PEW / INTERNET

PEW INTERNET & AMERICAN LIFE PROJECT

Spyware

The threat of unwanted software programs is changing the way people use the internet.

Embargoed until 4pm Eastern on 6 July 2005

Susannah Fox, Associate Director

PEW INTERNET & AMERICAN LIFE PROJECT 1615 L ST., NW – SUITE 700 WASHINGTON, D.C. 20036

202-419-4500 http://www.pewinternet.org/

Summary of Findings

Nine out of ten internet users say they have adjusted their online behavior out of fear of falling victim to software intrusions.

Spyware and the threat of unwanted programs being secretly loaded onto computers are becoming serious threats online. Tens of millions of Americans have been affected in the past year by software intrusions and many more have begun to take precautions by changing the way they use the internet. Overall, 91% of internet users say they have made at least one change in their online behavior to avoid unwanted software programs. Among the changes:

- 81% of internet users say they have stopped opening email attachments unless they are sure these documents are safe.
- 48% of internet users say they have stopped visiting particular Web sites that they fear might deposit unwanted programs on their computers.
- 25% of internet users say they have stopped downloading music or video files from peer-to-peer networks to avoid getting unwanted software programs on their computers.
- 18% of internet users say they have started using a different Web browser to avoid software intrusions.

Unfortunately, many internet users' fears are grounded in experience.

After hearing descriptions of "spyware" and "adware," 43% of internet users, or about 59 million American adults, say they have had one of these programs on their home computer. This is probably a conservative estimate since this survey may have been the first time that respondents had heard definitions of the programs. In addition, there are significant gaps between people's perceptions and the reality of what is on their computers and there is a very strong likelihood that a big portion of those who have had computer problems have been victimized by spyware or more aggressive computer viruses without their knowing the cause of their problems. For instance, in October 2004, the Online Safety Study by AOL and the National Cyber Security Alliance reported that 53% of respondents said they had spyware or adware on their computers, but a scan revealed that 80% of respondents actually had such programs installed.

Although most do not know the source of their woes, tens of millions have experienced

This Pew Internet & American Life Project report is based on the findings of a daily tracking survey on Americans' use of the internet. All numerical data was gathered through telephone interviews conducted by Princeton Survey Research Associates between May 4 and June 7, 2005, among a sample of 2,001 adults, aged 18 and older. For results based on the total sample, one can say with 95% confidence that the error attributable to sampling and other random effects is +/- 2%. For results based internet users (n=1,336), the margin of sampling error is +/- 3%.

Pew Internet & American Life Project, 1615 L St., NW, Suite 700, Washington, DC 20036
202-419-4500 http://www.pewinternet.org

computer problems in the past year that are consistent with problems caused by spyware or viruses:

- 52% of home internet users say their computer has slowed down or is not running as fast as it used to.
- 51% of home internet users say their computer started freezing up or crashing, requiring them to shut down or reset.
- 25% of home internet users say a new program appeared on their computer that they didn't install or new icons suddenly appeared on their desktop.
- 18% of home internet users say their internet home page changed without them resetting it.

In sum, 68% of home internet users, or about 93 million American adults, have experienced at least one of these problems in the past year. Sixty percent of internet users who report computer problems do not know the source, but those who do know cite viruses, spyware, adware, operating system flaws, and hardware glitches. Not everyone attempted a fix, but those who did often found that they needed help, paid or unpaid. About 28 million American adults ended up spending money to get their computer working again, typically in the range of $100.

The definitions of spyware and adware may not be clear to many internet users, but many believe that surveillance and unwanted software are serious threats to users' security and privacy.

Before exploring the issues in depth, we asked survey respondents if they knew what certain terms meant. Eight in ten internet users say they have a good idea about what spyware is, but only half of internet users claim to have a grasp of the concept of adware. In later questions, the following descriptions were used:

- "As you may know, certain software programs – sometimes called 'spyware' – can be installed on a person's computer without their explicit consent, either by 'piggy-backing' onto a file or program the person downloads from the internet or just by visiting a particular Web site. These programs can keep track of a person's internet habits and the sites they visit, and can transmit this information back to a central source."
- "Another kind of software program – sometimes called 'adware' – comes bundled with free files and programs people download from the internet, such as games, file-sharing programs, and screensavers. These programs can keep track of a person's internet habits and the sites they visit, and can use that information to provide targeted advertising on the person's computer."

