

Security Awareness TOPICS

2011-present

In an effort to provide ongoing security awareness, Security Awareness topics include useful information, 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. Please continue to check back frequently as we will continuously add new information.

We would like to hear from you on what topics you would like to learn more about. [Click here to send us suggestions.](#)



Blocked Websites
July 2013
Current Topic
Web Page | Poster



Audits
Web Page | Poster



Data Protection and Privacy
Web Page | Poster



Economic Espionage
Web Page | Poster



ID Theft and Fraud
Web Page | Poster



Iron Key
Web Page | Poster



Kids and Internet Safety
Web Page | Poster



March Madness & the Computer Network
March 2013
Current Topic
Web Page



Online Shopping
Web Page | Poster



Password Security
Web Page



Personal Devices
Web Page | Poster



Phishing
Web Page | Poster



Portable Devices
Web Page | Poster



Social Media
Web Page | Poster



Spyware, Malware, and Botnets
Web Page | Poster



Traveling Outside of the U.S.
Web Page | Poster

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



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

inside.FDA

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

Data Protection and Privacy Security Awareness

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

Data Protection and Privacy Security Awareness

Why do we need to protect data and personal information?

- Good security and business practices
- Federal and state laws require companies and Agency's to protect data and the privacy of individuals

Here are a few of the laws:

- Fair Credit Reporting Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach Bliley Act
- The Privacy Act of 1974

To find out more information on the laws above please visit: <http://business.ftc.gov/documents/art08-protecting-personal-information-know-why>

FDA invests in state-of-the-art technical controls to protect our assets. Even so, we rely on individuals to protect sensitive information. No matter how much is spent, one careless action can compromise the best technical controls.

FDA Policy

For more information on protecting FDA data, please reference SMG 3253.4 at the following link: <http://inside.fda.gov:9003/PolicyProcedures/StaffManualGuide/VolumeIIIGeneralAdministration/UCM007299>

If you are uncertain if data (i.e. documents, files, etc) is sensitive or contains Personally Identifiable Information (PII), ask for help. When in doubt, contact your Freedom of Information Act (FOIA)/Privacy Act Officer for guidance or your Center Information System Security Officer (ISSO).

What is PII?

PII is information that directly identifies an individual (i.e. name, address, social security number or other identifying number or code, telephone number, email address, etc), or by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

Did You Know?

Individuals who fail to follow specific requirements of the Privacy Act may be charged with a misdemeanor and fined up to \$5,000 per violation.

Here are few **GOOD** habits to follow that may reduce the chances that you and/or the Agency's information on a computer will be lost or corrupted.

- **Lock your computer when you are away from it.** Even if you step away for a few minutes, that is enough time for someone else to destroy or corrupt information on your computer. Locking your computer will prevent another person from accessing information on it.
- **Disconnect your computer from the network (Internet) when you are not using it.** High speed Internet (DSL, Cable, FIOS) has made it possible for users to be online all the time, but this convenience comes with risks. Attackers are always scanning the network for computers that are online. If your computer is always connected then it may become a target. Disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting the cables. When you are connected, make sure that you have a firewall enabled.
- **Evaluate your security settings.** Enabling certain features on software, web browsers, social networking sites, and email programs in order to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at risk. If you install a patch or a new version of software, reevaluate your settings to make sure they are still appropriate.

Keep in mind that all threats are not from other people, but can be from a natural or technological cause. Here are some steps you can take to help minimize the damage.

- **Protect your computer against power surges and brief outages.** Some power strips will protect your computer against power surges. There are products that offer an uninterrupted power supply when there are power surges or outages. During a lightning storm consider shutting your computer down and unplugging it from all power sources.
- **Back up all your data.** No system is completely secure so you should regularly back up your data to CDs, an encrypted flash drive, or a network. Determining how often to back up your data is a personal decision. Remember that your FDA systems are intended for business use, and should not be used for large numbers of personal photos. If there is a business need for storage space on the network, you might lose large personal photo files without notice. If you add or change data for business use frequently, you may find weekly backups to be the best; if you rarely make changes, you may decide that your backups do not need to be as regular.

Remember: Protecting privacy is everyone's responsibility! Avoid providing personal information such as your birth date and social security number online!

