Online access — beware of spyware!

The internet provides access to resources and services that used to be time-consuming and sometimes difficult to find, and none of us would want to return to the old ways of searching for information. However, the internet can also be used for unethical purposes.

Individuals and businesses are facing an increasing number of security threats to their computers and internet connections. One such threat is spyware, which is emerging as a serious concern for online security and privacy.

The Australian Government is currently investigating the problems caused by spyware. The Department of Communications, Information Technology and the Arts (DCITA) has published a *Spyware discussion paper* and is holding workshops to discuss the issues raised in the paper.

What is spyware?

Spyware is software that can be secretly installed on your computer to take information from it without your permission or knowledge. Spyware can take personal information, business information, bandwidth or processing capacity from your computer and give it to someone else to use for their own benefit.

When spyware is running, it is possible for all the data and activity on that computer to be captured or viewed by a third party. It can collect details of all the data stored on the computer including websites visited, e-mail addresses and online banking details. Spyware can even record the keystrokes a user is making. The information collected can be used for fraud or identity theft, or sold to other parties such as spammers.

During 2004 there was a substantial worldwide increase in the amount of spyware circulating on the internet. A recent study by Webroot Software, a US software company, and Earthlink, a US internet service provider, found an average of twenty-five instances of potential spyware on computers surveyed. Software company Microsoft reports that 50 per cent of computer crashes reported by its customers can be traced to spyware.

Spyware runs in the background during normal computer use and is often not obvious to the user. There are, however, some signs that may indicate the presence of spyware. Spyware may be to blame if you start receiving random error messages, are redirected to unwanted websites, receive unusual charges on your phone bill, or experience slow internet and computer performance.

There are a number of ways spyware may be installed on your computer without your knowledge or permission, including when you download software or other programs from the internet, or when you open attachments in e-mails. There have been instances where spyware was installed via computer viruses or other security breaches.

How to prevent invasion from spyware

If your computer does not have up-to-date internet security tools such as anti-spyware programs, firewalls and anti-virus software, it is more likely to be vulnerable to spyware.

You can deal with spyware through technical measures similar to those you use to respond to other e-security threats such as spam, phishing and worms.

There are a number of freely available and commercial tools that detect, remove and prevent spyware. You can find them on the internet or obtain them from retail outlets. Once installed, anti-spyware programs should be maintained and updated regularly. The *Internet security essentials* brochure, published by DCITA, contains a checklist of practical actions you can take to improve computer security. You can find it online at http://www.dcita.gov.au/ie/e-security/.

Public access computers

Computers accessed by a number of people, whether in an internet café, library or shopping centre, can be more difficult to monitor.

It is recommended that computers accessed by more than one person be equipped with up-to-date security software. This will minimise the risk of spyware.

Spyware that is installed on a multiple-access computer can raise questions and issues about liability. For example, someone installs a keylogger on a public computer. An unsuspecting person uses that computer to transact some online banking, not realising that their login details are being collected. In this situation, who is liable if these details are used to steal money from a bank account? Is it the bank, the person who installed the keylogger, the person who used the computer unaware their details were being collected, or the organisation providing access to the computer?

Public consultations

DCITA has written the *Spyware discussion paper* in consultation with key stakeholders. The Australian Government is seeking feedback from the public to help develop a pragmatic response to spyware and minimise its impact. The paper is available from http://www.dcita.gov.au/spyware/, and members of the public are invited to submit comments by 17 June 2005.

Workshops are being held in every Australian capital city in May and June 2005. If you are interested in participating in a workshop, visit http://www.dcita.gov.au/spyware/ or e-mail spyware@dcita.gov.au for details.

Australian Government Department of Communications, Information Technology and the Arts

Terms explained...

Keylogger **(or keystroke logger) — a computer application or hardware device that captures every keystroke on a computer. It has the ability to record anything you type, including passwords, e-mails and credit card numbers. Most keyloggers are invisible. They save the recorded keystrokes into a log file which is sent via the internet to someone else.**

Phishing **— a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses, most commonly banks. These authentic-looking messages are designed to lure recipients into divulging personal data such as account numbers and passwords and credit card numbers.**

Spam **— a generic term used to describe electronic 'junk mail', unwanted messages sent to your e-mail account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details. In Australia, spam is defined as 'unsolicited commerial electronic messaging'.**

Spammer **— a person or organisation responsible for sending spam.**

Virus **— a program or piece of code that is loaded onto your computer without your knowledge or permission. Once loaded on a computer, a virus is capable of reproducing itself by travelling from file to file and from computer to computer, often destroying files in the process.**

Worm **— a program that replicates itself and spreads from computer to computer across the internet. Like viruses, worms are a form of malicious code which may perform some harmful function in the process on infected computers. Worms often spread by exploiting software vulnerabilities in operating systems and applications software.** ■