Half of internet users see software programs like spyware as a serious threat to their online security. About a quarter say they are a minor problem and more should be done to control them and the rest say such programs are just part of life on the internet and don't really bother them. Not surprisingly, 61% of internet users who report having had

spyware say it is a serious threat, compared to 43% of internet users who say they have not had spyware on their home computer.

Eight in ten internet users (and 90% of internet users who report having had adware) say that more should be done to alert consumers to the presence of adware in files they are downloading. Only about one in ten internet users say the current practice of clicking through a user agreement or disclaimer is adequate consent to install adware on a person's computer.

Spyware: Summary of Findings at a Glance
Nine out of ten internet users say they have adjusted their online behavior out of fear of falling victim to software intrusions.
Unfortunately, many internet users' fears are grounded in experience.
The definitions of spyware and adware may not be clear to many internet users, but many believe that surveillance and unwanted software are serious threats to users' security and privacy.
Source: Fox, Susannah. *Spyware*. Washington, DC: Pew Internet & American Life Project, July 6, 2005.

Contents

Acknowledgements

The author would like to acknowledge the contributions to this study by the following people:

Kristen Purcell of Princeton Survey Research Associates designed survey questions that capture the slippery concepts of spyware, adware, and internet security. Lee Rainie, John Horrigan, and Katherine Murray of the Pew Internet Project provided editorial insights and analytical support.

The following people provided valuable advice on the survey instrument: Ari Schwartz, associate director, and Michael Steffen, policy analyst, of the Center for Democracy & Technology, a non-profit public policy organization (http://www.cdt.org/). D. Reed Freeman, chief privacy officer and vice president for legislative and regulatory affairs at Claria, a company specializing in online behavioral marketing (http://www.claria.com/). Lewis Rose, chair of the Advertising and Marketing Practice Group at Collier Shannon Scott, a law firm (http://www.colliershannon.com/). Avi Naider, president and co-founder of WhenU, a company specializing in software-based contextual advertising (http://www.whenu.com/). Richard Hunter, vice president and research director in Gartner Executive Programs, and his team: Richard DeLotto, Jay Heiser, Avivah Litan, Lydia Leong, and John Girard. Gartner provides research and analysis on the global IT industry (http://www.gartner.com/).

About the Pew Internet & American Life Project: The Pew Internet Project produces reports that explore the impact of the internet on children, families, communities, the work place, schools, health care, and civic/political life. The Project aims to be an authoritative source on the evolution of the internet through collection of data and analysis of real-world developments as they affect the virtual world. Support for the non-profit Pew Internet Project is provided by The Pew Charitable Trusts. The Project is an initiative of the Pew Research Center. The Project's Web site: www.pewinternet.org

About Princeton Survey Research Associates: PSRA conducted the survey that is covered in this report. It is an independent research company specializing in social and policy work. The firm designs, conducts, and analyzes surveys worldwide. Its expertise also includes qualitative research and content analysis. With offices in Princeton, New Jersey, and Washington, D.C., PSRA serves the needs of clients around the nation and the world. The firm can be reached at 911 Commons Way, Princeton, NJ 08540, by telephone at 609-924-9204, by fax at 609-924-7499, or by email at ResearchNJ@PSRA.com

Part 1.

Introduction

Consumers are receiving a crash course on security.

Over the past few years, many internet users have received a crash course about online security issues. Some have learned the hard way about how to deal with an invading virus or why they might want to monitor a family member's computer file-downloading habits. Once-obscure terms like "cookies" and "firewall" have become more commonplace. Complaints pour into technology companies' help lines about consumers' Web browsers being "hijacked" so that they are forced to visit certain sites. Millions of computers are becoming overwhelmed with unwanted software programs that slow performance. Many individuals have had the experience of getting alarmist pop-up ads on their computers that warn about the dangers of viruses and tout the virtues of programs that they should purchase in order to keep computer scourges at bay. Public officials have responded by introducing legislation and suing companies which allegedly exploit consumer ignorance about surveillance and online tracking mechanisms.[1]

