Identity theft: Are you the next target?

By MC1 (AW) Tim Comerford: The Flagship Staff Writer

NORFOLK-- The Naval Criminal Investigative Service (NCIS) is promoting identity theft awareness for service members around Hampton Roads.

“Identity theft is acquiring key pieces of someone’s identifying information in order to impersonate them,” said Chris Donnelly, Special Agent, NCIS. “The crucial information is your full name, your address, your date of birth, your Social Security number and your mother’s maiden name, which is the pass code for accounts a lot of the time.”

Identity theft is becoming more common.

“It’s getting bigger and bigger and part of the reason is because of the access that criminals have through the Internet and computers,” said Donnelly. “One of the things that many people are involved in is social networks. People need to be careful of what they are putting out on their network. Most people have their name on their page, their date of birth and they think they are smart because they don’t have their cell phone number or address on there. But they don’t understand that they can be unwittingly be giving out that information anyway. If you have a picture on Facebook of the front of your house where you are posing next to your new car, a person can zoom in on the house and get the number or zoom in on a street sign.”

According to the Federal Trade Commission’s annual Consumer Sentinel Network Data Book in 2010, Virginia was ranked 23rd out of all of the United States for identity theft with more than 5,000 complaints of identity theft. Of those, 19 percent were used for phone or utilities fraud, 17 percent were for credit card fraud, 12 percent involved government documents or benefits fraud, 10 percent involved bank fraud, six percent were employment-related fraud and four percent involved loan fraud.

“Also account numbers and information, the kind of stuff that comes in the mail, you want to protect that as well,” said Donnelly.

If a person isn’t vigilant, it can be easy for criminals to find the information that can compromise their identity’s security.

“The more common ways are to dig through trash, hacking into to a computer or it is given unwittingly through phishing type emails,” said Donnelly.

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity (such as a bank or a credit card) and it often directs users to enter details at a fake website that looks and feels identical to the legitimate site.

This actually happened in the Hampton Roads area recently.

“We had an instance where numerous Sailors came forth because they were having money transferred out of their account – having checks written out of their account when they didn’t have checks, having loan payments coming out of their account when they didn’t have any loans and credit card advances on credit card they didn’t have,” said Donnelly.

“Through investigative measure we came to the realization that the common denominator that they had was that they all had visited a cell phone kiosk at a local mall,” he explained. “An employee had been taking the pre-approval forms that they filled out for the company to run credit checks and sold hundreds of pages of information to two other people. They used the information to get into the online bank to transfer money out and open new accounts.”

There are some ways to be proactive against identity theft.

“Don’t leave mail in your mailbox and make sure that you drop off outgoing mail at a post office. Don’t give personal information out over the phone unless you know who is on the other side of the line. Shred any paperwork that has your Social Security number on it, credit card applications and receipts. Order your credit report, you get it twice a year free from any of the three credit bureaus and have your Social Security memorized. Social Security cards should stay at home in a safe deposit box, not in your wallet!”

For more information on preventing identity theft and what active duty service members can do if their identity is stolen, visit the Federal Trade Commission’s website at www.ftc.gov/idtheft.