

**Testimony of Thomas M. Dailey  
Chair and President U.S. Internet Service Providers Association  
General Counsel, Verizon Online**

**Before the Subcommittee on Technology, Information Policy,  
Intergovernmental Relations and the Census  
June 16, 2004**

Thank you Mr. Chairman and members of the Subcommittee for this opportunity to testify about the security challenges facing home and small businesses users on the Internet. The U.S. Internet Service Providers Association (US ISPA) is a leading Internet industry group, representing some of the nation's largest Internet service providers, portal companies and network providers (collectively "ISPs") on important policy issues with a focus on security related matters.<sup>1</sup> The US ISPA is pleased to present testimony before this Subcommittee.

Internet security for home users and businesses is an important and complex issue. While the tools to help protect computers and data from intrusion are commercially available from multiple sources, and public and private educational initiatives have made online materials readily available, educating users in the proper use of such tools and raising their level of cyber security awareness is a significant challenge. For varying reasons, many consumers have not been able to keep up with the technology or information necessary to protect themselves from Internet threats. Although ISPs can and do play an important and helpful role in the education process, ISPs do not make security software or hardware products, or control the end user's activities on the Internet, or the ability or desire of end users to learn and stay current about security issues. In the end, no single group or industry can dictate the behavioral change

---

<sup>1</sup> US ISPA's members include AOL, Bell South, EarthLink, eBay, MCI, Microsoft, SAVVIS, SBC, and Verizon.

necessary to significantly improve the security awareness of Internet users. Such change requires a joint public-private sector education effort targeted to enhancing the cyber security awareness of the Internet-using public.

**A. Understanding the challenges that home and small business users face in protecting their computers that are connected to the Internet.**

Home and small business users face a number of challenges in safeguarding their computers and personal information from hackers and scam-artists on the Internet. Here are a few of the more significant challenges from the ISP perspective: 1) recognizing the need for anti-virus and firewall software; 2) getting past the “barriers” to keeping software up-to-date; and 3) staying current on threats and how to spot, avoid and remedy them.

1) Recognizing the need for security. To stay safe online, the home or small business user must first understand that running anti-virus *and* firewall software is essential to securing any computer connected to the Internet, and that such software needs to be frequently used *and* updated. Security software solutions are widely available to consumers today. Many computers come with anti-virus software preloaded or available free for a trial period. Most major ISPs, including US ISPA’s ISP member companies, offer security services as part of their portal services or as standalone services that customers can purchase, often at a discount. Firewall software and hardware are also widely available, and some companies offer free firewall software programs that work well for home and small business users. Small business users can purchase security services from their ISP or from third party consultants. Thus, the challenge is not in the availability of security solutions, it is in helping home and small business users to recognize the need for and to install, use and update security hardware and software.

2) The “barriers” to use of security software. Despite the availability and relative ease of use security software, not all users run or update their software on a regular basis. A lack of time may be one cause. Another may be discomfort with technology – in a mass-market environment the technical knowledge of end users varies widely. Regardless of the reason, consumers need help to get past whatever barrier is keeping them from recognizing and using the security tools available. Doing so may require education in the proper use of security software and messaging about the risks of leaving a computer open to security threats. Such efforts should include helping consumers to understand the cost of not taking security precautions to fully gauge the risks of inaction.

3) Staying current on threats and how to spot and avoid them. Even if an end user installs and regularly runs his or her security software, he or she is not free of risk from intrusions, hacks and privacy loss. Software is just a tool – understanding the threats, how to spot them and therefore how to avoid and remedy them, is critical. Equally important is staying current on threats, whether in the form of the latest worm or identity theft scam. Knowing where to look for help – and who is a trusted source of information – can be a challenge for many users. The tools are there, if consumers know where to look.