Concurrently, businesses have developed "contextual" and "online behavior" marketing techniques that respond to consumers' interest in personally relevant advertising and product suggestions.[2] Internet users may be more familiar with the outcome of such techniques, such as product suggestions based on past purchases or searches, than with the technical details of how those suggestions are formulated. But tools for tracking user behavior are ubiquitous online. "Adware" or software that is downloaded to a consumer's computer, does exactly this and is often bundled with free software such as a screensaver or file-sharing program, so the recipient may be unaware of its installation on his computer. This software is then used to communicate that person's interests to a network of advertisers. For instance, when users install the free version of "ScreenScenes" screensavers, they also install the GAIN AdServer software that comes along with it and begin seeing ads on their computer screens that are labeled as part of the GAIN network of advertisers.[3]

The definitions of "spyware" and "adware" are in some dispute. Indeed, one of the core problems lawmakers are encountering as they ponder new legislation is how to define

[1] See: Internet Spyware (I-SPY) Prevention Act of 2005 http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00744:; SPY BLOCK Act http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02145:; New York v. Intermix Media, Inc. http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html; FTC v. Seismic Entertainment Productions, Inc. http://www.ftc.gov/opa/2004/10/spyware.htm.

[2] A 2004 Ponemon Institute survey found that 66% of consumers said they would welcome personalized banner ads, but do not want Web sites to collect personally identifiable information. (See http://www.mediapost.com/PrintFriend.cfm?articleId=268191)

[3] See http://www.screenscenes.com/

those terms – and thus determine which kinds of companies should be covered by new laws. Both types of software are associated to some degree with tracking internet users' online activities, which automatically raises concerns for many people. Still, the differences between adware and spyware are important.

Although significantly simplified, the following are definitions we used for the purpose of providing context for this report. For more in-depth information, please go to the Federal Trade Commission's information page on e-commerce and the internet.[4]

Spyware is software that is placed secretly on a computer in order to track a user's behavior and report back to a central source. Spyware's reputation is like that of a peeping tom or, at worst, a thief. It is almost universally derided and despised. It seems that no user wants to have spyware on her computer and few companies want to be associated with it.

Adware, on the other hand, is software that comes bundled as a package with programs that consumers download. In some cases, internet users check off on a "user agreement" before the download begins, though our survey shows that in many cases people are not paying much attention to those agreements (see discussion on page 6). In any event, the adware is installed during the download, much the way a "friend of a friend" might tag along to a barbecue. While an extra guest at a party may end up being welcomed, he might also end up being an unwanted pest.

Either way, adware is used to serve up targeted advertising based on the user's online behavior, much like a personal assistant who accompanies you in your online travels, making suggestions about what you might like or where you might find a bargain elsewhere. Hundreds of companies are involved in the adware business, either as advertisers or as purveyors of the software.

The Pew Internet & American Life Project set out to measure the impact of the recent wave of online activity related to adware and spyware. We wanted to know: Do average internet users understand the basic concepts? How many are dealing with the problems commonly associated with unwanted software programs? And are they taking steps to prevent software intrusions? Survey questions were developed in consultation with consumer advocates, adware company executives, and security experts.[5] Interviews with 1,336 internet users were conducted May 4 – June 7, 2005.

This survey finds that the threat of unwanted software programs is making people more cautious online. Most internet users think symptoms of spyware are serious problems rather than simply minor annoyances. Millions of internet users have first-hand experience with computer problems related to software intrusions and while many express confidence and knowledge of the issues, most think more should be done to guard against spyware and to notify people about adware.

[4] See http://www.ftc.gov/bcp/menu-internet.htm
[5] See Acknowledgements for a full list of consultants.

Part 2.

Threats Affect Online Behavior

Four in ten internet users have had spyware, adware, or both.

After hearing a description of spyware,[6] 34% of internet users, or about 47 million American adults, say they have had a spyware program on their home computer. Americans with high-speed internet connections at home are at higher risk for attacks because these connections are "always on" and have a permanent internet address, which can be more easily exploited by hackers. This survey finds that 44% of home broadband users say they have had spyware on their home computer, compared to 30% of home dial-up users who say that.[7]

After hearing a description of adware,[8] 30% of internet users, or about 41 million American adults, say they have had an adware program on their home computer. Forty percent of home broadband users have had adware on their home computer, compared to 23% of home dial-up users.

