Spyware has been identified as one of the emerging and growing threats to organizations. Because the Internet is an essential component of the student’s education experience, it is important to discern if our students are at risk and how to mitigate potential negative consequences. As a result, this paper describes spyware issues and empirically explores spyware incidence and student attitude. Findings suggest that undergraduates spend a considerable amount of time in activities that could result in spyware being installed on his/her computer. Moreover, results demonstrate that spyware incidence is prevalent, with an average of 141 spyware files found per student. An examination of student attitude also indicates that although 70% of students were either moderately or highly concerned about the existence of spyware on his/her computer, 25% indicated that he/she would not modify his/her behavior while 58% indicated only mild to moderate modification.

Keywords: Spyware, privacy, Internet, adware, survey

INTRODUCTION

Spyware, in general, is any technology that aids in gathering information about a person or organization without their knowledge (7). In terms of the Internet, spyware is software that is placed on a computer to surreptitiously gather information about the user and relay the information to advertisers or other interested parties. Spyware may get into a computer as a result of installing software or through a virus. Data collecting programs that are installed with the user's knowledge are not, technically speaking, considered spyware if the user fully understands what data is being collected and with whom it is being shared.

Most spyware programs are free and many are useful tools such as download utilities, games, media players, and accounting software (4). Spyware are considered two separate pieces of software shipped in one package. One component is the core functionality that is visible and useful to the user. The second component is the information-gathering functionality that gathers, maintains, monitors, and sends user and/or computer information in the background. To uniquely identify the data, either a Globally Unique Identifier is generated or a cookie is stored on the hard disk during the installation of the spyware program.

Spyware is comprised of three types of software: adware, key loggers, and Trojan horses (3). Adware is Internet jargon for “Advertising Supported software” (6). According to a recent report from the research firm Gartner C2, more than 20 million individuals have installed adware applications (3). Adware is a mechanism shareware authors can utilize to generate revenue from a product, other than by selling it to the users. Developers allow advertisers to place banner ads in the shareware products in exchange for a portion of the revenue from banner sales. By targeting ads based upon the user’s previous online browsing activities, marketers seek to
increase sales revenue. The downside is that the advertising companies also install additional tracking software on the system, which is continuously using the user’s Internet connection to report statistical data to the advertiser’s server. Companies such as DoubleClick and Gator use small files called cookies to track the user online (3). DoubleClick collects data such as Web log data, IP addresses, browser type and versions, screen resolution, time zone, and version numbers of installed software. Gator gathers the user’s first name, country, five-digit ZIP code, and list of installed software.

A second type of spyware is the key logger. Key loggers, such as those sold by WinWhatWhere, let others see the user’s every keystroke. The third type of spyware is the trojan horse. Trojan horses such as NetBus and Back Orifice enable hackers to not only track user behavior but also take control of the microcomputer.

Spyware is gaining the attention of the business community. In December 2002 and January 2003, 408 Information Technology professionals participated in an Internet threats study (9). The Emerging Internet Threats Survey 2003 published by Websense International Ltd. found that one in three companies have already detected spyware on their systems (8). Moreover, 68% consider spyware to be a growing and future threat. In addition, 70% of companies consider that peer-to-peer (P2P) file sharing is creating an "open door" into their organization. P2P networks help deliver and spread spyware. P2P applications include Kazaa, Morpheus, and Grokster (3). Kazaa, for example, includes DoubleClick and Morpheus includes Gator.

From an organizational perspective, spyware can result in several negative consequences. The immediate dangers relate to consumption of computing capacity, consumption of bandwidth, legal liabilities, and security issues (8). Because spyware is often loaded at system start-up and run continuously in the background, system processing can be greatly decreased. Moreover, the continual transmission of spyware data and pop-up banners can drain corporation Internet bandwidth. One of the largest problems is that spyware can result in an increase in spam. Spyware will often locate email addresses and pass the addresses to spammers. In January 2003, Ferris Research estimated that spam cost businesses $8.9 billion. Legal issues relate to file sharing programs such as Kazaa and their relation to copyright laws. Security issues are related to the covert operation of the spyware within the corporate systems.

