Protecting Yourself Online
Prepared by Barry Cowen

Florida is the #1 scam and ID theft state in the USA. Seniors are the most vulnerable victims. Follow the tips below to protect yourself.

1. Wherever possible, use two factor authentication (multiple logins).
2. Find information on the individual(s) you are dealing with.
3. Learn how to conduct safe transactions. Use credit instead of debit.
4. Never give your password, Pin #, or SSN. If they ask, hang up.
5. Use different special purpose (spam, shopping, etc) e-mail addresses from different providers (Gmail and Microsoft are safest)
6. Buy a shredder and use it to dispose of confidential information.
7. Use the Private or Incognito mode in your browser(s).
8. Don't send money in any form to someone you don't know.
9. Don't reply to e-mail or text messages asking for personal or financial information. Don't click on unfamiliar links in e-mails.
10. Don't click on unfamiliar links in e-mails or text messages. (Phishing)
11. Don't call phone numbers included in an e-mail link or text message.
12. Verify company e-mail addresses and (toll-free) telephone #s.
13. If it sounds too good to be true, it probably is.
14. Don't agree to deposit a check and wire money back.
15. Never give away your PIN code. Report anyone who asks for it.
16. Report all suspicious e-mails to the appropriate parties.
17. Monitor all financial statements on a regular basis.
18. Get a free quarterly report from each credit bureau through annualcreditreport.com.
19. Stay alert
20. What have you got to lose? Everything if you're not careful.