Overall, 43% of internet users, or about 59 million American adults, say they have had spyware, adware, or both types of programs on their home computer. This is probably a conservative estimate since this survey may have been the first time that respondents had heard definitions of the programs. In addition, there are significant gaps between people's perceptions and the reality of what is on their computers and there is a very strong likelihood that a big portion of those who have had computer problems have been victimized by spyware or more aggressive computer viruses without their knowing the cause of their problems. For instance, in October 2004, the Online Safety Study by AOL and the National Cyber Security Alliance reported that 53% of respondents said they had spyware or adware on their computers, but a scan of their machines revealed that 80% of respondents actually had those programs installed.[9]

[6] The description read as follows: "As you may know, certain software programs – sometimes called 'spyware' – can be installed on a person's computer without their explicit consent, either by 'piggy-backing' onto a file or program the person downloads from the internet or just by visiting a particular Web site. These programs can keep track of a person's internet habits and the sites they visit, and can transmit this information back to a central source."

[7] 53% of home internet users have a high-speed connection (DSL, cable, wireless, or T-1) and 44% of home internet users have a dial-up connection.

[8] The description read as follows: "Another kind of software program – sometimes called 'adware' – comes bundled with free files and programs people download from the internet, such as games, file-sharing programs, and screensavers. These programs can keep track of a person's internet habits and the sites they visit, and can use that information to provide targeted advertising on the person's computer."

[9] See http://www.staysafeonline.info/news/safety_study_v04.pdf

Those who have been victimized by spyware are among the most active online.

Internet users who report spyware on their home computers are more likely to have sampled a wider range of online activities, including those most associated with the risk of software intrusions onto their personal computer.

Risky Behavior Associated with Spyware

	All Internet Users	Internet Users Who Report Spyware	Internet Users Who Do Not Report Spyware
Download computer programs from the internet	39%	54%	33%
Play online games	36	44	33
Share files	27	33	25
Download music	25	36	19
Download computer games	21	29	16
Download video files	18	25	14
Visit an adult site	13	21	8

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups are higher.

Since internet users with broadband access are more at risk for software intrusions because of their "always on" connection and since they are likely to have tried many more activities than dial-up users, we wondered if their propensity to report spyware was simply another "broadband difference."[10] In doing further analysis, we found that broadband does have an independent effect on the likelihood of users reporting spyware. However, it is additionally true that engaging in certain online behaviors has an effect independent from having a high-speed internet connection. Holding all other factors constant, internet users who engage in the following activities are more likely to have had spyware or adware on their computer: visiting adult sites, downloading computer programs, playing online games, downloading music, sharing files, downloading computer games, downloading screensavers, and buying a product online. If an internet user avoids those activities online, he may be able to reduce his chances of contracting spyware.

Experience with spyware encourages people to take action to guard against software intrusions.

Internet users who report having had spyware on their home computers are more likely to say they are modifying their behavior to avoid such unwanted software programs.

[10] See "The Broadband Difference" (Pew Internet & American Life Project: June 23, 2002). Available at: http://www.pewinternet.org/PPF/r/63/report_display.asp

Once Burned, Twice Shy	All Internet Users	Internet Users Who Report Spyware	Internet Users Who Do Not Report Spyware
Stopped visiting particular Web sites	48%	60%	43%
Stopped downloading software from the internet	34	48	28
Stopped downloading music or video files from peer-to-peer networks	25	39	18
Started using a different Web browser	18	25	14

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups is higher.

Experience with adware also encourages preventive measures.

Internet users who say they have had adware on their home computers are also more likely to say they are changing some of their online habits.

Once Burned, Twice Shy (Part Two)	All Internet Users	Internet Users Who Report Adware	Internet Users Who Do Not Report Adware
Stopped visiting particular Web sites	48%	63%	44%
Stopped downloading software from the internet	34	50	29
Stopped downloading music or video files from peer-to-peer networks	25	44	19
Started using a different Web browser	18	28	14

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups are higher.

Further, when given the choice between paying to download files and programs that do not include adware or getting free downloads with adware, 62% of internet users say they would rather pay, 21% say they would rather get free downloads knowing they include adware, and 5% say it depends.

Current "notice and choice" practices are unsatisfactory to most internet users.

Adware companies say they seek to serve the online consumers who want free software and to serve companies who want to provide targeted advertising. They argue that such practices are similar to time-honored trade-offs in other media. For instance, people can watch broadcast television and listen to radio for free because those services are supported by advertisers. At issue is the notion of "clear notice and choice." There is

question over whether consumers actually know what they are getting when they download free software.