From a personal perspective, spyware can result in similar problems. There is a danger that personal information such as passwords, card numbers, and account details could be stolen. A Spring 2003 study conducted by the Federal Trade Commission found that number of identity theft victims in the U.S. was 9.9 million during the previous 12 months (1). In addition, the spyware may take control of the microcomputer. Xupiter, for example, is an advertising and marketing program that launches pop-up ads, hijacks the browser’s home page, adds bookmarks to the browser’s menu, and transmits information about the user’s computer and surfing habits to xupiter.com (3). Another consequence is the proliferation of spam. Emarketer estimates that 76 billion spam emails were sent worldwide in 2003 (2). According to Brightmail, a company that blocks spam for six of the U.S.’s top ten Internet Service Providers, 40% of all Internet email is unsolicited and unwanted. Studies have demonstrated the frustration. A January 2003 Harris Interactive survey of 2,221 U.S. adults who use the Internet found 74% support making spam illegal (10). A Hanrick Associates study found that 68% of Net users believe spam is an abuse
of their privacy. A final consequence relates to anonymity. A 2003 PC World survey of 1500 Internet users found that 68% of respondents are very/extremely concerned about being tracking while Web surfing (1). Interestingly, although 88% worried about sites sharing or selling email addresses, only 33% frequently read privacy policies and 34% never change their passwords. On a positive note, 44% of respondents indicated utilizing anti-spyware/adware applications.

Because spyware is a relatively new concept, little research has been performed in the academic community. It is important to discern if our students are at risk and how to mitigate potential negative consequences. As a result, this survey explores and describes student spyware incidence.

**RESEARCH DESIGN**

This study employs a survey research design. The research was conducted at a private, northeastern U.S. University. A Student Spyware survey instrument was developed and administered in the Spring 2003 semester to undergraduate students enrolled in a School of Business course. The courses were BIS-310 “Business Information Systems” and BIS-320 “Business Telecommunications.” A sample of two class sections was selected. The classes were conducted by the same faculty member.

Immediately subsequent to discussing the concept of spyware in class, the faculty member emailed a shareware copy of Lavasoft’s Ad-aware 6.0 to all students in the classes. Ad-aware 6.0 has been identified by PC Magazine and PC World as one of the best spyware identification and removal programs (1) (5). Ad-aware has both a free version and two types of modestly priced software.

Students were given instructions how to install the software and how to perform a system scan. Moreover, students were informed that participation in the study was voluntary. During the next class meeting, the Student Spyware survey was administered. The survey instrument was utilized to collect student demographic data, gather spyware statistics, and examine student perceptions regarding his/her Internet behavior. The survey requested that each student estimate the average number of minutes per week that he/she spent on various Internet activities such as participation in gambling, buying, selling, downloading, and so on. All surveys were anonymous and students were informed that results would have no effect on their semester grade.

Surveys were keyed into a computer-based database management system to improve the ease of tabulation. A program was written to summarize and filter data.

**RESULTS**

Surveys were distributed to 46 students. A sample of 24 usable surveys was obtained. It should be noted that in two computers, Ad-aware disabled the systems, resulting in the necessity to completely restore the hard drives. Table 1 indicates that 58% of the respondents were male and 42% were female.

**TABLE 1**
Spyware: An Exploration Of Incidence and Student Perception

<table>
<thead>
<tr>
<th>Response Rate By Gender</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>58%</td>
</tr>
<tr>
<td>Female</td>
<td>42%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

The response rate by academic class is relatively equally distributed among Sophomore, Junior, and Senior classes. Table 2 illustrates that 0% of respondents are freshmen, 38% are sophomores, 33% are juniors, and 29% are seniors.

<table>
<thead>
<tr>
<th>TABLE 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Rate By Academic Class</td>
</tr>
<tr>
<td>Class</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Freshmen</td>
</tr>
<tr>
<td>Sophomore</td>
</tr>
<tr>
<td>Junior</td>
</tr>
<tr>
<td>Senior</td>
</tr>
</tbody>
</table>

Table 3 details student Internet behavior by type. The overall predominate behaviors include non-school related surfing, school-related Internet searches, and downloading music/movies. 96% of respondents indicated non-school related surfing, 92% indicated school-related Internet searches, and 75% indicated downloading music/movies. Moderate incidence behaviors include buying items (42%) and playing games (29%). The least common behaviors include selling items (4%) and gambling (0%). Responses were further examined to determine, of those students indicating a given behavior, how many minutes were devoted to each activity during a week period. The most minutes per week were devoted to playing games (107 minutes), downloading music/movies (95 minutes), non-school related surfing (91 minutes), and school-related Internet searches (54 minutes). The least amount of time was devoted to buying items (33 minutes), selling items (30 minutes), and gambling (0 minutes). Overall, students spend more than four hours (253 minutes) per week in these types of Internet behavior.
Table 3 depicts spyware incidence. The average number of spyware files found per student was 141. Moreover, 63% of respondents indicated that prior to this study, he/she was aware that his/her system contained spyware. When comparing prior awareness, considerable variance arises. The number of spyware files found was 107 for those students who were prior aware. The number of spyware files found was 194 for those students who were not prior aware.

