

May 21, 2008 2:54 PM PDT

# Spyware Horror Story: Would you fall for this IM scam?

Posted by [Jessica Dolcourt](#)

[http://www.download.com/8301-2007\\_4-9949668-12.html?tag=cnetfd.mt](http://www.download.com/8301-2007_4-9949668-12.html?tag=cnetfd.mt)

Got your own spyware horror story?

▶ Share it with us

## Submitted by Scott, Vernon Hills, Ill.

This past April, a friend of mine, Jeff, called me on a Saturday afternoon, letting me know that I was instant messaging him right then. I obviously wasn't. He said that after some lines of basic text, *I* acted panicked and asked for money to be wired to an African bank account, which Jeff knew immediately was bad news for the real me.

I immediately changed some passwords in key accounts and found that my Hotmail account had been mysteriously compromised. The evildoers had got a ton of my contacts and sent out some boilerplate e-mails to unwitting friends and family, most of whom I assumed were smart enough to sniff a scam. I figured my first wave of defense would be good enough until I had more time to filter everything. That was really going to suck, I reasoned, but I had other things to do in the time being.

That evening we were at some friends' house for a dinner party. Our friends' 2-year-old child accidentally set off a carbon monoxide alarm in the basement, and in the ensuing chaos of children, the alarm, and a boisterous party, I received a call from my obviously distressed mother who had just been instant messaging *me* and was at her wit's end with worry.

Here's the conversation she relayed:

'ME': Hi Dad!

Parents: Hi Scott, it's Mom here

'ME': OK, how are things?

Parents: Good, how are the girls?

'ME': Good

Parents: Did you hear about Heidi's sister yet?

'ME': Yes [at this point, Mom was wondering why I was spewing all these one-liners]

'ME': Mom, in trouble and need help...[wire money pitch followed]

'Parents': Call me! What's going on? Are you serious?

'ME': Phone not work well...problems here

That's when my mother called my cell, and unlike all the other friends and family who ignored those obvious scam e-mails, poor Mom's stomach was sinking downward and her mind was scrolling through worst case scenarios like any good mother's would. I

answered the call in the middle of the carbon monoxide din, which only made me feel even more trapped when I discovered the true purpose of the call. It took a few minutes to calm Mom down, and after explaining the earlier incident with Jeff, we ultimately had a good laugh over the mess. Except now I had to deal with the keylogger Trojan ([TrojanSpy/ProAgent](#)) I had somehow contracted.

The villains had sent off about 10 messages and made contact with three people through IM before I was able to change the password. It was a bold and shocking violation of privacy. Amazingly, they preyed on the right folks from a contact list of over 100: my parents, the most likely to cave at an unknown peril to their first born.

I use [Norton Internet Security](#) on all my PCs and am very careful with my security all-around. When I called Norton, they said I was at fault for opening up a 'legit' program that Norton could not distinguish as good or bad. Can't Norton scan for keylogger code?! I purchased [XoftSpy](#), which appeared to do the trick of identifying and eliminating the keylogger, or so I thought. I used a second Trojan antispyware package for a "second opinion" to confirm it was gone and it identified some totally new Trojans! The horror! Realizing I was going to fall into a trap of continually spending \$30 registration fees, I figured an absolute confirmation was necessary, so I took Norton up on their \$99 eradication service and a nice representative gave my system a good natural cleansing. I showed him the results of the other package that reported my infection, and he pointed out it was a fake to entice someone to pay for the registration! My God, who can you trust?!

It took two hours for the representative to clear out all the infections and to this day I've had no other issues. The villains did send login ID requests to PayPal, eBay, Amazon, and other financial sites, a fact which will haunt me for years as I wonder when they'll mine all those prior e-mails for something I missed, something sensitive to my life.

One lesson learned is to purge old accounts. My Hotmail account had 8 years of old e-mails, many with password information requests that I had sent. Stupid. I removed those and thanked my lucky stars that the policies have changed over the past few years and that some sites now force you to change old passwords. If not, maybe *I* would have been cleaning out my bank account via eBay or PayPal.

I was hoping we'd have an 'ID Theft' registration site that financial sites could reference in case my life savings was in the process of being wired to Somalia or the like.

+++++

Editors Response to that story...

We don't have a lot of first-hand accounts of IM scams in our [annals of Spyware Horror Stories](#), but when they happen, the cons are mighty effective. Similarly to phishing e-mail, IM scams count on the recipient's assumption that their buddy is in truth the typist and on the recipient's conditioning to click the offered link.

Thanks to the speed and breadth of the communication medium, malicious message can spread widely and rapidly through a victim's buddy list. Even a bare link devoid of context can net a good deal of response from users who trust a friends' mysterious URL bait in hopes of an [entertaining payoff](#).

Most of the ruses I'm familiar with involve [phishing links such as this one](#) or a hidden

.exe download. Scott's haunt used the IM medium to deliver a twist on a '419' scam. Instead of asking for a bank account number in exchange for a percentage of some bogus money trade, this method took advantage of IM's personal touch by begging for a direct money wire. The tactic wouldn't be as convenient as an e-mail blitz that nets the numeric key to clean out a bank account, but it could well whip up enough panic in a dear relative or friend to elicit some cash. You would have been wise, Scott, to alert your IM provider and buddies of your compromised accounts.

Making matters worse is the keylogger that first got you into the mess and the successful [rogue antivirus trick](#) that dug you deeper. I may be a little biased here given my place of employment, but if you're not scouting software on a site that's known to offer safe downloads (a few spring to mind,) you should at the very least be using a link-rating tool such as [McAfee Site Advisor](#) or [AVG LinkScanner](#), the latter of which has also now been sewn in various degrees into the [premium](#) and [free](#) versions of AVG Anti-Virus.