One diagnostic site set out to test the thesis that most people click through disclaimers without reading them. The site included a clause in one of its own user agreements that promised $1,000 to the first person to write in to request the money. The agreement was downloaded more than 3,000 times before someone finally read the fine print and claimed the reward.[11]

This Pew Internet & American Life Project survey finds that 73% of internet users say they do not always read user agreements, privacy statements, or other disclaimers before downloading or installing programs. This is not dramatically different from the offline behavior of consumers when it comes to reading disclaimers. Sixty-five percent of internet users (and 69% of all Americans) say they do not always read disclaimers sent by their bank, credit card companies, or other financial institutions.

Few Are Vigilant About Reading Disclaimers

The question to internet users read as follows: How often, if ever, do you read user agreements, privacy statements, or other disclaimers…

	…before downloading or installing programs or files from the internet?	…from your bank, credit card companies, or other financial institutions?
Always	25%	34%
Most of the time	20	24
Only sometimes	18	17
Hardly ever	17	13
Never	18	11

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%.

Eight in ten internet users (83%) say that more should be done to alert consumers to the presence of adware in files they are downloading. Just 12% of internet users say the current practice of clicking through a user agreement or disclaimer is adequate consent to install adware on a person's computer.[12] Ninety percent of internet users who have had adware on their home computers say that more should be done to alert consumers to the presence of adware in files they are downloading.

[11] See "It Pays to Read License Agreements" at: http://www.pcpitstop.com/spycheck/eula.asp.

[12] The question read as follows: "Some adware is installed on a person's computer only AFTER they click 'I agree' to a user agreement or disclaimer stating that additional software may be included with the files they are downloading. In your opinion, should more be done to alert consumers to the presence of adware in files they are downloading, or is this adequate consent to install adware on a person's computer?"

Overall, most internet users say they have adjusted their online behavior because of fears of being harmed by software intrusions.

Overall, 91% of internet users say they have made at least one change in their online behavior to avoid getting unwanted software programs like viruses and spyware on their computer:

- 81% of internet users say they have stopped opening email attachments unless they are sure these documents are safe. (An additional 8% of internet users volunteered that they have never opened unsafe attachments.)
- 54% of internet users say they have started reading user agreements more carefully before downloading or installing new programs or files from the internet.
- 48% of internet users say they have stopped visiting particular Web sites.
- 34% of internet users say they have stopped downloading software programs from the internet. (An additional 33% of internet users volunteered they have never downloaded programs.)
- 25% of internet users say they have stopped downloading music or video files from peer-to-peer networks. (An additional 48% of internet users volunteered that they have never downloaded music or video files from peer-to-peer networks.)
- 18% of internet users say they have started using a different Web browser to avoid software intrusions.[13]

[13] For other tips on avoiding software intrusions, see "Protect yourself online, what you can do" (ConsumerReports.org: September 2004). Available at: http://www.consumerreports.org/main/detailv4.jsp?CONTENT%3C%3Ecnt_id+=461187.

Part 3.

The Internet's Multitude of Sins

Most people are confident and say they grasp the major online security concepts, but there are gaps, especially for newcomers to the internet.

Despite the computer woes they might have experienced, 61% of internet users are confident that they can keep things like computer viruses, spyware, and adware off of their home computer when they want to. Thirty-three percent of internet users say they are not confident that they can do so. Those who are confident are less likely to have experienced computer slowdowns, unexpected home page changes, or uninvited icons on their desktop in the past year. Sixty-three percent of confident internet users report at least one problem, compared to 79% of not-confident internet users.

Most internet users claim to have a grasp of some major concepts:

- 88% of internet users say they have a good idea what "spam" means.[14]
- 78% of internet users say they have a good idea what "firewall" means. [15]
- 78% of internet users say they have a good idea what "spyware" means.
- 68% of internet users say they have a good idea what "internet cookies" means (by comparison, 43% of internet users said they knew what an "internet cookie" was in 2000).[16]

But fewer say they understand some of the newer or more obscure terms:

- 52% of internet users say they have a good idea what "adware" means.
- 29% of internet users say they have a good idea what "phishing" means (described as "internet phishing, spelled with a P-H at the beginning"). Fully 15% of internet users volunteered that they had never heard the term before.[17]

[14] Spam is unsolicited bulk email. See http://en.wikipedia.org/wiki/Spam_%28electronic%29
[15] A firewall is a piece of software or hardware that protects a network from unauthorized entry. See http://en.wikipedia.org/wiki/Firewall_(networking)
[16] Cookies are bits of encrypted information deposited on a computer's hard drive after the computer has accessed a particular Web site. See "Trust and Privacy Online" (Pew Internet & American Life Project: August 20, 2000). Available at: http://www.pewinternet.org/PPF/r/19/report_display.asp.
[17] Phishing is unsolicited email requesting personal financial information. See: http://en.wikipedia.org/wiki/Phishing

Years online and broadband connections correlate with an overall understanding of the risks – and a sense of control over them.

