What to do when your personal information has been compromised/How to be safe in our connected world.

1. Notify the police.
2. Nearly everyone's Social Security information has been compromised.
    a. What else should you protect?
        i. Home address, employment, all phone numbers, email, DOB, Place of Birth, best friends name, mother's maiden name, first dog's name, first school, first home, checking account number.
        ii. ALL passwords.
    b. What is best practice to protect your personal information (PI)?
        i. Limit use of PI for identification.
        ii. Do not allow vendors to store your credit cards.
        iii. Use complex passwords/use a password manager
        iv. Use Dual Factor/Multi Factor authentication
3. Report your PI compromises to: Visit https://identitytheft.gov
4. Lock your credit.
    a. Contact each of the Credit bureau's: Equifax, Experian, TransUnion.
    b. Download the Credit bureau APPs for your phone to turn it off and on.
5. Set your credit cards to notify you if someone is trying to access them.
    a. Every credit card company has this service, log into your account or call them and set it up.
6. Use Mobile payment systems from Apple or Android instead of Credit cards.
    a. It is more secure than using physical credit cards
7. RFID credit cards should be stored in a RFID protective sleeve or protective case/wallet/purse.
    a. You can buy sleeves on Amazon at reasonable prices.
8. Do not use Debit cards, get an ATM Card instead.
    a. Trade in your Debit card for an ATM Card.
    b. Use credit cards to make purchases and pay them off weekly, online.
        i. Use Credit card with no fee and that get rewards, do not carry a balance.
9. Do a Dark Web search to explore your exposure.
    a. It is NOT an exact science, but it will give you an idea to the extent your data is exposed.
    b. The big three Credit bureaus will do this once a year free.
    c. Your bank or credit card company may do it for free.
    d. You can subscribe to services that do it.
    e. Your employer may have the service.
10. Make sure you have good Antivirus on:
    a. ALL your PC's, Cell phone and tablets.
11. Employer and home networks should be protected.
    a. Every network you use should have a quality firewall.
    b. You should never just have an Internet Service providers Router.
12. Setup/use Dual Factor/Multi Factor Authentication for anything that allows it.
    a. Phone App's like Duo ($$) or Authy (free) can make this easier.
    b. Microsoft requires you use their Authenticator APP.
13. Do not store confidential information on your phone or in your contacts.
    a. Use a Password manager or Vault service.
    b. There will be a cost for this, your employer may help.
14. Other things to consider
    a. If you trade in a vehicle make sure to wipe all data out of the on-board systems, including integrated garage door opener.
    b. Shred EVERYTHING that has PI on it!
    c. Limit wireless use at your home and work and when used, make sure it uses the highest security possible.