CIS
Centre for Internet Safety

September 2011 - ISBN 978 1 922017 00 0

Password Security

A SURVEY OF AUSTRALIAN ATTITUDES TOWARD PASSWORD USE AND MANAGEMENT

Key Findings

The key findings of this survey are:

- Over three quarters (77%) of Australians have more than three online passwords
- Nearly all (90%) of Australians are confident others wouldn't be able to guess their online passwords
- Nearly two thirds (60%) of Australians use the same password across more than one of their online accounts
- Almost half (48%) of Australians only change their password when required to by a system
- Nearly half (42%) of Australians have shared their password with a friend, family member or work colleague
- Over a third (36%) remain logged into their online accounts

PayPal tm

Introduction

From logging on to a corporate network or conducting online banking, to accessing social media or unlocking a mobile phone, passwords are the default and almost ubiquitous first (and often only) line of security for online accounts. Depending upon how they are used and maintained, they can be a powerful first line of defence in protecting personal information and privacy or at worst a time-wasting interruption, lulling users into a false sense of security.

Regardless, passwords impact every online user and given their dominant role as the means of unlocking online accounts, will remain an important part of our online lives for the foreseeable future.

Confidentiality is one of the three aspects (along with Integrity and Availability) of trustworthy computing and a critical element of computer security. To work, it requires authentication mechanisms, such as passwords, to safeguard access to information. Traditionally, to ensure confidentiality of a system, two procedures are used: identification (User ID), to identify the user; and authentication, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a password.

The following document outlines a survey commissioned by The Centre for Internet Safety (CIS) and PayPal, examining consumer behaviours and perceptions relating to their use of online passwords.

About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech Crime Centre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia’s capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

About PayPal

PayPal allows people to send and receive money without sharing financial information. PayPal’s secure online payment platform gives consumers the freedom to transact securely and with greater confidence from any connected device they choose, utilising their preferred funding source, be it a savings, cheque, credit account or a stored PayPal balance. Online safety and security sits at the heart of PayPal’s proposition, and with more than 4 million active accounts in Australia, operating in 190 markets and 24 currencies around the world, PayPal enables global e-commerce.

What is a password?

Passwords are secret words or phrases and ideally should contain a string of letters, characters and numbers (this makes it harder to guess). They may be machine generated or allocated by the provider of the service, but in most cases are user-generated.

The types of passwords we select are dictated to some extent by the policies of the organisations with which we interact online. Some may require passwords of a minimum length; some may require a password of an exact length; some may force us to use numbers and characters; while others may have no overt structural requirements at all.

At the end of this document is a simple guide to generating and maintaining safer passwords, but at a minimum they should:

- not be a proper noun
- not be a common word (out of the dictionary), and
- not be identifiable in relation to the user ID.

How criminals abuse passwords

Online criminals capture passwords in several ways, each necessitating different security behaviours on the part of both the consumer and the provider of the online service.

Trickery

Online criminals may manufacture an email address and/or a website mimicking a real company, and convince users to enter or provide their passwords (phishing), or convince the password owner to disclose passwords by providing a plausible story or reason (social engineering).

Consumer defence: Type in the URL of the legitimate website and implement security software to identify false websites. Consider the legitimacy of emails and other approaches, and decide on a case-by-case basis their merit.

Service provider defence: Actively monitor for fake websites and spam emails using your brand. Work with CERTs and security companies to take down and block offending sites where possible. Build internal capacity to monitor user accounts for anomalous behaviour.

Theft

Online criminals may deploy malicious computer software onto victim computers, or the websites they use, in order to steal passwords (and other information).

Consumer/service provider defence: Implement security software, educate system users, regularly patch operating system and applications.

Gaming

Online criminals may present themselves to the company providing the online service and pretend to have forgotten “their” password. They then provide the necessary personal details (like answers to the “secret question”) to have a new password issued to them.

Consumer defence: Choose a secret question it is likely only you know the answer to (do not have the answer contained on any social networking site, for example).

Service provider defence: Tighten automated forgotten password processes and educate frontline customer support staff. Build internal capacity to monitor user accounts for anomalous behaviour.

Guessing

Online criminals may attempt to access accounts by entering common passwords or by using information they know about the user to guess their password (for example, knowing their favourite football team) – often this information is now obtained from social networking sites.

Consumer defence: Choose a password that is difficult to guess, including numbers and characters (see page 8).
Do not have a password that relates to any personal information readily identifiable via social networking sites.

Service provider defence: Limit the number of failed login attempts allowed. Implement minimum standards for consumer password strength.

