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.