November 1, 2013
Securing Your Computer and Mobile Device
Prepared by Barry Cowen

1. **Use strong passwords containing letters, numbers, and symbols.**
2. **Install and update automatically and/or manually only <u>ONE ANTIVIRUS PROGRAM</u>.**
3. **Install and update antispyware programs automatically and/or manually**
3. **Turn on your software and hardware firewalls.**
4. **Install the latest security updates and patches for your Operating System. Update your iOS versions for Apple devices and install the Avast! Mobile Security and Malwarebytes Mobile apps from the Google Play Store for Android phones and tablets.**
5. **Use the most updated and secure version of your browser. (XP Users: Do not use IE)**
6. **Don't open, forward, or reply to e-mails with suspicious links, ads, and attachments.**
7. **Read the fine print on the EULAs (End User Licensing Agreement) before installing.**
8. **Download files from trusted sources. Look for https:// and a closed yellow padlock.**
9. **Never run software from borrowed removable media without scanning the content.**
10. **Never accept free toolbars or other unsolicited software offered by a website**
11. **Malicious software (malware) includes Trojan horses, backdoors, viruses, worms, spyware, and adware. Rootkits hide malware from security applications.**
12. **A virus is a self-replicating program that spreads by inserting copies of itself into the executable code of programs or documents that already exist on a computer.**
13. **A worm differs from a virus because it does not depend on using other programs. It usually replicates and spreads through networks through infected e-mail.**
14. **Trojan horses are malware that masquerade as legitimate programs and hide themselves inside a computer often without the user's knowledge.**
15. **Scan downloaded files before running them on a computer or mobile device.**
16. **Avoid sites offering free commercial software serial numbers, keygens, and hacks.**
17. **Configure your antivirus program to scan incoming e-mail and attachments.**
18. **Disconnect your computer from the Internet or external storage media when not in use.**
19. **Don't share access to your computer with strangers.**
20. **Back up your computer regularly to a variety of media.**
21. **Do not remain logged onto computers in public areas that are unattended.**
22. **Try to enable secure mode in e-mail accounts and social networking sites.**
23. **Turn off Wi-Fi until you reach a public area. Turn it off when you leave it.**
24. **Configure your router to use WPA or higher level security.**
25. **Don't click on e-mails or popups offering to remove malware from your computer**
26. **Learn how to identify, deal with and report phished messages and scams.**
27. **Don't jailbreak or root your device.**
28. **READ AND THINK BEFORE YOU CLICK.**
29. **TRUST BUT VERIFY.**