



Information Circular No: **2011/41** Date: 9 August 2011

TO: All PCN Users

Parliamentary Computing Network SECURITY UPDATE

1 An important aspect of the recent weekend maintenance work related to Parliamentary Computing Network (**PCN**) security. This circular is intended to provide some guidance on IT security, which will help maintain the security of your personal PCN account and data, and of the PCN more widely.

2 Two major threats to IT security are:

- (a) unauthorised access to individual accounts; and
- (b) compromises of network security through malicious software¹ being loaded onto the PCN.

Unauthorised account access

3 You should keep your password confidential and not disclose it to anyone—DPS IT support staff do not need to know your password to provide support to you. Be suspicious if anyone asks for your password.

4 To help maintain password confidentiality:

- (a) PCN passwords must be changed every 90 days—you will be automatically prompted to enter a new password when the 90 day limit is reached;
- (b) if you use an RSA token for remote access, the PIN will expire after 90 days—the new PIN must be 6 to 8 digits in length; and
- (c) you can elect to change your password at any time.

5 You do not need to share your password within offices and workgroups. There are mechanisms to allow you to share access securely to online calendars and mailboxes, including allowing specific staff to send an email on your behalf. Access to documents can also be shared. Advice on how is available from the Helpdesk on extension 2020.

6 Users will now automatically be locked out of their accounts after five unsuccessful attempts to log in using your password. You will need to either wait six hours for your account to be unlocked, or call 2020 to have your account

¹ Malicious software (also known as malware) has many forms, and new versions are constantly being developed. The most common aims are to interrupt email operation of a network or access to an organisation's public website (known as a denial of service attack), insert software that is able to covertly export information from within the network, and insert software that is able to shutdown a network completely.

enabled. 2020 will need to positively identify you as the account holder before you are issued with a new password.

7 This password lockout, and the minimum standard for password length and complexity are preventative measures against password hacking. A short and simple password is virtually defenceless against a "password cracking" program, as indicated in the table below.

Time taken to crack a password		
Password length (number of characters)	Simple (lower case letters only)	Complex (duo case letters, numbers and symbols)
4	Less than 1 second	4.8 seconds
6	1 hour	11 hours
8	5 months	10 years

8 If you find your account locked out for no apparent reason, you should advise 2020 so that a possible unauthorised access attempt can be investigated.

Risk of malicious software

9 Although there are sophisticated virus scanning systems in place on the PCN which will intercept and block incoming malicious software, there are things you can do (or not do) to help.

10 Do not download any executable files (programs and applications) from the internet onto the PCN. If you need to load software or updates, this can be done with 2020 assistance in a secure manner.

11 Do not load executable files onto a PCN computer through portable media such as thumb drives.

12 Be aware of unsolicited emails, especially where there is an attachment, or a request to access a website via a link embedded in the email. Apart from the widely known "Nigerian scam" type of email, we are now seeing much more sophisticated social engineering in the construction of false emails. They look authentic and may appear to come from someone you know or someone important—however, they are generally carriers for malicious software. If you receive an email which doesn't feel right, please report it to DPSIT.Incidents@aph.gov.au .

13 Do not open suspicious emails or click on links within suspicious emails. Report them to the 2020 helpdesk or email to DPSIT.Incidents@aph.gov.au

14 Do not plug wireless access devices, such as wireless routers, into the PCN or any device connected to the PCN without prior approval, which can be sought by contacting 2020.

Security upgrades

15 DPS technical staff regularly apply security upgrades to all computers on the PCN, including urgent upgrades where a new virus or threat has been identified. This typically happens overnight, and requires the computer to be connected to the PCN and switched on.

16 As a general rule, you are advised to log off and shut down your computer at the end of each day. This has several benefits, including clearing and resetting the computer's memory. However, from time to time you will be asked to leave your computer connected and switched on (but logged out) so that software upgrades can be installed overnight.

17 If possible, it is also good practice to connect all computers (laptops and desktops) to the PCN at least once a week so that security upgrades can be applied. This will reduce extended logon times that occur when devices are left disconnected for long periods, and there is a backlog of software upgrades.

18 For further information, please contact the 2020 helpdesk on (02) 6277 2020.

David Kenny
Deputy Secretary