

Guarding Your Identity Protects More Than Just You!

October 2006



ON CYBER PATROL



As covered or mandated by AR 25-2

Civilians don't normally run the same risks as military personnel -- IEDs and RPGs on their way to work -- just the occasional DUI and the SIWCMO (Stupid Idiot Who Cut Me Off). But, there is a danger that we all share -- the chance that someone will steal your identity.

In our technology driven society our numbers are just as important as our names. Who we are is often reduced to digits on a card -- Military, Social Security, Bank Account, or Passport. Combined with online IDs and passwords, these are who we are. They are also our first line of personal security in the vast cyber community. Defensively, it's a very thin line.

The thought of having these numbers compromised so that others can assume our identity for profit, harm, or simple chaos is a real concern for all of us, or it should be! There's a good chance you have seen some of the public service ads telling people how to protect their identity. Many of us know about the risks. Few of us actually protect ourselves adequately. Most of us are not doing anything. All of us need to protect our financial and personal data in order to safeguard our credit scores.

These days, the person who is stealing your identity and creating new ones with your data is no longer the little old guy with thick glasses huddled in a dark apartment with engraving tools, magnifying glasses, and an X-acto® knife. It's a young kid with the laptop next to you in Starbucks, or a member of an organized crime syndicate, or a terrorist operative in a mud hut. They all want to be you. If you are in the military, this is a double threat because being you might give enemies access to information that will put your fellow soldiers at risk.

Those trying to steal your identity range from the sophisticated (creating phishing programs) to the heavy handed (digging through your trash for paper with identity information). They will use phishing techniques and misinformation (social engineering) to trick you into giving up critical personal information. They could simply look over your shoulder while you are online or conducting business in a bank or store. Awareness of potential risks and threats is critical to protecting yourself.

For example, I was in a government agency office that was issuing access badges for employees and contractors. There was a large group of people sitting in the room within a few feet of the desk where the agency security official was checking authorizations and identifications. He asked everyone for his or her ID number. Most of the applicants gave it to him verbally. I clearly heard four Social Security numbers and was able to see the names on the newly issued or updated badges as they walked by my seat.

Anticipating his question, I wrote my number on a piece of paper and handed it to him. I got it back immediately and later shredded the note. My ID was safe for the moment, but I could have easily stolen the identity of four other people at that agency simply by being attentive. While Army procedures, policies, and applied technologies go a long way in keeping your identity safe, it's what you do on your own that makes the difference.

From a personal point of view, having your identity stolen is a nightmare. You could be financing someone's new SUV -- maybe one that eventually becomes a car bomb. The damage to your credit rating, finances, and reputation could take years to fix.

On top of that, think what stealing your identity as a member of the U.S. military could mean. Someone pretending to be you could gain access to Army facilities and systems that could cause significant damage or create paralyzing confusion. A few simple precautions will reduce or even eliminate that risk. Guard your identity and you are guarding your fellow soldiers, your family, and yourself.