Security and privacy on the Internet

There are a lot of benefits from an open system like the Internet, but we are also exposed to hackers who break into computer systems just for fun, as well as to steal information or propagate viruses. So how do you go about making online transactions secure?

Security on the Web

The question of security is crucial when sending confidential information such as credit card numbers. For example, consider the process of buying a book on the Web. You have to type your credit card number into an order form which passes from computer to computer on its way to the online bookstore. If one of the intermediary computers is infiltrated by hackers, your data can be copied. It is difficult to say how often this happens, but it's technically possible.

To avoid risks, you should set all security alerts to high on your Web browser. Netscape Communicator and Internet Explorer display a lock when the Web page is secure and allow you to disable or delete 'cookies'.

If you use online bank services, make sure your bank uses digital certificates. A popular security standard is SET (secure electronic transactions).

E-mail privacy

Similarly, as your e-mail message travels across the net, it is copied temporarily on many computers in between. This means it can be read by unscrupulous people who illegally enter computer systems.

The only way to protect a message is to put it in a sort of 'envelope', that is, to encode it with some form of encryption. A system designed to send e-mail privately is *Pretty Good Privacy*, a freeware program written by Phil Zimmerman.

Network security

Private networks connected to the Internet can be attacked by intruders who attempt to take valuable information such as Social Security numbers, bank accounts or research and business reports.

To protect crucial data, companies hire security consultants who analyse the risks and provide security solutions. The most common methods of protection are passwords for access control, encryption and decryption systems, and firewalls.

Virus protection

Viruses can enter a PC through files from disks, the Internet or bulletin board systems. If you want to protect your system, don't open e-mail attachments from strangers and take care when downloading files from the Web. (Plain text e-mail alone can't pass a virus.)

Remember also to update your anti-virus software as often as possible, since new viruses are being created all the time.

HELP box

- **hacker:** a person who obtains unauthorized access to computer data
- **cookies:** small files used by Web servers to know if you have visited their site before
- **certificates:** files that identify users and Web servers on the net, like digital identification cards
- **encryption:** the process of encoding data so that unauthorized users can't read it
- **decryption:** the process of decoding encrypted data transmitted to you