Government agencies like the Federal Trade Commission (FTC) and the Department of Homeland Security (DHS), and organizations like the U.S. Chamber of Commerce, the National Cyber Security Partnership (NCSP),<sup>2</sup> and the National Cyber Security Alliance (NCSA), are committed to the education effort and are providing key leadership in this area. The NCSA

---

<sup>2</sup> The National Cyber Security Partnership is a coalition of trade associations, including the U.S Chamber of Commerce, the Information Technology Association of America, TechNet and the Business Software Alliance. See <http://www.cyberpartnership.org>.

website, [www.staysafeonline.info](http://www.staysafeonline.info), is a good example of the benefits of public-private partnership to address the security issues confronting Internet users today. Another is the U.S. Computer Emergency Readiness Team (CERT) website, [www.us-cert.gov](http://www.us-cert.gov), sponsored through a partnership between DHS and the public and private sectors. Industry, too, is working to provide education and self-help sites to assist consumers in finding information about current threats and ways to avoid them. Personalfirewallday.org and Getnetwise.org are two good examples.<sup>3</sup> The websites and resources US ISPA members make available to their customers (*see* Exhibit A to this testimony for a sampling of such sites) is a further example of the private sector's commitment to helping consumers to protect themselves from Internet threats.

With all the government and private resources available, however, the ultimate responsibility for maintaining security rests with the end user. A critical challenge facing consumers, industry and policy-makers alike, therefore, is educating millions of end users not only about the tools and strategies available in the market, but also about threats and threat-avoidance.

**B. Some of the Internet threats facing home and small business users, including phishing, zombies, spyware, worms, spackers and denial of service attacks.**

There is a multitude of threats facing all Internet users, including home and small business users. Many bear imposing or even slightly comical names, like "Slammer," "MyDoom," "Bagel," "phishing" and "distributed denial of service" (DDoS) attacks. The risks these threats bring to bear are real and fall into several categories. The first includes "worms,"

---

<sup>3</sup> See <http://www.personalfirewallday.org>; <http://www.getnetwise.org>. Personal Firewall Day is a website sponsored by security software firms Microsoft, McAfee, ICSA Labs, Sygate and TruSecure that provides general advice and encouragement to novice Internet users about anti-virus and firewall software and the importance of upgrades. Getnetwise is a public service website sponsored by a broad group of Internet companies and public interest organizations, including several US ISPA members.

Trojans” and viruses, which typically infect a user’s computer and either affect its operation or serve as a tool to accomplish some other end, such as a DDoS attack or spam propagation.

“Spackers” represent a new and problematic union between hackers and spammers. Spammers pay hackers for compromised computer ID’s or to hack into systems to install “zombie” software for later use as an e-mail relay. Once the software is triggered, the compromised “zombie drone” computer sends volumes of e-mail or other messages to a pre-determined set of e-mail addresses or addresses taken from the host computer’s address book.<sup>4</sup>

“Spyware” is another security issue that has attracted attention of late. Arriving at a widely accepted and correct definition for “spyware” has proven problematic for the industry and policy-makers alike. Defining the term too broadly runs the risk of ensnaring legitimate and even beneficial forms of software. The most intrusive forms of “spyware,” however, are programs installed on a user’s computer that monitor the user’s keystrokes or Internet activity and can secretly collect personal information or enable a computer to be hijacked. Anti-spyware software is now available in both free and fee-based forms. It removes many unwanted programs, but some spyware can be difficult to find and uninstall, especially where it is bundled with other software.

---

<sup>4</sup> The Committee expressed specific interest in recent news reports that hackers could purchase computers infected with worms or viruses (10,000 infected computers for just \$500.00 in one news story) and use those computers to launch DDoS attacks, to send spam (spacking referred to above) or engage in other unlawful activities. See *Phatbot arrest throws open trade in zombie PCs*, [theregister.com, http://www.theregister.co.uk/2004/05/12/phatbot\\_zombie\\_trade.html](http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade.html) (05/12/04). The particular instance described in the story is a form of “spacking.” The fact that the Internet underground has attached a value to compromised or zombie machines is a sobering but not necessarily surprising development. With the millions of dollars spammers make through the distribution of unsolicited e-mail, it is little wonder that a market for zombie machines, which are difficult to trace and provide a degree of anonymity to the spammer, has evolved.

