

PROTECT YOUR COMPUTER



TIPS TO PROTECT YOUR COMPUTER

- **NEVER ANSWER AN AD OR POP-UP CLAIMING YOUR COMPUTER IS INFECTED WITH A VIRUS, SPYWARE OR MALWARE.** This is a common scam where someone will try to convince you to let them in your computer to “fix” it by removing the malicious source. In fact, they want to infect your computer and even take it over from you.
- **ALWAYS USE A FIREWALL.** A firewall acts as a gatekeeper to your computer. Firewalls monitor when someone or something attempts to gain access to your computer operating system, then takes action and blocks unwanted or unrecognized sources.
- **DON'T USE USBs OR OTHER EXTERNAL DEVICES UNLESS YOU OWN THEM AND KNOW EXACTLY WHAT IS ON THEM.** To avoid getting infected with malware or viruses, you need to know where external devices came from.
- **ENSURE YOUR PASSWORDS ARE WELL-CHOSEN AND PROTECTED.** It's best to use a password generator/keeper to protect your passwords. We encourage you to use passphrases as opposed to passwords.
- **NEVER OPEN SUSPICIOUS ATTACHMENTS OR CLICK UNUSUAL LINKS IN MESSAGES.** Dangerous links or attachments can be in emails, tweets, posts, online ads, messages or attachments, and are sometimes disguised as trusted sources.
- **KEEP ALL SOFTWARE UP TO DATE.** Make sure to turn on automatic updates to keep your operating system and all applications up to date, especially browsers, Adobe Acrobat Reader and other applications you may regularly use.
- **USE AN ANTIVIRUS SOFTWARE** but know how important it is to keep it updated to the most recent version.
- **NEVER USE PIRATED MATERIAL.** This includes streaming or downloading movies, music, books or applications that may be downloaded outside of trusted sources like official app stores.