Not surprisingly, internet users with six or more years of online experience are significantly more likely to express confidence and to say they know what key security terms mean.

Experienced Users More Likely to Say They Understand Key Terms

	All Internet Users	Internet Users with 6+ Years of Experience	Internet Users with 2-3 Years of Experience
Confident about keeping unwanted programs off their machine	61%	68%	44%
Have a good idea what "spyware" means	78	86	60
Have a good idea what "adware" means	52	63	31
Have a good idea what "phishing" means	29	35	22

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups are higher.

Broadband users are significantly more likely than dial-up users to say they understand key security terms. But many broadband users do not know the full meaning of these terms and that is doubly important because broadband users are more vulnerable to software intrusions than dial-up users.

Broadband Users More Likely to Say They Understand Key Terms

	All Internet Users	Internet Users with Home Broadband Connection	Internet Users with Home Dial-up Connection
Confident about keeping unwanted programs off their machine	61%	69%	57%
Have a good idea what "spyware" means	78	88	75
Have a good idea what "adware" means	52	65	43
Have a good idea what "phishing" means	29	35	25

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups are higher.

Internet users who say they know what "spyware" and "adware" mean are also more likely to read user agreements before downloading programs from the internet. Twenty-seven percent of "spyware-savvy" users say they always read such agreements, compared to 17% of those who do not know the term. Twenty-eight percent of "adware-savvy"

users say they always read such agreements, compared to 22% of those who do not know the term.

Although many users have an imprecise understanding of internet threats, most retain strong attitudes about them.

Half of internet users (49%) say that software programs like spyware are a serious threat to their online security. An additional 28% of internet users say they are a minor problem and that more should be done to control them. Sixteen percent of internet users agree with the statement, "They are just part of life on the internet and don't really bother me."

Internet Users' Attitudes Toward Spyware

Internet users who have first-hand experience with spyware are significantly more likely than their counterparts to take it seriously.

	All Internet Users	Internet Users Who Report Spyware	Internet Users Who Do Not Report Spyware
Software programs like spyware are a serious threat to my online security	49%	61%	43%
They are a minor problem and more should be done to control them	28	28	29
They are just part of life on the internet and don't really bother me	16	10	19

Source: Pew Internet & American Life Project May-June 2005 Survey (N=1,336). Margin of error for internet user sample is +/- 3%. Margins of error for comparison of subgroups are higher.

Many internet users are deeply bothered by the possibility that a program they download could slow down their computer or generate pop-up ads. Even the widely-used practice of tracking online behavior using tools such as "cookies" was rejected by most internet users.

Spam zombies

Spam – unsolicited bulk email – is despised by most internet users[18] and most people would shudder at the thought of becoming a "spam zombie," which means that their computer has been covertly taken over and turned into a terminal to send out bulk emails.[19] Therefore it is not surprising that 89% of internet users say it would be a serious problem if a program they installed or a Web site they visited sent out unauthorized email messages from their email account. Seven percent of internet users say that would be a minor annoyance and 3% say it wouldn't really bother them at all.

[18] See "Spam and Phishing" (Pew Internet & American Life Project: April 10, 2005). Available at: http://www.pewinternet.org/PPF/r/155/report_display.asp.

[19] See the Federal Trade Commission's "Operation Spam Zombies" page at: http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm.

System slow-downs

Eighty percent of internet users say it would be a serious problem if a program they installed or a Web site they visited caused their computer to slow down or freeze up. Seventeen percent of internet users say that would a minor annoyance and 2% say it wouldn't really bother them at all.

Big Brother is watching

Seventy-eight percent of internet users say it would be a serious problem if a program they installed or a Web site they visited transmitted information about their internet habits back to a central source. Fifteen percent of internet users say that would a minor annoyance and 6% say it wouldn't really bother them at all.

Home page hijack

Sixty-five percent of internet users say it would be a serious problem if a program they installed or a Web site they visited reset their internet home page. Twenty-six percent of internet users say that would a minor annoyance and 6% say it wouldn't really bother them at all.

