IS SPYWARE AN Internet Nuisance or Public Menace?

Why are so many users seemingly complacent about the presence of spyware on their PCs? Research findings suggest several factors influence users to take action against it.

Recent media attention to spyware [2, 5, 7, 8] has brought to light the blunt intrusion into individual privacy and the uncertain hidden cost of free access to Internet sites, along with freeware and shareware. Most spyware programs belong to the more benign category of adware that delivers targeted pop-up ads based on a user’s Web surfing habits. The more malicious type of spyware tracks each keystroke of the user and sends that
information to its proprietors. Such information could be used for legitimate data mining purposes or it could be abused by others for identity theft and financial crimes.

Unlike other Internet-spawned malicious software programs, such as computer viruses that evoke trepidation among users and cause millions of dollars worth of direct damages to organizations, spyware seems to generate a more lackadaisical reaction from users in spite of the predicted dire consequences [4, 10]. Many users seem to accept spyware as the price for getting freeware and shareware online or are simply unaware of it and its consequences [9]. “I can’t surf the Web and I can’t trade files if I uninstall the spyware. Why can’t the college let me do what I want to do with my computer? The school computer security guys are being way more annoying than the spyware was,” said a college student in reaction to his university’s decision to block access to spyware servers from its campuses [4].

It is not that spyware is any less disruptive or damaging than computer viruses. While viruses such as the infamous “I Love You” virus could cause serious disruptions to corporate networks and the entire Internet, spyware could inflict as much damage to organizations and individuals [10]. The most destructive scenario is perhaps that spyware on corporate desktops could compromise the regulatory compliance efforts by leaking private customer data entrusted to protect and therefore open up potential legal vulnerabilities [6].

Moreover, cleaning spyware from infected systems is not any easier than ridding computers of viruses. In many ways, spyware intrusion is more difficult to defend against and disinfection is more complicated than viruses. Most anti-virus software packages now prevalent on corporate computers cannot detect the existence of spyware¹ and many spyware programs have a feature that will automatically reinstall if removed. It takes a special breed of anti-spyware software to do the job properly.

### Table 1. Computer knowledge and awareness of spyware.

<table>
<thead>
<tr>
<th>Action Taken</th>
<th>Overall (%) N=229</th>
<th>MIS/CS (%) N=140</th>
<th>Business Majors (%) N=74</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>12.2</td>
<td>7.9</td>
<td>20.3</td>
</tr>
<tr>
<td>Rarely</td>
<td>16.7</td>
<td>15.7</td>
<td>18.9</td>
</tr>
<tr>
<td>Sometimes</td>
<td>23.9</td>
<td>25.7</td>
<td>21.6</td>
</tr>
<tr>
<td>Often</td>
<td>32.9</td>
<td>34.3</td>
<td>27.0</td>
</tr>
<tr>
<td>All the time</td>
<td>14.4</td>
<td>16.4</td>
<td>12.2</td>
</tr>
</tbody>
</table>

### Table 2. Actions (cleaning or protecting computers) against spyware.

<table>
<thead>
<tr>
<th>Action Taken</th>
<th>Overall (%) N=229</th>
<th>MIS/CS (%) N=140</th>
<th>Business Majors (%) N=74</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>12.2</td>
<td>7.9</td>
<td>20.3</td>
</tr>
<tr>
<td>Rarely</td>
<td>16.7</td>
<td>15.7</td>
<td>18.9</td>
</tr>
<tr>
<td>Sometimes</td>
<td>23.9</td>
<td>25.7</td>
<td>21.6</td>
</tr>
<tr>
<td>Often</td>
<td>32.9</td>
<td>34.3</td>
<td>27.0</td>
</tr>
<tr>
<td>All the time</td>
<td>14.4</td>
<td>16.4</td>
<td>12.2</td>
</tr>
</tbody>
</table>

So how do we explain the lack of action among Internet users against spyware? Is it true to assume most users are oblivious to spyware? To understand the user behavior about spyware we must start with user attitudes and what influences them [10]. We report our research findings on spyware in an attempt to shed some light on user attitudes, and subsequent behavior toward, protecting from and cleaning up spyware.

