

By XIAONI ZHANG

What Do Consumers Really Know

Technology has revolutionized information collection and distribution to the point where marketers have expanded and implemented new technologies to enable efficient consumer information acquisition. Such sophisticated data collection methods have raised serious concerns about consumer privacy, as some marketers have quickly discovered ways to abuse this power.

Although relatively unknown a year ago, spyware is now simply exploding and finding its way into millions of computers worldwide. The top three spyware firms in the U.S. claim their software is installed on approximately

Most users know spyware is “out there,” but are woefully lost when it comes to preventing it or removing it.

About Spyware?

100 million PCs [4]. EarthLink/Webroot reports an average of 28 spyware programs running on each PC it scanned. Websense, a network monitoring firm, reports the presence of spyware on 92% of the PCs examined in an April 2004 study of firms with 100+ employees [12]. In addition, industry leaders like Microsoft have accused spyware of causing application crashes and deteriorating PC performance [12].

Spyware resides on PCs, tracking users' movements on the Web, and hijacking Web browsers. It monitors a user's online activities and triggers unwanted advertisement displays. Spyware represents one of many plagues on the Internet, comparable to spam and viruses. Spyware is also devious as it resides on a PC without the user's knowledge. The nature of spyware contributes to unfair information practices, yet many consumers do not even realize its existence and the harm it can impart. As a result, they do not take appropriate procedures to protect their privacy.

Spyware falls under the category of privacy invasion. It poses a serious violation of fair information practice principles developed by U.S. Federal Trade Commission [5]. Ethical information collection should (at the very least) be based upon transparency,

adequate notice, and consumer choice. Its existence raises legitimate privacy and security risks as well as prevents consumers from reaching the Web sites they desire.

Because of the significance of privacy concerns and the prevalence of spyware, it is crucial the general public knows how to protect themselves. Here, we present the findings of a study on consumers' spyware awareness, particularly regarding general PC use habits, security procedures performed, and the general spyware knowledge. To protect consumers and develop educational goals to minimize the risks associated with spyware, we focused on three questions: How much does an individual understand spyware? What are the individual's PC hygiene habits? What are the factors that relate to spyware awareness?

CONCEPTUAL FRAMEWORK

The theoretical bases for this work are drawn from two streams of research—consumer Web behavior and consumer knowledge [2, 11]. The concepts we draw from consumer Web behavior literature are Web security and Web usage. Consumer Web behavior

It is critical for consumers to understand Internet-based risks and to realize

**THEIR OWN ROLE
IN PROTECTING
THEMSELVES IN
A DIGITAL
ENVIRONMENT.**

literature suggests Web usage includes functional activities, such as information searching, communication, and online shopping, as well as entertainment activities, such as listening to music or watching video clips. Prior works conclude that such motivation contains both utilitarian and hedonic dimensions [2]. Others contend that identifying consumer Internet shopping behavior is critical in effective market segmentation. Consumers use search engines to primarily look for needed information. Search mechanisms and shopping enjoyment are surely correlated, and thus affect the consumer's intention to purchase online [6].

Consumer knowledge literature argues strongly that knowledge has a significant and essential influence on the consumer's decision making. Knowledge encompasses two components: product familiarity and expertise. Consumer knowledge is found to relate to privacy protection, consumer defection, consumer choice, information search, and perceived product

category uncertainty. Knowledge enables consumers to shorten the time needed to make decisions and reduce the cognitive effort to perform the tasks [1]. We adapted the concept of consumer knowledge in marketing and psychology to the spyware context and incorporated other variables pertinent to our research questions related to spyware.

As an emerging topic with severe consumer privacy implications, spyware demands immediate attention. It was initially created for target marketing and was adopted by advertisers because of its effectiveness. Today, online advertising represents a \$6.9-billion-a-year market and adware is among the fastest-growing segments, according to the research firm eMarketer [7]. Marketers use spyware to collect users' buying information so that personalized marketing messages can be delivered to the users.

Web users may perform some activities that unknowingly cause spyware to be loaded on their computers. The main sources of spyware infections are pop-ups, free downloads, and shareware. Some spyware has the capability of recording everything users type such as user names, passwords, and credit card numbers. Spyware can take control of the user's browser, display unwanted ads, collect confidential information, redirect users to erroneous Web sites, and even monitor Web user's behavior for potentially malicious purposes.

The consumer's knowledge about the PC and Internet affect their behavior toward personal protection with computers. Because of the privacy invasions spyware brings, anti-spyware utilities are becoming necessary software to safeguard desktop security [3]. Spyware is resilient, therefore multiple anti-spyware programs should be installed in order to effectively combat it.

