

**For Immediate Release**

Press Contact:  
Andrew Weinstein  
America Online, Inc.  
(703) 265-0185  
[andrewwstn@aol.com](mailto:andrewwstn@aol.com)

Susan Engley  
O’Keeffe & Company, Inc.  
(703) 883-9000 ext. 129  
[sengley@okco.com](mailto:sengley@okco.com)

**LARGEST IN-HOME STUDY OF HOME COMPUTER USERS SHOWS MAJOR  
ONLINE THREATS, PERCEPTION GAP**

**Joint AOL/NCSA Online Safety Study Finds That:**

**77% Think They Are Safe from Online Threats But...**

**67% of Computers Lack Current Anti-Virus Software, 1 in 5 Are Infected with Virus  
80% of Home Computers Infected with Spyware/Adware; 88% Didn’t Know They Were  
Infected**

**49% of Broadband Users Lack Any Firewall Protection**

WASHINGTON, DC – OCTOBER 25, 2004 – The National Cyber Security Alliance (NCSA), a not-for-profit, public-private partnership focused on driving awareness and promoting education of cyber security, and NCSA member America Online, Inc., the world’s leading interactive services company, today released the results of one of the largest and most comprehensive in-home studies ever conducted on the security of computer users.

The AOL/NCSA Online Safety Study – conducted by technical experts in the homes of 329 typical dial-up and broadband computer users – found that most computer users think they are safe but lack basic protections against viruses, spyware, hackers, and other online threats. In addition, large majorities of home computer users have been infected with viruses and spyware and remain highly vulnerable to future infections. Yet at the same time, most keep sensitive personal and financial information on their computers.

Among the key findings:

**PERCEPTION GAP:** The large majority of users falsely believe that they are safe from online threats.

- More than three quarters (77%) said they think their computer is very or somewhat safe from online threats.
- Almost the same percent (73%) said they think their computer is very or somewhat safe from viruses.
- Three in five (60%) said they feel very or somewhat safe from hackers.

**VIRUSES:** Yet most computer users do not have updated anti-virus protection on their computers and either have been or are currently infected by viruses:

- Two-thirds of users (67%) do not have current anti-virus software (updated within last week).
- One in seven users (15%) has no anti-virus software at all on their computer.
- Almost two-thirds of respondents (63%) said they have been the past victim of a virus infection.
- One in five users (19%) has at least one virus infection currently on their home computer.

**SPYWARE:** Spyware and adware infections were endemic but almost completely unknown to users.

- Four in five users (80%) have spyware or adware programs on their computer.
- The average infected user has 93 spyware/adware components on their computer, and the most components found on a single computer during the scan was 1,059.
- An overwhelming majority of users (89%) who were infected with spyware/adware said they didn't know the programs were on their computer.
- Nine in ten infected users (90%) said they don't know what the programs are or do.
- Almost all of the infected users (95%) said they never gave permission for the programs to be installed.
- All but a handful of infected users (86%) asked the technicians doing the study to remove the programs.

**FIREWALL:** Most computer users don't have adequate protection against hackers.

- Two-thirds of all computer users (67%) do not have any firewall protection at all – half of those with a broadband connection lack a firewall.
- Almost three-quarters (72%) do not have a secure firewall (with no open ports).
- Almost two in five wireless network users (38%) leave their connection completely open (without any WEP or WPA-PSK encryption).

**SIGNIFICANT CONFUSION:** Users said that they are confused by the protections they are supposed to use and how to use them:

- Three in five users (58%) said they don't understand the difference between a firewall and anti-virus software very well or at all.
- More than half (53%) said they don't understand what a firewall is and how it works.

**SENSITIVE INFORMATION:** Despite this confusion and lack of cyber-protections, online users are increasingly moving sensitive information and activities online:

- The vast majority of respondents (84%) said they keep sensitive information like health or financial records on their home computer.
- Nearly three-quarters (72%) said they use their home computer for sensitive online transactions like banking or reviewing personal medical information.

**PARENTAL CONTROLS:** Despite the importance of protecting children online, most users – including parents – do not use parental controls software.

- More than four out of five users with children (83%) do not use parental controls software.
- Less than one in 20 broadband users (4%) uses parental controls software.