### About the Research

In order to understand the apparent passivity of Internet users toward spyware, we conducted a survey of IS professionals and students in a large state university located in the southeastern U.S. The survey instrument was developed based on a theoretical model developed from Azjen’s Theory of Planned Behavior (TPB) [1], which contends that a person’s actions are determined by his or her intention to perform the behavior of interest. This behavioral intention is in turn determined by three factors: attitude toward the behavior (ATB), subjective norm (SN), and perceived behavioral control (PBC). ATB refers to a person’s judgment on whether it is good or bad to perform a behavior of interest; SN is a person’s perception of the social pressure to perform or not perform the behavior in question; and PBC refers to the perceived ease or difficulty of performing the behavior. Figure 1 shows the proposed relationships in the TPB as described in [1].

Considering the unique context of spyware, we introduced a number of factors that influence the three original determinants of the behavioral intention—

---

¹This situation may change in the near future. For example, McAfee recently announced an add-on for its enterprise anti-virus products to offer increased protection against spyware to be available by the end of the year.
the most important being awareness. There is limited IS research on the importance of awareness mainly because IT adoption happens mostly in the workplace rather than at the individual level, and because awareness is primarily related to user-initiated actions instead of organizational ones covered in technology acceptance literature. For example, social and medical sciences have long recognized the importance of raising public and personal awareness in fighting against political and social injustices or protecting from diseases. Spyware belongs to the class of technologies that have emerged as a problem, a threat, a “disease,” as compared to the traditional technologies intended to be beneficial to organizations and individuals. Thus, the importance of awareness in technology acceptance must be conceptualized in spyware research. In addition, we included two important factors of the well-known technology acceptance model (TAM) [3]—perceived usefulness and perceived ease of use—as predictors of user attitudes and behavior toward spyware and anti-spyware technologies.

We developed a survey instrument based on this theoretical model. Since a rich body of literature on TPB and TAM is available, we adapted published measurements for all the factors, with the exception of awareness factor for which we developed our own measurements. The instrument was then pilot tested for clarity, consistency, and validity using students from one of the authors’ programming classes. The pilot test resulted in only minor changes to the instrument, which was then posted on the research Web site. We asked students enrolled in various MIS and business classes to fill out the online questionnaire during class time. We also sent email messages to IS professionals who are graduates of the university requesting their participation in the study. Over a three-week period, 229 respondents completed the online survey, of which seven were unusable because of missing responses and were removed from the sample. Among the remaining respondents, 62% were male and 38% female, 63% either had or were pursuing an MIS/CS degree, 34% had or were pursuing business-related degrees, and 3% had degrees in other disciplines. Some background information is shown in Tables 1 and 2.

It is interesting to note that only a small percentage of all respondents (<15%) indicated they never heard of spyware or didn’t know the details. Understandably, this percentage is higher among the respondents with or pursuing non-MIS/CS degrees (23%), but it is still significantly higher than a recent AOL survey in which over 90% of the respondents didn’t know what spyware programs were [9].

Another observation from Tables 1 and 2 is that respondents with or pursuing MIS/CS degrees are much more knowledgeable about spyware than their business counterparts. This is not surprising. Interestingly, however, the percentage of respondents who actually took actions against spyware is significantly lower in both MIS/CS and non-MIS/CS samples. This reinforces our research
question: Why do users appear not to be very concerned about spyware?

To answer this question and test our model, we analyzed the survey responses using LISREL software to identify the key predictors of user actions or inaction toward spyware. The diagnostic statistics suggest that overall the model shows strong internal consistency and external validity, confirming the validity of the measurement instrument and the predictive power of the model. What is interesting, however, is the significant relationships among the major factors of the behavioral model that shows why users take active measures to protect their computers from spyware and what motivates them to move in that direction. The result of the structural equation model is presented in Figure 2. The numbers shown are the statistical indicators of the strength of the relationships between the factors; the asterisks indicate the statistics are significant at 1% level.

Awareness is a key predictor of taking actions. It is clear that the awareness factor emerged as the most significant determinant of user behavior of taking active measures to protect against spyware intrusion and clean spyware from infected systems. Awareness not only influences ATB and SN, but also has a direct influence on the intention to protect and clean, thus on the actual behavior of protecting and cleaning. This result suggests if users are aware of the potential damage spyware might inflict on them, there is a strong likelihood they will take action to protect themselves. Once users are aware their systems are infected with spyware, it is highly likely they will attempt to clean them. This lack of awareness might explain why more than 80% of the computers examined by AOL experts had spyware on them; and about 90% of those whose computers were infected with spyware didn’t know about the infection and had no clue what spyware was [9]. We want to emphasize that awareness in the structural equation model is not a single categorical measure of “know” or “not know,” but a psychological construct measured using multiple items to indicate degrees of user knowledge about spyware and anti-spyware technologies.

