Computer Security

New Generation of Computer Security Tools Available for Identity Theft Protection

(NAPSA)—You can protect yourself from modern computer crime.

Less than a decade ago, the most probable security risk computer users faced came from sharing an infected floppy disk. As Internet use increased, a few more threats arose as simple viruses slowly made their way across the Web. Then came worms and Trojan horses, each one a little more destructive and fast-moving than the last.

Computer users must now deal with far more serious threats of identity theft, phishing attacks, online fraud, extortion and other cybercrime. Hackers are no longer in it for a pat on the back from the cyber-underground. Today's cybercriminals are in it for the money.

Worse yet, anyone with confidential information is at risk—and a single bad cybermove by just one rogue or unwitting user is sometimes all it takes to put sensitive data into the wrong hands. For example, a government employee in Oregon recently put more than 1,300 taxpayers at risk of identity theft when he used an office computer to surf porn sites and, in the process, unknowingly downloaded a Trojan horse. The Trojan horse captured and relayed keystrokes—including names, addresses, and Social Security Numbers—for four months before being detected.

What's more, all this happened at an agency that was otherwise fortified with firewall, anti-virus, and intrusion detection software that was updated many times a day. And it's not just porn sites that are home to malicious code. Cybercriminals often set up phony sites that look like legitimate ones in order to lure consumers into divulging data.

That's why a new generation of protection tools is needed. Consumers must know when they're on a legitimate site versus a bogus or spoofed site. Many of today's tools determine the authenticity of a site simply by checking to see if it is on the "good" or the "bad" list of known sites. The problem is, the average phishing site stays up for only six hours, after which opportunistic cybercriminals dismantle and move on in order to evade detection by authorities. Consequently, a variety of mechanisms must be used before a site is declared safe or unsafe, from verifying its security certificates to analyzing its behavior.

Consumers also need to be protected against keystroke loggers and the like at the moment they are most vulnerable to attack—that is, at the scene of the potential crime as a transaction takes place. Doing so requires more than the intrusion detection tools of yesterday that could identify known threats by their fingerprint. With new threats being unleashed at a record pace, consumers need tools that can detect crimeware that is so new that its fingerprint is not yet known—but its conduct gives away its malicious nature.

Moreover, all this protection must not get in the way of the consumer's online experience. After all, users who no longer trust or enjoy their Internet interactions will likely return to doing business the brick-and-mortar way.

Fortunately, a growing number of security providers, such as Symantec, are taking notice and now offer increasingly sophisticated technologies designed to protect online transactions and interactions.

And as more consumers embrace these new tools, the Internet will become a safer environment for everyone.