

Cybercrime and the Consumer  
**Dean Turner**, Sr. Manager  
Development

## **Cybercrime and the Consumer**

Written by Dean Turner - © 2006, Symantec Corporation. Reprinted with Permission.

It should come as no surprise to consumers that cybercrime is on the rise. Cybercrime is defined as any criminal act that incorporates a computer or Internet component. Cybercrime includes, but is not limited to, identity theft, theft or manipulation of data or services, online fraud, and extortion.

But what is behind this trend? Is it that more cybercrime can be committed when more potential victims go online? Or that the tools cybercriminals are using have become more powerful or stealthy?

Or is it simply that hackers are no longer in it for fun and fame—that now they're in it for money?

In a word, yes.

## **More is Better**

Today, digital interactions are everywhere. Home users routinely use the Internet to check their bank accounts, transfer funds, and more. They make purchases over the Web, often leveraging specialized online payment services to complete transactions. They pay bills, manage investments, share photos, stay in touch with family and friends, play games, do research, and even work from their home PCs. Indeed, the convenience and efficiencies of such digital interactions give consumers more time to devote to other important issues.

At the same time, hackers view online computer users as potential targets — and the more targets there are, the better chance they have of successfully hitting their mark.

Statistics bear this out. The United States not only has the highest percentage of broadband users, but also has the highest percentage (26 percent) of all bot-infected computers in the world. That's according to the most recent semiannual Internet Security Threat Report from Symantec Corp., which covered Internet activity over the last six months of 2005. Bots (short for "robots") are computer programs that are covertly installed on a targeted system; they allow an unauthorized user to remotely control that computer for a wide variety of purposes.

China, whose broadband adoption rate is skyrocketing, experienced the second largest increase in bot-infected computers, with 37 percent growth. To put that in perspective, China's growth rate was 24 percentage points above the average increase. Clearly, an increase in always-on Internet connections often coincides with an increase in bot-infected systems.

Moreover, bots accounted for 20 percent of the top 50 malicious code samples reported to Symantec from July 1, 2005 to Dec. 31, 2005.

Once a computer is infected with bot malicious code, a remote attacker can use that system and other similarly infected computers to launch a denial-of-service (DoS) attack against a company. DoS attacks sound innocuous, but they can be a serious financial problem for businesses that rely on Internet services for communication or revenue generation. According to the Internet Security Threat Report, an average of 1,420 DoS attacks were observed worldwide each day—a 51 percent increase over the previous reporting period.

Bots and bot networks—a collection of machines invisibly infected by Trojans and remotely controlled to issue viruses or Internet threats in to the wild—are also often used for cybercrime activities such as fraud, extortion attempts, malicious code propagation, and the unauthorized distribution of adware and spyware onto users' systems.

Worse yet, some security experts speculate that there will be a boom in bots and bot networks as attackers begin to leverage an increasing number of Web-based application vulnerabilities and vulnerabilities in Web browsers.

## **Tools of the Trade**

Crimeware is also making cybercriminals' jobs easier. Crimeware is software that is built with the purpose of committing online scams and stealing information. It includes, but is not limited to, bots, keystroke loggers, spyware, backdoors, and Trojan horses. When used by itself, each tool can be effective; when used together, they can be even more powerful.

Today, it is not uncommon to see a threat utilize more than one type of crimeware. What's more, malicious code is becoming more modular—that is, it initially possesses limited functionality such as disabling antivirus software or a firewall, and can also update itself with code that has new, potentially more damaging capabilities.

Modular malicious code often reveals confidential information. Many modular malicious threats are taking the form of Trojan horses that compromise a system by providing a means for another computer to gain access to it.

But threats to confidential information can be present in virtually any form of malicious code, including worms, and viruses. Many contain keystroke logging and backdoor functionality as well.

According to the Symantec Internet Security Threat Report, modular malicious code accounted for 88 percent of the top 50 malicious code samples—up from 77 percent in the previous reporting period. And malicious code that could reveal confidential information grew in volume from 74 percent of the top 50 malicious code samples to 80 percent.

Why the interest in modular malicious code and threats to confidential information? That's where the money is. Threats of these types are often used in identity theft, credit card fraud, or other cybercrime activities. Moreover, there is likely to be an increase in the theft of confidential, financial, and personal information for financial gain, according to security experts.

Of course, hacking is not always about the tools. Sometimes it's about the target. Take phishing, for example. Phishing is a technique that uses social engineering to steal confidential information. In other words, hackers try to dupe users into actually revealing credit card numbers, passwords, and other information, and they use that data in identity theft, online fraud, or other cybercrimes.

Phishing attempts made up one in every 119 e-mail messages, or an average of 7.92 million phishing attempts per day. That marks an increase over the first six months of 2005, when one of every 125 messages processed was a phishing attempt, for an average of 5.70 million attempts per day.

## **Self-Protection**

Guarding against today's broad range of Internet threats requires the use of overlapping, cooperative defensive systems. Home users, especially those with always-on cable or DSL Internet connections, need to use an Internet security solution that includes antivirus, intrusion detection, antispyware, and firewall technologies for maximum protection. Consumers can also mitigate their risk by keeping their systems up-to-date—not only with operating system and application patches but also with the most current virus and spyware definitions as well as intrusion detection and firewall updates.

Consumers can further protect themselves against online scams by never responding to requests for confidential or financial information online without first confirming the source and validity of the request. Consumers should also never view, open, or execute any e-mail attachment unless the attachment is expected and the purpose of the attachment is known.

Consumers should also learn to recognize computer hoaxes. Hoaxes typically include a bogus e-mail warning the user to "send this to everyone you know" and they often incorporate improper technical jargon intended to frighten or mislead. Upon receiving such a message, the best course of action is to delete the email.

Best practices for password protection call for consumers to use a mix of letters and numbers when choosing a password. Consumers should not use dictionary words, and they should change their passwords often.

Cybercrime will likely continue to put online consumers at risk as they use the Internet for business and pleasure. However, by employing a formidable combination of protection technologies and following common sense best practices for safe computing, consumers can continue to enjoy the efficiencies of the today's digital world in a safer, more trustworthy environment.

For more information: [www.symantec.com](http://www.symantec.com)