2011 Parent-Teen Internet Safety Report

GFI®

GFI Software

June 2011

TABLE OF CONTENTS

INTRODUCTION PAGE 3

STUDY METHODOLOGY PAGE 3

KEY FINDINGS AT A GLANCE PAGE 4

- CONTENT PAGE 4
- COMMUNICATIONS PAGE 4
- MALWARE PAGE 4
- INTERNET SAFETY EDUCATION PAGE 5

ANALYSIS PAGE 5

STUDY FINDINGS: INTERNET CONTENT SAFETY PAGE 6

- PEOPLE WHO AGREE: *FIGURE 1* PAGE 6
- TEEN OPINIONS: *FIGURE 2* PAGE 6
- FREQUENCY OF TEEN INTERNET USAGE: *FIGURE 3* PAGE 7
- PARENTAL MONITORING AND FILTERING: *FIGURE 4* PAGE 7
- TEENS VISITING ADULT WEBSITES: *FIGURE 5* PAGE 8
- FREQUENCY OF PARENTAL FACEBOOK MONITORING: *FIGURE 6* PAGE 8
- FACEBOOK "FRIENDS" & TEENS THAT CONTROL THEIR PRIVACY: *FIGURE 7* PAGE 9
- TEENS AVOIDING PARENTS: *FIGURE 8* PAGE 9

STUDY FINDINGS: COMPUTER AND MALWARE INFECTION PAGE 10

- CONFIDENCE VS INFECTION RATES: *FIGURE 9* PAGE 10
- NFECTION AT HOME: *FIGURE 10* PAGE 10
- ANTIVIRUS DEFINITION UPDATES: *FIGURE 11* PAGE 11
- PERSONAL USE: *FIGURE 12* PAGE 11

STUDY FINDINGS: COMMUNICATIONS HABITS AND SAFETY PAGE 12

- TEENS AND CELL PHONES: *FIGURE 13* PAGE 12
- ONLINE TEEN COMMUNICATIONS: *FIGURE 14* PAGE 12
- STRANGER DANGER: *FIGURE 15* PAGE 13
- DO PARENTS COUNSEL TEENS ON INTERNET SAFETY: *FIGURE 16* PAGE 13
- INTERNET SAFETY EDUCATION: *FIGURE 17* PAGE 14
- INTERNET ACCESS: *FIGURE 18* PAGE 14

CONCLUSION PAGE 15

Introduction

Compromised desktops have become hackers' preferred entry point into corporate networks. As more workers adopt mobile technologies and bring their work home with them, home computing practices have become a serious source of risk not only to consumers, but also to enterprises. A corporate laptop that becomes infected by a virus, worm or other "malware" in an employee's home can drive a gaping hole in security defenses when it is connected to the corporate network.

There are multiple vectors for malware infection today. There is the traditional email channel, as well as infected USB sticks, tampered commercial software and malicious websites – that is, websites that download malware onto visitors' computers. Even legitimate sites today can become distributors of malware because hackers compromise them using a technique called SQL injection, which embeds code that infects subsequent visitors with malware. There are also sites that are designed specifically to distribute malware. These sites typically attract visitors with pornographic or other adult content – which makes teen visitation of such sites a serious security concern both to parents and enterprises, if teens are using their parents work computers to do so.

To gain a better understanding of home computing practices, GFI® Software commissioned a scientific study of home Internet use by parents and their teenage children. This population represents a particularly interesting "risk pool" not only due to their usage patterns in the home, but also due to the theory that "tech savvy" teens, who have spent their entire cognizant lives in the Internet age, may prove to be a harder human target for social engineering attacks than their elders.

The study focused on education practices relative to Internet safety, as well as three major risk areas:

- **Content –** The sites and other content teens visit, and parental activity around monitoring and regulating those activities.
- **Communications –** Particularly relative to bullying and "stranger danger," the survey sought to identify the risk teens face from unwanted and unsolicited communication over the Internet.
- **Malware –** Family practices relative to protecting home and portable business computers from viruses, Trojans, worms and other malware variants.

Study Methodology

GFI commissioned a probability survey that was rigorously designed for methodological validity and reliability – so that the results from this sample can be generalized to all U.S. parents and their teenage children in households with Internet access. GFI contracted with independent polling expert Mike Mokrzycki to design this study. Mokrzycki's more than 15 years of survey research experience includes hundreds of polls for major media organizations, including as founding director of the Associated Press polling unit and as a consultant managing NBC News' live reporting of exit poll results on election nights.

The study comprised interviews with 535 pairs of parents and their teens nationwide living in households with Internet access. By interviewing the sampled parents' own teens – rather than discrete, unrelated groups of each - this design allows comparison of the safety practices and perceptions of parents and their own children (e.g., "What parents think their teens are doing" vs. "what their teens are actually doing.")

To be included in the sample, parents were required to have at least one child age 13-17 and consent to have their teens surveyed. If parents in the sample had just one child age 13-17, that teenager was interviewed; if parents had more than one teen, one teen was selected randomly to take the survey. Respondents were assured that their answers would remain confidential, and parents were asked to give their teens privacy while they completed the survey.