Identity theft is yet another category of threat facing home and small business users. Identity theft has been around in different forms for many years. For example, in the past credit card users worried that a credit card receipt left behind with a merchant might allow an unscrupulous person to copy the credit card number and use the credit card to run up charges. The Internet version of this type of fraud is known as “phishing”.<sup>5</sup> The term phishing applies to hackers who imitate legitimate companies in e-mails or create fake websites designed to look like a legitimate website to entice users to share their passwords, credit card numbers and other personal information. The hacker then uses the information to steal the target’s identity or to sell that identity to others.

Over the years, phishing attacks have grown from stealing dialup Internet accounts into more sinister criminal enterprises. Phishing attacks have risen sharply and now target users of online banking, payment services such as PayPal, and online e-commerce sites, among others, and the attacks represent a significant threat to the branding and reputation of the legitimate companies whose brands are spoofed. Many phishing sites operate either from off-shore locations or from hijacked servers with exposed vulnerabilities. The sophistication of phishing schemes is increasing and it has become more and more difficult to determine if phishing e-mails are real or not. Phishing scams threaten to erode customer confidence and decrease use of online systems and brands.

---

<sup>5</sup> The word "phishing" refers to Internet scam artists who use e-mail lures to "fish" for passwords and financial data from the “sea” of Internet users. The term was coined in the mid-1990s by hackers who were stealing ISP accounts by scamming passwords from unsuspecting users. By 1996, hacked accounts were called "phish", and by 1997 phish were actually being traded between hackers as a form of currency where hackers would routinely trade 10 working “phish” for a piece of hacking software.

The variety of threats on the Internet underscores the reason home and small business users must remain vigilant in using and maintaining their anti-virus and firewall software. While desktop software solutions can effectively limit exposure to many forms of viruses and worms or even spyware that captures personal information, there is no substitute for consumer awareness of Internet scams and schemes and knowledge about the ways to spot and avoid them.

**C. The tools and strategies available to home and small business users to help mitigate their exposure to malicious attacks and scams over the Internet**

The key to mitigating risk from exposure to security threats on the Internet is a combination of the effective use of software and hardware tools, and an awareness of cyber threats and how to avoid them. Home and small business users have an array of tools available to them through the major ISPs, such as US ISPA's members. ISPs not only provide a host of security products directly to their customers or through third party relationships, they play an important role in the education effort by providing useful resources about a variety of online safety and security issues. But ISPs can only provide a part of the solution. Software and hardware manufacturers as well as government organizations, such as the FTC, CERT and DHS, and consumers themselves all have a critical role to play in the education and awareness effort.

The members of the US ISPA fully support online security and safety education. For example, AOL, Bell South, EarthLink, Microsoft, SBC and Verizon Online, and each provides its customers with access to extensive Internet security websites (and other online help areas) that include child protection, anti-spam, anti-spyware and firewall software and other security services. ISPs also provide advice on password use, threat alerts and links to security software and government informational resources and websites. Attached as Exhibit A to this testimony are sample screen shots from some of our member's security-oriented websites. As these

website screenshots show, ISPs take very seriously the role of educating their customers about Internet security and helping consumers to help themselves in this important area. USISPA members realize that Internet security is no longer an add-on feature, but must be part of the basic service offering. Taking advantage of these services is an important part of any home or small business user's cyber security strategy.

Software and hardware manufacturers also offer an array of tools commercially. Many such tools are bundled with portal client software or computers sold by major computer makers. As described above, this software includes anti-virus, firewall, anti-spyware and anti-spam applications that can effectively limit the functioning and distribution of viruses, worms, spyware and Trojans. Government agencies like the FTC, CERT and DHS, and public-private partnerships like the NCSA and the NCSP, also provide valuable information on threat alerts and cyber tips for limiting exposure to security risks. While no security solution provides absolute protection against Internet threats, the combination of security software tools and access to online resources should be a major part of any user's cyber security strategy.

