



Identity theft occurs when a person illegally obtains another person's name; Social Security Number; bank or credit card account number; or other identifying information and uses it to commit fraud or another crime. Among other things, the criminal can use this information to set up credit card and bank accounts, take out loans and counterfeit checks. This serious crime can cost victims considerable time and

expense to resolve.

The Federal Trade Commission (FTC) report on National and State Trends in Fraud & Identity Theft January – December 2003 says the FTC received over 500,000 consumer fraud and identity theft complaints. It should be noted that this number just represents the *reported* number of incidents. The September 2003 FTC Identity Theft Survey report concluded that approximately 9.91 million Americans were victims of some form of identity theft in 2003. The study also estimated the financial cost to victims at \$5 billion, and the total hours victims spent resolving the theft at 297 million.

Department of the Navy (DON) personnel are not at higher risk than the average American for having their identities stolen. But the DON is taking steps to further protect the identities of Navy personnel. Section 208 of the E-Government Act of 2002 requires that all federal agencies perform Privacy Impact Assessments (PIAs) on their information systems. This requirement is for identifying only the privacy impact on the public, not the federal employee. Going a step further than the Act requires, the DON is conducting PIAs on information systems to identify the privacy impact on civilian and military personnel.

Public Key Infrastructure (PKI) is used to securely authenticate a user's identification to networks and Web sites that may contain personal identifying information. It can also allow digitally signed electronic transactions and encrypt information. The combination of the Common Access Card (CAC), PKI certificates stored on the CAC, the individual's CAC Personal Identification Number (PIN), and Public Key enabled networks and Web sites, is a more secure method for authentication to networks and Web sites than user ID and password, which can easily be compromised by someone with criminal intentions.

Using PKI to digitally sign electronic transactions guarantees that the initiator of the transaction cannot later deny having initiated the transaction, and ensures that the information was not changed. Using PKI to encrypt e-mails that may contain personal identifying information protects information at the desktop and in transit.

The Department of Defense (DoD) formed the Identity Protection and Management Senior Coordinating Group (IPMSG), chaired by the DON Chief Information Officer (CIO), Dave Wennergren. This group rolls the work of the smart card, biometric and PKI steering groups into one group. The IPMSG is looking for new ways to further protect the identities of DON personnel.

The DON has taken steps to protect employees' personal information in its information systems, but the Department also encourages personnel to be proactive in protecting their information. Below are some precautions to take to help protect your identity from being stolen.

Personal Security Tips

- ✓ Call the organization handling your account and follow up with a letter if you suspect someone is illegally using your identity or making charges in your name.
- ✓ Shred all credit card, bank and other financial statements for disposal.
- ✓ Order your credit report once a year and look for any anomalies. Title II of Public Law Number 108-159, The Fair and Accurate Credit Transactions Act of 2003, requires certain nationwide consumer reporting agencies to furnish free credit reports upon consumer request once during any 12-month period.
- ✓ Be wary of anyone calling or sending you an e-mail, also known as "phishing," to "confirm" personal information. Phishing is a tactic that uses spam e-mail to trick consumers into disclosing sensitive personal information such as passwords, credit card and bank account numbers.
- ✓ Review all bank, credit card and phone statements for unusual activity and report problems to appropriate authority immediately.
- ✓ Properly dispose of ATM receipts.
- ✓ Monitor when new credit cards, checks or ATM cards are being mailed to you and report any that are missing or late.
- ✓ Close all unused credit/bank accounts, destroy old credit cards and shred unused credit card, insurance or subscription offers.
- ✓ Ask for the carbon copies of credit card receipts.
- ✓ Use secure Web sites for Internet purchases.
- ✓ Never use any easily recognizable information, such as your date of birth or mother's maiden name as a password for ATMs or access to Web sites.
- ✓ Do not discuss financial matters on wireless phones.
- ✓ Do not leave credit card payments in your mailbox.
- ✓ Do not place your Social Security Number on checks.

For more information regarding identity theft, please refer to guidance published by the FTC at <http://www.consumer.gov/idtheft/>. Darla Tomes is on the DON CIO Information Assurance Team. **CHIPS**