

## News Room Archive

### Title Agents Warned of Virus Attacking Escrow Accounts

July 29, 2010



A title agent in northern Virginia recently was unable to log onto their online banking during the course of a few days. During that time, three unauthorized wires went out of the agent's escrow account to banks in New York and then immediately overseas to Russia.

The agent suffered a loss of more than \$200,000 and had to fund the escrow account for the shortage. The bank as well as the FBI and various other entities are investigating.

A Zeus botnet virus infected either the bank's or the title agent's computer system and enabled the theft to occur. If it is determined that the hack occurred from the agent's system and not of the lender, the agent will not be able to recover the theft from the bank.

The Zeus botnet is very hard to detect despite having virus or malware systems on your computer. Agents are reminded to take the time to analyze computer security and internal procedures. [Click here](#) for more information on the Zeus botnet virus. Don't miss a coming article in *TitleNews* that will address best practices to protect private information and prevent fraud. In the meantime, Dick Reass, president of RynohLive, offers several suggestions for title agents to protect their computer systems and prevent virus attacks:

- | Initiate wire transfer payments only under dual control, with a transaction originator and a separate transaction authorizer.
- | Use tokens for all online transactions to provide an additional layer of authentication.
- | If possible, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and web browsing (beyond the secure online banking site) is not possible.
- | Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information.
- | Opening file attachments or clicking on web links in suspicious e-mails could expose the system to malicious code that could hijack your computer.
- | Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connecting to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- | Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- | Install commercial anti-virus and desktop firewall software on all computer systems.
- | Free software may not provide protection against the latest threats compared with an industry standard product.
- | Ensure virus protection and security software are updated regularly.
- | Ensure computers are updated regularly, particularly the operating system and key applications with security updates. It may be possible to sign up for automatic updates for the operating system and many applications.
- | Consider installing spyware detection programs.
- | Recommend clearing the browser cache before starting an online banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preference menu.

[Close Window](#)

How To Find Us:  
 American Land Title Association®  
 1828 L Street, NW, Suite 705  
 Washington, DC 20036-5104  
 P. 202.296.3671 F. 202.223.5843  
[www.alta.org](http://www.alta.org)  
[service@alta.org](mailto:service@alta.org)

Quick Site Links:  
[ALTA® Home & News](#)  
[LTI Home](#)  
[TIAC Home](#)  
[TIPAC Home](#)  
[ALTA® Calendar](#)  
[ALTA® Store: Shop/Subscribe/Register](#)

Do You Want To:  
[Contact ALTA® Staff?](#)  
[Join ALTA®?](#)  
[Find A Title Company?](#)  
[Update Your Contact Information?](#)  
[Update Your Login & Password?](#)  
[Report A Site Problem?](#)

Copyright © 2004-2010 American Land Title Association®. All rights reserved.