure it is the site you intend to visit. Anytime you are dealing with confidential information online, make certain the URL begins with https://. This ensures the transmission between you and the web site is secure and protected from outsiders.

HTTPS (secure) communications are not all the same. When a web site purchases a certificate, the programming that encrypts and decrypts information between you and the web server, the certificate can validate that the site owner is who they say they are. Information varies from no validation with basic certificates, to in depth validation with EV (Extended Validation) certificates. EV certificates create the green lock and text before or after the url and shows the name of the certificate holder. These certificates provide the most assurance your information is safe and secure. Many online retailers and virtually all banking and financial institutions will use EV certificates.

As with the web, apply the same basic principles to your email. If you are unsure, don't know the sender, or the message is SPAM, just delete it. Most malicious emails will require some interaction before it will infect your system. Email is a commonly used method to infect computer systems and usually utilizes social engineering techniques to move its readers to action.

For more information regarding email security and how to protect yourself, view our Avoid Phishing Scams newsletter
. After you finish removing unwanted emails, remember to empty your trash folder to permanently delete emails.

By following some simple rules and using common sense, you can fully utilize the Internet with safety and security.