Finally, respondents indicated his/her degree of concern and level of behavior modification as a result of his/her spyware findings (Table 5). 70% of students were either moderately or highly concerned about the existence of spyware on his/her computer. In terms of behavior modification, 25% indicated that he/she would not modify his/her behavior while 54% indicated moderate modification.
**TABLE 5**

<table>
<thead>
<tr>
<th>Resultant Behavior</th>
<th>None</th>
<th>Mild</th>
<th>Moderate</th>
<th>High</th>
<th>Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concern About Existence of Spyware On Your Computer</td>
<td>4%</td>
<td>13%</td>
<td>33%</td>
<td>37%</td>
<td>13%</td>
</tr>
<tr>
<td>Will You Modify Your Internet Behavior?</td>
<td>25%</td>
<td>4%</td>
<td>54%</td>
<td>13%</td>
<td>4%</td>
</tr>
</tbody>
</table>

**CONCLUSIONS AND FUTURE RESEARCH**

Results suggest that undergraduates spend a considerable amount of time in activities that could result in spyware being installed on his/her computer. 96% of respondents indicated non-school related surfing, 92% indicated school-related Internet searches, and 75% indicated downloading music/movies. Moderate incidence behaviors include buying items (42%) and playing games (29%). The least common behaviors include selling items (4%) and gambling (0%). The most minutes per week were devoted to playing games (107 minutes), downloading music/movies (95 minutes), non-school related surfing (91 minutes), and school-related Internet searches (54 minutes). The least amount of time was devoted to buying items (33 minutes), selling items (30 minutes), and gambling (0 minutes). Overall, students spend an average of 253 minutes, or more than four hours per week, in these types of Internet behavior.

Moreover, findings demonstrate that spyware incidence is prevalent. The average number of spyware files found per student was 141. The 63% of respondents indicating prior awareness of spyware on his/her system had an average of 107 spyware files. The remaining respondents found an average of 194 spyware files. In terms of concern, 70% of students were either moderately or highly concerned about the existence of spyware on his/her computer. In terms of behavior modification, 25% indicated that he/she would not modify his/her behavior while 58% indicated mild to moderate modification.

There are two important implications as a result of these findings. One implication is that non-school related Internet behavior is common. Although 92% of students indicated using the Internet for school-related searches, only 21% (54 minutes per week) of total time is devoted to school-related activities. From an academic standpoint, the 8 minutes per day may suggest that either students are extremely efficient Internet searchers or Internet resources are not being fully utilized and need to be better incorporated into academic curriculum.

A second implication relates to spyware incidence and student attitude. Spyware incidence is common, even though most students are aware of its existence. For students who are unaware, the amount of spyware nearby doubles. Student attitude provides further mixed results. Even though 70% of students are moderately to highly concerned, 25% indicated that he/she would not modify his/her behavior and only 17% indicated a high or extreme modification. It is possible that students are not concerned about potential spyware problems and/or need further education regarding privacy issues.
The limitations of this study are primarily a function of sample size, academic class, and type of research. A larger sample size and use of additional universities would increase the robustness of results. In addition, a better distribution among academic class may provide additional detail regarding behavior. Another limitation relates to the self-reported nature of the survey. Students are using recall to estimate activity. Memory may be unreliable and recency effects may occur. In addition, the Hawthorne Effect may be evident. This effect is minimized due to respondent anonymity.

Future research should be directed examining which factors are the most influential and can be manipulated to modify student behavior to minimize the level and risks of spyware. Analysis of the spyware list may lead to greater understanding of the behavior source. Also, an examination by academic class and attitude could provide further insight into cause and effect. Overall, the current results and future research will assist educators in improving the student education experience and decreasing student exposure to potentially negative situations.

REFERENCES