Wireless-security campaign steps up

March 8 2006

Talking about connectivity on-the-go and being concerned about storage capacity is no longer a sign of being a geek, but rather very much part of everyday life for many people. Yet as the number of Internet users rises and the use of the Web proliferates to every facet of everyday life, the need for security in cyberspace and bolstering public awareness of that need is only intensifying.

"Sales of laptops and portable devices continue to skyrocket as more and more Americans demand mobile Internet access, but with this increased usage come added security risks," said Rep. Mike Honda, D-Calif., at a briefing on cybersecurity Tuesday.

As the representative from Silicon Valley, Honda has been one of the more active members of Congress when it comes to issues regarding technology and is indeed the chairman of the Congressional Internet Caucus' wireless task force.

But Honda warned that not only is there greater personal risk by depending too heavily on mobile devices under the current circumstances, but that the threat to national security too rises unless both the government and corporations as well as individual users become more responsible in their use of technology.

"Reliance on computers and computer networks raises the vulnerability of the nation's critical infrastructures to cyber-attacks. The federal government consistently receives inadequate grades for its information security efforts," the Honda argued.

As such, Honda was on hand at the launch of the wireless-security initiative to boost public awareness of the threats in cyberspace that is a joint project with the non-profit Internet Education Foundation's GetNetWise coalition together with Web security group Symantec.

With advanced technology come "complexity and security risk as wireless networks and handheld mobile devices become a new target for hackers and thieves looking to disrupt usage and steal personal information and business-critical data. The increased risk of information theft and malicious code affecting handheld mobile devices demands more education and vigilance from consumers and small office and home office users alike," said Sarah Hicks, vice president of mobile and wireless solutions at Symantec.

Indeed, Symantec pointed out that in places like New York's Brooklyn Heights and Harlem, 52 percent of wireless access points in residential areas had no encryption of online information whatsoever, while 11 percent of the WiFi users detected a default service set identifier.

At the same time, the number of wireless users at home is estimated to increase to 28 million by 2008, according to Jupiter Research, which will make it more important than ever for individuals to ensure that their wireless networks are secure from attacks.

Symantec found that presently, "a large percentage of Wi-Fi users are leaving their doors wide open for hackers and crooks to steal their identities and personal information."

"As wireless devices proliferate, we must ensure that their security is taken as seriously as their contribution to our lives," said Tim Lordan, executive director of the Internet Education Foundation.

The group has launched a Web site to provide information to consumers

on how to protect themselves, and the information will be update throughout the year. Further information can be found at www.GetWirelessSecure.org.

Copyright 2006 by United Press International