Helpful Resources:

For more information on protecting FDA data, please reference policy SMG 3253.4 at the following link:
[Policy SMG 3253.4](#)

Also, please check out the Personally Identifiable Information (PII) training guide from the HHS Cybersecurity Program:
[PII Training Guide](#)

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.

ID Theft & Fraud

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

Identity Theft and Fraud...
happens each day. Don't become a victim.

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 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.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/4-id/1113228>
 - o **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.
 - o **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.
 - o **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).
 - o **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.
 - o **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.
 - o **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):**
 - o Equifax - 1-800-525-6285
 - o Experian - 1-888-397-3742
 - o TransUnion - 1-800-680-7289

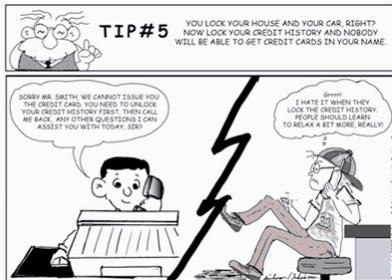
Helpful Resources:

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



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

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 Security Awareness**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.

Helpful Resources:

For more information on online shopping, please reference the following resources:

- OnGuard Online:
[Shopping Online](#)
- Better Business Bureau (BBB):
[BBB Tips for Holiday Budgeting and Shopping](#)
- United States Computer Emergency Readiness Team (US-CERT):
[Shopping Safely Online](#)
- Microsoft:
[Six Rules for Safer Financial Transactions Online](#)



- **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. Indications that your information will be encrypted include a URL that 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 Eve to advertise fake deals.



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 Security Awareness



Social Media Awareness

Social Media includes forms of electronic communication (such as web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, videos and other content. Social media includes networking sites such as Facebook and LinkedIn, content communities like YouTube, blogs and microblogs as with Twitter and virtual social worlds such as Second Life.

Social media sites have both a positive and negative effect on today's technology world. These sites have created a way to get useful information out to a specific audience, such as job openings or sharing videos with family in other parts of the country or even the world. It is important to understand the safety measures you should take when utilizing social media. Below is some guidance for using social media at the FDA as well as tips for protecting yourself.



FDA Guidance for Using Social Media

- Do not use your FDA or any government email address for personal social networking accounts.
- Do not engage in discussions of opinion about FDA's actions or initiatives.
- FDA users with social networking accounts as part of their job should abide by the FDA's Guidance for representing FDA using Web 2.0-Social Media.
- Whenever a user provides an affiliation with FDA (whether implicitly or explicitly), they will not make any political or social advocacy statement or product/service endorsements.

In the news:
When, Why and How to Permanently Delete Your Facebook Account:
<http://blog.kaspersky.com/delete-facebook-account/>

How to Protect Yourself Personally

- Remember! Everything you post online becomes accessible by others forever!
- Do not post:
 - Information about events you are attending or vacations you are taking that will let people know you will not be home. Social networking sites such as Facebook offer services like Foursquare which allow users to "check in" at their current locations.
 - Personally identifiable information about yourself (i.e. address, phone numbers, etc).
 - Be wary of any photos you post. They could identify where you live, work or spend your free time. Also people can easily gain access to your photos and alter or share them with others.
- Protect your privacy by enabling all privacy settings on social networking sites.
- Do not give anyone on a social networking site your credit card or account information because it could be a phishing scam. If you are directed to a web site, check for privacy policies and third-party seal of approvals such as Better Business Bureau Online (BBBOnline) or Truste.
- Keep your computer's software up to date to minimize vulnerabilities.

Interesting Facts

- People spend more than 700 billion minutes per month on Facebook.
- Twitter is adding nearly 500,000 users per day.
- More than 2.5 million web sites have integrated with Facebook.
- More than 350 million active users currently access Facebook through their mobile devices.
- As of November 3, 2011, LinkedIn operates the world's largest professional network on the Internet with more than 135 million members in over 200 countries and territories. Fifty-nine percent of LinkedIn members are currently located outside of the United States.
- More than 800 million active users are on Facebook and the average user has 130 friends.

Note: Some of the content was provided by Merriam Webster, jeffbullas.com, facebook.com, and linkedin.com.

Other Resources:

- [HHS Intranet - Social Media: 5 Ways to Protect Yourself Online](#)
- [HHS Intranet - 5 Riskiest Social Media Sites](#)

Posters

[Social Media Poster](#)



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.