Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Using Consumer-Grade Email Services

JANUARY 2019

Introduction

Using consumer-grade email services to conduct business is often attractive due to the low costs (if any) and minimal effort required setting up new email accounts. However, given the uncertainly around the security provided by consumer-grade email services, particular care should be taken when choosing to use such services, especially when using the services for sensitive business transactions. This includes considering the provider's ability to delete or recover communications if required, and the legislation service providers may be subject to in the countries they operate from.

Recommendations

If using consumer-grade email services, the following measures are recommended to lower the risk of using such services:

- use separate email accounts for work and personal purposes
- use a strong password that is unique for each email account
- use multi-factor authentication when supported by the service provider
- do not share passwords for email accounts
- do not store passwords for email accounts in emails or in documents
- do not elect to remember passwords for email accounts when offered by web browsers
- avoid configuring mobile or desktop applications to automatically sign in to email accounts
- if asked to set up security questions to recover email accounts, do not provide answers that could easily be obtained from public sources of information
- do not access email accounts from untrusted devices in internet cafes or hotels
- always remember to sign out of email accounts after use
- use lock screens and a password on devices that have access to email accounts
- where possible, access email accounts using devices that are using the latest versions of software and have had all recent patches applied
- remember to close old email accounts when they are no longer required.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

The ***Detecting Socially Engineered Messages*** publication provides additional guidance on how to identify socially engineered messages. It can be found at https://www.acsc.gov.au/publications/protect/Socially_Engineered_Messages.pdf.

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).