Software Counterfeiters Prey On Consumers

(NAPSA)—Every day, consumers are losing money to software pirates who sell counterfeit software at temptingly low prices such as 90 percent off. Counterfeiters frequently peddle their bogus wares through spammed e-mail, promising name-brand, top-quality software at a fraction of retail prices. Consumers are then encouraged to make their purchases via credit card before inventory of the bargain programs is depleted and prices go back up.

The problem is, the software is not legitimate and is not supported by a legitimate vendor; many times, the software doesn't even work. Furthermore, the counterfeiter's online ordering site is far from secure to handle credit card numbers. For his or her investment, the consumer gets junk programs or no software at all. The counterfeiter, in turn, gets $39.95 or so and another credit card number to harvest.

Victims of security software scams face additional risks. Security software such as antivirus, firewall, and intrusion detection programs require regular (often weekly) updates of current signatures or rules in order to detect emerging threats; such updates are possible only by connecting with and downloading code made available through the program's legitimate vendor. If consumers are using counterfeit software whose code is faulty, as is often the case, they risk not having access to those updates.

Consumers who purchase bogus security programs are also at risk of receiving software that not only doesn't protect them, but that has been booby-trapped with malicious code such as a virus or spyware. Consequently, the very program that was supposed to prevent the destruction of their computer actually helps cause it.

Software manufacturers are responding to counterfeiting by taking steps to protect their software as well as to track down and prosecute violators. Various companies now embed their software with digital rights management (DRM) technology to prevent the duplication of copyrighted material. Security software giant Symantec Corp. recently established its Brand Protection Task Force to stamp out piracy and is testing the use of a product activation program to establish that a consumer is using a legitimate product.

However, until a "silver bullet" is developed that actually prevents piracy, educated consumers remain the most formidable line of defense against counterfeiters. Consumers can reduce their risk of falling victim to software pirates by following a few simple steps: 1) purchase software only through the vendor's legitimate partners, which are often listed on the vendor's Web site; 2) do not participate in offers that seem "too good to be true," even if an ad describes the product as "genuine"; 3) do not respond to suspicious spammed e-mails or click on the link asking to be taken off the sender's list (both actions confirm the recipient's address and result in even more spam); and 4) purchase only from secure sites, which are identifiable by the locked padlock icon that appears on the bottom bar of the user's Web browser.

Consumers can also help curb software piracy by reporting suspicious activity to law enforcement agencies as well as to software companies such as Symantec's spamwatch Web site, www.symantec.com/spamwatch.