CRIME PREVENTION ASSIST

No. 85 May 2013

A multifaceted strategy for businesses to prevent computer security incidents

Businesses face a number of potential computer security risks (Hutchings 2012; Richards 2009). The outcomes of a security incident, such as websites or data not being accessible and loss of reputation, can have a significant impact on a business's ability to operate. A multifaceted strategy including the implementation and regular review of technical prevention measures, organisational policies, staff training and physical security can assist in preventing computer security incidents.

Technical prevention measures include:

- Ensuring application and operating system patches are up-to-date and automated. These fix vulnerabilities in computer programs that may be used to gain unauthorised access.
- Enabling firewalls, which provide a barrier between the computer and the internet.
- Using effective and reputable anti-malware software that is renewed and updated as required.
- Employing fraud control measures for businesses trading online to ensure that orders are genuine. Stay Smart Online (2010) provides advice about what to look out for in suspect orders, how to check if an order is likely to be fraudulent and steps that a business can take to guard against fraud.
- Offering a secure site for customers to enter personal information, including account names and passwords and payment details.

Organisational policies and staff training include:

- Having IT-acceptable use policies that set out how a business's computer resources should be used, expectations in relation to personal use of resources, the handling of sensitive information and the installation of applications or the forwarding of emails.
- Employing a user access management policy that sets out the access rights for staff on a business's computer system, the restriction of administrative privileges and the discontinuation of access when a staff member leaves an organisation.
- Using account/password management policies that set out how often passwords used to access accounts should be changed, as well as the complexity and length of passwords.
- Developing employee education and awareness programs including courses and seminars to inform staff about computer security issues.

The physical security of computer systems can be enhanced by ensuring that servers are kept in secure rooms and that staff computers are not easily accessible by others. Guidelines for the use of portable business equipment may also be integrated into staff policies.

Further information and resources are available from the Australian Government's Stay Smart Online (2010) website.

Contact Us

Providing crime prevention policy makers and practitioners with evidence-based resources and training to prevent and reduce crime.

www.cpassist.aic.gov.au

Australian Government
Australian Institute of Criminology

NEED TO KNOW MORE?

All URLs correct at May 2013

1 Hutchings A 2012. Computer security threats faced by small businesses in Australia. *Trends & Issues in Crime and Criminal Justice* no. 433. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx

2 Richards K 2009. The Australian assessment of computer user security: A national survey. *Research and public policy series* no. 102. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp102.aspx

3 Stay Smart Online 2010. *Business*. http://www.staysmartonline.gov.au/small_and_medium_business

ISSN 1448-1383