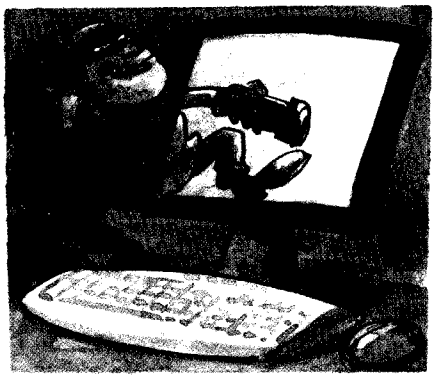
26 Internet security

A Internet crime



Crackers are a new type of criminal

The Internet provides a wide variety of opportunities for communication and development, but unfortunately it also has its dark side.

Crackers, or black-hat hackers, are computer criminals who use technology to perform a variety of crimes: virus propagation, fraud, intellectual property theft, etc.

Internet-based crimes include **scam**, email fraud to obtain money or valuables, and **phishing**, bank fraud, to get banking information such as passwords of Internet bank accounts or credit card details. Both crimes use emails or websites that look like those of real organizations.

Due to its anonymity, the Internet also provides the right environment for **cyberstalking**, online harassment or abuse, mainly in chat rooms or newsgroups.

Piracy, the illegal copying and distribution of copyrighted software, information, music and video files, is widespread.

But by far the most common type of crime involves malware.

B Malware: viruses, worms, trojans and spyware

An email virus spreads through an email address book

Malware (**mal**icious **software**) is software created to damage or alter the computer data or its operations. These are the main types.

- **Viruses** are programs that spread by attaching themselves to executable files or documents. When the infected program is run, the virus propagates to other files or programs on the computer. Some viruses are designed to work at a particular time or on a specific date, e.g. on Friday 13th. An email virus spreads by sending a copy of itself to everyone in an email address book.
- **Worms** are self-copying programs that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks. Worms are self-contained and don't need to be attached to a document or program the way viruses do.
- **Trojan horses** are malicious programs disguised as innocent-looking files or embedded within legitimate software. Once they are activated, they may affect the computer in a variety of ways: some are just annoying, others are more ominous, creating a backdoor to the computer which can be used to collect stored data. They don't copy themselves or reproduce by infecting other files.
- **Spyware**, software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software. It usually comes hidden in fake freeware or shareware applications downloadable from the Internet.

C Preventative tips

- Don't open email attachments from unknown people; always take note of the file extension.
- Run and update **antivirus programs**, e.g. virus **scanners**.
- Install a **firewall**, a program designed to prevent spyware from gaining access to the internal network.
- Make backup copies of your files regularly.
- Don't accept files from high-risk sources.
- Use a **digital certificate**, an electronic way of proving your identity, when you are doing business on the Internet. Avoid giving credit card numbers.
- Don't believe everything you read on the Net. Have a suspicious attitude toward its contents.