The surveys were administered online between March 22 and April 5, 2011, by Knowledge Networks of Palo Alto, California, which uses probability (random) methods to recruit members of a national panel to take surveys. Knowledge Networks provides Internet access to the approximately one in five recruits who don't have it; the GFI study excluded those people from the sample, so the study would be representative of typical home Internet users. GFI's sponsorship was not divulged at the start of the survey so as not to potentially bias responses; separately from the survey, respondents could ask their Knowledge Networks representative who sponsored the survey and GFI's sponsorship would be disclosed. The margin of sampling error is plus or minus 5 percentage points for all parents in the sample and the same for teens.

Key Findings at a Glance

Content

• 36% of parents use Web monitoring software or a Web filter to keep tabs on their teens' activities online, and to block inappropriate content. Among teens who say their parents aren't using such software, 10% actually are.

• 49% of teens say they do not know whether or not their parents are monitoring their Internet browsing. Within that population, 66% of their parents actually are monitoring their browsing.

• 72% of teens say they use computers at school to go online, but 26% of parents are unsure whether or not their teen's school monitors Internet use by students.

• 42% of teens have cleared their browsing history at some point after using the Internet, and 5% do it often.

• 24% of teens admit to visiting a Web site intended for adults. 31% of boys admit they've visited adult sites, and 13% say they do so "often" or "sometimes".

• 53% of teens who have visited an adult Web site also say they lied about their age to get in.

• In more than half of the households surveyed, both the parent and their teen have a Facebook profile. Of these, 87% of parents are "friends" with their teens on Facebook. In cases where parents don't have Facebook profiles but their teen does, 43% of parents say they "very closely" or "somewhat closely" monitor their teens' Facebook activity. Only 20% of teens indicate that their parents monitor them on Facebook with such rigor.

• 83% of teens with Facebook accounts indicate they understand how to use privacy settings on the social network, so some may hide content from their parents.

• 34% of teens say they have created online accounts that their parents do not know about.

• Among teens who are not "friends" with their parents on Facebook, one third admit to posting content on their Facebook "wall" that they would not want their parents to see.

Communications

• 29% of teens say they have been contacted online by a person who has no connection to them or their friends. 62% of those say this has happened more than once. Of all those who have been contacted by a stranger, 23% say they responded to the person who contacted them.

• 11% of teens say they have been bullied online or by text messages. Girls report a higher incidence of bullying (15%) than boys (7%). Only 4% acknowledge bullying other people.

• 31% of teens admit they have communicated something to someone online that they would not have said to the person's face.

• 79% of teens own a mobile phone, and of that group 29% own smart phones, providing them with Internet access at any time and any place.

Malware

• 76% of parents and 77% of teens say they are "very" or "somewhat" confident that they won't be infected by a virus.

• 65% of parents say a virus has infected their home computers, and 55% of those respondents say this has happened more than once. And 62% of all parents who have had a virus attack say that the problem was either "somewhat" or "very" serious.

• 47% of teens say they have been infected by a virus while using a computer in the home. Of those parents who use a work computer at home, 37% say they let their teens use them as well. 90% of parents themselves use their work computers at home for personal business, including 25% who do so "often."

• 89% of parents say they have antivirus software installed on their computers. However, only 28% of these say they update their virus definitions daily, and 24% are not sure if they are updating these definitions at all.

• 21% of parents who work have connected personal computing devices (devices not issued by their employer) to their corporate networks, and 42% say they are not required to take any security measures before connecting those devices to the network.

• 60% of parents and 57% of teens say they use thumb drives or flash drives to transfer data from one computer to another.

Internet Safety Education

- 33% of parents are unsure whether or not their child's school teaches safe Internet practices. 24% of teens indicate that either their schools do not provide such training, or they are unsure whether or not it provides such training.
- 94% of parents say they have spoken to their teens about Internet safety. 10% of teens say their parents have never spoken to them about Internet safety, and another 6% don't know if such a conversation ever took place.
- 73% of parents believe most teens do things online that they wouldn't want their parents to know about. Their children are in close alignment on this point: 74% of teens indicate that most of their peers do things online that they wouldn't want their parents to know about.

Analysis

Parents and Teens: The Timeless Cat-and-Mouse Game Moves to the Internet

It is part of the human condition that parents will try to keep their children safe, and children will test their parents' limits by trying to get away with doing things their parents don't want them doing. This is particularly true in the teenage years, when children embark on the natural process of breaking away from the protective shield of their parents and experiment with various "adult" behaviors. This creates a game of cat-and-mouse where parents try to educate their teenagers on the dangers associated with behaviors like smoking, drinking and sex, and impose curfews and other house rules designed to deter such behavior. Of course, many teenagers go to great lengths to break these rules and cover their tracks. For most people, this is one of the central themes of their teenage years.

In more recent times, this cat-and-mouse game has taken on a new dimension, as the Internet has become a fundamental part of daily life. Today, parents not only have to be concerned about the safety of their teens in the physical world; they also have to be concerned about the dangers their teens face in cyberspace. In many ways, controlling teen behavior on the Internet is a far more daunting challenge than controlling it in the physical world. Teens face a broad array of dangers on the Internet, including malware, inappropriate content and predatory behavior from both known and unknown people. For parents, protecting teens from these dangers is extremely difficult, due in large part to the growing ubiquity of Internet access. Teens today can access the Internet from almost anywhere – home, school, mobile phones, friends' houses, etc.

