Computer Security A Top Concern

(NAPSA)—Dozens of insidious new, complex electronic attacks on desktop computers have provided a wild ride for the nation's 25 million small to medium-sized businesses (SMBs) in 2004.

The Problem

SMBs are plagued by viruses and worms that lure employees into opening infected e-mail messages. Even worse, recent virus attacks implant hacker software on computers owned by Web site visitors.

"Companies such as Hewlett Packard, Microsoft and Intel have retooled their products and software to defend against these problems," said Andrew Levi, chairman of the Information Technology Solution Providers Alliance (ITSPA), a national, nonprofit group that helps SMBs understand how technology and technology providers help them succeed.

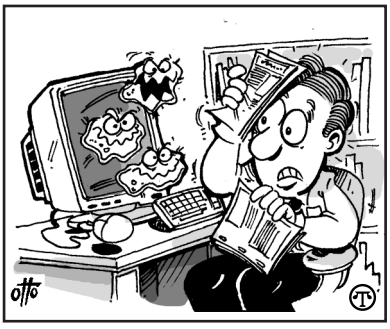
A Solution

"ITSPA recommends SMBs buy new technology such as personal computers that offer embedded security chips and software that keep information safe by encrypting data to prevent unauthorized users from accessing business or personal files," said Levi. ITSPA's Technology Committee suggested SMBs follow industry security recommendations:

- Always install latest updates to operating systems and browsers
- Install anti-virus software and update it weekly
- Turn off file and print sharing features (to prevent hackers from accessing other workstations)
- Restrict network and Internet settings
- Make sure your Internet browser security/privacy option is set on the highest level
- Install firewall software or hardware
- Test the computer system frequently using an on-line service.

Plug wireless security holes, too

With 85 percent of notebooks and 60 percent of handheld devices expected to be wireless-enabled by 2006, SMBs should also adopt formal wireless security policies now, advised ITSPA.



A big problem for small businesses can be averted by adopting a few simple safeguards.

"Although wireless equipment is a boon to SMB productivity and profits, companies should expect to see wireless attacks in the not-too-distant future," said Levi.

"Because SMBs have multiple types of wireless users and devices, it's important they have multiple layers of security and flexible policies," Levi added.

To combat this problem, SMBs are adopting a wireless standard called 802.11i that prevents intruders from accessing wireless networks. 802.11i builds on many existing standards that are addressing wireless LAN security today, including WiFi Protected Access (WPA) and 802.1x.

ITSPA recommends SMBs develop a wireless security policy that includes intrusion detection to minimize attacks from worms, viruses and hackers. Also, SMBs should protect anything that is shared with a strong password, install wireless encryption, and change encryption keys regularly. Coupled with mobile devices that feature hardware based security options for added data encryption and user authentication features, such as pre-boot Smart Card access, companies can increase the safety of sensitive company data at all points of access.