PC Club General Meeting

April 12, 2016

Identity Theft

Are You a Victim? These signs are tip-offs!

1. You're contacted in attempt to collect an unknown debt or loan
2. You're contacted about delinquent rent, taxes, fines, etc.
3. You received a notice – usually delinquency – from an unknown credit card company.
4. Your bank(s) contact you about unusual – and often large – activity in your checking account.
5. You receive an alarming call, message or letter from the IRS, SSA, etc.

Q: What do I do if I find that I'm actually a victim of ID Theft?
A: Go to this website and get to work – this is going to require a lot of time and effort - https://www.identitytheft.gov/Steps [877-438-4338] You are encouraged to fill out their online form and use their experience, guidance and assistance.

What must you do now? [cited by Bank of America]

1. File the *fraud alert*.
2. Initiate a *credit freeze*. [it's good for only 90 days]
3. File the *ID Theft* report.
4. Contact these *Credit Bureaus:*
   a. Experian - http://www.experian.com/ [888-397-3742]
   b. Transunion - http://www.transunion.com/ [800-680-7289]
   c. Equifax - http://www.equifax.com/home/en_us [888-766-0008]
5. Establish an *extended fraud alert* (7yrs.)

What can you do to ***prevent*** ID Theft?

1. Obtain a current copy of your credit report.
   https://www.annualcreditreport.com/index.action

Visit this site and get one from each different once, once per year: January, May, September.

2. Place credit limits on your accounts and closely monitor all credit and debit cards.
3. Use *strong* passwords; if not using a password management app, change them every 90 days. Don't use *the same, or same few* passwords for all your online life.
4. Be extremely cautious when using public, free Wi-Fi!
5. Pause and think before clicking on email links or responding to requests for ANY of your personal information.
6. Don't put any personal information on web forms, applications, etc. *unless the site is encrypted* – shown as such by **https://** in the url. Often a padlock icon somewhere in the address box also indicates this security feature.
7. Use the "In-Private" features in web browsers: IE, Edge, Chrome, Firefox, etc.
8. If you travel with a laptop or tablet, secure it with appropriate software so it cannot be accessed by others.
9. Save at least one copy of all your key personal documents – financial, retirement plans and health – on an external storage device - USB drive, ext. HDD or CD. Remove it from your home and give it to a family member or trusted friend; or place it in a safety deposit box if available.

In addition – read the information available at the following websites:

https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services

http://www.idtheftinfo.org/

http://www.bbb.org/council/bbb-scam-stopper

http://www.huffingtonpost.com/adam-levin/consumer-reports-got-it-d_b_2904286.html [2014]

http://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm [2013]

http://www.topconsumerreviews.com/identity-theft/