



# Defend Your Computer & Yourself

Everyday, cybercriminals are working relentlessly to install malicious software like viruses and spyware on your computers in an effort to damage your computer/software, use your email to spread malware or monitor online activities in an attempt to steal sensitive personal information and money. Don't be an easy target for them. The following are steps you can take to help protect your computer & yourself from would-be thieves.

ANTIVIRUS PROTECTION

STRONG PASSWORDS

SOFTWARE UPDATES

PERSONAL FIREWALLS

EMAIL LINKS/ATTACHMENTS

- **Install Antivirus and Antispyware programs from a trusted source**

Anti-malware programs scan and monitor your computer for known viruses and spyware. When they find something, they warn you and help you take action

- \* Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your computer or offers to remove viruses.
- \* Get an anti-malware program from a vendor you trust. (McAfee, Norton, AVG are only a few examples)

- **Use Strong Passwords**

Password strength is another important consideration. Obviously, the more complex a password, the harder it is to guess.

- \* Strong passwords are at least 10 characters long and should be a mix of letters, numbers and symbols if possible.
- \* Keep passwords a secret and don't share them with anyone.
- \* Don't use the same passwords for every site.

- **Keep all software updated**

Most software companies release patches and updates to their products regularly to repair vulnerabilities and bugs within the software.

- \* Install the updates for all your software especially your antivirus software, operating systems and internet browser.
- \* Setup automatic software updates if available.
- \* Uninstall and remove any software that you do not use.

- **Turn on personal firewalls**

A firewall puts a protective barrier between your computer and the Internet. Turning it off increases the risk that your PC will be infected with malware.

- **Don't be tricked into downloading anything**

Emails are one of the easiest ways for cybercriminals to gain the access they need to infect your computer or steal your personal information.

- \* Use caution when opening attachments or clicking on links within an email even if you know the sender. If you're not sure, delete it.
- \* Avoid clicking **Agree, OK** or **I accept** in banner ads, unexpected pop-up windows or warnings on websites that may not seem legitimate.
- \* Beware of "free" offers and only download software from websites that you trust and know are legitimate.