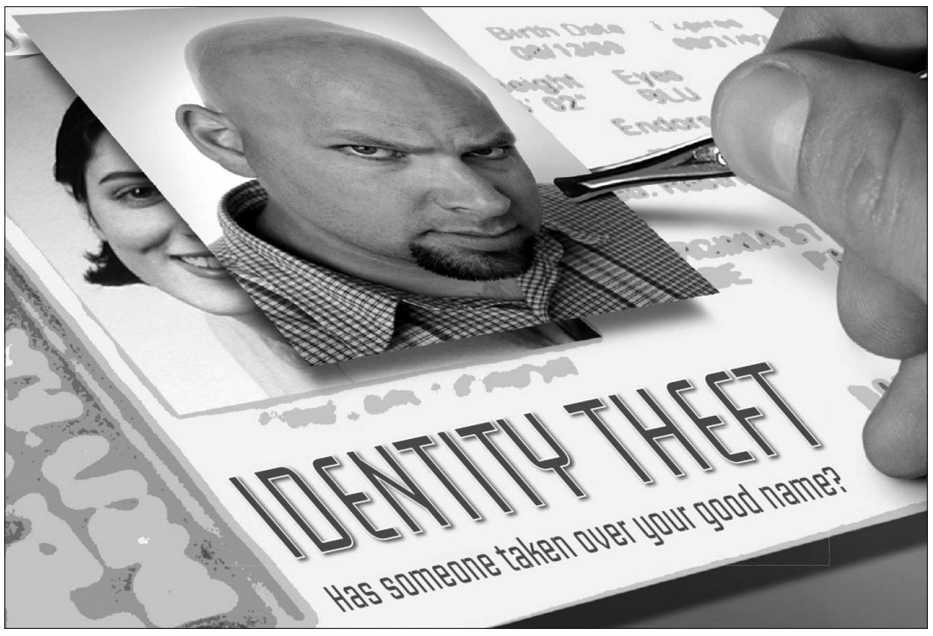
Identity theft: Protection measures everyone should know

By Jeffrey C. Doepp, CFAY Public Affairs

On any given day onboard Commander Fleet Activities Yokosuka (CFAY) you may write a check at the commissary, purchase Japanese baseball game tickets with a credit card at the Morale, Welfare and Recreation Information, Tours and Ticketing Office, rent a car from the Navy Exchange, mail your tax returns, change service providers for your cell phone out in town, or apply for a credit card online. You probably wouldn't give these everyday transactions a second thought, but an identity thief might.

Identity theft is a serious crime. People whose identities have been stolen can spend several months or maybe years and thousands of dollars cleaning up the mess the thieves have made of a good name and credit record.



According to data from a 2010 Identity Fraud Survey Report from www.fightidentitytheft.com, 11.1 million people in the United States became a victim of identity fraud at a total cost of $54 billion in 2010. Despite any best efforts to manage the flow of personal information or to keep it safe, skilled identity thieves may use a variety of methods to gain access to the data.

Image courtesy of id-protect.org

According to data from a 2010 Identity Fraud Survey Report, from www.fightidentitytheft.com, last year, 11.1 million people in the United States became a victim of identity fraud at a total cost of $54 billion - up 37 percent since 2007. Victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit.

Despite any best efforts to manage the flow of personal information or to keep it safe, skilled identity thieves may use a variety of methods to gain access to the data.

"Identity thieves get information from businesses or other institutions by stealing records or information while they're on the job, bribing an employee who has access to these records, hacking these records or conning information out of employees," said Naval Criminal Investigative Service (NCIS) Yokosuka Special Agent Anthony Britt.

"Additionally, identity thieves may steal your mail, including bank and credit card statements, new checks and tax information. They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as 'dumpster diving,'" Britt said. "Identity thieves may steal your wallet or purse. They may complete a 'change of address form' to divert your mail to another location. And, they may steal personal information they find in your home."

