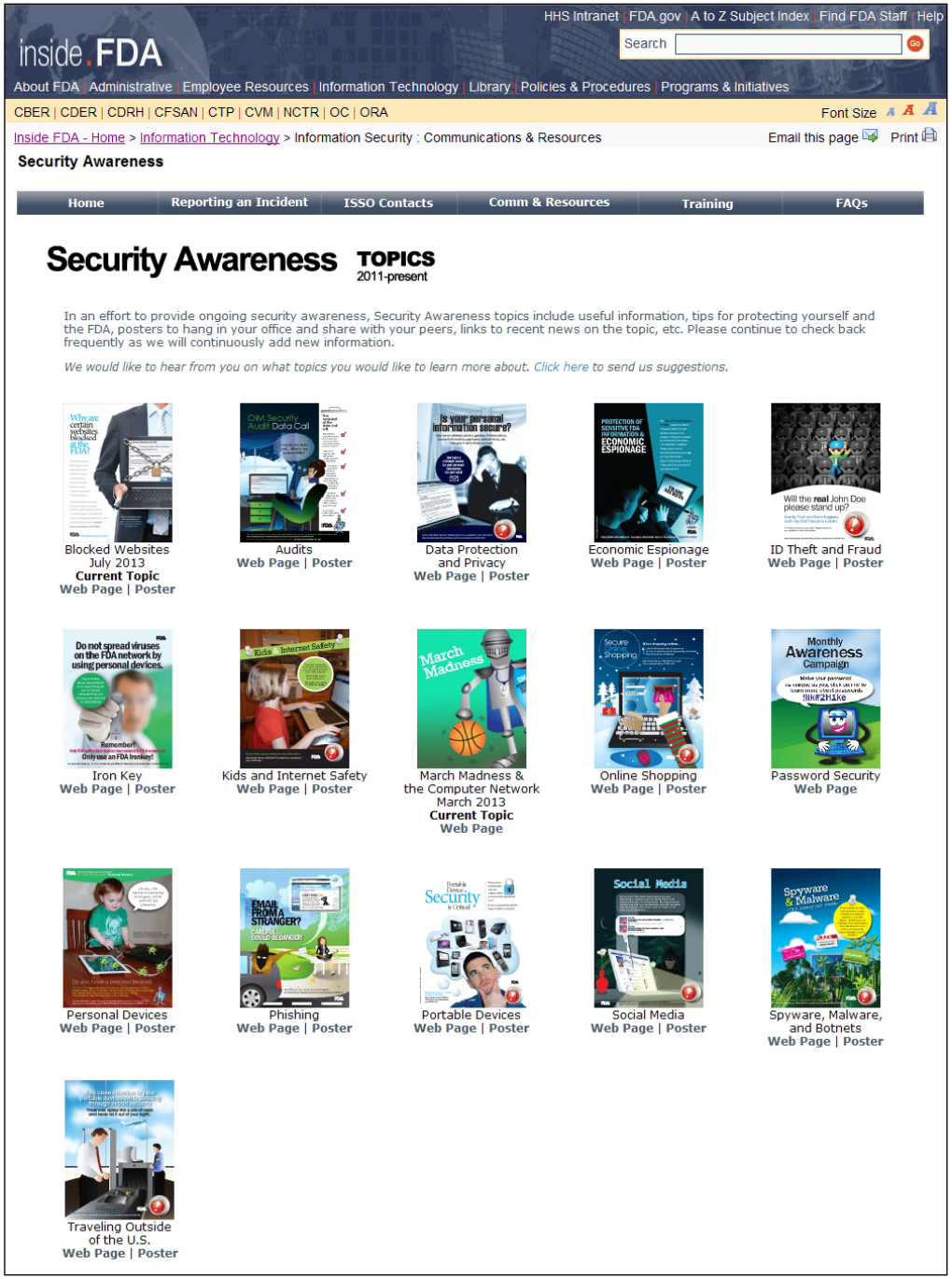


FDA Security Awareness Web Site

The Security Awareness Web Site provides ongoing security awareness including useful security awareness topics, tips for protecting yourself and the FDA, posters to hang in your office and share with your peers, links to recent news on the topic, etc.

Highlighted pages include:

- Data Protection and Privacy
- Identity Theft and Fraud
- Online Shopping
- Social Media

Data Protection and Privacy

The Data Protection and Privacy Security Awareness page includes an explanation of Personally Identifiable Information (PII), why we need to protect PII, FDA Policy, facts, news, posters, and additional resources/guidance.

HHS Intranet | FDA.gov | A to Z Subject Index | Find FDA Staff | Help

inside.FDA

Search

About FDA | Administrative | Employee Resources | Information Technology | Library | Policies & Procedures | Programs & Initiatives

CBER | CDER | CDRH | CFSAN | CTP | CVM | NCTR | OC | ORA

Font Size

Inside FDA - Home > Information Technology > Information Security : Communications & Resources

Email this page Print

ID Theft & Fraud

Home | Reporting an Incident | ISSO Contacts | Comm & Resources | Training | FAQs

Identity Theft and Fraud Security Awareness

Identity theft is the criminal act of stealing an individual's identity. According to the FTC, this issue affects as many as 11 million Americans each year.

