SECURITAS

SECURITY SPOTLIGHT

An Informational Guide for Securitas USA Clients and Employees

October 2010 | Securitas Security Services USA, Inc. | Number 79

Guarding Against Cybercrime

In an increasing networked world, the threat of a cyber attack is a 24/7/365 possibility. Any company or individual connected to the Internet is vulnerable to computer crime.

The most recent annual survey of U.S. corporations and institutions by the Computer Security Institute (CSI) reports

- 64.3 percent of respondents experienced malware infection (up from 50 percent in 2008)
- 29.2 percent experienced denial-of-service attacks (compared to 21 percent in 2008)
- 17.3 percent experienced password sniffing (up from 9 percent in 2008)

Cyber criminals are continually finding new ways to access computer systems, steal information and use it for profit. So, what can you do protect yourself and your workplace?

End-User Awareness

While some hackers target weak spots in operating systems software or search engines, cybercrime often cannot occur without a user's help. In fact, the 2009 CSI Survey revealed that over 16 percent of respondents indicated that nearly *all* of their losses from cybercrime were due to

employees who merely acted carelessly and disclosed sensitive data or downloaded malware.

Employee awareness is key to cybercrime prevention in the workplace. Fundamental advice to workers from the FBI includes:

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase)
- Change your passwords regularly (every 45 to 90 days)
- Keep your usernames, passwords and other computer access codes to yourself
- Do not open emails or attachments from

strangers, and don't click on pop-up ads or web links included in unsolicited offers
- Do not install or connect any personal software or hardware to your company's network or hardware without permission from the IT department
- Log off and shut down your computer at the end of the day
- Report all suspicious or unusual problems with your computer to security, IT or other appropriate authority

Cybersecurity includes Physical Security

The CSI Survey reports malware as the leading cause of data loss in the workplace; laptop and mobile hardware loss or theft is the second. Employees can help prevent data breaches by keeping laptops and other mobile devices secure both at the workplace and out of the office. Keep devices locked up and out of sight when not in use, and don't leave equipment unattended in public places like a car, convention hall, restaurant or airport.

Professional security officers play an important role in cybersecurity, by providing access control at a jobsite. They can help keep unauthorized people away from company computers, and monitor and record when devices are taken off-site. They can also observe and report security breaches like passwords in plain sight or computers left logged on to the network. Patrol officers in public spaces can spot and report unattended laptops and mobile devices and detect the presence of suspicious characters waiting for the chance to scoop them up.

October 2010 marks the seventh annual National Cybersecurity Awareness Month sponsored by the Department of Homeland Security. For the latest materials, tips and best practices for Internet security visit

www.us-cert.gov

www.onguardonline.gov

www.staysafeonline.org

www.fbi.gov/cyberinvest/cyberhome.htm

Phishing: Don't Take the Bait

Whether at work or at home, any time you are connected to the Internet you need to look out for scams, viruses and other cyberthreats, such as phishing, spam or pop-up messages designed to lure information from unsuspecting victims. Follow these additional practices to protect your information, your computer and your money:

- Know who you are dealing with before sharing sensitive information—phishing attacks often look like they come from a trusted source
- Avoid malware by being careful when opening attachments or downloading files, regardless of who sent them (see above)
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly
- Keep your operating system and Web browser up-to-date, and learn their security features
- Be cautious about clicking on—or even mousing over—links to videos and URLs in messages on social networking sites (e.g, Facebook, Twitter); not everyone is your "friend"

SECURITAS