



News

Hackers Swiping Retirement Accounts

March 21, 2007 (PLANSPONSOR.com) - If you travel – or you have participants who do - and access retirement accounts online while on the road, those accounts may have been targeted by hackers, according to a news report.

ABC News is reporting that cybercriminals are hacking their way into accounts and looting 401k and online stock trading accounts, citing comments from officials at the Federal Bureau of Investigation and the Securities and Exchange Commission. The report says that in many cases workers have had their user IDs and passwords stolen when they use computers at hotel business centers and other Internet connection points.

Keystroke Tracking

"You could wake up one morning and find all your money in your retirement account or in your trading account is gone," said John Reed Stark, Chief of Internet Enforcement at the Securities and Exchange Commission. The FBI says the criminals bug those computers in the business resource centers with programs to record every key typed. That kind of keystroke recording was recently at issue in a case involving the Federal government's own Thrift Savings Plan (see [Hackers Make Off with \\$35,000 of TSP Participant Money](#)).

In addition to the Russian rings, authorities have also seen hackers in India, Hong Kong and Malaysia going after similar online accounts, according to the report. Victims have included customers of E-trade, Scott Trade, Ameritrade, Fidelity, Merrill Lynch, Charles Schwab and Vanguard.

As part of an ABCNews.com investigation, a Russian speaking ABC News intern logged on to a Moscow-based hackers forum and was offered the user IDs and passwords of six U.S. trading accounts - worth about \$100,000 - for a cost of \$350. A transcript of the transaction is online at <http://abcnews.go.com/WNT/print?id=2966583>

Avoiding Trouble

The FBI's Henry offered the following advice to avoid becoming a victim of such Internet theft, according to ABC News:

- Always use a trusted computer when conducting financial transactions.
- Going into a hotel or an airport or an Internet cafe, assume you may be at risk.
- Closely scrutinize reports from your online trading firm to make sure the reported trades are ones you authorized.
- Frequently change your password and when traveling, consider using a special program that will change your password every 10 seconds.
- Make sure your own computer has anti-virus protection.

A video report is online at

http://blogs.abcnews.com/theblotter/2007/03/russian_crimina.html

Nevin E. Adams

editors@plansponsor.com