Perceived usefulness provides motivation for action. Even though awareness is the most important determinant of user action against spyware, our results suggest that users must also be motivated by the perceived usefulness of anti-spyware programs in order to develop a favorable attitude toward taking actions to protect and clean their computers. The perceived usefulness (PU) factor is a strong and significant determinant to attitudes toward ATB and SN. It is intuitive why PU influences ATB. However, the impact of PU on SN is not immediately apparent. A closer look at how social pressures are formed and exerted on members of a social group reveals that only if members of the social group believe certain actions are useful and beneficial, then social norms related to the action begin to merge and to shape the behavior of its members. Thus, perceived usefulness must precede the formation of social norms and its influence on behavior.

Perceived ease of use is the final hurdle to action. Technology acceptance literature has long recognized the significance of perceived ease of use in the users’ decision whether or not to adopt a certain technology. There seems to be no exception in the case of user acceptance of anti-spyware practices and tools. Our results suggest that two ease-of-use related factors, the perceived ease of use (PEOU) of anti-spyware programs, and the perceived controllability (PC) of taking action against spyware are determinants of the perceived behavior control (PBC). Since PBC is defined as the perceived ease or difficulty of performing the behavior and it is assumed to reflect the past experience as
well as anticipated impediments and obstacles, it is understandable why PEOU is one of its determinants. Furthermore, a higher degree of perceived controllability is an indication of a higher degree of certainty, thus higher degree of perceived behavior control.

In the case of spyware, if a user knows how to use an anti-spyware program to clean infected computers or has had the experience of configuring computers to prevent the infection of spyware, he or she would feel a higher degree of control when performing these tasks. On the other hand, even if a user has a favorable attitude toward actions against spyware and is motivated to do so, he or she still might not perform the tasks for fear of not being able to clean the computer or changing the current system settings in a way that might result in more severe disruptions to his or her work than those caused by the presence of spyware. This might explain why the percentage of respondents indicating spyware awareness is much higher than the percentage of respondents taking actions against spyware.

From attitude, subjective norm, and perceived behavior control to action. The TPB posits that the more favorable the attitude and subjective norm with respect to a behavior, and the greater the PBC, the stronger should be an individual’s intention to perform the behavior under consideration [1]. In the context of spyware, our analyses yield strong evidence to support this theory. All of the purported relationships in the theory as shown in Figure 1 are supported by the statistics of the structural equation model. The results suggest that whether a user takes action against spyware is most influenced by whether he or she has the intention and the resources (tools and skills) to perform the task. The intention, in turn, is determined by his or her attitudes toward performing such a task, the social pressure (from peers and influential figures in their social group), and the resources involved. Ultimately, it comes down to four key determinants: awareness of spyware, perceived usefulness of the action, perceived controllability of the action (tools, skills, and experience), and perceived ease of the action.

Conclusion

The rampant invasion of spyware into home and business computers threatens the foundations of the networked economy with far-reaching legal and financial consequences. Yet many computer users appeared to be complacent with the status quo and either willingly or unwillingly accommodated the blatant invasion into their privacy by spyware and its proprietors.

Our study shows that in most cases such behavior is not the result of a rational decision but rather a consequence of lack of understanding of the real implications of privacy and security in the Internet age. It essentially comes down to a simple question: How do you solve a problem if you don’t recognize its existence?

Spyware is more than an Internet nuisance. At
the very least, it is an abuse of public trust by marketers, at the worst, a computer crime that can inflict real financial damages and uncertain legal consequences to individuals and organizations. The most effective way to win the battle against spyware is to first educate the public and increase public awareness of spyware—and its consequences—and then provide the tools and the training to detect and disinfect. Recent moves by some major system and anti-virus software companies to integrate anti-spyware programs in their product offerings [11] will certainly empower the public and enable the containment of spyware to a similar level of awareness and control of computer viruses today.

References