



SCAMS, FRAUD & ID THEFT

What is it?

The information and communications technologies (ICT) widely used in Australian households are also misused by those with a criminal agenda.

The Australian Bureau of Statistics (ABS, 2008) recently found that in 2007 nearly half a million Australians were victims of bank fraud, credit card fraud or identity theft at a financial loss of almost \$1 billion.

What are the risks?

Spam: electronic 'junk mail' – unsolicited commercial messages sent to a person's email account or mobile phone. Spam messages may contain offensive material, promotions for fraudulent services, solicitations of personal information and bank details, and malicious software.

Viruses: a program or piece of code that is loaded onto your computer without your knowledge and may damage or disrupt your system. Your computer can be infected by a virus through email messages, using the Internet, and downloading software.

Phishing: A phishing email directs recipients to a website that looks like the real website of a retailer or financial institution. The website is designed to encourage the visitor to reveal financial details and 'phish' for information, such as credit card numbers, account names and passwords or other personal information.

Mule Recruitment: Mule recruiters seek Australians to launder money on behalf of criminal organisations. The recruitment is made to look legitimate under the guise of a job advertisement. These are often manipulated to appear as if they were sent by legitimate companies or well-known Australian recruitment websites. Mules can be liable for prosecution themselves.

Social engineering: Con artists will conduct activities to manipulate people into performing certain actions or providing personal information known as "social engineering."

How to stay safe?

- Don't open or respond to emails or messages from people you do not know.
- Turn on any junk mail filters provided by your account provider.
- Delete junk emails immediately.
- Do not share sensitive personal information in an email or instant message.
- Use strong passwords and keep them secret.
- Use an Internet firewall.
- Install and maintain antivirus and antispyware software.
- Do not access sites that contain personal or sensitive information (such as internet banking) from public computers.
- Remember: "If it sounds too good to be true, it usually is!"

Report spam to ACMA, www.spam.acma.gov.au. Visit Scam Watch, www.scamwatch.gov.au, for advice on reporting scams. For fraud and identity theft visit www.protectyourfinancialid.org.au or contact your local police.

For more information visit www.thinkuknow.org.au



Australian Government
Australian Communications
and Media Authority

Microsoft®

