Internet Security

You Are the Weakest Link, Say Hackers

(NAPSA)—Perhaps it was only a matter of time before hackers began shifting their focus away from noisy attacks on businesses and towards quiet, stealthy advances on unsuspecting home users. After all, end-user systems are often more vulnerable than their owners know, and by simply exploiting an unpatched weakness in such a system a hacker can often gain access to sensitive—and highly lucrative—information, including credit card data, Social Security numbers and more.

So says the latest Internet Security Threat Report released by Symantec Corp. The report takes a comprehensive look at Internet threat activity that has occurred throughout the world over a six-month period, identifies the current and emerging threat trends and provides recommendations for protection.

And so far, 2006 looks like the Year of the User. In fact, home users were by far the most targeted sector during the first half of 2006, accounting for 86 percent of all targeted attacks. The financial services sector was a distant second, with 14 percent of attacks. Clearly, hackers are still in it for the money; it's just that now they reach their objective through a slightly different route.

Attackers see end users as the weakest link in the security chain and, in turn, are launching lower profile, more targeted attacks and using evasive techniques to avoid detection and increase their likelihood of being successful. Among attackers' favorite client-side targets are Web browsers and Web applications, and Symantec expects to see new threats emerge that take advantage of the next generation of one of the world's most commonly used operating systems.

An attacker who launches a successful attack on a Web browser typically becomes able to compromise the end user's system and gain the privileges of whomever is currently logged on. And if that just happens to be the administrator, then the attacker is authorized to do just about anything on that compromised system.

Vulnerabilities in Web applications, such as shopping cart implementations at e-commerce sites as well as Web-based e-mail and Web logs, can turn a seemingly harmless transaction by a user with a browser into an opportunity to unknowingly introduce malicious code into a vulnerable Web server. From there, a hacker might gain access to confidential information.

Why the shift? Unfortunately, home users are less likely to have well-established security measures and practices in place. However, there have never been more—and more effective—tools available to keep home users' online experiences safer. While anti-virus software is a good start, consumers can also benefit from firewalls that control inbound and outbound Internet traffic, as well as intrusion detection software that identifies any malicious code that might be trying to sneak onto their system. New transaction security technologies identify known phishing Web sites in order to help prevent consumers from becoming victims of online identity theft. In some cases, these tools are available in a single integrated suite, which makes security as easy as pointing and clicking.

What's more, security providers, financial institutions and other organizations are beginning to work together to provide consumers a more trustworthy environment for working and playing over the Web.

Good timing. Because with attackers now eyeing home users as their potential ticket to fraud and fortune, having a more secure, connected world is the only way to continue to enjoy the benefits of an online world.

To learn more about how to protect your computer from hackers, visit www.symantec.com.