

## SPYWARE AND IDENTITY THEFT

### Introduction

The Federal Trade Commission has proposed defining spyware as “software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer’s consent, or that asserts control over a computer without the consumer’s knowledge.”<sup>1</sup> Spyware is rapidly becoming the tool of choice for cyberthieves looking to commit identity theft using the Internet. The term “spyware” encompasses a variety of unwanted technologies<sup>2</sup> and is a threat to computers and any other devices that connect to the Internet (such as cell phones).

Spyware can be disseminated in a variety of ways. It is often bundled as part of free software, such as games and screen savers, and offered on the Internet. In other instances, it is distributed through email attachments, web links, and music or video downloads. Spyware can also exploit web browser vulnerabilities in “drive-by” downloads, where the computer user is unaware that he or she is downloading software. In other cases, the user is fooled into downloading spyware, believing it is a legitimate program such as a web browser update.

Infection by spyware can have a number of potentially harmful consequences and can result in the computer user’s having to spend considerable time and money to resolve these problems.<sup>3</sup> One potential effect is a dramatic slowing of the infected computer’s performance or system crashes. Another potential consequence of spyware can be changes to the computer’s settings, including security settings,

that can substantially reduce the consumer’s ability to control his or her own computer.

Spyware is capable of more serious harm: the theft of personal information resulting from the spyware monitoring a computer user’s activities. Further, spyware can lead to security breaches of personal information stored in computerized databases maintained by businesses, universities, and government agencies. While there are legitimate uses for monitoring software, such as employers monitoring the computer use of employees and parents monitoring their children’s online activities, cyberthieves are increasingly using these programs to facilitate identity theft.<sup>4</sup>

### How Spyware Can Lead to Identity Theft

Cyberthieves can use several different kinds of spyware to commit identity theft:

- **Keyloggers.** These programs monitor the actions of a computer user in order to gain access to financial accounts on the web by targeting specific information such as passwords, account numbers, and usernames. Keylogger programs can record every keystroke a computer user makes, thereby capturing email addresses and websites visited as well as any information the user enters on the computer. A file containing this information is sent to the cyberthief, who can extract the computer user’s sensitive personal information. One study estimates that nearly 10 million households in America have a computer infected with a keylogger program.<sup>5</sup> Researchers have noted that the number of websites spreading keylogger programs has increased dramatically in recent months (Chart 1).

---

<sup>1</sup> Federal Trade Commission. Public Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software. 69 Fed. Reg. 8538 (Feb. 24, 2004).

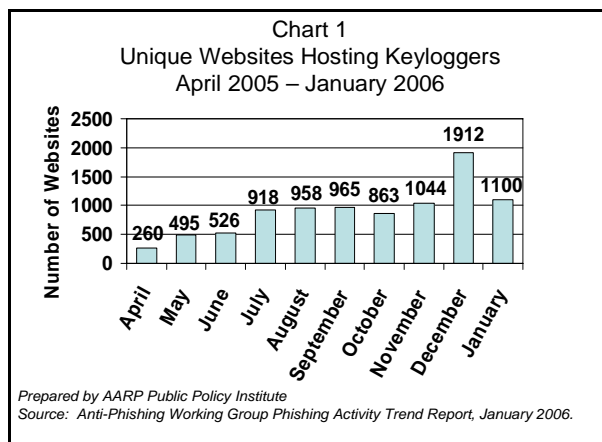
<sup>2</sup> Anti-Spyware Coalition. “Anti-Spyware Definitions and Supporting Documents—Working Report October 27, 2005.” <http://antispywarecoalition.org>

<sup>3</sup> Federal Trade Commission Staff Report. Public Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software (March 2005).

---

<sup>4</sup> T. Zeller Jr. “Cyberthieves Silently Copy Your Passwords as You Type.” *New York Times*, February 27, 2006.

<sup>5</sup> B. Krebs. “Hacking Made Easy.” *Washington Post*, March 16, 2006.



- **Redirectors.** These programs redirect web traffic to websites the user did not intend to visit. For example, a computer user types in the name of his or her financial institution and is unknowingly redirected to a fraudulent website that mimics the legitimate website to trick the user into providing password, username, and account information.
- **Remote access.** This type of spyware allows remote access to and control of the user's computer system by cyberthieves and can allow them to collect and share personal information without the user's knowledge. Remote access can also allow the user's computer to be used for illegal activities, such as sending spam or phishing emails or spreading keylogger programs.

### Responses to Spyware

Authorities are currently pursuing a number of responses to the challenge of spyware:

- **Technological.** Anti-spyware software that identifies and removes spyware from a user's computer is commercially available. Such anti-spyware programs typically can only identify known spyware programs, creating a lag time between distribution of a spyware program and the ability of anti-spyware programs to detect it.<sup>6</sup> Anti-spyware programs must also be updated continually to be effective. An AARP survey found that computer users age 65 and older were less likely to update anti-spyware programs than were younger computer users, thus diminishing the potential protective value of such programs.<sup>7</sup>

<sup>6</sup> Federal Trade Commission Staff Report, op. cit.

<sup>7</sup> R. N. Mayer. *Defending Your Financial Privacy: The Benefits and Limits of Self-Help*. Washington, DC: AARP Public Policy Institute, publication number #2006-06 (February 2006).

- **Behavioral change.** Another response to the threat of spyware is for computer users to change their online behavior to minimize their risk of encountering spyware. This can include not opening email attachments, not visiting particular websites, not downloading music or video files, or changing web browsers. A recent study indicates that computer users who have been victimized by spyware are more likely to make these types of behavioral changes than are individuals who have not been victimized.<sup>8</sup>
- **Legislative.** State and federal legislators have addressed the problem of spyware. In 2005, anti-spyware legislation was introduced at the federal level<sup>9</sup> and in 28 states.<sup>10</sup> Such legislation typically seeks to establish criminal penalties for unauthorized dissemination and use of spyware programs.

### Summary

While Internet users can reduce the possibility of being victimized by spyware, cyberthieves have substantial financial incentives to continue to develop newer and more sophisticated spyware programs. As a result, spyware programs probably will become more numerous, more difficult to detect, and more effective at gathering personal information. Therefore, consumers need additional defenses against the identity theft that can result from spyware. One such defense includes the imposition of a security freeze on their credit report information to prevent cyberthieves from using stolen personal information to open fraudulent accounts.

Written by Neal G. Walters  
AARP Public Policy Institute  
601 E St., NW  
Washington, DC 20049  
202-434-3910; E-Mail [ppi@aarp.org](mailto:ppi@aarp.org)  
April, 2006  
© 2006 AARP <http://www.aarp.org/ppi>  
Reprinting with permission only.

<sup>8</sup> S. Fox, *Spyware: The Threat of Unwanted Software Programs Is Changing the Way People Use the Internet*. Pew Internet & American Life Project (July 6, 2005).

<sup>9</sup> For example, H.R.29, H.R.744, H.R.1099, S.472 and S.687 were introduced in the 109th Congress.

<sup>10</sup> National Conference of State Legislators. "2005 State Legislation Relating to Internet Spyware or Adware." Accessed March 15, 2006, from [www.ncsl.org](http://www.ncsl.org).