Unfortunately, both parents and their children may not understand that risky behavior on the Internet can have repercussions that extend beyond the teens themselves. For example, visiting malicious Web sites can infect the family computer with malware that enables criminals to steal the personal identification information of both teens and their parents, which can result in financial loss and other problems. It can even lead to larger issues if the teen is borrowing the parent's work computer to surf the Internet – a practice that this study found is relatively common. The following sections go into further detail on the study's findings relative to Internet safety education, as well as the three main risk areas for teens: content, communications and malware.

STUDY FINDINGS: Internet Content Safety

As can be seen in Figure 1, parents and teens are in almost complete alignment when it comes to teen behavior on the Internet. 73% of teens and 74% of parents agree with the statement: "Most teens do things online that they wouldn't want their parents to know about."

PEOPLE WHO AGREE:

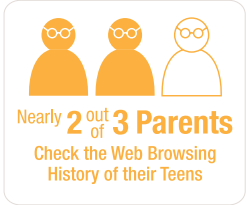
that most teens do things online that they wouldn't want their parents to know about

FIGURE 1

This dynamic appears to be fueling the Internet content cat-and-mouse game between parents and their teens. Nearly two-thirds of parents surveyed in the study indicate that they check the Web browsing history of their teens after they use the Internet at home, and 24% of teens say they know their parents are doing this. (See Figure 2)

TEEN OPINIONS:

do parents check their web browsing history?



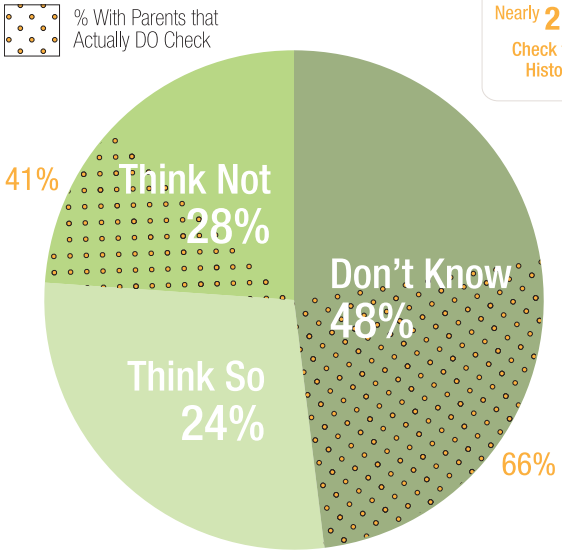


FIGURE 2

However, a substantial number of parents are checking on their teens' browsing history without their teens' knowledge. Out of the 28% of teens who say their parents are not checking their Web browsing history, 41% of their parents indicate they actually are doing this. And among the 49% of teens who say they do not know whether or not their parents are checking their browsing history, 66% of their parents confirm that they are checking that history.

Teens are wary of this monitoring behavior: 42% of those responding to the survey indicate that they have cleared their browsing history after using the Internet. (See Figure 3)

FREQUENCY OF TEEN INTERNET USAGE:

by activity

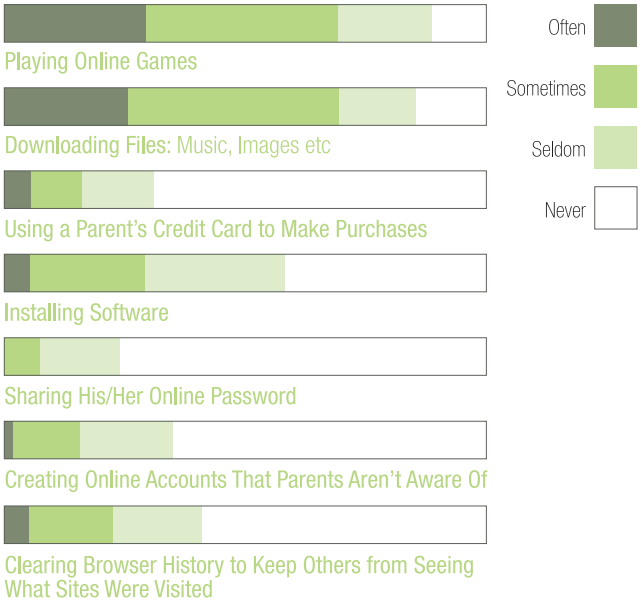


FIGURE 3

The study results indicate that parents rely more on "manual monitoring" of their teens than they do on automated monitoring. As indicated earlier, 64% of parents say they monitor where their teens go on the Internet. However, only 36% of parents say they are using monitoring software or a Web filter on their home computer. (See Figure 4) And most are doing so without their children's knowledge. 44% of teens say their parents are not using monitoring or filtering software – and yet 10% of their parents indicate they are using such software. Among the 32% of teens who say they do not know if their parents are using monitoring or filtering software, 27% of parents say they do use such software.

PARENTAL MONITORING AND FILTERING:

do teens think that parents try to keep teens from visiting certain websites using monitoring software and filters?

