The Attorney General of Florida provides some excellent tips to help protect teens against cyber danger. If you feel uncomfortable while surfing on the web, you can report it:

- To a parent or other trusted adult
- To the CyberTipLine (https://secure.missingkids.com/CyberTipline) at the National Center for Missing and Exploited Children, or call 1-800-THE-LOST

Source: Internet Safety for Teens http://www.safeflorida.net (accessed August 1, 2014).

Identity Theft

An identity thief does not need to be a genius. It is actually very simple to steal an identity. Remember the BIG THREE? **All an identity thief requires is your: 1) name, 2) date of birth, and 3) social security number.** While the majority of **identity theft** is low tech (i.e. stealing a credit card, purse, or financial statements), high tech **identity theft** is on the rise. According to the FBI, a stolen identity is a "powerful cloak of anonymity for criminals and terrorists." It is also a danger to private citizens. The primary way an identity thief steals your identity is not by stealing information. Rather, they use **social engineering**; they use deception to make people provide information themselves. They may call or send emails pretending to be the victim's bank or credit-card company. Then they ask for account numbers, PIN's and other information. Do not provide this information! Also beware of the following:

1) **Hacking:** There are three major Consumer Reporting Agencies **CRA's**: Experian, TransUnion, and Equifax: All three have been hacked into. This is part of organized crime. Thieves hoard information and sell identities. How does this all happen? In many cases, the hacking occurs either by someone inside or by an insider providing access.
2) **Cracking:** A **hacker** can bombard a network with data. For example, a **hacker** can send several hundred spam emails and inundate a system until it shuts down. Then the **hacker** can gain access into a system and hoard information to sell.
3) **Tracking:** There are ways that identity thieves can track and record your information off of your debit/credit cards. Here are two examples:
    a. Clone Debit Cards: There are small devices that attach to debit machines and record data. These are usually insider jobs. In order to avoid this problem, do not let someone walk away with your card. Observe them as they scan your card into the official machine.
    b. **Gypsy ATM's:** These are ATM machines that are not connected to a network. You can put in a debit card and most often withdraw small amounts of money. However, these are not connected to a bank and while your card is inside, they track or record all of your data. In order to avoid these, find your own bank machine. It will be more secure. If a bank machine looks suspicious: DON'T USE IT!

Source: http://www.fbi.gov/about-us/investigate/cyber/identity_theft (accessed, August 2, 2014)

How To Avoid Indentity Theft:

The Federal Trade Commission (FTC) states that your personal information is valuable. They provide tips on how to protect your information and online identity:

1. Limit unwanted messages.
2. Use computer security to protect against scammers, **hackers**, and identity thieves.
3. Protect your identity: keep important papers secure and shred, shred, shred documents with sensitive information.

How To Stop Indentity Theft:

1) Get copies of your credit reports. You are entitled to obtain, one from each of the three major credit bureaus (Equifax, Trans Union, Experian) per year. Go to the http://ftc.gov and link on Identity Theft and read how to get a free credit report. Read and look at credit report. Report any suspicious activity to these agencies. Take initiative. Once a victim, you need to make it right. Contact these people!
2) Demand notices and statements: Demand that companies send notices and statements in the mail and keep a record that they arrive. This way you will know that someone else is not intercepting your mail.
3) Do not give out information to someone on the phone. One day you may get a call and the person will say, "We have found your personal data." Never provide info over the phone. Do it in person. If they don't want to meet in person it is probably a scam.

Source: Federal Trade Commission, Consumer Education, Identity Theft http://www.consumer.ftc.gov/features/feature-0014-identity-theft (accessed August 7, 2014)

For more information: Visit websites like OnGuardOnline.gov, which provide tips from the federal government and technology industry to help you: 1) defend yourself against internet fraud; 2) defend your computer; and, 3) defend your personal information online.

Recap: What important points have you learned so far about Identity Theft?

_____

_____

_____

What To Do If You Think Your Identity Has Been Stolen

Oh no! You think you may be a victim of identity theft. Well, never fear, MyFloridaLegal.com is here, to help guide you through the processes. The following is a shortened version of what you will find in the online **Florida Identity Theft Victim Kit:**

1) Report the incident to the fraud department of the three major **Consumer Reporting Agencies, CRA's** (Equifax, Trans Union, Experian) Ask them to place a "fraud alert" on your credit reports. Request a victim statement. Keep a log that notes with whom you talked and what you told them.
    a. Equifax P.O. Box 740241 Atlanta, GA 30374-0241 To order your report: 1-800-685-1111 To report fraud: 1-800-525-6285 TDD: 800-255-0056 www.equifax.com
    b. TransUnion Fraud Victim Assistance P.O. Box 6790 Fullerton, CA 92634-6790 Email: fvad@transunion.com To order your report: 1-800-888-4213 To report fraud: 1-800-680-7289 TDD: 877-553-7803 www.transunion.com
    c. Experian P.O. Box 9532 Allen, TX 75013 To order your report: 1-888-EXPERIAN (397-3742) To report fraud: 1-888-EXPERIAN (397-3742) TDD: 800-972-0322 www.experian.com
2) Contact the fraud department of your creditors. Follow up in writing and include: The Federal Trade Commission provides an **Identity Theft Affidavit** (attached), a standardized form used to report new accounts fraudulently opened in your name. Phone the Federal Trade Commission at 1-877-IDTHEFT (438-4338) Request: "Identity Crime: When Bad Things Happen to Your Good Name." This brochures is available through their website at http://www.ftc.gov and contains information on solving credit difficulties and sample dispute letters.

3) Contact your bank or credit union.

a. If you think your accounts are compromised, cancel accounts and obtain new numbers.

b. Call SCAN at 1-800-262-7771 to find out if someone has passed bad checks using your name.

c. If checks have been stolen, stop payment. Contact the check verification companies. Request they notify retailers not to accept your checks:

i. **TeleCheck** 1-800-710-9898 or 927-0188

ii. **Cetergy, Inc** 1-800-437-5120

iii. **International Check Services** 1-800-631-9656

4) Report to the Police

a. Contact the local police to file a report.

b. Provide as much information as you can when you file the report.

c. Request a copy of the report to provide to creditors.

Source: Florida Office of the Attorney General: Florida's Identity Theft Victim Kit
http://myfloridalegal.com/pages.nsf/Main/CBBEBA3F2583433385256DBA004BC600?OpenDocument (accessed August 7, 2014)

For extra information (and some fun) use the ID Theft Interactive FaceOff
http://www.onguardonline.gov/games/id-theft-faceoff.aspx

Based on the information in the text and from online sources, what would you do if your identity were stolen?

_____

_____

_____

Now that you have become an expert in Internet Safety and Identity Theft, review your knowledge:

1) What are the **three** vital pieces of information a thief needs to steal your identity?

a. _____ b. _____

c. _____

2) The **three** major credit reporting bureaus are:

a. _____ b. _____

c. _____

3) What are some ways to avoid identity theft? _____

_____

4) What are the four steps you should take if you think you are a victim of identity theft?

a. _____ b. _____

c. _____ d. _____

5) List safety tips for shopping online: _____

_____