# Security Awareness - Personal Identifiable Information & Identity Theft

Last Updated: 04/25/2013
Overview

There are important things that you can do to protect your own personal identity and critical responsibilities that anyone who works with CABQ data must be aware of.

Identity theft criminals are always looking for new ways to get your personal information. This can range from digging through your trash to sending malicious e-mail messages to deceive you. There are important steps to take to make sure your personal information, such as credit card numbers, bank account information, Social Security Number, passwords, or other sensitive information, is not exposed. Here are some recommendations to help protect you against identity thieves.

- If you get an e-mail or pop-up message that asks for personal or financial information, do not reply; in fact don't even click on the link in the message. Legitimate companies don't ask for this information via e-mail. If you are concerned about your account, contact the organization in the e-mail using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- Be cautious of browser add-ons that websites may push to allow access to content.
- Use anti-spyware to protect your computer. CABQ utilizes anti-spyware on their central email services
- Don't e-mail personal or financial information. E-mail is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a web site that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus and keep it up-to-date. Some phishing e-mails contain malicious software that can harm your computer or track your activities on the Internet without your knowledge.
- Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.
- Always keep your browser software up to date

If you get a message that is phishing for personal information, contact the ITSD Service Desk (helpdesk@cabq.gov or 768-2930) to find out if it has been reported. If you are able to confirm that the message in question has not yet been reported, then it should be forwarded, with full headers, to the ITSD Service Desk.

## Each of our Responsibilities

CABQ employees have access to, and are responsible for protecting, a wide variety of sensitive information. Unauthorized exposure of information such as credit card information, and social security numbers can have a harmful effect on people's lives. Failure to take care of this information places people at risk of identity theft, misuse of personal funds, or unauthorized modification of information. We therefore all have a responsibility to educate ourselves on how best to protect the information we store electronically. ITSD has specific requirements intended to ensure adequate protection of information we store from potential risks such as loss or modification. It is your responsibility to be aware of and understand these policies and procedures.

In an effort to better secure sensitive data at CABQ, the ITSD Security Office has compiled this quick reference guide for private data. This type of data should not be stored on workstations or mobile computing devices (laptops, PDAs, flash drives, etc) unless a strong business need exists and proper security precautions have been taken.

Private data and some common occurrences:

- Social security numbers
    - Administrative documents like travel authorizations from prior to the use of employee ID
    - Documents requesting changes to benefits that might include the SSNs of family members
- Credit card numbers
    - Orders or receipts for purchases using Credit Cards/PCards

- Personally identifiable information that could be used for identity theft
    - Documents containing combinations of information like name, birth date, address, drivers license number, etc Bank account information
    -
    - Documents regarding employee direct deposit
- Medical records
    - Patient records

Important practices to keep in mind when dealing with private data include:

- Never post private data on the web
- Never send private data via e-mail
- It is best to store sensitive information on servers rather than desktop computers. Those can either be servers maintained by your organizational unit or provided by ITSD. Unfortunately, you can't always trust that your information is safe on a desktop or laptop computer.
- If you think you might have sensitive information on a desktop computer, contact ITSD or your supervisor to have them help you remove the data or move your information to a secure server.
- If for some reason you can't store your sensitive information on a server, ensure that the data is encrypted and backed up. If you are unsure how to do this, ITS can help you.
- Use your CABQ account and password to login to the network; never share your account or password with others.
- Whenever feasible, use complex passwords on any system storing sensitive information.
- Always enable your screen saver to lock your computer during inactivity and require it to be password protected.
- Always have current antivirus software installed and keep your security patches up to date.
- Always ensure sensitive information sent or received via email or at a web site is encrypted.
- Always destroy electronic media containing sensitive information prior to its decommission.
- Always securely remove all sensitive information from electronic media before re-using it.
- Make an inventory of the sensitive information your department uses or stores
- Obtain supervisor permission to remove sensitive information from the office.
- On mobile devices and workstations, limit the amount of information stored to the minimum necessary needed to do your job. Encryption on mobile devices is critical to prevent data loss in the event of a loss or stolen device.

## Learn More

See Protecting Private Information for more information on protecting portable devices