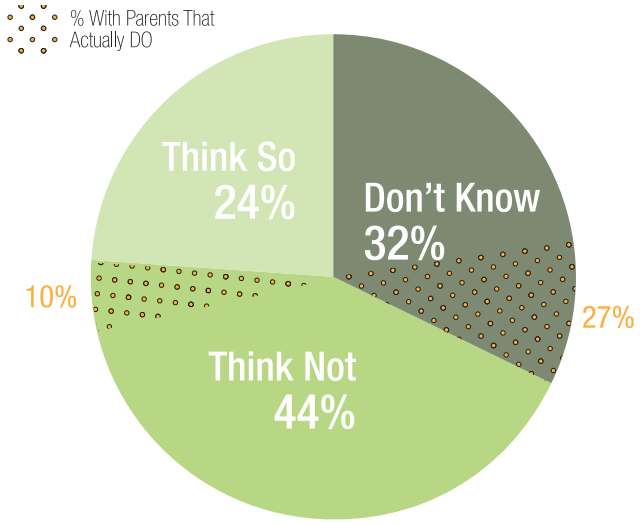


FIGURE 4

As can be seen in Figure 5, 24% of teens admit to visiting a Web site intended for adults. Of those, 53% indicate that they have lied about their age to gain access to an adult site. 31% of boys admit to visiting adult sites, and 13% say they do so "often."

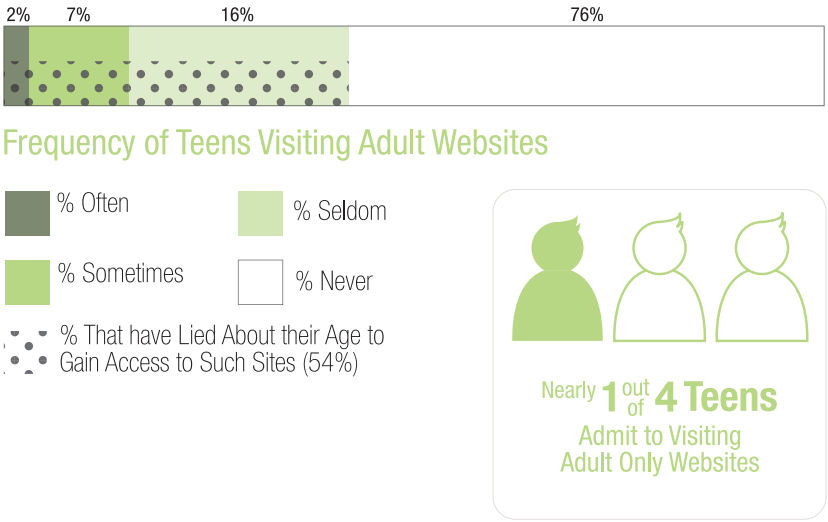


FIGURE 5

Facebook represents an interesting content category, since it is both a site for consuming content and for communicating with others. The study indicates that parents pay closer attention to their teens' Facebook pages than they may think. As can be seen in Figure 6, 43% of parents who are not Facebook friends with their teens still "very closely" or "somewhat closely" monitor their teens' Facebook usage, while only 20% of these teens say that is the case.

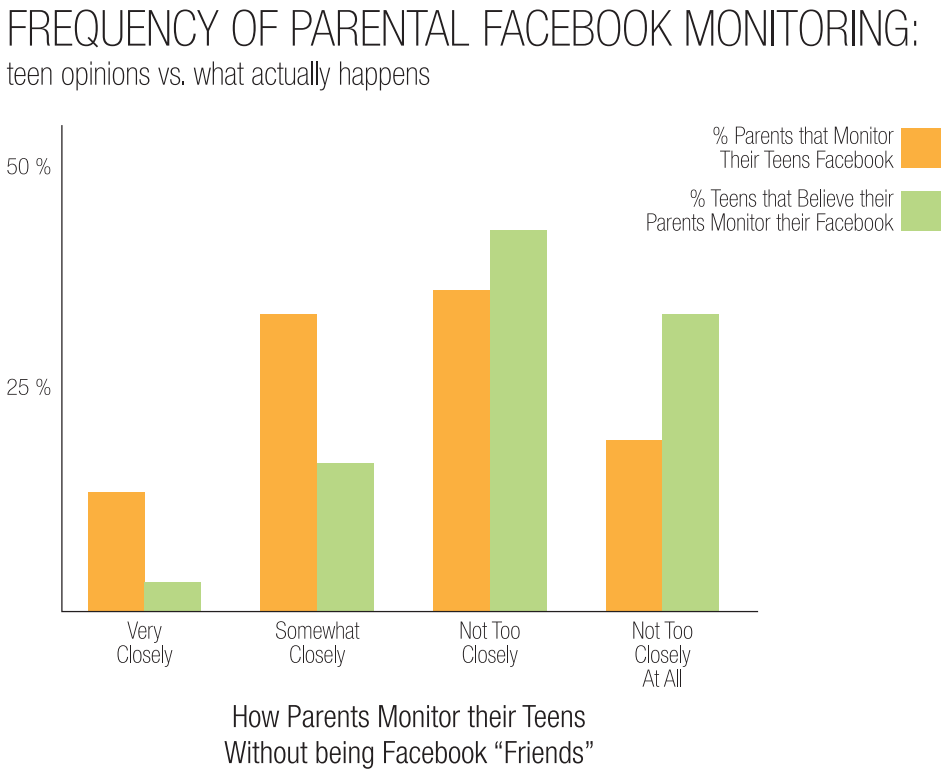


FIGURE 6

In households where the parent and teen both have Facebook profiles, 87% of parents indicate they are "friends" with their teens on Facebook. However, 83% of teens with Facebook accounts say they have a good idea about how to control privacy settings – meaning they understand how to hide content from "friends" and other visitors.
(See Figure 7)