Pop-up ads

Fifty-nine percent of internet users say it would be a serious problem if a program they installed or a Web site they visited caused pop-up ads to appear on their computer screen. Thirty-five percent of internet users say that would a minor annoyance and 4% say it wouldn't really bother them at all.

Cookies

Fifty-seven percent of internet users say it would be a serious problem if a program they installed or a Web site they visited collected information about their internet habits but did not transmit that information to any outside source. Twenty-eight percent of internet users say that would a minor annoyance and 13% say it wouldn't really bother them at all.

This question essentially described the near-universal use of "cookies" or bits of encrypted information deposited on a computer's hard drive after the computer has accessed a particular Web site. The results underscore the gap between consumers' perceptions and the reality of how the Web works.

There is additional evidence that the threat of spyware is having a chilling effect on daily online life. Recent reports by WebTrends and JupiterResearch find that more internet users are now rejecting cookies from Web sites than in 2004, with as many as 28% of internet users saying they selectively reject these widely used tracking devices which

enable some of the Web's most attractive features, such as customization.[20] Forrester Research has reported that many users are regularly removing cookies from their computers in an attempt to foil spyware but are in fact preventing legitimate online vendors from plying their trade as well.[21]

[20] See "Cookie Rejection Cited as Next Major Advertiser Problem" (ClickZ Stats: May 23, 2005). Available at: http://www.clickz.com/stats/sectors/advertising/article.php/3507186.

[21] See "Web Users Toss Their Cookies" (Forrester Research: December 9, 2004). Available at: http://www.forrester.com/Research/Document/Excerpt/0,7211,35957,00.html.

Part 4.

Computer Problems Vex Millions

Although most do not know the source, tens of millions are dealing with computer problems that are consistent with problems caused by spyware or viruses:

- 52% of home internet users say their computer has slowed down or is not running as fast as it used to.
- 51% of home internet users say their computer started freezing up or crashing, requiring them to shut down or reset.
- 25% of home internet users say a new program appeared on their computer that they didn't install or new icons suddenly appeared on their desktop.
- 18% of home internet users say their internet home page changed without them resetting it.

In sum, 68% of home internet users, or about 93 million American adults, have experienced at least one of these problems in the past year. There is no difference between internet users who are the sole users of their home computer and those who share the computer with other people. There is also no difference between those who bought the computer within the past year and those who have an older machine.

Of those who have experienced problems, 31%, or about 29 million, would describe the problems as major. Eight in ten of those experiencing problems (79%) said they have taken action to fix the situation and 20% said the problems were not that severe.

Most do not know the problem's source, but those who do often blame family members or friends for doing things online that cause unwanted programs to be installed or other computer problems.

Sixty percent of those who had problems on their home computer in the past year say they do not know the source of the problem; 39% say they know the source. Internet users who know the source of their problems name viruses, spyware, adware, and software glitches, along with complaints about the age or shortcomings of the computer or operating system. Family members are often accused by one another of downloading materials that lead to computer problems. For example, respondents mentioned a cousin who downloaded porn, a son who "filled the computer with a lot of junk," and multiple citations of children's downloading activities. (Again, there is no difference between internet users who are the sole users of their home computer and those who share the computer with other people. Both groups experience computer problems to an equal degree. Respondents may be more apt to provide details about a family member's online

exploits than their own. The questionnaire associated with this report contains verbatim responses about the exact nature of the problem and the suspected source.)

Internet users who report having spyware are especially likely to say they have had computer problems in the past year.

Internet users who say they have had spyware on their computer are more likely to report these problems. Seventy-eight percent of those who report spyware say their computer has had one of these problems in the past year, compared to 59% of internet users who do not report spyware on their computers.

Again, malfunctions and interference other than spyware may be behind some of the reported computer problems among internet users, but the higher incidence of problems among those who report spyware suggests that these unwanted programs are the source of computer problems for many internet users.

Broadband users are more likely than dial-up users to say a new program or icon appeared unexpectedly.