**D. What responsibility do hardware and software vendors have to ensure that their products are secure "out of the box"?**

Hackers and others bent on exploiting the Internet and Internet users are constantly coming up with new threats and scams. Keeping up with the changing nature of the threats and ensuring that software and hardware is secure "out of the box" is undoubtedly a difficult task. Software vendors and hardware manufacturers have strong incentives to make their products secure and to find ways to simplify the automatic update process. It is also critical that users understand the importance of making sure they are using the appropriate security software and that their software is properly updated, and the consequences of not doing so. Thus, the

responsibilities of software and hardware manufacturers cannot be entirely separated from the responsibilities of users -- or from the overall need for better education.

**E. Education is the key to improving the security of home and small business users**

Educating the mass market of consumers and small businesses, who have widely differing levels of technical and Internet knowledge, is essential to reducing security risks on the Internet. But this education effort requires a concerted effort from all stakeholder groups, including the information and technology industry, government and the schools. Raising consumer awareness of technical issues, like anti-virus protection, password protection and firewall usage, takes time to work itself into the fabric of the average user's experience. For this reason, it is important to develop a multi-pronged education and awareness campaign that targets all segments of the Internet using public, including the schools, starting with K-12 programs.

Significant effort should be focused on educating our children in the safe and lawful use of the Internet. Our schools need to build Internet security and online safety into their curricula. Parents need to take time to learn about proper cyber security techniques to protect their computers and their children from Internet threats. Kids often learn technology faster than their parents, but without training and direction they are just as likely to engage in activity that could open a computer to attack or allow privacy to be compromised (file sharing is a quick and often painful way to learn that your anti-virus software is not up-to-date). Moreover, kids need to learn at an early age how to protect themselves from online predators and scam artists. We teach kids to be wary of strangers when walking home; we should do no less to teach kids how to avoid threats on the Internet.

The education effort does not end with our children, however. Consumer awareness must also be built through advertising, public-service messaging (as others have testified, a Smoky the Bear campaign for online security) and through other key touch points, like contact with software and hardware manufacturers and ISPs. While the messaging need not be identical, there should be continuity on the basic messaging points. The Top Ten Cyber Security Tips on the NCSA website<sup>6</sup> is a good place to start. Companies can take those portions of the Top 10 tips and reinforce the messaging through their own websites and programs. Many if not all US ISPA members are already doing so.

Awareness building is not just a private sector responsibility. The efforts of the FTC, CERT and DHS (and others) and their various public-private sector partnerships should be encouraged and supported. Policy-makers should also look to new and creative ways to generate interest in cyber security, such as through federal training grants and scholarships and national public service advertising campaigns targeted to enhancing security awareness.

### **Closing Remarks:**

The timing of this Subcommittee's inquiry into information and Internet security is right. Now is the time to explore the issue of enhancing the education and awareness of Internet users. But the task ahead is large and complex. Consumers come with all levels of technical knowledge and commitment to protecting their security and privacy. To continue the advancements in security attained to date, a multi-pronged approach that encourages each element of the Internet community, including the public and private sectors, to participate separately and collectively, is necessary.

---

<sup>6</sup> See <http://www.staysafeonline.info>.

On the public sector side, government should continue the outstanding work it has begun to enhance consumer awareness. Public-private partnerships should be supported. On the private sector side, market-based solutions should continue to drive innovation among software and hardware manufacturers, ISPs and others in the online security industry. The impact of competition is already apparent. Software is smarter, easier to use and more powerful than ever before. Updates are now broadcast automatically to millions of anti-virus and operating system users. Security specialists and network companies provide a wide array of services to help protect home and small business users. These advancements in online security have taken place in a cooperative environment with government agencies, driven by concern for consumers and protection of the network. The incentives are in place for continued development; government mandates are not the answer.

Finally, home and business users must step up their efforts to educate and protect themselves, with the help of the public and private sectors. The key to home and small business user acceptance and use of Internet security tools is to identify more effective ways to alert the public to the security solutions that are available, to make them simple to use, and that the consequences of not maintaining adequate cyber security awareness can be severe. At the end of the day, even the most effective tools will be of limited utility unless end users are aware of and choose to use them.

The US ISPA and its member companies are working hard to protect consumers and to make their online experience as safe and satisfying as possible. The US ISPA thanks the Subcommittee for this opportunity to testify today.