FACEBOOK "FRIENDS" & TEENS THAT CAN CONTROL THEIR PRIVACY:

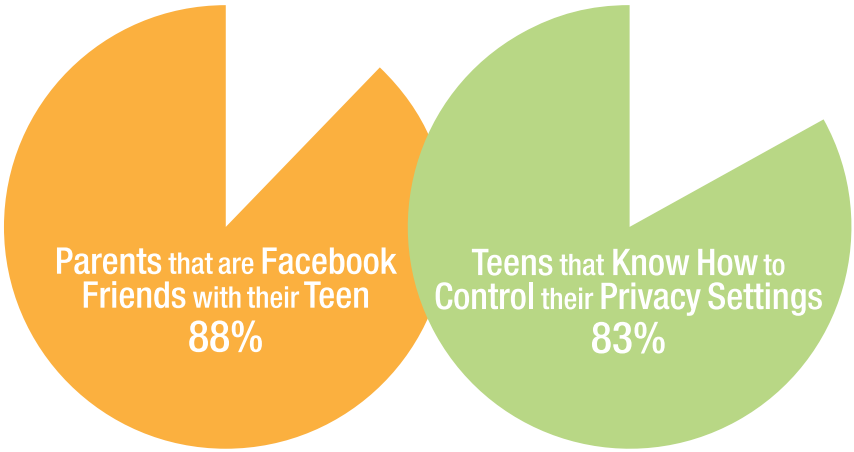


FIGURE 7

33% of teens who are not "friends" with their parents on Facebook say they post things on their "Wall" that they would not want their parents to see. Additionally, 34% of teens say they have created an online account that their parents do not know about.
(See Figure 8)

TEENS AVOIDING PARENTS:

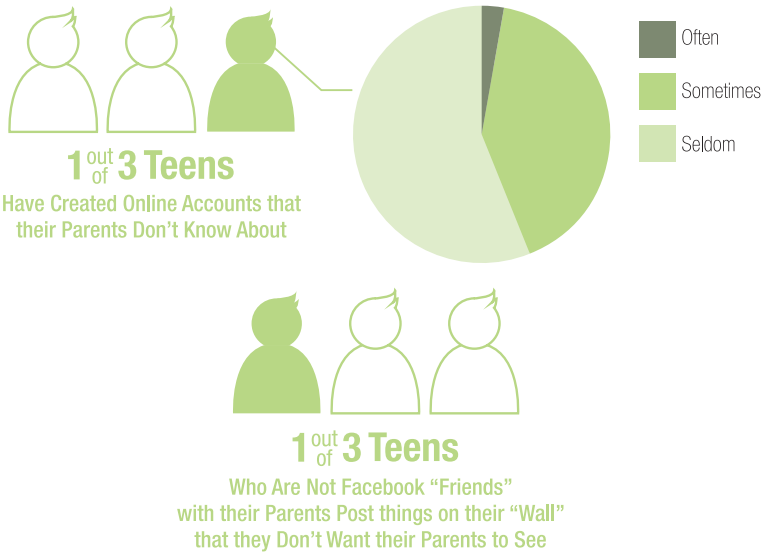


FIGURE 8

STUDY FINDINGS: Computer and Malware Infection

Although 76% of parents and 77% of teens say they are either "very" or "somewhat" confident they won't be infected by viruses, a large percentage are being infected. Nearly two-thirds (65%) of the parents surveyed say their home computer has been infected by a virus. In fact, 55% of these parents say they have not only been infected by a computer virus, but that it has happened more than once. Nearly two-thirds (62%) of those that have been infected rate the problem that resulted as "somewhat" or "very" serious. (See Figure 9)

CONFIDENCE VS INFECTION RATES:

