NEWSWORTHY TRENDS

Guarding Against Hidden Hackers

(NAPSA)—A few simple tips could help protect Web surfers from a low-tech tactic used by high-tech thieves: disguise. Hackers have found ways to impersonate banks online, to pretend to be your social networking acquaintances and even to disguise themselves as long-lost friends.

It's all in an effort to spread computer viruses and other malicious software that allow criminals to hijack personal information, trick users into purchasing fake anti-virus programs and more.

Fortunately, some basic safe-surfing practices and the right security software can help keep you safe. Computer security experts at Kaspersky Lab offer these tips:

•**Looks Can Be Deceiving.** Always visit banking and financial sites directly, not through links you receive via e-mail. Such links often take you to Web sites that look exactly like your bank's but are actually clever forgeries that steal whatever passwords or account numbers you enter.

• **Friend Or Fraud?** Criminals often use malicious software to target people on social networking sites. If you receive a link from a friend, confirm that he or she actually sent it to you. If not, don't open it. The now infamous Koobface virus spread to millions of social networkers who clicked on video links supposedly sent by people they knew. The virus then infected their computers and began transmitting any credit card numbers or other valuable information it could find back to its creator. It also sent copies of itself to all the contacts in the victim's profile, again disguised as a friendly video message from its latest victim.

• **Frequently Asked And Fake.** Web searches for common phrases such as "free screen savers"
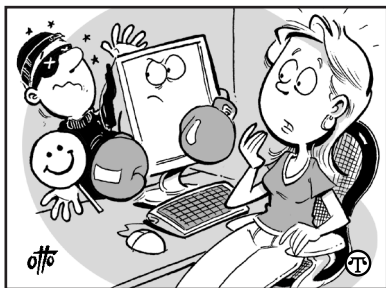
The right security software can help protect you from hackers disguised as friends.

or "song lyrics" will often lead to sites that infect visitors with malware, even if they only view the Web page. Protect yourself by making sure your anti-virus scanner is always on and up to date.

• **Think Before You Share.** A quick search of a social networking site can reveal where people work, the town they live in, where they went to high school, their interests, hobbies and more. Scams can then be custom-made to fit that information. If you use social networking sites, use privacy settings to limit the information that can be viewed by people who aren't in your circle of friends. Be wary of strangers who claim to know you through an old connection, and remember, if they try to involve you in a financial transaction, odds are it's a con.

• **Beware Of Scareware.** If you receive a message warning that your computer is infected with viruses and that only a certain anti-virus program can remove them, beware. The programs—which are offered as free trial versions or as pay services—are often malware in disguise. Be suspicious of all "free" anti-virus programs, and only rely on programs purchased from reputable sources.

For more information, visit www.kaspersky.com.