Brute force attack

Cyber criminals bombard the online service with passwords until the correct password is entered.

Service provider defence: Limit the number of failed login attempts allowed. Implement minimum standards for consumer password strength.

Why we conducted the survey

Research on password security often focuses on designing technical mechanisms to protect access to systems, however this usually results in cumbersome policy and procedures, which once implemented are regularly breached by users.

We decided instead to focus on user behaviour and attitudes towards the use of passwords, such as whether the user considered them secure, and their habits relating to remembering and changing them.

Who We Asked

We asked a broad cross section of Australians about their attitudes to password security. The survey was completed by over 1000 respondents, with an even split of male/female respondents; a near even breakup of ages; and a state/territory representation based on population numbers. This validates the survey outcomes and gives us a solid basis for making sound deductions.

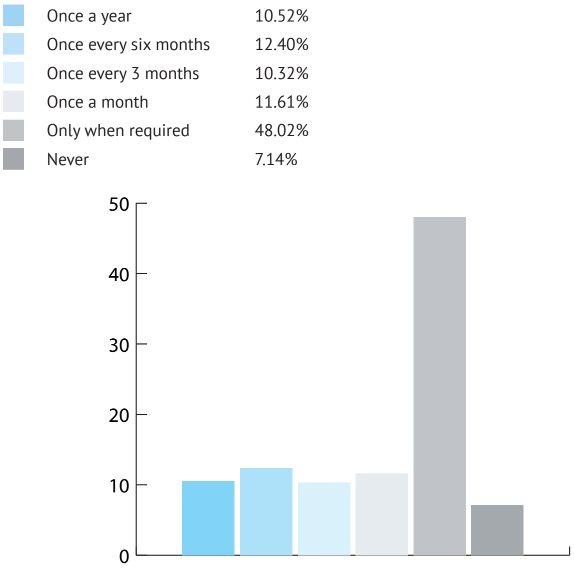
As Australians continue to embrace eCommerce, Internet banking, social media, and other online services there will be a growing requirement to log into many different systems and platforms, necessitating more passwords.

Nearly two thirds (63%) of respondents use the same password across more than one online account. Interestingly, this number grows to 77% when looking at the 18-24 year old category.

This finding suggests that many Internet users underestimate the threat from cyber criminals who abuse this habit: stealing passwords via one site and then attempting to replay them across others.

Critical to the use of the same password for multiple login's is how often users change their passwords.

Nearly half (48%) of respondents said they only changed their passwords when required to by a system. 7% never do.



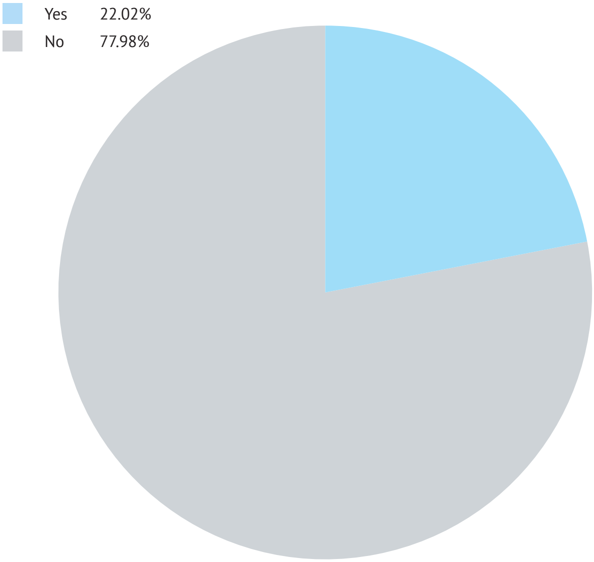
How often do you change your passwords?

While time consuming – and possibly resulting in more forgotten passwords initially – regularly changing passwords can be a very effective tool in keeping accounts secure.

Since there is an active blackmarket trade in passwords between criminals, the habit of changing passwords degrades the value of that criminal economy: the stolen password is useless once it has been changed by the owner.

Password guessing attacks can be mitigated by consumers ensuring that passwords are sufficiently complex and by system operators limiting the frequency of authentication attempts.

A pleasing result is that over three quarters (78%) of respondents said their passwords didn't contain any personally identifying information.



Do your passwords contain personal information (eg name, nickname, birthday, work, address, place of birth)?

Only 10% of respondents thought their online passwords could be easily guessed.