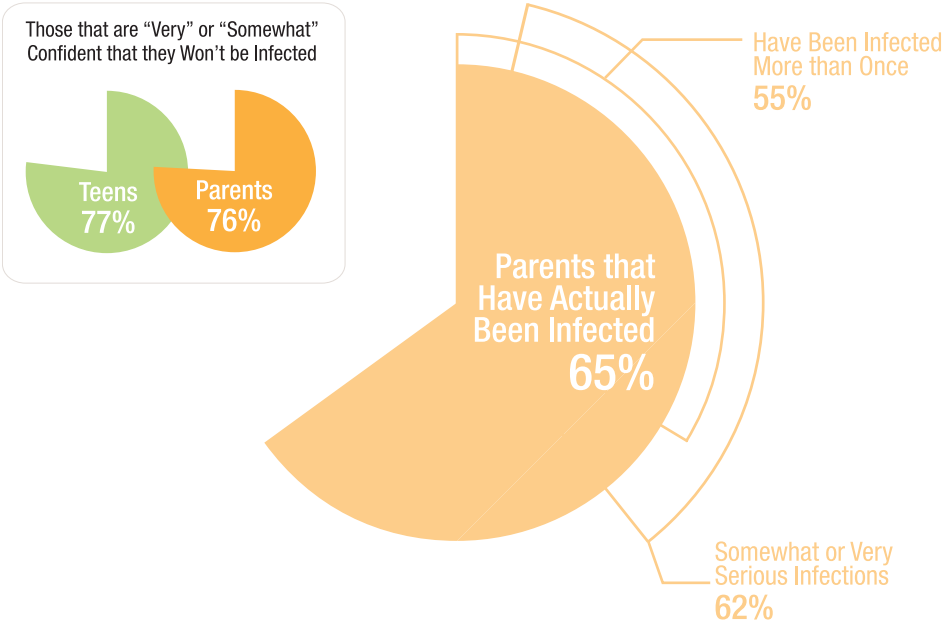


FIGURE 9

47% of teens say they have been infected by a virus on a computer they were using at home. Corporate IT departments have reason to be concerned about this behavior, because 37% of parents who bring their work home with them say they let their teens use their work computers there. (See Figure 10)

INFECTION AT HOME:

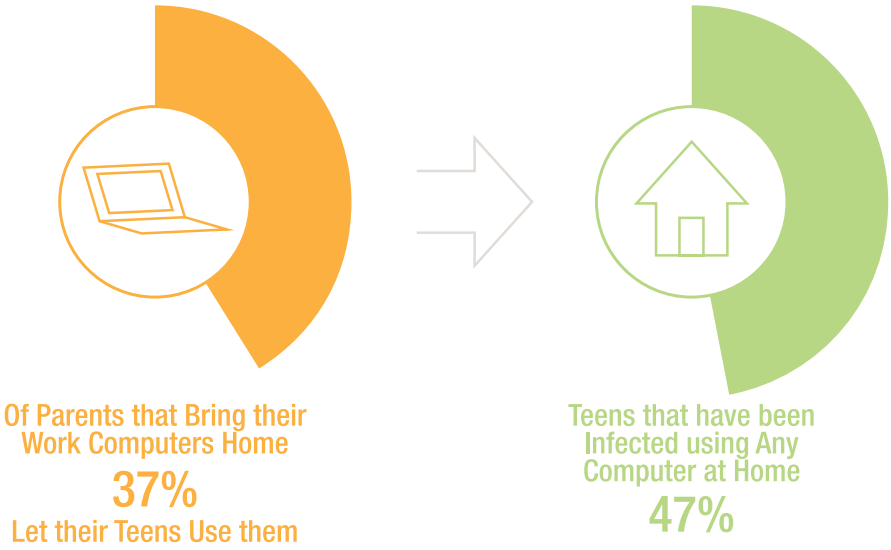


FIGURE 10

While most parents indicate they have antivirus software in place (89%), only about one quarter (28%) of these say they update their virus definition files on a daily basis. Worse yet, 24% say they don't know if they update their virus definition files at all (see Figure 11). Without frequently updating virus definition files, users are susceptible to new malware attacks.

ANTIVIRUS DEFINITION UPDATES:

are parents up to date on their antivirus software?

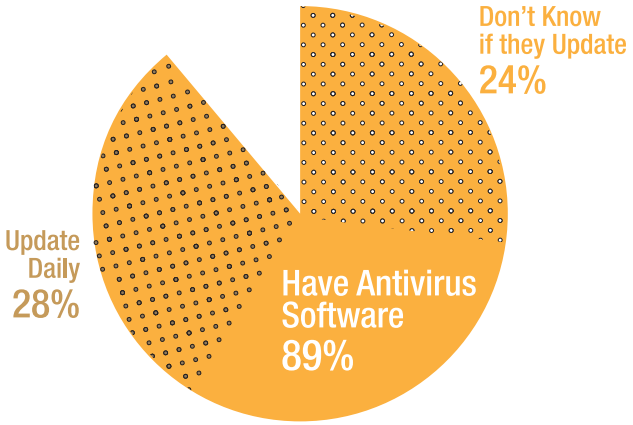


FIGURE 11

90% of parents say they use their work computers at home for personal business. Additionally, 21% of parents who work connect personal computing devices to their corporate networks, and 42% say they aren't required to take any security measures before connecting that device to the network. Additionally, 60% of parents and 57% of teens said they use thumb drives to transfer data from one computer to another, thereby risking the transfer of any number of malicious files or viruses between machines.
(See Figure 12)

