Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-66-2005
July 22, 2005

SPYWARE
Guidance on Mitigating Risks From Spyware

Summary: The FDIC is issuing the attached guidance to financial institutions recommending an effective spyware prevention and detection program based on an institution's risk profile. This guidance and the attached informational supplement discuss the risks associated with spyware from both a bank and consumer perspective and provide recommendations to mitigate these risks.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:
. GLBA, Section 501b
. FFIEC Information Security Handbook, issued November 2003
. Guidance on Developing an Effective Computer Virus Protection Program (see FIL 62-2004, issued June 7, 2004)
. Interagency Informational Brochure on Phishing Scams (see FIL-113-2004, issued September 13, 2004)
. Guidance on the Risks Associated with Instant Messaging (see FIL 84-2004, issued July 21, 2004)
. Putting an End to Account- Hijacking Identity Theft Study, issued December 2004

Attachments:
. Guidance to Financial Institutions on Mitigating Risks From Spyware
. Informational Supplement: Spyware Prevention and Detection

Contact:
Senior Technology Specialist Aurelia Cardamone at ACardamone@FDIC.gov or 202 898-8541

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

Highlights:

- Spyware refers to software that collects information about a person or organization without their knowledge or informed consent and reports such data back to a third party.
- Spyware is designed to collect personal or confidential information, some of which can be used to compromise a bank's systems or to conduct identity theft.
- The guidance recommends practices that banks should employ to prevent and detect spyware on their own computers.
- The guidance also suggests practices that banks should recommend to customers to ensure the security of the online banking relationship.

Guidance to Financial Institutions on Mitigating Risks From Spyware

The Federal Deposit Insurance Corporation (FDIC) is issuing the following guidance to financial institutions to inform them about the risks posed by spyware[1] within an institution's network and on customers' computers. The guidance also recommends actions to mitigate those risks.

The attached informational supplement recommends best practices that financial institutions can use to prevent spyware from being downloaded to their computers and for mitigating the risk of thieves obtaining online banking IDs and passwords from spyware installed on customers' computers.

Introduction

The term spyware refers to technologies that collect information about a user without his or her knowledge and reports that information to a third party. Certain forms of spyware can intercept sensitive and confidential information about an organization or user, including passwords, credit card numbers and other identifying data. As a result, spyware has significant confidentiality, integrity and availability implications for both a bank and its customers. Financial institutions should consider anti-spyware strategies for their enterprise information security programs and customer awareness programs.

Risks Associated With Spyware

Financial institutions should be aware of the risks of spyware on their own computers and on computers used by customers connecting to online banking Web sites. Spyware increases the risk to financial institutions by:

- Compromising confidentiality by allowing attackers to eavesdrop and intercept sensitive communications, such as customer IDs and passwords.

- Damaging an institution's reputation by potentially allowing unauthorized access to user accounts.

- Misappropriating bank resources and permitting unauthorized access to bank systems.

[1] "Spyware" is a commonly used term to describe software that collects data without the prior knowledge or informed consent of the data's owner. The FDIC expresses no views about spyware beyond those contained in this document.

- Increasing vulnerability to other Internet-based attacks, such as phishing[2] and pharming.[3]

Recommended Actions to Mitigate the Risks Associated With Spyware

Financial institutions should evaluate the risks associated with spyware and strengthen enterprise information security programs by:

- Considering threats from spyware as part of the risk assessment process. This ensures that the financial institution considers all risks to private customer information and takes appropriate steps to mitigate those risks, such as implementing anti-spyware technologies.

- Enhancing security and Internet-use policies to address risks associated with spyware and acceptable user behavior (e.g., prohibiting Internet downloads and visits to inappropriate Web sites). In addition, management should take steps to enforce these policies and reprimand staff who fail to comply with them.

- Expanding employee training to include the risks associated with spyware so that users will become cognizant of the behavior they should adopt to prevent spyware on bank computers and on personal computers that are used to connect to the bank's network.

- Educating customers about the risks associated with spyware and encouraging them to implement steps to prevent and detect spyware on their own computers. In addition, advise customers of the risks in using public computers – such as those in hotels, libraries or Internet cafés – to connect to online banking Web sites because of the uncertainty of what spyware may have been installed on the public equipment.

- Investigating the implementation of multi-factor authentication methods, which would limit the ability of identity thieves to compromise customer accounts, even when a thief has a customer's ID, password and account numbers.

