Keep it Legal, Volume 8
Keeping Sheisty Identity Thieves At Bay

Dumpster diving, phishing, and straight up thieving. Whatever the method, there are an alarming number of folks who want your personal information. Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. The rigors of military life can then compound the problems that identity theft creates (remember that duty to be "financially responsible?").

It is important to be aware of the common tactics of identity thieves. Thieves might go through dumpsters looking for and taking documents with sensitive information, such as credit card numbers, dates of birth, or social security numbers. Thieves also might steal your personal information while they are at work (a dishonest medical files clerk), send you emails that trick you into revealing information, or steal your wallet or laptop, both of which are ripe with information. You might think that a thief having just one piece of your personal information is harmless. These criminals, however, are crafty. They might take your name and the one piece information they stole, go online and find your address, and then maybe even go onto a social networking site to find your birthday or your mother's name and voila, they have enough information to do some serious damage!

You, however, are the first line of defense against these sheisters. Here are some ways to protect yourself:

- Read your bank, credit card, and medical statements, compare such to your receipts, and promptly notify of any mistakes;
- Shred all documents that have personally identifiable information;
- Sign your new cards as soon as they arrive;
- Do not respond to telephone calls, emails (phishing), or texts (smishing) that ask for personal information;
- When shopping online, only use websites that protect your financial information with encryption (secure sites begin with "https," the "s" being for secure, and have the lock icon on the status bar);
- Set passcodes for your devices themselves, and do not use automatic login features that save your user names and passwords for financial sites; and
- Use anti-virus and anti-spyware software and a firewall on your devices.

Just as important as prevention is early detection. Keep in mind the following red flags that your identity has been stolen: Mistakes on your bank, credit card, or explanation of medical benefits statements; bills, collection notices, or calls from debt collectors for products or services you never received; notification from the IRS that more than one tax return was filed in your name; and businesses turning down your checks or credit cards.

Finally, in the unfortunate event your identity has been stolen, there are three immediate steps. First, ask one of the three credit reporting agencies to put a fraud alert on your credit report; this makes it harder for an identity thief to open more accounts in your name. Second, order your credit reports from each agency, review, and report any errors. Third, create an Identity Theft Report by filing a complaint online with the FTC, printing your Identity Theft Affidavit, and then using that to file a police report. You can then use the resulting Identity Theft Report to get fraudulent information removed from your credit report and stop companies from collecting bogus debts.

For more information regarding identity theft as well other consumer issues, including understanding credit products and dealing with bad credit, saving and investing money, choosing and funding education (ever hear of a diploma mill?), making charitable donations, and even purchasing a car, visit http://www.consumer.ftc.gov/features/feature-0009-military-families.