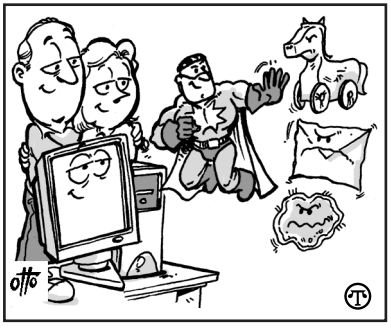
Safeguarding Your Computer

Home Computer Users: The Last of the Unprotected

(NAPSA)—With declining prices for most high-tech products, consumers are purchasing additional PCs and laptops. But are consumers also purchasing security products to protect their new computers? And have they secured the computers they already own?

Identity theft is widespread and the Internet is crawling with worms, viruses, Trojan horses and other threats. These menacing programs can take control of a user's computer system or e-mail service and cause great annoyance, if not damage. And even more software variants called spyware and adware are rampaging over the Internet to monitor and try to wrest control of users' online activities.



Identity theft is widespread and the Internet is crawling with worms, viruses, Trojan horses and other threats.

Andrew Conry-Murray, editor for IT Architect magazine, noted in his book The Symantec Guide to Home Internet Security that fraud attacks against home users have increased dramatically. "Computer fraud attempts to separate you from your money by offering shady products via e-mail or pop-up ads or by tricking you into revealing personal information or financial account data such as passwords. Identity theft, phishing, or spam are prime examples of computer fraud."

Despite the grim outlook, users can protect their personal information stored on their PCs and laptops by taking a few basic security measures:

1. Be suspicious—open e-mail responsibly. Never open attachments from unknown senders and don't respond to spam.

2. Increase security settings on Web browsers and do not enable file sharing.

3. Create strong passwords with at least eight characters combining alphanumeric and special characters and change passwords every 45-60 days.

4. Keep current with operating system and security software updates to provide the latest protection for every computer—that includes laptops.

5. Install antivirus software on all desktop and laptop computers to prevent virus infection.

6. Use a firewall on all desktop and laptop computers to block intruders.

7. Back up important data regularly and store extra copies offsite.

8. Secure wireless connections with a virtual private network (VPN) and install firewalls.

It's clear that as more users "surf" the Internet on their desktop and laptop computers, the potential for attack is growing at the same time. By implementing these security measures, users should easily improve security. Still, the best approach to online security is to stay aware, educated and up to date.

To learn more about how to protect yourself from identity theft and harmful viruses, visit www.symantec.com.