

Identity Crisis

by Jennifer G. Williams

I have heard a lot about scam emails, and individuals trying to trick people out of their money, but I had never actually received one — except for the spam-type messages to earn big bucks at home or that I am the lucky winner of a new iPad.

The other day, I saw an email in my inbox titled simply, “Can We Work Together?” It was from an individual’s name, and as I edit several magazines, I receive inquiries from writers and such on a pretty regular basis. But when I opened the email, I was surprised to see that such a scam was trying to ensnare me.

The email claimed to be from an attorney for a family with the same name as mine who unfortunately was killed in an automobile accident overseas. Of course, these supposed relatives were apparently very wealthy and this kind attorney said he would be more than happy to share their millions with me, but I needed to contact him to make it happen.

Now, I know there are lots of Williams in the world, but I also do my share of reading the newspaper and watching the news. I can only predict how this conversation would go: “of course, we will send you the cashier’s check for the amount if you wire us back the percentage we are asking in return...” But, as has played out in homes across America, the “relatives” receive their “official” cashier’s check and deposit it in their bank. They wait a day or two and wire the money from their account as requested... but soon find that the cashier’s check was bogus and their account is now empty, with overdrawn charges rapidly accumulating.

But instead of simply deleting this email, as I usually do for my other “spam,” I took it one step further and reported it to the Internet Crime Complaint Center at www.ic3.gov. The IC3 is a partnership between the Federal Bureau of Investigation, National White Collar Crime Center and Bureau of Justice Assistance. It took a few minutes, and I had to enter my information, but thankfully, I did not have to complete the section that asked how much money I had lost. I figured by forwarding the email and its contents to the IC3, I could help spread the word about this possible scam.

The complaint database not only links complaints for potential referral to law enforcement, but also uses complaint information

to identify emerging trends and patterns to alert the public to new criminal schemes.

Internet scams are as old as the Internet itself, but criminals are getting more sophisticated, say officials. Special agents from the U.S. Army Criminal Investigation Command say they continue to receive hundreds of reports of various scams involving persons pretending to be U.S. Soldiers serving in Iraq or Afghanistan. The victims are most often unsuspecting women, 30 to 55 years old, who think they are romantically involved on the Internet with an American Soldier, when in fact they are being cyber-robbed by perpetrators thousands of miles away.

“We cannot stress enough that people need to stop sending money to persons they meet on the Internet and claim to be in the U.S. military,” said Chris Grey, Army CID’s spokesman. “It is heartbreaking to hear these stories over and over again of people who have sent thousands of dollars to someone they have never met and sometimes have never even spoken to on the phone.”

The majority of the “romance scams” as they have been dubbed, are being perpetrated on social media dating-type websites where unsuspecting females are the main target. The criminals are pretending to be U.S. servicemen, routinely serving in a combat zone. The perpetrators will often take the true rank and name of a U.S. Soldier who is honorably serving his country somewhere in the world, marry that up with some photographs of a Soldier off the Internet, and then build a false identity to begin prowling the Internet for victims.

“We have even seen instances where the Soldier was killed in action and the crooks have used that hero’s identity to perpetrate their twisted scam,” said CID Special Agent Russel Graves, who has been fielding the hundreds of calls and emails from victims for months.

The scams often involve carefully worded romantic requests for money from the victim to purchase special laptop computers, international telephones, military leave papers, and transportation fees to be used by the fictitious “deployed Soldier” so their false relationship can continue. The scams include asking the victim to send money, often thousands of dollars at a time, to a third party address. Once victims are hooked, the criminals continue their ruse.

“We’ve even seen instances where the perpetrators are asking the victims for money

What You Can Do

- Report the incident to the Internet Crime Complaint Center at www.ic3.gov.
- Report any theft to the Federal Trade Commission at www.ftc.gov/idtheft.
- You can report scams by phone at 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261.
- You can report scams by mail at Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580.
- If you think your bank account or other financial account has been compromised, contact your institution directly and see what has happened and ask what can be done.
- Contact the three major credit bureaus and request an alert be put on your file

to “purchase leave papers” from the Army, help pay for medical expenses from combat wounds received, or help pay for their flight home so they can leave the war zone,” said Grey. These scams are outright theft and are a grave misrepresentation of the U.S. Army and the tremendous amount of support programs and mechanisms that exist for Soldiers today, especially those serving overseas, said Grey.

No matter who you are or what you think you know about someone who has contacted you over the Internet, take the extra time and precautions to ensure you do not fall prey to a scam. I make it a rule to never pledge money or give out any kind of personal information to anyone who contacts me first. If I am interested in donating to a charity group, I go to their website and check them out before I contact them with a donation. Even if my credit card company calls me about “suspicious activity” on my account, I tell them I will call them back... then call the number listed on the back of my card and ask to be connected with their fraud department.

A little kooky? Maybe. But I know in this day and age of instant information, sometimes it is better to slow down a bit and take it slowly. ●