**DIAL-UP vs. BROADBAND:** The study also found that narrowband users are at particular risk from viruses and spyware, perhaps because their use of a firewall is dramatically lower:

- 25% of NB users currently have a virus infection (vs. 15% of BB users)
- 88% of NB users have spyware/adware on their computer (vs. 74% of BB users)
- Only 7% of NB users have any firewall (vs. 51% of BB users).

**SPYWARE SYMPTOMS:** Although the overwhelming majority of users are infected, most users don't recognize the symptoms of spyware/adware:

- Nearly two-thirds of users with a pop-up blocker (63%) said they get pop-ups anyway.
- Two in five users (43%) said their home page has been changed without their permission.
- Almost the same number (40%) said their search results are being redirected or changed.
- Users with spyware/adware said they get twice as many pop-ups on average each week as users without spyware/adware (31 vs. 15).

## **REACTION TO THE STUDY:**

“For the first time, we’ve reviewed the actual security protections that consumers use for the sensitive information they keep on their home computers, and the results validate our purpose — to raise awareness and change behavior,” said Ken Watson, Chairman of the National Cyber Security Alliance. “Extrapolating the percentages in our survey, this indicates that millions of Americans are at risk – and are already infected – by viruses, spyware, and adware. With October as National Cyber Security Awareness Month, now is the perfect time for every American to review the protections they have and make sure those protections are up-to-date and complete.”

“Protecting the safety of our technology infrastructure means protecting the computers of individual Americans. Using viruses, remote attacks, and drone machines, a single attacker could mobilize thousands of compromised computers from unsuspecting users. This study highlights just how important it is for individual Americans to take their cyber-security seriously, not just as a matter of personal safety, but as a matter of our country's security as well,” said Dan Caprio, Chief Privacy Officer and Deputy Assistant Secretary for Technology Policy at the U.S. Department of Commerce.

“No consumer would walk down the street waving a stack of cash or leave their wallet sitting in a public place, but far too many are doing the exact same thing online,” said Tatiana Gau, AOL's Chief Trust Officer and Senior Vice President for Integrity Assurance. “Without basic protections like anti-virus, spyware protection and a firewall, consumers are leaving their personal and financial information at risk. Now that we know the scope of the problem, we can redouble our efforts to educate consumers about the solutions to staying safe online.”

Additional information about the National Cyber Security Alliance, including tips to stay safe online, and the complete results of the AOL/NCSA Online Safety Study are available at [www.staysafeonline.info](http://www.staysafeonline.info).

## **METHODOLOGY**

The AOL-NCSA Online Safety Study was conducted through in-person interviews and technical analyses with a typical sample of 329 dial-up and broadband adult computer users, at least 18 years of age, from September 15 to October 8, 2004. The sample included 194 broadband users (59%) and 135 dial-up users (41%). The margin of error for the survey portion of the study was +/- 5.4% with a 95% confidence level.

Study participants were interviewed in more than 22 cities and towns and a dozen different states and metropolitan areas. Metropolitan areas from which participants took part included Los Angeles, California; metropolitan Washington, D.C.; Naples, Florida; Atlanta, Georgia; Minneapolis/St. Paul, Minnesota; Rochester, New York; Raleigh, North Carolina; Houston, Texas; Seattle, Washington; and Virginia Beach, Virginia. Subjects were questioned on various aspects of online security to assess their understanding and awareness of the issue. The subjects' computers were then examined by technicians using commercially-available products to examine their firewall settings, anti-virus software, potential virus infections, parental control software, and spyware. Participants were selected by an independent market analysis organization.

### **About The National Cyber Security Alliance**

A not-for-profit 501(c)(3) organization, the National Cyber Security Alliance (NCSA) is the go-to resource for cyber security awareness and education for home user, small business, and education audiences. A public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations. NCSA provides tools and resources to empower home users, small businesses, and schools, colleges, and universities to stay safe online. For more information, and to see the top 10 cyber security tips, visit [www.staysafeonline.info](http://www.staysafeonline.info).

### **About America Online, Inc.**

America Online, Inc. is a wholly owned subsidiary of Time Warner Inc. Based in Dulles, Virginia, America Online is the world's leader in interactive services, Web brands, Internet technologies and e-commerce services.

###