PERSONAL USE:

parents putting work computers at risk

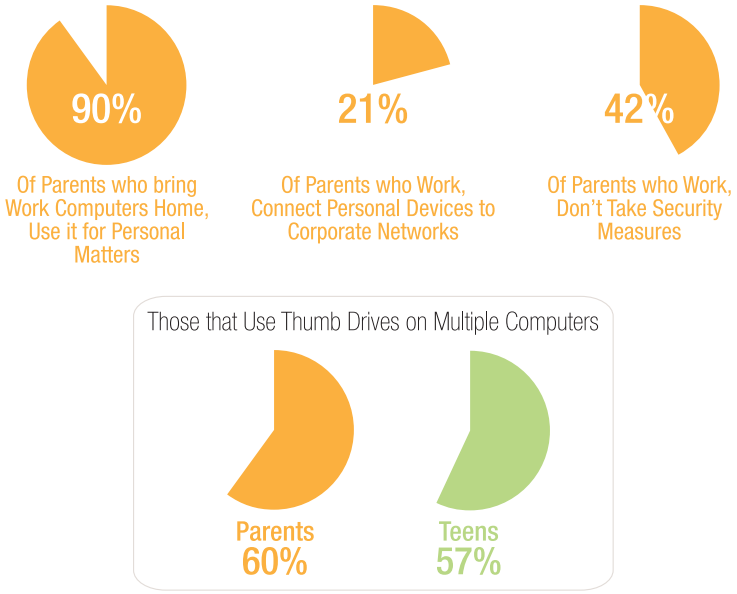


FIGURE 12

STUDY FINDINGS: Communications Habits and Safety

Teens are a very "connected" group, with 79% of them indicating that they have a mobile phone, enabling them to make and receive both calls and text messages. Of those, 29% (or 23% of all the teens surveyed) report owning a smart phone, granting them access to the Internet from any location at any time. (See Figure 13)

TEENS AND CELL PHONES:
smart phone capability

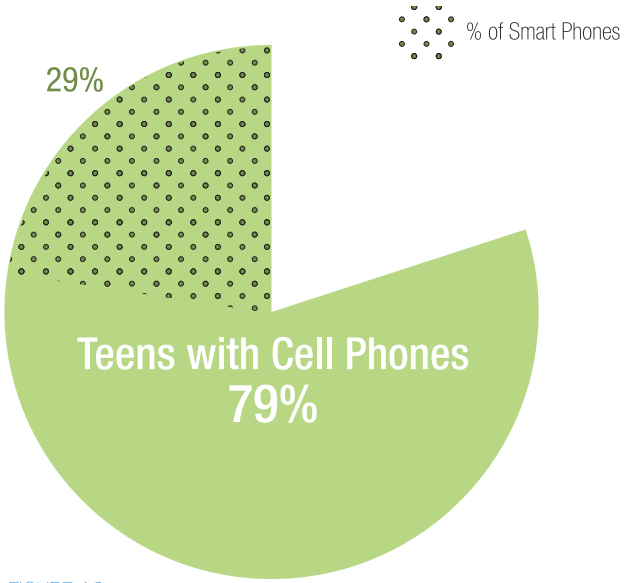


FIGURE 13

However, being more connected may have a deleterious effect on person-to-person communication. (See Figure 14) 31% of teens admit that they have communicated something to someone online or via text message that they would not feel comfortable saying to them in person. 4% of teens admit to having bullied someone via electronic communications, while 11% report having been bullied either online or via text messages. Girls report a higher incidence of being bullied (15%) than the 7% of teenage boys who admit it. (See Figure 14)

ONLINE TEEN COMMUNICATIONS:
risks and bullying

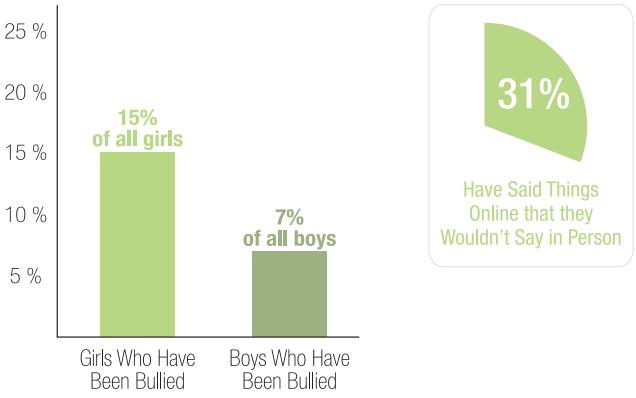


FIGURE 14

29% of teens report that they have been contacted online by a person they would deem a stranger – someone with no known ties to them or their friends. Of that group, 62% report that they have been contacted by a stranger on more than one occasion, and 23% confess they have responded to the stranger in some way. (See Figure 15)

STRANGER DANGER:

teens that have been contacted by strangers online

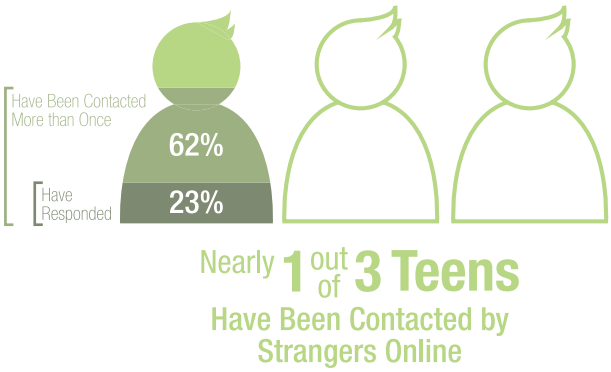


FIGURE 15

STUDY FINDINGS: Internet Safety Education

Regardless of the accepted expectations of teen behavior (Figure 1), a majority of both parents and teens say they've talked with each other about Internet safety, though parents are a bit more likely (94%) to say they've had that discussion than are teens (84%). (See Figure 16)