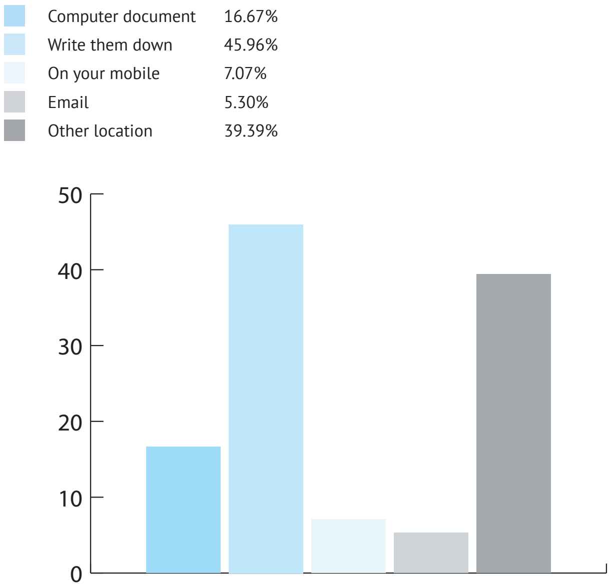
These last two results are interesting as the user-assessed level of complexity and perceived low "guessibility" indicate that Australian Internet users believe they are more disciplined with their online passwords. This is in contrast to analysis of large scale public password breaches (such as Sony's recent losses, and others from web based email services and social networking sites). Analysis of those breaches show users still use dictionary words, names and nicknames and rarely use numbers and symbols.

In a more troubling set of results, 41% of survey respondents (63% of 18-24 year olds) have shared their password with a friend, family member or work colleague, with only one third (36%) having changed the password since sharing.

Ensuring the confidentiality of passwords is challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves. For example, requiring passwords be long and complex makes it less likely that attackers will guess or crack them, but it also makes the passwords harder for users to remember, and thus more likely to be stored insecurely.

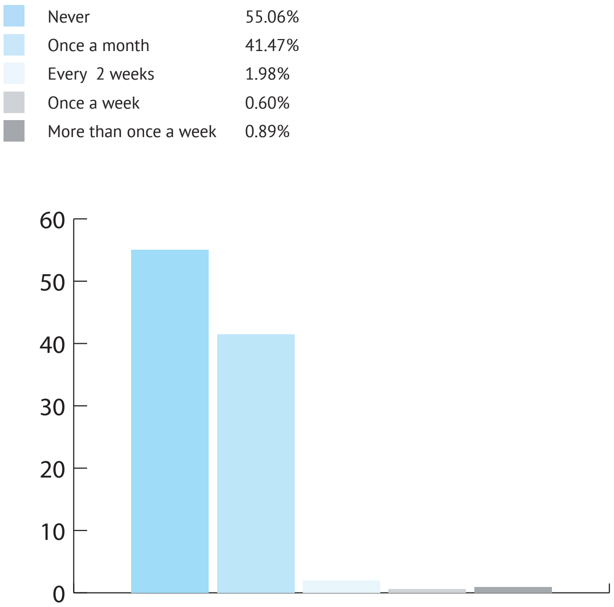
46% of respondents store their passwords on a piece of paper. In itself, this is a harmless practice assuming that the piece of paper is not stuck to the computer hardware and is stored in a separate location.

18-24 year olds use paper to store their passwords, but they also like to store passwords on their mobile phones.



Where do you store your passwords?

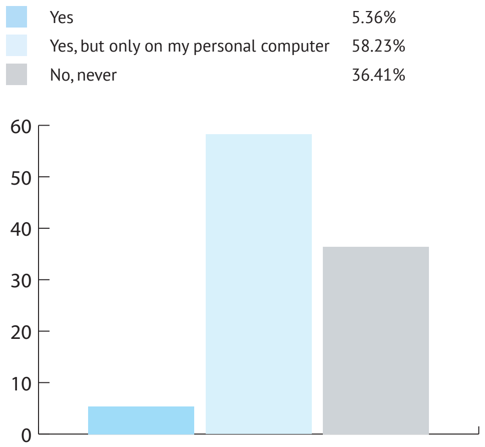
41% of respondents forget at least one of their online passwords once a month and have a new one emailed to them. Social engineering attacks, in particular phishing attacks, often pretend to be an official system administrator seeking to trick a user into resetting a password.



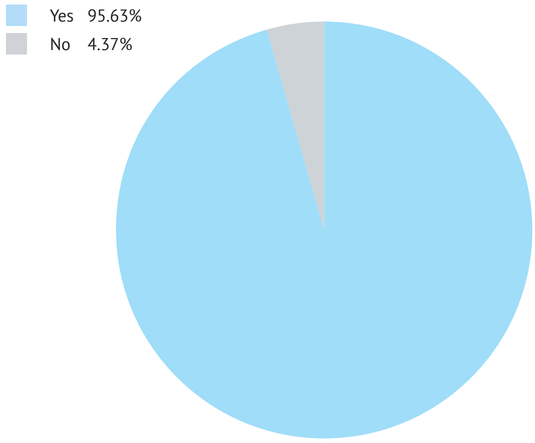
How often do you forget your password and have it emailed to you?

