# Scareware—a whole new breed of threat

Contributed by: Ryan Pringnitz, Secant Service Technician, MCTS, ACMT

There was a time when reading about a security breach in the Wall Street Journal or other major news outlet was a novelty. But now it's almost a daily occurrence. Security breaches in 2011 affected over 30 million records, the biggest of which included: Sony's cloud services for PlayStation; the breach at email marketing giant Epsilon which affected customers Walt Disney, JPMorgan/Chase, and Best Buy among others; the Anonymous hack at HB Gary Federal.

Even as organizations grapple to secure data from existing security vulnerabilities and malware, a whole new breed of threat has recently emerged called "**Scareware**". Where an annoying pop-up or erratic browser performance might foreshadow a security breach or malware presence, Scareware is dangerously different as it virtually renders a computer inoperable and unable to launch applications.
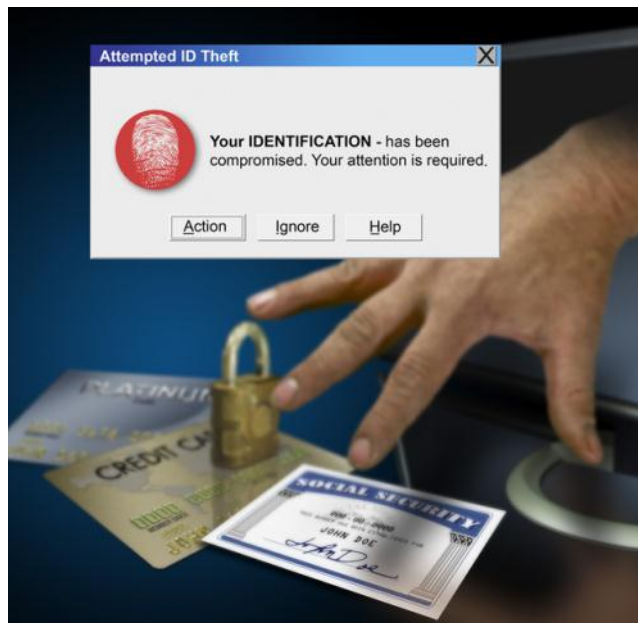
With Scareware, you find yourself confronted with a piece of software that appears to be a legitimate anti-virus scanner identifying a series of problems and often includes a "feature" to purchase the software to remove this infection. The Scareware also attempts to phish personal data which has been frequently linked to payment processing companies in Russia. There are practical steps and precautions to Stop Fake Anti-Virus.

2012 is a whole new year and the way in which attackers and malware are now targeting systems and data illustrates the importance of continuously reviewing your own security methods and identifying new vulnerabilities. Mobile devices continue to proliferate and often include very little or even no built in security. Attackers are taking a broader approach to infiltrate IT systems and look for exploits in a variety of products including software by Adobe, Oracle/Java, Cisco, and Microsoft.

Secant can help you manage security risks as an *ongoing process, not just a singular event* with innovative solutions from industry leaders such as Cisco and Sophos.

Don't have time to manage the nuts and bolts of every computer in your organization? Let us show you how DesktopCare from Secant can provide you with a "virtual" employee who takes care of proactive maintenance on a regular basis. With DesktopCare, we monitor and manage your desktops to keep them in peak performance, and secure from threats from viruses, malware and web browsing threats which can lead to potential security breaches and potential loss of critical data..