Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Security for Agents of Government Services

MAY 2020

Introduction

Agents of government services, such as taxation agents, BAS agents and taxation (financial) advisers, have authorisation to access valuable or personal information on behalf of their clients, which makes them attractive targets for cybercriminals. To protect your clients, please consider the following cyber security advice.

Use multi-factor authentication

Use multi-factor authentication[1] for accessing government services, as well as any computers that you control (where supported). Multi-factor authentication adds an additional layer of protection against cybercriminals trying to compromise your devices or gain access to government services.

Encourage your clients to use multi-factor authentication when accessing government services. For example, myGov offers the ability to use security codes when logging in[2].

Also encourage your clients to protect email accounts they use for passphrase resets.

Use strong passphrases

If multi-factor authentication cannot be used, ensure your password is a passphrase that is strong, unique and memorable instead[3].

Cybercriminals will often guess poor passwords. They may do this by using commonly used passwords or information from websites that list compromised account details[4]. Social media can also expose peoples' personal details that cybercriminals may exploit.

When developing a passphrase, consider the following:

- use at least four words that represent at least 14 characters
- use random words – categories of similar words (such as types of fruit) are easier to guess
- create something that is unique – lyrics and quotes are publicly available and not suitable.

In addition, use unique passphrases for each computer, mobile device and government service you access.

Finally, use a dedicated 'password manager' to keep track of your passphrases. Some password managers also have a password generation feature.

[1] https://www.cyber.gov.au/publications/implementing-multi-factor-authentication
[2] https://my.gov.au/mygov/content/html/help.html#securityCode
[3] http://cyber.gov.au/publications/small-business-cyber-security-guide
[4] https://haveibeenpwned.com/

Secure your computers and mobile devices

It is critical that you keep your computers and mobile devices secure. This can be achieved by:

- using only legitimate and vendor supported software
- enabling automatic updates
- encrypting all data
- backing up data regularly
- using a screen lock
- enabling remote tracking, locking or wiping for mobile devices
- avoiding public Wi-Fi networks
- locking away mobile devices when not in use or outside of business hours.

Prepare for cyber security incidents

Prepare for, and know how to respond to, a cyber security incident[5]. If a cybercriminal gains access to your computer or mobile device, they may be able to access sensitive information on your clients or government services you have access to.

Finally, re-familiarise yourself with data breach reporting obligations[6]. Being prepared and responding quickly will minimise damage to your clients should a cyber security incident occur.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).

[5] https://www.cyber.gov.au/publications/preparing-for-and-responding-to-cyber-security-incidents
[6] https://www.ato.gov.au/general/online-services/online-security/data-breach-guidance-for-tax-professionals/