Heartbleed and Shellshock/Bash Bugs Highlight Need for Cyber Security and Vigilance

First there was the Heartbleed bug and then, most recently, the Shellshock exploit, or commonly referred to as the Bash bug. These security vulnerabilities exposed computer systems and data around the world to hackers for possible exploitation.

"These security flaws point to the need for stringent cyber security," said Marilyn Piccolo, vice president, Information Risk and Compliance Office of Assurant, Inc. "Assurant has many security controls in place to protect our systems, but ongoing cyber vigilance and the ability to respond quickly is essential in combating these issues."

©iStock.com/weerapatkiatdumrong

October, National Cyber Security Awareness Month, is a good time to think about proactive steps to safeguard both personal and work devices and data from cybercriminals.

Piccolo said that October, National Cyber Security Awareness Month, is a good time to think about proactive steps to safeguard both personal and work devices and data from cybercriminals. And, as more people use their mobile devices and laptops for both business and personal use, an accidental click on a suspicious email or a misplaced laptop can lead to a significant security breach. This can expose clients or customers' information to unauthorized use.

"Many security breaches are inadvertently caused by users. It is natural that you want to read the email with the subject line 'You're a Winner,' but you won't be if you click it open," said Piccolo. "Opening such phishing emails, logging onto unknown Wi-Fi networks, using weak passwords and plugging in external devices into your laptop without running a security scan all make you vulnerable to online pirates."

Assurant has adopted strict data security measures to protect client and consumer information. The Assurant Corporate Technology (ACT) Information Security and Technology team relies on an Incident Response Plan to bring company resources together quickly to address issues that threaten the safety and security of Assurant computer resources and data. For example, Piccolo said the ACT team immediately began to assess, scan and plug security gaps created by Bash Bug to ensure that the computer systems and client data were protected.

"Securing our customers' information is a high priority for us and we take these matters very seriously," said Piccolo. "While we work to respond to incidents swiftly, containing and remediating the issue, we also focus heavily on preparing our defenses. We are constantly assessing our environments, implementing preventive controls, monitoring technology and applying necessary security countermeasures."

For more information on how you can secure your information, go to http://staysafeonline.org.