It was pleasing to discover nearly all (96%) of respondents say they take care to protect their personal information when using a public computer, like those found in a library, internet café or an airline lounge. It is unclear how they actually protect themselves, however, as using such services is inherently risky.

In addition, over a third (36%) never ticked 'yes' when asked by a website to remember their details. Some websites have this option pre-selected and can easily fool a user into accidently divulging their personal information in the context of better user experience. This is a critical issue for those using shared or public computers, as the next user may be able to gain access to the previously logged in application.



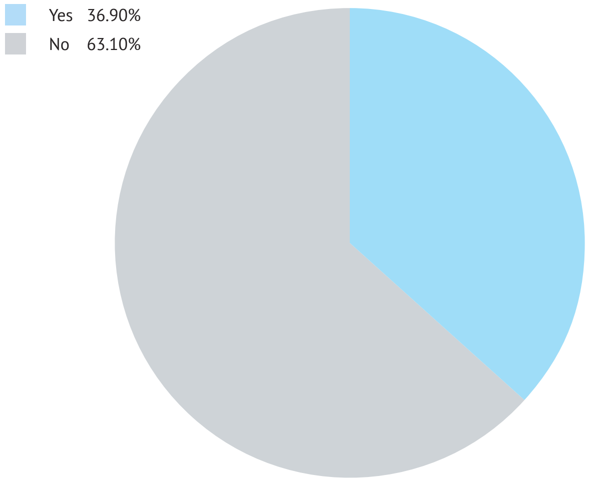
Do you often tick 'yes' when asked if you would like a site to remember your details?



Do you take more care to protect your personal information when using a public computer?

Australians are leading the worldwide trend in the use of "smart" mobile devices, particularly younger generations, and are increasingly accessing the Internet from these devices.

A third (36%) of respondents remain logged into online accounts, such as social media, including on their mobile phones. 76% of 18-24 year olds remained logged into such online accounts. This is potentially dangerous, especially if the phone is not locked (or set to auto lock within a short period).



Do you stay logged in to any of your online accounts, such as social networking sites and email, including those on your mobile phone?

Conclusion

Unfortunately many operating systems and applications do not require the use of strong passwords. It is critical that Australian consumers are aware of the characteristics of strong passwords and the importance of having strong passwords and protecting them.

A password is a partnership between the end user and the service provider.

Online service providers still legitimately rely on passwords for account security, but they would be tempting fate if that is all they relied upon for such security.

Online service providers need robust password policies and procedures (like minimum strength and routine changing), and to actively monitor accounts for anomalous behaviour.

Consumers of those services need to know that their attitude towards passwords will be a major influence on their online safety.

The attachment gives further advice on creating and managing passwords.

Centre for Internet Safety

September 2011 - ISBN 978 1 922017 00 0

PayPal and the Centre for Internet Safety's guide to creating and managing a secure password

1. Take stock of your current passwords

- The first step is to work out how many passwords you actually have – this can take time, as most people have a number of accounts online, ranging from bank accounts to social media platforms to newsletters
- Allocate a unique password to each account – do not use the same password across multiple online accounts

2. Create your passwords

- When creating a password, do not use personal information such as your name, your address, your birthday, your nickname, pet's or children's names, or your place of work.
- Avoid using words you can find in a dictionary, people's names, or phrases that can be easily guessed.
- Choose a password with the following criteria: at least 1 number, 1 special character, 1 uppercase letter, and ensure it is at least 8 characters long.
- Here is one way of generating a harder to guess password:
- think of a phrase like "I love it when it rains on weekends!"
- take the first letter from each word: Iliwirow!
- Convert the letter "o" to a zero: Iliwir0w!
- We now have a 9 character password with a capital, a number and a special character

3. Manage your passwords

- Never share your password with anyone. Simple.
- Change your passwords regularly – not only when you are prompted to change them by your online accounts. A good start is to change all your online passwords when daylight saving time comes into effect and stops (even if you are in a state where daylight saving time is implemented.
- When entering your password on a public computer, be aware that others may be watching you type or recording what you are doing using malware. Change your password asap upon returning to your usual computer.
- If you can't remember all your passwords, avoid saving them on your desktop or your mobile device, but rather write them down and keep this in a safe place away from your computer.

PayPal™