# ID theft: Are we doomed

**Email scams abound, and hackers have been stunningly successful at getting access to 'private' data. But being aware of the problem is far different from solving it.**

Opening my email reminds me of walking through the bazaar of a Third World open-air market -- pickpockets are everywhere.

In the past 30 days I have received spam purporting to be from the Better Business Bureau, the Internal Revenue Service, the United States Post Office, the FBI and, most recently, from the AICPA -- the **American Institute of Certified Public Accountants**, a group of which I am not a member. The subject line was "Termination of your Accountant Status," and the body of the email explained that my status as a CPA was about to be terminated as a result of my participation in the filing of a fraudulent tax return. I was directed to take immediate action by clicking on a link called "complaint."

An eternal cynic and professionally paranoid, I did some research and determined that the logo of the AICPA was correct, as were the return addresses and phone numbers listed in the email.

While I am a credit guy, not a debits-and-credit guy (and have no degree in accounting), I didn't take the threat seriously; similarly, since I had neither sent any packages through the post office nor become a member of the Better Business Bureau, I wasn't too concerned about the dire warnings I received from those folks. I guess these emails are about as credible as the ones from exiled **Nigerian diplomats** -- remember those? But since a half-dozen of these emails appear in my mailbox each day, I know these scams must fool some of the people some of the time.

Hacking is a continuously evolving epidemic that is often perceived as a battle between evil and good forces. I am not impressed by the proposals that I have seen, since they treat the symptoms without paying attention to the infection.

Earlier this year, both the House and the Senate held cybersecurity hearings again (so many hearings, so much time, so few results -- sigh). As one might imagine, the testimony was filled with justifiably dire warnings about the vulnerability of important elements of the U.S. infrastructure, particularly the power grid. Additionally, a fair amount of time was devoted to the hack of **DigiNotar**, which was owned by the Chicago-based public company Vasco Data Security, and was an important provider of security certificates for domains based in the Netherlands and beyond.

Apparently, the hacker was able to issue about 500 phony certificates for major websites including Google, enabling that fraudster to impersonate legitimate sites and thereby intercept, for example, Gmail communications. The person who claimed responsibility for the attack had asserted namelessly that he was a 21-year-old Iranian student, who had hacked several other security certificate issuers, and was cooperating with the Iranian government. Allegedly, the hack of DigiNotar occurred in June 2011; it was discovered in July, announced in August, and the company filed for bankruptcy in September. Such is the impact of being an unlucky target.

The hearings also mentioned a report from December that hackers in China had breached the U.S. Chamber of Commerce's castle walls, gaining access to information on its 3 million members and pretty much everything else stored in its systems. The complex infiltration, which involved at least 300 Internet addresses, occurred during a six-month period ending in May 2010, when it was shut down after the FBI got involved. Although it doesn't seem to get a lot of attention, what happened to the Chamber of Commerce is just one skirmish of an apparently well-known war between Chinese hackers and American companies. We live in era in which personal, identifying information and intellectual property are hot commodities, and the ancient battle for superpower pre-eminence has transformed into digital ninjas' attacks.

My point is very simple: Why couldn't a 21-year-old Iranian student be cooperating with the Chinese hackers and sending emails masquerading as the AICPA to you and me? Talented young hackers are the equivalent of someone who finds a skeleton key for all the safe deposit boxes in a bank. All they have to do is figure out how to get into the bank, and then they can loot the treasure of all the depositors, whether those depositors are individuals, businesses or power grids.