STUDY APPROACH AND FINDINGS

Our survey explored consumers' general knowledge on security concerns and spyware invasions, surfing habits, security awareness, and Internet usage habits.

A total of 500 surveys were given to business majors; their responses were voluntary. In the end, we received 252 usable responses; 54% from males and 46% from females. To determine the participants' computer experiences, we ask years of computer usage, years of Internet usage, years of online banking, and years of online bill paying. Table 1 shows the descriptive statistics of computer usage experience in this study.

Five factors emerge from the sample we surveyed: PC hygiene, online transaction habits, knowledge on spyware, knowledge on security, and spyware sources.

Most survey questions are based on a 7-point Likert scale with 1 indicating strongly disagree and 7 indicating strongly agree. Table 2 indicates the mean scores of the measures of the five factors examined.

PC hygiene refers to the activities respondents perform to keep their PC healthy. Specifically, we look at issues related to updating Windows, updating Web browser, and updating anti-virus software. Of the participants, 29.8% installed Windows Service Pack 2 on their computer; 41.7% installed anti-spyware software; and 84.7% installed anti-virus software. Among those respondents who installed anti-spyware, only 22% turn on real-time monitoring features. Among those who installed anti-virus software, only 39.2% turn on real-time monitoring features. By comparing the mean scores of the three measures, it seems the respondents are more aware of updating anti-virus software than updating Windows and Windows Explorer. The responses also show that some misconceptions exist about spyware and viruses. Some respondents think spyware is equivalent to a computer virus.

Online transaction habits. On average, respondents spend 8.55 hours per week surfing the Net. With this amount of the usage, it is very likely that most respondents have spyware on their computers whether or not they are aware of its existence. With respect to online activities, 84.4% purchased goods online; 58% conducted e-banking; and 45.5% paid bills online. These results indicate that Internet shopping is well accepted by respondents, but financially sensitive activities such as e-banking and online bill paying are not as popular.

Knowledge of spyware examines the basic concepts about spyware, what it is, and what it does. We used four measures to assess the respondents' knowledge of spyware: tracking keystrokes, recording online transactions, monitoring online surfing habits and residing on computers. Spyware is capable of per-

| | Means | Std. Deviation |
|------------------------------|-------|----------------|
| Years of Computer Use | 10.22 | 3.69 |
| Years of Internet Use | 7.17 | 2.64 |
| Years of Internet Purchase | 3.22 | 2.45 |
| Years of Online Banking | 1.40 | 1.590 |
| Years of Paying Bills Online | 0.96 | 1.380 |

Table 1. Computer experiences.

| | Means | Cronbach's Alpha |
|---|-------------|------------------|
| PC Hygiene | 3.67 | 0.82 |
| • Updating Web browser | 3.39 | |
| • Updating Windows | 3.65 | |
| • Updating anti-virus software | 3.98 | |
| Online Transaction Habits | 3.59 | 0.82 |
| • Online shopping | 3.87 | |
| • Online banking | 3.85 | |
| • Online bill paying | 3.06 | |
| Knowledge on Spyware | 3.90 | 0.88 |
| • Tracing keystrokes | 3.75 | |
| • Residing on computers | 3.94 | |
| • Monitoring surfing behaviors | 4.30 | |
| • Recording online transactions | 3.62 | |
| Spyware Sources | 2.23 | 0.70 |
| • Downloading free music | 2.14 | |
| • Downloading shareware | 3.29 | |
| • Clicking pop-up | 1.27 | |
| Knowledge on Security | 3.76 | 0.93 |
| • Knowledge on privacy violation | 3.42 | |
| • Knowledge on security issues | 3.83 | |
| • Knowledge on protecting oneself | 4.03 | |
| • Updating knowledge on security related technologies | 3.43 | |

forming these activities, but most respondents are only familiar with one aspect of spyware—monitoring surfing habits. Among these four measures, recording online transactions has the lowest mean. In addition, 45.6% of the respondents are aware of their PC being infested by spyware, indicating the majority of respondents do not fully understand the nature of spyware.

Spyware sources. A PC may become infected with spyware when users click pop-ups, download free music, and/or download shareware. The mean scores, indicating how often users engage in these activities are 1.27, 2.14, and 3.29 respectively, indicating the

general annoyance of and lack of interest in pop-up ads. However, respondents are more likely to download shareware, although only 6.4% read the end-user agreement carefully; while another 4% read “most” of the agreement.

Knowledge on security examines users' knowledge of Internet privacy, security issues, self-protection on the Internet, and updating knowledge on security technologies. Among these four measures, Internet privacy had the lowest score, suggesting respondents' lack such knowledge. Although 45.6% are aware of the existence of spyware on their computer, only 41.7% take protective efforts to fight it.

Table 2. Factors and measures.

