

# Protecting Your Business

## Reduce Your Company's Risk of Unlicensed Software Use

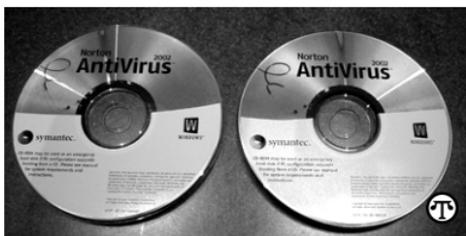
(NAPSA)—When many people think of piracy, downloading music and movies from the Internet is often the first thing that comes to mind. Yet software piracy—unlicensed software use—is also a very serious problem for a wide variety of businesses, maybe even for the company for which you work. In 2006, all businesses—especially small businesses—that want to avoid a potential costly mistake should make routine internal software audits part of their standard operating procedures.

Using company networks to install or download unlicensed software is illegal. First, unlicensed software often functions improperly, or typically has viruses. And the manufacturer support necessary to fix these problems is not available without genuine licensed software. Third, unlicensed software use can reduce a company's efficiency and expose it to legal and financial risk.

Fortunately, the Business Software Alliance (BSA) says well-implemented software asset management can add significant cost savings, improve software purchasing arrangements, enable more strategic infrastructure planning and reduce IT costs. It also lets the IT department control exactly what software an employee has access to and significantly reduces the opportunity for users to introduce unlicensed software to corporate networks.

BSA encourages companies to establish software policies clarifying purchasing procedures, including lists of approved suppliers and rules preventing staff from buying or downloading software without approval.

In addition, organizations should audit their software assets,



**Real or fake? It is difficult to spot any differences between the genuine software on the left and the counterfeit software on the right.**

developing an inventory of programs and comparing them to the company's licenses, so any illegal copies can be identified and new licenses acquired, if necessary.

Signs of pirated software include:

1. Software prices that seem "too good to be true";
2. Software without original materials;
3. Software without the manufacturer's security features;
4. Software that lacks the original license or materials such as the original registration card or manual that typically accompany legitimate products;
5. Software on an unlabeled disk, a disk with a handwritten label, or a disk that is gold instead of silver;
6. Software offered on auction sites;
7. Suites of software packages from different vendors on the same CD; and
8. Software distributed by mail-order or online by sellers who fail to provide appropriate guarantees of legitimate product.

To learn more software asset management strategies and to access free tools, visit [www.bsaaudit.com](http://www.bsaaudit.com). To report someone who may be illegally distributing pirated software, contact BSA at [www.nopiracy.com](http://www.nopiracy.com) or call 1-888-NO-PIRACY.