December 7, 2012
PC Security 101
Prepared by Barry Cowen

1. **Install and update automatically and/or manually only <u>ONE ANTIVIRUS PROGRAM</u>.**
2. **Install and update antispyware programs automatically and/or manually**
3. **Turn on your Firewall(s).**
4. **Install the latest security updates and patches for your Operating System.**
4. **Use the most updated version of your browser.**
5. **Don't open, forward, or reply to suspicious e-mails with links, ads, or attachments.**
6. **Read the fine print on the EULAs (End User Licensing Agreement) before installing.**
7. **Download files from trusted sources. Look for https:// and a closed yellow padlock.**
8. **Never run software from borrowed removable media without scanning the content.**
9. **Never accept free toolbars or other unsolicited software offered by a website**
10. **Malicious software (malware) includes Trojan horses, backdoors, viruses, worms, spyware, and adware. Rootkits hide malware from security applications.**
11. **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.**
12. **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.**
13. **Trojan horses are malware that masquerade as legitimate programs and hide themselves inside a computer often without the user's knowledge.**
14. **Scan downloaded files before running them.**
15. **Avoid sites offering commercial software serial numbers, keygens, and hacks.**
16. **Configure your antivirus program to scan incoming e-mail and attachments.**
17. **Disconnect your computer or external storage device when not in use.**
18. **Don't share access to your computer with strangers.**
19. **Back up your computer regularly to a variety of media.**
20. **Use strong passwords containing letters, numbers, and symbols.**
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. **Don't click on evil twin (fake) sites or unfamiliar rogue (phished) sites.**
25. **Configure your router to use WPA or higher level security**
26. **Don't click on e-mails or popups offering to remove malware from your computer**
27. **When the grandkids visit, establish a guest or limited user account (LUA)**
28. **Learn how to identify, deal with and report phished messages and scams.**
29. **After a computer has been cleaned of infections, disable System Restore.**
30. **THINK BEFORE YOU CLICK.**