FINAL

Contact Information:

Melissa Smolensky
Porter Novelli
512-241-2232
melissa.smolensky@porternovelli.com

Jessica Cassady
CA
202-513-6306
jessica.cassady@ca.com

CA / NATIONAL CYBER SECURITY ALLIANCE SURVEY REVEALS CONSUMERS ENGAGE IN RISKY ONLINE BEHAVIOR ON SOCIAL NETWORKING SITES, LEAVING THEM VULNERABLE TO POTENTIAL CYBER-CRIME

83 Percent of Adults Who Social Network Expose Themselves To Hackers and Identity Thieves

ISLANDIA, N.Y. and WASHINGTON, D.C., October 4, 2006 – Kicking off October as National Cyber Security Awareness month, CA (NYSE: CA) and the National Cyber Security Alliance (NCSA) today announced results of the first social networking study examining the link between specific online behaviors and the potential for becoming a victim of cyber-crime. Although social networking sites, such as MySpace and FaceBook, have been examined from the standpoint of physical security issues, including sexual predators, this survey examines users' online behavior and the possibility of other threats such as fraud, identity theft, computer Spyware and viruses. Highlights of the survey include:

- Although 57 percent of people who use social networking sites admit to worrying about becoming a victim of cyber-crime, they are still divulging information that may put them at risk. For example 74 percent have given out some sort of personal information, such as their e-mail address, name and birthday.
- 83 percent of adults social networking are downloading unknown files from other people's profiles potentially opening up their PCs to attacks.
- 51 percent of parents aware of their children social networking do not restrict their children's profiles so only friends can view, leaving their child's profiles unrestricted to potential predators.
- Furthermore, 36 percent of these parents surveyed do not monitor their children on social networking sites at all.

In contrast to the popular perception that social networking is an activity enjoyed almost exclusively by tweens and teens, the CA/NCSA social networking research study reveals a large number of adults (48 percent), 18 plus, social network. It is not just young adults social networking, 53 percent of adults who use social networking sites are over the age of 35. The growing number of adults using social networking sites is an indicator of the increasing popularity—and potential security risks—of these sites.

“Although the general community thinks most social networking users are teens, the CA/NCSA survey showed the popularity of these sites is extending beyond young early adopters to other segments of the population,” said Ron Teixeira, executive director of NCSA. “Those who frequent these sites should be aware the data they share may make them prey for online attacks. Giving out a social security number, paired with a birthday and name, could provide enough ammunition for criminals to hack into financial records and compromise users’ personal information.”

The CA/NCSA survey also revealed users of social networking sites are not only giving out potentially harmful information, but they are also engaging in other risky behaviors, such as downloading unknown files and responding to unsolicited emails and instant messages, all of which may lead to identity theft, computer spyware, viruses and other risks. 83 percent of social networking participants have downloaded content from another user’s profile. 31 percent of adults who use social networking sites have responded to phishy unsolicited email or instant messages.

Adults who use social networking sites may be putting themselves at risk, and may be placing their businesses and places of employment in harm’s way. Of those who have access to a computer at work, 46 percent engage in social networking at the office, potentially making the workplace vulnerable to online security threats.

“As social networking use continues to increase in popularity, it is imperative that people take steps to safeguard their information at home and at work,” said David Luft, senior vice president of Product Development for CA. “Not only is it important to install and frequently update firewalls, anti-spyware and anti-virus software, users must be aware of the specific unsafe behaviors which make them vulnerable to online predators, hackers and thieves.”

On an encouraging note, the survey revealed that adults are taking safety precautions with their children. Of the parents that know their children under 17 use social networking sites, 64 percent monitor their children’s profiles and 49 percent have only allowed their children’s profile to be seen by his/her friends. Many adults have discussed safety precautions with their children: 94 percent have discussed how to watch for predators, 72 percent have discussed how to watch out for malicious software and 64 percent have discussed how to watch out for fraudsters trying to steal money.

In order to protect yourself, follow the NCSA and National Consumers League’s pointers to stay safe while on social networking sites:

- Guard your financial and other sensitive information. Never provide or post your Social Security number, birth date, address, phone number, bank account or credit card numbers, or other personal information that could be used by criminals.
- Picture social networking sites as billboards in cyberspace. Police, college admissions personnel, employers, stalkers, con artists, nosy neighbors—anyone can see what you post.
- Be cautious about meeting your new cyber friends in person. After all, it’s hard to judge people by photos or information they post about themselves.
- Think twice before clicking on links or downloading attachments in emails. They may contain viruses or spyware that could damage your computer or steal your personal information—including your online passwords and account numbers.

- Protect your computer. Use a spam filter, anti-virus software, anti-spyware software and firewall.
- Beware of con artists. Criminals scan social networking sites to find potential victims for all sorts of scams, from phony lotteries to bogus employment and business opportunities to investment fraud.

For the complete CA/NCSA survey on social networking, as well as more information on the steps to stay safe on social networking sites, please go to www.staysafeonline.org.

Survey Methodology

This research was conducted as part of the Russell Omnibus conducted by Russell Research of New York, NY. Interviewing was conducted August 25 - 28, 2006 and September 5 - 7, 2006. They interviewed 2,163 adults 18 years old and over. The sample was weighted to provide a national representative and projectable estimate of the adult population. Sampling error for a survey of this size is 2.1 percent at the 95 percent level of confidence.

About The National Cyber Security Alliance

A not-for-profit 501(c)(3) organization, the National Cyber Security Alliance (NCSA) is a central clearinghouse for cyber security awareness and education for home users, small businesses, and the education community. A public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations. For more information, and to review the top 8 cyber security practices, visit www.staysafeonline.org.

About CA Home & Home Office

CA Home and Home Office products are offered by leading Internet Service Providers (ISPs) and are used by more than 12 million consumers. The products are based on CA's enterprise-grade solutions and include a full range of security and utility software solutions. For more information, please visit http://ca.com/consumer.

About CA

CA (NYSE: CA), one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT. Founded in 1976, CA is headquartered in Islandia, N.Y., and serves customers in more than 140 countries. For more information, please visit http://ca.com.

###