---

[2] Phishing is a scam that encompasses fraudulently obtaining information by sending an e-mail that appears to originate from a trusted source, such as a financial institution, government agency or other entity.

[3] Pharming refers to the redirection of an individual to an illegitimate Web site through technical means. For example, an Internet banking customer, who routinely logs in to his online banking Web site, may be redirected to an illegitimate Web instead of accessing his or her bank's Web site.

Conclusion

Spyware poses a significant risk to financial institutions and its customers. Practices to prevent and detect spyware should be regularly reviewed to ensure that an institution is aware of all risks to its systems and to sensitive customer information.

Informational Supplement

Best Practices on Spyware Prevention and Detection

The Internet has become a popular method for both conducting business and managing finances through online banking relationships. While most financial institutions and some individuals have taken steps to protect their computers, many firewall and anti-virus software packages do not protect computers from one of the latest threats, "spyware" – a form of software that collects personal and confidential information about a person or organization without their proper knowledge or informed consent, and reports it to a third party.

This informational supplement describes the various challenges and best practices related to spyware. Financial institutions should consider these recommendations to prevent and detect spyware on both bank-owned and customer computers.

Spyware Infection

Spyware is usually installed without a user's knowledge or permission. However, users may intentionally install spyware without understanding the full ramifications of their actions. A user may be required to accept an End User Licensing Agreement (EULA), which often does not clearly inform the user about the extent or manner in which information is collected. In such cases, the software is installed without the user's "informed consent."

Spyware can be installed through the following methods:

- Downloaded with other Internet downloads in a practice called "bundling." In many cases, all the licensing agreements may be included in one pop-up window that, unless read carefully, may leave the user unaware of "bundled" spyware.

- Directly downloaded by users who were persuaded that the technology offers a benefit. Some spyware claims to offer increased productivity, virus scanning capabilities or other benefits.

- Installed through an Internet browsing technique called "drive-by downloads." In this technique, spyware is installed when a user simply visits a Web site. The user may be prompted to accept the download believing it is necessary in order to view the Web page. Another method is to prompt the user to install the program through pop-up windows that remain open, or download the software regardless of the action taken by the user.

- Automatically downloaded when users open or view unsolicited e-mail messages.

Behaviors Associated With Spyware

Spyware can be difficult to detect and remove because it:

- Does not always appear as a running program in the Window's Task Manager; therefore, the user may be unaware that his or her computer is infected.

- May not include a removal option in the Windows "Add/Remove Programs" function. When such an option is present, the removal process may not eliminate all components, or it may redirect the user to an Internet site to complete the removal. This often results in new or additional infection rather than removal. In addition, some spyware includes a feature to reinstall itself when any portion is deleted.

- May cause a further infestation by installing other spyware programs onto users' computers.

Risks Associated With Spyware

Spyware increases the risk to financial institutions by:

- Exploiting security vulnerabilities or settings, changing the computer configuration to relax security settings, or allowing a channel into the institution's systems by circumventing the firewall. The result is that attackers can eavesdrop and intercept sensitive communications by monitoring keystrokes, e-mail and Internet communications. This monitoring may lead to the compromise of sensitive information, including user IDs and passwords.

- Providing attackers the ability to control corporate computers to send unsolicited "junk" e-mail (SPAM) or malicious software (Malware), or to perform denial of service (DoS) attacks against other organizations.

- Draining system resources and productivity and consuming system resources, even when the user is not browsing the Internet, such as when adware[1] results in voluminous unwanted pop-up advertisements.

- Compromising the bank's ability to conduct business by disrupting Internet connections as a result of the improper removal of spyware.

- Increasing the incidence of SPAM to corporate e-mail accounts.

- Compromising confidentiality. Certain types of spyware route all Internet communications through their own servers, often without the user's knowledge. This allows a third party to read sensitive Internet communications even when Secure Socket Layer (SSL) or other encryption protocols are used. Other forms of spyware install an application on the user's computer that monitors and records all

[1] Adware is software that tracks a user's Internet browsing habits.

Internet communications and sends the report back to the originator. Identity thieves may then impersonate the customer using the IDs and passwords collected.

