Consumer Alert

Eight Tips To Help Avoid Computer Infections

(NAPSA)—Consumers and companies are being victimized by spam e-mails offering counterfeit software and pharmaceuticals. For the average consumer, his identity could be in jeopardy or he could unknowingly be funding criminal activity initiated by groups based in Eastern European countries.

The software industry's biggest problem in Internet piracy over the past four years has been caused by Internet storefronts that sell pirated software for pennies on the dollar. The criminal activities of these counterfeit spammers extend beyond software piracy. They include threats to public safety such as counterfeit pharmaceuticals, child pornography and identity theft.

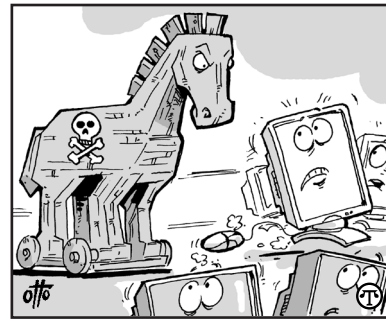
Criminal Operation

The perpetrators reach consumers via mass spam e-mail, as well as ads on popular search engines. They lure customers to Internet storefronts that appear legitimate, and then deliver unauthorized copies of products to them via both postal mail and electronic download.

According to industry estimates, the criminals make more than $10 million annually for software that sells legitimately for more than $100 million. Illegal revenue is generated in two ways: directly from the illegal activity, whether it involves software, pharmaceuticals or child pornography; and identity theft via the unauthorized reuse of harvested credit card information and the resale of credit card and customer data to third parties.

Beware of Trojan Horse and Other Attacks

Purchasers from these Internet storefronts have also reported that viruses and "trojans" have appeared on their computers. Trojan horse attacks pose one of the most serious threats to computer security. The result is that buyers of pirated software also often unknowingly propagate spam, since their computers are secretly "hijacked" and turned into spamming robots.



Trojan horse attacks pose one of the most serious threats to computer security.

Here are some practical tips to avoid getting infected:

1. Never download blindly from people or sites of which you are not 100 percent sure.

2. Even if the file comes from a friend, you still must be sure what the file is before opening it.

3. Beware of hidden file extensions.

4. Never use features in your programs that automatically open or preview files.

5. Never blindly type commands that others tell you to type, go to Web addresses mentioned by strangers, or run prefabricated programs.

6.Don't be lulled into a false sense of security just because you run anti-virus programs.

7. Don't download an executable program just to "check it out."

8. Finally, if the price is too good to be true, it's probably counterfeit.

For free resources or more information on software piracy, visit www.autodesk.com/piracy or call (800) NO COPIES.