About this article: *Protect your agency from cybercrime. The most potent tools to fight this threat are to keep a wary eye and practice proactive online security techniques and policies. Danielle Johnson, Vice President of InsurBanc, suggests several steps to protect personal privacy, banking information, and agency data, including adoption of recent advancements in banking security.*

Combat Cybercrime and Protect Your Agency With Simple Security Steps

By Danielle Johnson

What is Cybercrime?

Like traditional crime, cybercrime covers a broad scope of criminal activity and can occur anytime and anyplace. What makes it different is that the crime is committed using a computer and the Internet. You may recognize some of its most common forms such as identity theft, computer viruses and phishing, and at a corporate level, computer hacking of customer databases.

Most people are aware of these and protect themselves and their PCs with anti-spyware and anti-virus software such as Norton or McAfee programs. As an agency owner, you should be alert to the fact that cybercrime is becoming more and more sophisticated and not only targets consumers and large corporations, but small to medium sized businesses as well. Single programs against these intrusions are not enough.

An alarming cybercrime now affecting small to medium sized businesses is “corporate account take over.” This involves cyber criminals penetrating the computer network of a business and spreading malicious software, such as a “keylogger” which records the words typed, Web browsing history, passwords and other private information. This in turn allows them access to programs using your log-in credentials.

If they steal your password and breach your online banking system, the cyber criminal can begin an online session to initiate funds transfers, by ACH or wire transfer, to their accomplices. The accomplices withdraw the money almost immediately.

Take the first steps to prevent fraud at your agency – become aware of the latest cybercrimes and how they can access a business’s computer network. An agency should also employ the most up-to-date online security practices on a pro-active basis.

Agencies can also take the opportunity to present these online security practices to their clients, as many are also instituting internet-based online programs at their businesses.

Online Security Practices

While no tools or automated software is 100% effective, the best solutions to protect your agency are to be well informed and use common sense. Using a multiple vendor, multi-layer approach to system design can significantly reduce your chances of being a victim of cybercrime. To assess the risks associated with a cyber intrusion of your agency's online systems and critical client data, ask yourself the following questions:

1. Does your agency have a hardware based firewall at the network level?
2. Does the network firewall include anti-virus, anti-spyware and anti-spam services along with content filtering and intrusion prevention, detection and real-time reporting?
3. At the individual PC level, does each computer have centrally updated and monitored anti-virus, anti-spyware and anti-spam software loaded?
4. Are your computers set up to automatically update your operating system and applications for the latest available security and critical updates?
5. Do you consider your browser security setting to determine how much or how little information the browser can accept from, or transmit to, a website?
6. Does your agency have a security policy in place that includes such policies as disaster recovery, use/storage of passwords, use of social media on work computers, etc.?
7. Does your agency back-up critical files in case of an issue that disables your systems?
8. Has your agency identified an individual to review security policies and practices on an ongoing basis?
9. Are you aware of the laws governing the protection of personal information in your state?
10. Do you have cybercrime insurance to protect your data and liability exposure in the event of an intrusion?
11. Does your agency have a training program to educate employees on best practices to avoid becoming a victim?
12. Does your online banking system provide multiple layers of security tools to prevent intrusions into the system such as token-based authentication? Agency principals should consider the types of transactions they conduct within online banking and check with their banking institution for available security enhancements.

These are just some of the basic steps an agency can implement to assess and protect itself from cybercrime. Your agency should have a network security assessment and review conducted by a certified information technology firm that specializes in network security. This

evaluation will help you to identify the "next steps" in securing your network and data from unauthorized access and distribution.

If Your Agency Becomes a Victim
If you discover, or even suspect, your agency has fallen victim to corporate identity theft, you should proceed as follows:

- Immediately cease all online activity and contact your IT administrator.
- Remove the affected computer from the network and any other computer stations involved.
- Contact your financial institution to disable online access to the accounts and close affected accounts. You can then open new accounts and reset passwords.
- Consult your counsel and your state's data breach notification law and regulations to ascertain the process you need to follow.
- Notify other business partners that may have been affected, such as your insurance carriers.
- File a report with the police department.

Common Online Fraud Definitions

- **Malware** refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include spyware, keyloggers, and viruses.
- **Spyware** is a type of malware installed on your computer without your knowledge. It collects small to large pieces of personal information including Internet surfing habits. It can redirect web browser activity and change computer settings. Spyware is typically hidden from the user, and can be difficult to detect once installed without proper antispyware tools.
- ***Keyloggers***, as with spyware, are installed on your computer without your knowledge. It is the action of tracking (or logging) the keys struck on a keyboard, typically in a hidden manner so that the person using the keyboard is unaware that their actions are being monitored. Keystroke logging can record the words typed, Web browsing history, passwords and other private information. This is extremely dangerous in all aspects of computer usage.
- **Viruses** are an ever changing and constant threat to all systems. Based on their digital makeup they can deliver malicious content to your data and systems in an effort to either collect data, destroy data, or turn your systems into a machine that spreads the virus or other malware.
- **"Phishing"** is the act of obtaining personal information or spreading malware using emails, calls, text messages or pop-up messages from what appear to be friends or legitimate banks, retailers, government agencies or other organizations.

All of the security tips presented here are simply guidelines to aid agencies in not becoming a target for cybercriminals. However, none can be guaranteed 100% effective.

Editor's Note: *Please also refer to ACT's "Security & Privacy" page for a prototype agency information security plan and recorded webinar which will help agencies fashion their written* *security plan and implement their security program. Go to www.iiaba.net/act and click on "Security & Privacy" in the gray shaded area on the left side of the page.*

Danielle Johnson is the VP, Director of Information Technology at InsurBanc, which IIABA and the W.R. Berkley Corporation established to assist independent agencies, businesses and consumers with their specific banking needs. Danielle prepared this article for ACT and she can be reached at technology@insurbanc.com. This article reflects the views of the author and should not be construed as an official statement by ACT.