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.
Identity Theft and Fraud 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 gain access to your money or credit. Financial identity theft is the most common, because it is profitable and often hard to trace.
- **Criminal Identity Fraud** - When someone assumes the identity of another person.
- **Medical Identity Theft** - When an impostor 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.

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.infosecurityweek.com/security/attacks-and-breaches/target-breach-16-facts/d/diff-1112228
- **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 hacking 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 provided by 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.
- **Dumsters 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 skimmer 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 alert 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 any 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.

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

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.

Online Shopping Security Awareness

Shopping online is popular and convenient, but be aware of the security risks involved. Take a few simple precautions to prevent cyber criminals from spoiling your online experience.

How do hackers target online shoppers?

There are three common ways that hackers take advantage of online shoppers:

- **Targeting vulnerable computers**: If you do not take steps to protect your computer from viruses or other malicious code, hackers may be able to gain access to your computer and all of the information on it.
- **Creating fraudulent sites and email messages**: It is relatively easy for cyber criminals to create fake shopping websites or phishing messages that appear to have come from a business. Hackers create these malicious sites and email messages to try to trick you into giving them personal and financial information. If you enter a username and password, or credit card number into the wrong site, a cyber criminal could go on a shopping spree using your information!
- **Intercepting insecure transactions**: If a vendor does not use encryption, hackers may be able to intercept your information as it is being transmitted.

How can you protect yourself?

- **Use and maintain anti-virus software, a firewall, and anti-spyware software**: Use antivirus and firewall software to protect yourself against viruses and Trojan horses that may try to steal or modify the data on your own computer. Make sure to keep your virus definitions up to date.
- **Keep software, particularly your web browser, up to date**: Hackers take advantage of known software vulnerabilities, so install software updates and security patches. Many operating systems offer automatic updates.
- **Evaluate your software’s settings**: The default settings of most software enable all available functionality. It is especially important to check the settings for software that connects to the Internet (browsers, email clients, etc.). Apply the highest level of security available that still gives you the functionality you need.
- **Conduct business with reputable vendors**: Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Hackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information.
- **Look for third-party seals of approval**: Although it is not a guarantee that a site is safe, look for labels such as Better Business Bureau Online (BBBOnline), Truste, Norton Secured Seal, and McAfee SECURE symbol. Click on the seal to make sure it links to the organization that created them.

- **Find out what other shoppers say**: Sites like Epinions.com or BizRate have customer evaluations which can help you determine a company’s legitimacy.
- **Be wary of emails requesting information**: Hackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email and use caution when clicking on links in email messages.
- **Check privacy policies**: Before providing personal or financial information, check the website’s privacy policy. Make sure you understand how your information will be stored and used.
- **Make sure your information is being encrypted**: Many sites use SSL, or secure sockets layer, to encrypt information. Indicate that your information will be encrypted by the URL, which begins with “https,” instead of “http,” and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser; for example, it may be to the right of the address bar or at the bottom of the window. Hackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
- **Use a credit card**: A debit card draws money directly from your bank account; unauthorized charges could leave you with insufficient funds to pay other bills. If you recognize fraudulent charges and report them promptly, credit card companies may minimize your liability. Consider dedicating a single credit card with a low credit line for all of your online purchases.
- **Avoid shopping from your mobile phone**: If your phone is lost, stolen, or remotely hacked, your personal information could be exposed. Create and use a unique PIN number to access your smart phone.
- **Check your statements**: Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.
- **Trust your instincts**: If a deal appears too good to be true, it probably is. Scammers target popular shopping days such as Black Friday (the day after Thanksgiving), Cyber Monday, and Christmas to advertise fake deals.
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.