DO PARENTS COUNSEL TEENS ON INTERNET SAFETY?:

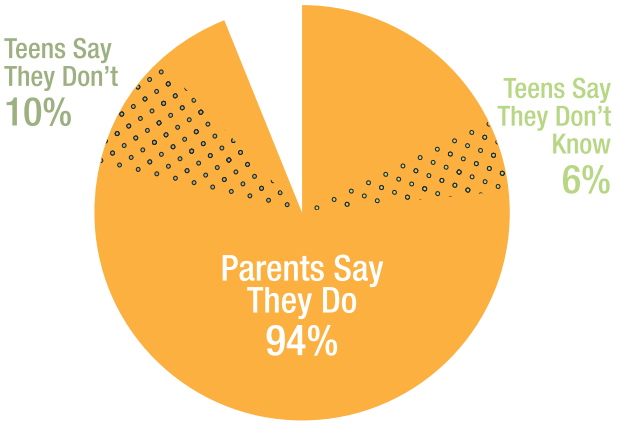


FIGURE 16

As seen in Figure 17, there is also uncertainty as to how much Internet safety education is occurring in schools. 33% of parents say that they do not know if their teen's school offers Internet safety education, while 24% of teens say that their schools do not have such a program in place or do not know if there is one available.

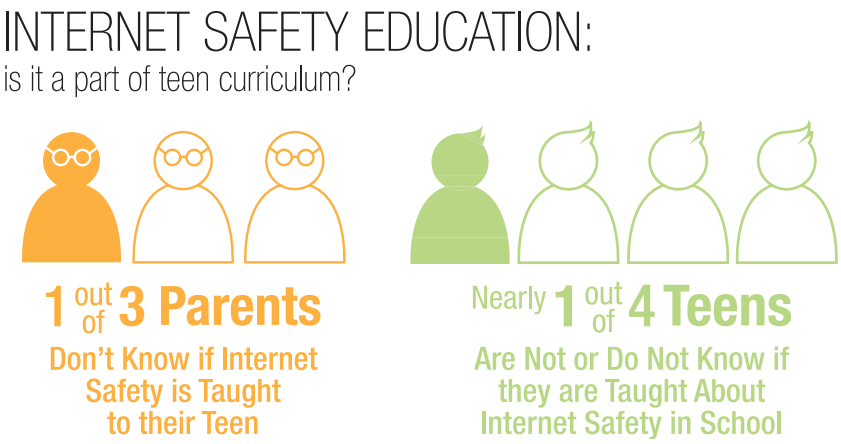


FIGURE 17

Parents are also unsure of how much access their children have to the Internet when they are in school. 72% of teens say that they use either a desktop or laptop computer to go online at school, yet 26% of parents do not know if their teen's school monitors their Internet use. (See Figure 18)

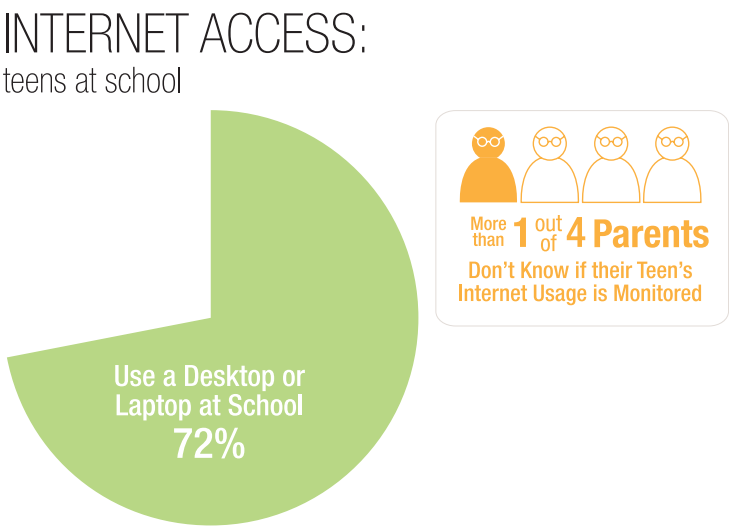


FIGURE 18

Conclusion

Study results indicate that substantial numbers of parents and teens are both engaged in highly risky online behavior in the home. In general, there would seem to be room for significant improvement in Internet safety education among parents and teens, as well as in school systems. Given the potential ramifications of improper Internet use today, it would seem to merit at least the same degree of educational vigilance as other lifestyle risk categories like sex, drugs and alcohol. Some key areas for improvement would include:

- Education on the need to have antivirus software installed and up to date on their computers.
- Education about the potential dangers of visiting adult websites, which are often used by cyber criminals as malware-delivery vehicles.
- Education about the danger of inappropriate content in general – and how the Facebook photo a teen posts today could come back to haunt them when they apply to college or to a company.
- Education about proper communications etiquette, with a focus on online bullying and "stranger danger."
- Education on responsible use of employers' computers so irresponsible home usage does not impact ones professional livelihood.

Copyright © 2011 GFI Software. All rights reserved. All trademarks used are owned by their respective companies. To the best of our knowledge, all details were correct at the time of publishing.