- Increasing vulnerability to "phishing" and "pharming" attacks, as some spyware can redirect Internet page requests. Phishing seeks to lure a user to a spoofed Web site using an e-mail that appears to come from a legitimate site. Pharming seeks to redirect a user to a spoofed Web site by introducing false data into a legitimate domain name server (DNS). The spoofed Web sites are set up to collect private customer information, such as account user IDs and passwords. In addition, objectionable or inappropriate information received by the customer from redirected Web sites can ultimately damage the financial institution's reputation.

Recommended Actions to Mitigate the Risks Associated With Spyware

Financial institutions should evaluate the risks associated with spyware and mitigate those risks by considering the following:

- Restricting users from downloading software, especially software not previously approved by the bank. This would prevent users from unwittingly downloading spyware.

- Ensuring that user settings are set to prompt the user whenever a Web site tries to install a new program or Active X control.[2] If possible, configure the browser to reject Active X controls to lessen the likelihood that spyware could be installed on computers through normal Internet browsing.

- Maintaining software patches. Several spyware programs take advantage of reported vulnerabilities that, if patched, would limit the spyware's effectiveness.

- Installing and maintaining current versions of anti-virus and anti-spyware programs.

- Expanding the risk-assessment process to consider threats from spyware. This ensures that the financial institution considers all risks to private customer information and takes appropriate steps to mitigate those risks.

- Expanding security and Internet use policies to include risks associated with spyware and acceptable user behavior (e.g., prohibiting Internet downloads and visits to inappropriate Websites). In addition, management should take steps to enforce these policies and reprimand staff who fail to comply with them.

- Expanding user awareness sessions to include the risks associated with spyware. Users will then become cognizant of the behavior they should adopt to prevent

[2] An Active X control is a set of instructions that will automatically run on a computer when downloaded by the browser.

spyware on bank computers and on personal computers that are used to connect to the bank's network.

- Installing and configuring firewalls to monitor both inbound and outbound traffic. If possible, block outbound ports that are not necessary for business functions. Financial institutions should assess the need for employee access to instant messaging as well as peer-to-peer services, and prevent access when a legitimate business need is not present.

- Implementing tools to scan e-mail for SPAM and either block the e-mail or designate it as SPAM. E-mail scanning can limit the likelihood that users could unknowingly infect their computers by viewing or reading e-mail that contains spyware.

- Implementing tools to restrict or prevent pop-up windows. This limits the likelihood that spyware will be downloaded through pop-up windows, either automatically or through user error.

- Following industry trends and developments regarding spyware and its prevention. Awareness enables the financial institution to adjust its practices as new spyware threats and prevention methods emerge.

- Reviewing the list of trusted root certificates[3] on a regular basis. Some spyware installs its own trusted certificates allowing it to intercept secure Internet communications or the execution of malicious code. Organizations that audit their trusted root certificates are more likely to identify certificates installed by unknown or untrusted sources. After researching the validity of these certificates, the financial institution can remove the ones that are installed by spyware.

- Analyzing firewall logs to determine whether a significant number of customers are connecting to Internet banking Web sites using the same Internet address. If research determines that the Internet address belongs to a service that intercepts Internet communications, consider blocking access to the Internet banking site from that address.

- Educating customers about the risks associated with spyware and encouraging them to implement steps to prevent and detect them on their own computers. In addition, advise customers of the risks of using public computers to connect to online banking Web sites.

- Investigating the implementation of multi-factor authentication methods, which would limit the ability of identity thieves to compromise customer accounts, even when a thief has a customer's ID, password and account numbers.

---

[3] Trusted root certificates enable the secure transmission of private information over the Internet through a protocol called Secure Socket Layer (SSL). A certificate is the electronic confirmation of the identity of an individual or organization by a reliable authority.

Actions Financial Institutions Should Recommend to Customers

Financial institutions also incur risks when customers connect to Internet banking sites using computers infected with spyware. Therefore, financial institutions should consider informing customers about the risks associated with spyware and recommending actions that customers can take to prevent spyware from being downloaded on their computers.

Customers can prevent and detect spyware by:

- Installing and periodically updating anti-spyware, virus protection and firewall software.
- Adjusting browser settings to prompt the user whenever a Web site tries to install a new program or Active-X control.
- Carefully reading all End User Licensing Agreements and avoiding downloading software when licensing agreements are difficult to understand.
- Maintaining patches to operating systems and browsers.
- Not opening e-mail from untrustworthy sources.