



**THE HON NICOLA ROXON MP
ATTORNEY GENERAL**

**THE HON JASON CLARE MP
MINISTER FOR HOME AFFAIRS
MINISTER FOR JUSTICE**

**SENATOR THE HON MARK ARBIB
MINISTER FOR SMALL BUSINESS**

MEDIA RELEASE

Tuesday, 7 February 2012

CYBER CRIME REMINDER FOR SMALL BUSINESS

Attorney General Nicola Roxon and Minister for Home Affairs and Minister for Justice Jason Clare are today reminding small businesses and their customers to be vigilant in protecting themselves against cyber crime.

Ms Roxon and Mr Clare today used 'Safer Internet Day' to release a report from the Australian Institute of Criminology into cyber threats faced by small business in Australia. The report identifies the most common cyber threats facing small business and outlines ways to combat them.

"Most small businesses can't function without the internet," Ms Roxon said.

"So it's important small businesses can identify threats and can put in place measures to protect themselves and their customers."

Mr Clare said small business account for around 95 per cent of all Australian businesses, contributing around 34 per cent of private industry value to the economy.

"Cyber attacks can stop a small business being productive and this can have wider economic implications for the country," Mr Clare said.

"This report will help arm small business owners with the information about what attacks they are vulnerable to and how they can secure their business against cyber crime."

Minister for Small Business Senator Mark Arbib said small business is at the heart of our economy and cyber-crime can have a devastating impact on a small business.

"We understand that many small businesses are already stretched and are time-poor, but they can save themselves a large headache by taking a few basic steps to protect themselves from cyber criminals," Senator Arbib said.

"Small businesses may even be able to take advantage of a simple security strategy on cyber-crime by using it to build trust with their existing and future customers."

To help protect against cyber attacks, small businesses can take the following actions:

- Install security patches to fix vulnerabilities in computer programs;
- Install firewalls to provide a barrier between computers and the internet to protect them from unauthorised access;
- Businesses trading on-line can offer a secure site for customers to enter personal information to authenticate data with a digital certificate;
- Introduce staff internet usage policies and security awareness training; and
- Improve physical security of computers and servers like keeping servers in secure rooms.

“With cyber threats constantly evolving, Australian small businesses need to remain vigilant to protect themselves,” Mr Clare said.

“Investing in cyber security measures now can save small business a lot of money and inconvenience in the future.”

Cyber threats:

The report identifies possible cyber security threats to Australian small businesses.

They include:

Malware:

Malware, or malicious software, includes viruses, worms, spyware and botware which can be used to send spam and conduct denial of service attacks.

This is the most common computer security issue for small business with 65 per cent experiencing one or more incident involving a virus and 44 per cent reporting spyware infections.

Wireless internet vulnerabilities:

Small businesses, particularly in the hospitality industry, are offering free wireless internet connection to customers.

Users could be at risk of having their sessions hijacked or their accounts and passwords hacked and stolen. Free wireless could also be use to download illegal content.

Online fraud:

Small business may be vulnerable to a number of online scams.

This includes the use of compromised or fraudulent credit card details to purchase goods. Overpayment scams involve the use a fraudulent or stolen credit card to overpay for goods – the seller is then out of pocket if it returns the overpaid amount before payment is cleared.

Compromised websites:

A hacked website can be used to host prohibited material or to deliver malware. This leads to a loss of reputation and potential illegal activity being conducted on a business' website.

The report is available from the AIC website: <http://aic.gov.au/>

Media enquiries:

Attorney-General's office: Chris Owens – 0409 945 476

Minister Clare's office: Korena Flanagan – 0418 251 316

Minister Arbib's office: Josh McIntosh – 0409 198 374