

## How You Can Avoid Cyber Fraud While Others Lose Millions



by **Richard Reass, President,**  
**RynohLive**

**I**n today's economy, commercial banking is too large and tempting of a target for criminals to ignore, and they're raking in money through schemes that attack online businesses. Due to the nature of our business, the title agent is a prime target. In the past few months alone, several title agents have had hundreds of thousands of dollars illegally wired from their escrow accounts due to a not-so-new form of cyber crime: the Botnet.

A Botnet comes in many forms and is malicious software (malware) that can steal information and, in the case of our industry, be used to wire funds from your escrow account. The primary culprit for the title agent is the ZeuS Botnet. The ZeuS Botnet is commercially available over the Internet and may be "purchased" for as little as \$3,000. The latest version of this cyber-crime toolkit comes in a \$10,000 module that lets attackers completely take control of a compromised PC.

In targeting a title agent, the hacker uses ZeuS to steal financial credentials and initiate fraudulent transactions, primarily through the agent's online banking portal. The hacker also can access automated clearing house (ACH) networks

and payroll systems. ZeuS is a very sophisticated Botnet variant that spreads by concealing itself in many formats (e-mail, drive-by downloads and open Internet browsers). ZeuS and other Botnets have taken over hundreds of thousands of desktops, and sometimes even servers.

The typical spyware and antivirus programs will not necessarily protect you. More often than not, the Botnet remains undetected. Once the ZeuS Botnet infects your computer, it sends instructions to the criminal(s) waiting to access your account and use the collected credentials. Cybercriminals masquerade as the agent to execute wire transfers to onshore or offshore banks. Even the use of an RSA token will not prevent a successful cyber attack! (An RSA token is a random number generator that is used to reduce wire fraud). Once the money has moved offshore, the likelihood of recovery is nil.

I've spoken with agents who have recently lost money from their escrow accounts due to the ZeuS Botnet, and all have one thing in common. They didn't use dual controls or "best practices" for initiating wire transfers. This problem is especially prevalent in small agencies, which I've surveyed at recent NS3, ALTA and VLTA meetings. A great percentage of them only use single-wire controls because: a) They would never steal from their escrow account; or b) It is a "real imposition" for them to use dual controls. They don't fully appreciate the magnitude of the problem; after all, it's a much bigger imposition to lose \$200,000 or more.

If your practice is at risk, you must at a minimum adopt the best practices outlined here (see [page 9](#)) in order to "harden" your online banking process. There also are other available products that combat the ZeuS

Botnet and other malware programs ([www.ironkey.com](http://www.ironkey.com)).

### ◆ Recent examples

The reality is that this type of crime is occurring with costly consequences. One Missouri agent recently lost \$400,000. A post mortem with the company revealed that it was only using a single individual for the online bank-wiring process. Had it not been for daily reconciliation and alerting with RynohLive, the escrow account would have been drained. However, since wire transfers are instantaneous, RynohLive was only able to alert the agent after the fact. They notified the agent's bank the next day, before the ZeuS Botnet came back to further drain the agent's account of the remaining \$800,000.

A large, Midwestern title agency lost more than \$800,000 due to wire fraud. The agency was canceled by its underwriter and saddled with the loss. This agency, too, failed to utilize best practices.

Don't join the growing list of victims. Use best practices to protect your agency and your business. (See [page 9](#) for highlights of important best practices.)

*continued on page 9*

### For More Information

RynohLive provides innovative technology that prevents fraud and automates escrow accounting management, positive pay and three-way account reconciliation. To learn more, contact Richard Reass, President, RynohLive. Call 877.467.9664 or 877.GO.RYNOH (tollfree); or visit [www.rynoh.com](http://www.rynoh.com).

## Get Started Today! RynohLive Shares Best Practices That Can Protect Your Agency

### ONLINE ACCOUNT best practices

- ◆ Reconcile and review all banking transactions on a daily basis.
- ◆ 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.

### COMPUTER SYSTEMS best practices

- ◆ If possible, carry out all online banking activities from a standalone, hardened and completely locked-down computer system from which e-mail and Web browsing (beyond secure online banking) are not available.
- ◆ 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 you have a broadband or dedicated connection to the Internet, such as DSL or cable.

- ◆ 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 that virus protection and security software are updated regularly.
- ◆ Ensure that computers are updated regularly, particularly the



- operating system and key applications, with security updates. Sign up for automatic updates when offered.
- ◆ Consider installing spyware detection programs.
  - ◆ Clear 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. (This function is generally found in the browser's "preferences" menu.)

### ONLINE best practices

- ◆ Train staff with access to online

- accounts on best practices.
- ◆ Create a strong password with at least 10 characters that includes a combination of mixed-case letters, numbers and special characters. Change passwords regularly.
  - ◆ Prohibit the use of "shared" user names and passwords for online banking systems.
  - ◆ Use a different password for each Web site that is accessed.
  - ◆ Never share username and password information for online services with third-party providers.
  - ◆ Verify use of a secure session (https, not http) in the browser for all online banking.
  - ◆ Avoid using automatic log-in features that save usernames and passwords for online banking.
  - ◆ Never leave a computer unattended while using any online banking or investing service.
  - ◆ Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and log-in information, leaving you vulnerable to fraud.

### For more information

To learn more, contact Richard Reass, President, RynohLive. Call 877.467.9664 or 877.GO.RYNOH (tollfree); or visit [www.rynoh.com](http://www.rynoh.com). ■