Their insufficient action against spyware may be due to the lack of knowledge about the potential damages it can bring or the lack of knowledge about how to use technologies to defend themselves.

IMPLICATIONS

The results of our survey show respondents do not have sufficient knowledge about security, privacy, and spyware. Privacy is currently self-regulated by industries. Consumer privacy lies in the hands of industry, which has an obligation to perform fair information practices. It is critical for consumers to understand Internet-based risks and to realize their own role in protecting themselves in a digital environment.

Safe surfing and PC hygiene habits affect consumers' ability to protect their personal information. Because shareware and freeware are sources of spyware infections, consumers must be aware of the trade-off involved when downloading freeware or shareware.

The most effective way to defend privacy is to be educated about privacy-related technologies and to be constantly vigilant. Consumers must be empowered—and take proactive steps—to control their personal information and safeguard their privacy. Indeed, it is useful to educate consumers about the latest protective tools on privacy and security and so raise awareness of the security and privacy. More and better information concerning consumer rights, Internet threats, and technological tools available to protect consumers must be provided to consumers.

In the academic environment, developing courses related to security and privacy seems imperative. Such a course should be designed as a requirement for all majors because of the increasing computer-based threats. Better educating future technologists will benefit future employers.

Educating businesses with the proper information collection and distribution is also necessary. Developing corporate policies and values on privacy is vital because corporate IT and marketing actions visibly influence the way organizations deal with customers, prospects, employees, shareholders, and the media. In the long run, business success depends on ethical behavior and the development of privacy and data protection should be valued as a key component of organizations' business strategies. Marketers must balance their information needs with consumer privacy and perform fair information practices ethically and responsibly.

Businesses must also develop best practices to collect and use consumers' personal information by notifying and getting consent from consumers instead of surreptitiously collecting and disseminating information. An alternative to educating customers and business is government regulation, but this approach would add substantially to the cost of doing business.

CONCLUSION

Internet threats are constantly evolving and developing. This study examines consumers' awareness of spyware, safe Web practices, and consumers' knowledge of spyware removal mechanisms. The results show that privacy invasions created by spyware are not noticed adequately by respondents. Despite experience with computers and the Internet, many consumers are neither aware of spyware intrusion nor knowledgeable of spyware

removal tools available to them. Due to this lack of knowledge, they have not taken adequate steps to protect themselves. This calls for an urgent need for consumer education.

The right to privacy in Internet activities is a serious issue facing society. Spyware represents a serious privacy invasion brought on by technologies. Providing consumers with more knowledge and control over information exchange can best protect their privacy [9]. In the information age, it is important for consumers to realize that privacy can be invaded without entering the home or in any other visible or disruptive ways. Consumer online behaviors are monitored insidiously by spyware. Technological innovations make consumers particularly vulnerable to lose control of their basic human right—the right to privacy. **C**

REFERENCES

1. Alba, J.W., and Hutchinson, J.W. Dimensions of consumer expertise. *J. Consumer Research* 13, 4 (1987), 411–454.
2. Childers, T.L., Carr, C.L., Peck, J., and Carson, S. Hedonic and utilitarian motivations for online retail shopping behavior. *J. Retailing* 77, 4 (2001), 511–536.
3. Clyman, J. Antispyware. *PC Magazine* 23, 13 (Aug. 3, 2004), 89.
4. Economist. A hidden menace. (June 5, 2004), 61–66.
5. Federal Trade Commission. *Self-Regulation and Privacy Online: A Report to Congress* (July 1999). Washington, DC.
6. Koufaris, M., Kambil, A., and Labarbera, P.A. Consumer behavior in Web-based commerce: An empirical study. *Intern. J. Electronic Commerce* 61, 2 (2001), 115–138.
7. Martin, R. Spy vs. spy. *Fortune Small Business* 14, 4 (May 2004), 59–61.
8. Metz, C., Clyman, J., Karagiannis, K., Carroll, S. and Rubenking, N. SPY stoppers. *PC Magazine* 23, 4 (Mar. 2, 2004), 79–92.
9. Milne, George R. Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview. *J. Public Policy & Marketing* (Special Issue) 19, 1 (2000), 1–6.
10. Nunnally, J.C. *Psychometric Theory, 2nd Ed.* McGraw-Hill Book Company, New York, 1978.
11. Page, K. and Uncles, M. Consumer knowledge of the World Wide Web: Conceptualization and measurement. *Psychology & Marketing* 21, 8 (2004), 573–591.
12. Spring, T. Striking back at spyware. *PC World* 22, 7 (July 2004), 36–38.

XIAONI ZHANG (zhangx@nku.edu) is an assistant professor of information systems at Northern Kentucky University, Highland Heights, KY.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