Broadband users are at higher risk than dial-up users for software intrusions because the "always on" connection makes a tempting target for hackers, especially if users do not put security measures such as a firewall in place. But hackers are not the only threat to home broadband users who take advantage of the speed to visit more sites and try more online activities. The faster the connection, the greater the chance for unwanted software to sneak onto a machine. For example, when researchers from Symantec Corporation plugged in a new computer and surfed on an unprotected connection for an hour, they found that adware software had been installed without their knowledge and pop-up ads began cluttering the screen.[22]

This survey finds that broadband users are more likely than dial-up users to say a new program appeared on their computer that they didn't install or new icons suddenly appeared on their desktop. Broadband users and dial-up users are equally likely to report home-page changes or system glitches.

Fixing the computer is not at the top of most people's to-do list.

Twenty percent of internet users who said they had experienced at least one computer problem in the past year decided not to attempt a fix. Of those who decided that the problem was worth trying to fix, 43% took action within a week of the first symptoms appearing. Another 26% of those who tried to fix the problem said they lived with it for at least a week, but less than a month. A third group, 29% of those who tried to fix their

[22] See "Spyware firms targeting children" (MSNBC: May 5, 2005). Available at: http://www.msnbc.msn.com/id/7735192/.

computer, said the problem had been going on for a month or longer before they got around to attempting a remedy.

Sometimes it takes a village to fix a computer.

Thirty-nine percent of those who tried to fix the problem on their home computer said they tackled it alone. Forty-two percent got help from a friend, family member, or colleague. Seventeen percent hired someone to repair their computer and 6% used a free user-support service.[23]

Half of computer fixes are quick and easy, but one in five problems is never solved.

Half of those who tried to remedy the situation with their home computer said the problem was fixed quickly and easily (48%). Thirty-one percent said the problem was fixed but only after considerable time and effort. Fully 20% of those who attempted a fix said the problem has not been solved.

Most figure out a free solution, but some must spend significant sums to fix their ailing computer.

Most people (58% of those who tried to fix the problem) did not have to spend any money to repair their home computer. However, 39% of those who attempted a fix, or about 28 million American adults, did have to spend money to get their computer working again – $129.15 is the mean amount spent by those who tried to fix the problem.[24]

Some people are protecting themselves with anti-virus programs and firewalls.

The great majority (88%) of home internet users say they have virus protection on their main home computer. Broadband users are more likely than dial-up users to say they have virus protection (92% vs. 83%).

One-fifth (22%) of those with virus protection say that they are using the program set up by their internet service provider. Thirty-nine percent of those with virus protection say someone else set it up for them. Thirty-seven percent of those with virus protection say they set up the program themselves.

[23] Percentages exceed 100% due to multiple responses.

[24] The question read as follows: "Altogether, approximately how much money, if any, have you spent fixing the problem you were having on your home computer?" Of those who had attempted a fix: 58% said zero; 10% gave a dollar amount between $1-50; 12% gave a dollar amount between $51-100; 9% gave a dollar amount between $101-200; 8% gave a dollar amount of $201 or more; 2% didn't know or refused to answer.

Sixty-five percent of those with virus protection say that it updates automatically; 26% say they have to download updates on their own; and 9% do not know. Twenty-three percent of those with virus protection say it updates daily, 33% say it updates weekly, 26% say it updates less often than weekly, and 18% do not know.

More than half (56%) of home internet users say they have firewall protection on their main home computer. Broadband users are more likely than dial-up users to say they have a firewall (68% vs. 44%).

These findings are in line with other studies of home computer security measures. In a July 2004 study conducted online, the Bentley Survey on Consumers and Internet Security found that 75.6% of broadband users have installed a firewall to protect their home computer and 90% of all home users have installed anti-virus software, although only 46% always update it.[25] In September-October 2004, the AOL/NCSA Online Safety Study combined in-person interviews with computer scans to reveal that respondents' perceptions pretty much matched the reality when it came to the presence of anti-virus protection and firewalls on their home computers, but the majority were not up-to-date or set up properly. Only 33% of anti-virus programs had been updated in the past week. Seventy-two percent of respondents did not have a properly configured firewall on their computer.[26]

[25] See http://www.bentley.edu/events/iscw2004/survey_findings.pdf.
[26] See http://www.staysafeonline.info/news/safety_study_v04.pdf.

Methodology

This survey, sponsored by the Pew Internet & American Life Project, obtained telephone interviews with a nationally representative sample of 2,001 adults living in continental United States telephone households. The survey was conducted by Princeton Survey Research International. Interviews were done in English by Princeton Data Source, LLC from May 4 to June 7, 2005. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ±2.3%.

Details on the design, execution and analysis of the survey are discussed in the questionnaire associated with this report.