There are several different types of identity theft:

- **Financial Identity Theft** – Involves stolen personal information to get access to your money or credit. Financial identity theft is the most common, because it is profitable and often hard to trace.
- **Criminal/Impersonation** – When someone assumes the identity of another person.
- **Medical Identity Theft** – When an imposter steals medical insurance or health record information to receive benefits such as treatments and/or prescriptions in another person's name.
- **Child Identity Theft** – When someone steals the identity of a child or infant. A child's Social Security number could be used to obtain a driver's license or a credit card, and may be used for many years before the young victim becomes aware of the issue. The child victim may start life credited with someone else's criminal record or bad credit rating.

Helpful Resources:

For more information on protecting yourself from identity theft and fraud, check out the following brochures from the **Federal Trade Commission (FTC)**:

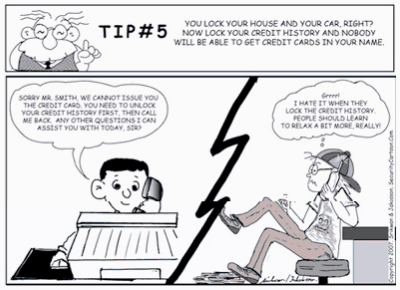
- 10 Things You Can Do to Avoid Fraud
- Fighting Back Against Identity Theft
- 10 Ways to Avoid Identity Theft While Traveling
- 5 Things You Probably Didn't Know About Identity Theft

For more information from FTC on what to do if you are a victim of identity theft and fraud go to the following link:

- Taking Charge: What to do if your Identity is Stolen

Here are common ways identity theft happens and how to protect yourself:

- **Data Breach** – When personal or financial information is stolen from a government or company network. In November and December 2013, as many as 40 million credit and debit cards may have been compromised as the result of a Target department store point of sale network data breach: http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228
  - **How to protect yourself**- *Monitor credit card and financial statements carefully for suspicious transactions, and periodically request free credit reports from annualcreditreport.com to look for unauthorized accounts.*
- **Hacking** – A person or group hack into your email or your online accounts to access personal or financial information.
  - **How to protect yourself** - *Use complex passwords and do not use the same password for every account. Use and maintain anti-virus software and a firewall. For further information about password security click here.*
- **Phishing** – Messages that appear to be legitimate messages from a person, institution, company or government agency, but are actually messages intended to trick the recipient into revealing personal information or to compromise their systems.
  - **How to protect yourself** – *Do not open email attachments or click on links received from unknown senders. Use caution when providing information. Double and triple check the person(s) you are dealing with are legitimate. For further information about phishing click here.*
- **Dumpster Diving** – Thieves go through your trash looking for anything that has personal information on it (such as bills, junk mail, anything with your Social Security number, etc).
  - **How to protect yourself** – *Shred or burn anything that contains personal information on it.*
- **Skimming** – This happens when you use an ATM machine that has been compromised, or when your card is run through a phony card reader. The devices obtain your card information from the magnetic strip on the back of your card. This information can then be used to access your account or produce a fake credit card with your name and details on it.
  - **How to protect yourself**- *Be vigilant when you use your credit, debit, or ATM card, and checking your account activity on a regular basis. When possible, use an ATM in a relatively secure location such as a bank lobby. Avoid using ATMs that a criminal might be able to place or access freely, such as free- standing ATMs in public places like convenience stores or on the street. In addition, be wary of an ATM machine that has loose parts or otherwise looks suspicious. Some ATM skimmers use small cameras to film a victim entering their PIN number, so consider covering your hand as you type your PIN.*
- **"Old-Fashioned" Stealing** – Thieves will steal wallets, purses, pre-approved credit offers, tax information to name a few.
  - **How to protect yourself** – *When you are out, be aware of your surroundings and keep your personal items with you at all times. Pick up your mail every day and have it placed on hold when you are out of town.*



Reproduced with permission. Please visit www.SecurityCartoon.com for more material.

If you feel you are a victim of Identity Theft, FTC recommends the following three immediate steps to protect yourself:

- **Place a Fraud Alert with one of the following Credit Reporting Companies (they will alert the other two):**
  - **Equifax** - 1-800-525-6285
  - **Experian** - 1-888-397-3742
  - **TransUnion** - 1-800-680-7289

Identity Theft and Fraud

The Identity Theft and Fraud Awareness page includes helpful information on the various types of identity theft, methods of stealing data and ways to protect yourself, helpful tips, facts, posters, and additional resources/guidance.

Online Shopping

Shopping online is popular and convenient, but users need to be aware of the security risks involved. The Online Shopping Awareness page shares a few simple precautions and resources to prevent cyber criminals from spoiling the online shopping experience.

Social Media

The purpose of the Social Media Security Awareness page is to help users understand the safety measures recommended when utilizing social media. The page includes facts, resources, tips, posters, and guidance for using social media at the FDA to protect yourself.