According to the Federal Trade Commission (FTC), in order to protect yourself from possible identity theft, don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and pose as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their social security number (SSN), mother's maiden name, account numbers, and other identifying information.

"Before you share any personal information, confirm that you are dealing with a legitimate organization," said Britt. "Check an organization's website by typing its web address in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly."

Additionally, the FTC recommends you treat your mail and trash carefully. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding and credit offers you get in the mail. To stop receiving offers of credit in the mail, call: 1-888-567-8688). The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. Other ways to protect from identity theft are:

• Don't carry your SSN card; leave it in a secure place.

• Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your policy number.

• Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

• Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

• Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

• When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

According to CFAY Security Manager Tara Houlden, depending on what your personal computer is used for, an identity thief may not need to set foot in your house to steal your personal identifying information (PII).

"If you store PII such as your SSN, financial records, military orders, tax returns, birth date and bank account numbers on your computer, you may be at risk of identity theft," Houlden said.

Houlden offers up the following tips that can help you keep your computer - and the PII it stores, safe.

• Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files or passwords.

"Ideally, virus protection software should be set to automatically update each week," Houlden said. "The operating system can be set to automatically check for updates and download them to your computer."

• Don't open files, click on hyperlinks or download programs sent to you by strangers. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.

• Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

"Use a secure browser, which is software that encrypts or scrambles information you send through the Internet to guard your online transactions," said Houlden. "Be sure you are using the latest version available from the manufacturer. You can also download some secure browsers for free from the Internet."

• Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password a combination of upper and lower case letters, numbers and symbols. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. So, if your laptop is stolen, it's harder for a thief to obtain your personal information.

"Before you dispose of a computer, delete all the PII it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive," Houlden said.

• Look for website privacy policies. They should answer questions about maintaining accuracy, access, security and control of PII collected by the site, how the information will be used, and whether it will be provided to third parties.

"Identity thieves may also be able to steal PII from you through email or phone by posing as legitimate companies claiming that you have a problem with your account. This practice is known as phishing online, or pretexting by phone. Legitimate companies, especially your bank and credit card companies, will never notify you of account issues and errors with a generic email. They will require you to log in to their secure system in order to address the issue," Houlden added.

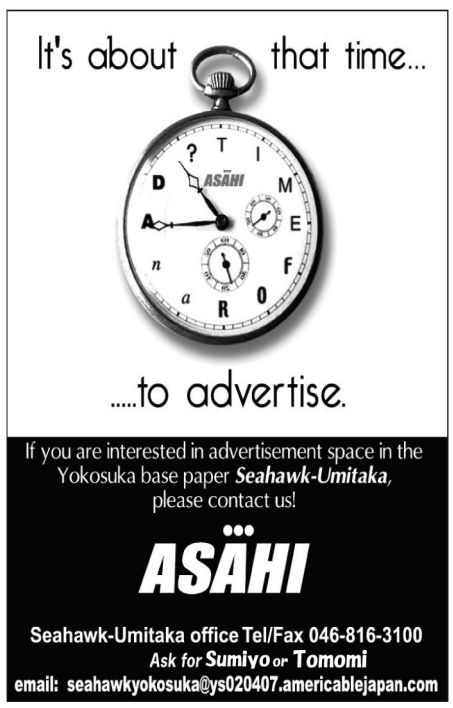
If you've lost personal information or identification, or if it has been stolen from you, the FTC recommends you perform the following steps quickly, to minimize the potential for identity theft:

• Close all financial accounts, like credit cards and bank accounts, immediately. After you have created a new account, place a password on it. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

• Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. An alert can help stop someone from opening new credit accounts in your name.

• Contact the agency that issued the driver's license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you've taken these precautions, watch for signs that your information is being misused. If your information has been misused, file a report about the theft with the police, and file a complaint with the FTC, as well. If another crime was committed for example, such as your purse or wallet was stolen or your house or car was broken into, report the incident to the police immediately.

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then.