

**Top Tips From Our Classes**  
**Prepared by Barry Cowen**

Print out and share these tips. During the break, review our YouTube class videos, handouts, and Gold Mine entries on our Club site. Find a quiet place and practice what you have learned. Have a safe, healthy and malware-free summer. *Barry*

1. Think before you click or tap.
2. Everything you send or post stays on the Internet. Would you put it on your front door?
3. Don't make your life an open book to criminals on social media.
4. Shred personal and confidential documents that could be useful to criminals.
5. Do not throw materials containing confidential information into a dumpster.
6. Purchase an external backup drive. We recommend Western Digital or Seagate.
7. Develop and implement a rational backup plan and strategy on a regular basis.
8. Keep your antivirus program and antispyware programs updated.
9. Install recommended computer and mobile security updates.
10. Always scan flash and external drives when you use them- before and after use.
11. Do not download from unknown or unauthorized sources.
12. When installing programs on a computer use the Customize option.
13. Never install unfamiliar PC and Registry cleaning utilities.
14. For privacy, cover your webcam with a piece of tape, etc.
15. Secure your router/network using WPA security or higher. Change its SSID (service set identifier) from its default (manufacturer's name) to prevent unauthorized use.
16. Always use a VPN at a public hotspot.
17. Use unique strong alphanumeric passwords and change them regularly.
18. When forwarding e-mails, use blind copy( Bcc) to protect recipients' identities
19. Do your homework and research before sending out anything.
20. Check out charities on reputable sites before donating anything.
21. Use the Task Manager to close a process or unfamiliar pop-up box.
22. Delete any e-mail that has no subject.
23. Don't click on an unfamiliar link or ad in an e-mail or on a web page.
24. Hover your mouse over links in emails you receive to reveal them.
25. Surf only to secure sites with a closed padlock and https: in the address line.
26. E-mails with numerous spelling and grammatical errors are usually bogus.
27. Check your monthly statements for suspicious or unusual entries.
28. Contact the companies if you are not receiving printed or online statements.
29. To get free credit reports from Experian, Equifax, and TransUnion, go to:  
<https://www.annualcreditreport.com/index.action>.
30. Place fraud alerts on your accounts. Report any suspicious activity immediately.
31. Open a new browser window each time you log on to a web site that displays personal information. When you are done at that site, log out and close that browser window.
32. Never do business with sites that have no street addresses or phone numbers.
33. If you lose your internet connection, use power cycling techniques.
34. When nothing else seems to work, restart the computer several times.
35. Keep your computer, keyboard, and mobile device screens clean.