

Unisys Security Index

Additional Research: Cybercrime and preventing identity theft Australia – October 2010

As part of the Unisys Security Index, we regularly survey Australians on a range of additional security issues. For the October 2010 wave we gauged Australian attitudes towards a range of measures to prevent cybercrime and identity theft. The results indicate that Australians have taken charge of protecting their identity on social networking sites, but are leaving themselves exposed by not securing their mobile devices.

The research found six out of 10 (58 percent) Australians never secure their mobiles, PDAs or smartphones by using, and regularly changing, a password or PIN. Only 18 percent said they always secured their mobile device.

This means that the majority of Australians are leaving themselves vulnerable to cyber crime and identity theft by not locking their mobile devices with a password or PIN. The risk isn't just to phone owners, but also to the companies they work for as any gadget that has access to the internet presents a risk to an organisation if it isn't secured properly. This has national security implications when you consider the interconnectedness of the infrastructure that drives our aviation, electricity and water supply, banking and finance, and telecommunications networks.

The good news is that it appears that young Australians are protecting their identities online by limiting the information they post on social networking sites with 70 percent of 18-34 year olds saying they do it always, compared with only 44 percent of those aged 50+. Interestingly, when [similar research was conducted in 2007](#), 18-34 year olds were twice as likely as those aged 50-64 to be comfortable providing personal details such as email addresses, full name and age on a social networking site. Comparing this finding with 2010 survey results suggests that younger people may now be getting the message about the importance of protecting their personal information online.

Proportion of Australians who say they always or never take the following precautions against cyber crime and identity theft:

	Always	Never
Use, and change regularly, passwords on their main mobile device	18%	58%
Use and regularly change hard to guess passwords when using the Internet	37%	29%
Read and comply with policies and privacy statements of companies you do business with	43%	20%
Securely shred and dispose of personal paperwork, such as bills, tax documents and medical papers	57%	21%
Limit personal information posted to social networking websites, and set privacy settings to restrict who can access your information	60%	22%
Update security and virus protection software on their computer	64%	14%

Background

These results represent findings of one of two additional questions asked alongside the October 2010 Unisys Security Index. The Unisys Security Index is a bi-annual global study that provides insights into the attitudes of consumers on a wide range of security related issues. Conducted in Australia by market research firm Newspoll, the Unisys Security Index provides a regular, statistically robust measure gauging levels of concern about various aspects of security. The survey on which the latest Australian Unisys Security Index is based, was conducted nationally between 17-19 September 2010 by Newspoll using a nationally representative sample of 1,202 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data. The study measures consumer perceptions on a scale of zero to 300, with 300 representing the highest level of perceived concern. For more information on the Unisys Security Index including additional resource material visit: www.unisyssecurityindex.com.au.

Respondents were asked:

Please say whether you take each of the following precautions against cybercrime and identity theft – always, sometimes or never?

1. Update security and virus protection software on your computer.
2. When using the Internet, use hard to guess passwords which are changed regularly.
3. Use, and change regularly, passwords on your main mobile device.
4. Securely shred and dispose of personal paperwork such as bills, tax documents, medical papers.
5. Read and comply with policies and privacy statements of companies you do business with.
6. Limit personal information posted to social networking sites, and set privacy settings to restrict who can access your information.

Contact Information

Media requests

Julian Brophy, Perception Partners
ph: 02 9699 2722 or 0408 276 749
email: julian@perceptionpartners.com.au

Claire Hosegood, Unisys
ph: 0411 253 663
email: claire.hosegood@au.unisys.com

Briefing requests

Jane Evans, Unisys
ph: 0400 362 275
email: jane.evans@au.unisys.com

For more information on the Unisys Security Index visit: www.unisyssecurityindex.com.au
For more information on Unisys Security offerings visit: www.unisys.com.au

©2010 Unisys Corporation. All rights reserved.

Unisys and the Unisys logo are registered trademarks of Unisys Corporation. All other brands and products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders. Printed in Australia 04/10