Identity Theft

Strategies to Deter

1. Shred financial documents before discarding them - including credit card offers. On the credit card offer there might be a checkbox to change address. Go to www.optoutprescreen.com to reduce pre-approved credit card offers.
2. Reduce what comes to your mailbox. Leverage online statements.
3. Carry only what you need. Take out Social Security Number, blank checks, receipts, and excess Cash.
4. Pay with a credit card rather than debit card. That way you don't expose your bank account information. Credit card companies can reverse fraudulent charges. Banks would recover only up $500 if loss reported within 60 days.
5. Block RFID scanners. Many credit card companies have stopped sending out cards with RFID. You can identify them on the card by the antenna symbol. Call your credit card company to issue a card without RFID. RFID can be blocked by aluminum foil or carbon fiber.
6. Cloud Storage encrypts data, but most data breaches come from compromised passwords.
7. Properly remove digital data from devices before recycling them. Do a full hard reset on iPhones. Software tools: Gutman method. Could also physically destroy hard drive.
8. Passwords should be minimum 8 characters, multiple character types, use encrypted password storage applications such as Last Pass. Change your passwords at least once a year and do not save passwords on financial websites.
9. Limit use on public Wi-Fi. Use your own Mi-fi when travelling. Make sure you are logging into the right network. Pay for a VPN like NordVPN to encrypt your data.
10. Update virus scanners regularly. Virus scanners remove viruses from programs, documents and e-mail messages and prevent new infections.
11. File your taxes as early as possible to prevent someone from filing taxes under your Social Security Number.

Identity Theft Detection

1. Be alert: Mail or bills that don't arrive. Denials of credit for no reason. Google yourself!
2. Inspect your credit report at least once a year: www.annualcreditreport.com
3. Inspect financial statements at least once a month: look for charges you did not make.

Strategies to Defend

1. Report identity theft to the police and Federal Trade Commission, www.ftc.gov.
2. Put a fraud alert on accounts by calling your financial institutions. Ask financial institution about their policy if someone steals money from account through security breach at firm.
3. Check homeowners' policy for ID theft provisions.

Other tips:

1. Get rid of your Yahoo or Sbcglobal email and use Gmail. Older addresses signal that you are older and may be more vulnerable to attacks.
2. Do not use USB changing stations at Starbucks or airports. Hackers can download your data from your phone. Bring your own charger.
3. Do not allow kids to use your phone. Downloaded apps could rob your data. The FBI cannot track down developers in the Cayman Islands or British Virgin Islands.
4. Change the default password on your routers. Default passwords can be found online.
5. Remove old applications from your computers. Old software is lacking in security updates.

Khloé U. Karova, CFP® can be reached at khloe@moderncapitalconepts.com. Financial planning updates can be found at www.facebook.com/moderncapitalconcepts.