How safe are you?

Keep your data protected.

Checklist

- This cybersafe check list is designed for RMIT staff and students, to help you implement steps to help keep your RMIT data safe
- We recommend that ALL steps are implemented ASAP
- The more 'ticks', the safer you will be!

This checklist is specific to RMIT. Click here for a personal information protection guide.

PASSWORDS **Did you know?** The longer a password is, the stronger it is. A min 8- alpha numeric password is acceptable, but the more characters, the stronger a password is, and the more secure your information.	**√**
I lock my computer and mobile device every time I move away from my desk, both in the office and in a public place	
My RMIT Login is not used for any other account	
I would never write or share my passphrase with anyone	
My password is a passphrase Example: My grandma has 6 chickens and 2 ducks in her yard. I wish she had a pool! = Mgh6c&2dihy.Iwshap!	
I have set up the RMIT self-service password reset tool, so I'll be able to reset my password myself and get connected to RMIT apps when I want: https://www.rmit.edu.au/students/support-and-facilities/it-services-for-students/password-assistance/set-up-your-self-service-details	
I have set up mobile verification for my RMIT Google mail	
I have a strong password which is now a minimum of 18 alpha numeric characters	
I have different passwords for all my services	
I have established two factor authentications on my phone and laptop	
My back up security questions do not reference historical facts such as my real mother's maiden name, first school or pet. They are fictitious and would not be available on any public record	
I have set up a password manager to help me manager my passwords across my services. Common managers available: LastPass, 1Password, enpass	
From time to time I check www.haveIbeenpwned to check if my accounts have been compromised in a data breach	
SCORE	**_/12**

THINK BEFORE YOU CLICK – PHISHING AND MALWARE	√
I have familiarised myself with the RMIT Cyber security materials and 2020 guide to Cyber safety.	
I am familiar with how phishing messages may be identified from normal mail	
I don't send unencrypted financial and/or personal data of RMIT colleagues/ data bases external to RMIT	
I know that when in doubt about a link or URL in an email, I should manually type the web address into my browser and check that the address displays properly (no added letters, numbers or symbols)	
I know to look out for common types of domain name inaccuracies such as the substitution of the letter 'o' with '0 (Zero)' or bogus words to a legitimate address for example: ANZcard.com.au (is not a typical format)	
I know never to respond to a request for my password via email, SMS, phone or social media	
I am wary of phones, SMS and email requests where personal information is requested	
I am aware of the RMIT Cyber Ambassador program: https://www.rmit.edu.au/staff/our-structure/operations/its/office-of-ciso	
I have subscribed to receive online threat alerts	
I always forward any suspicious mail to reportphishing@rmit.edu.au	
SCORE	**_/10**

SAFE DATA STORAGE	√
I store all my information either on OneDrive or SharePoint	
I do not store or backup RMIT data on non RMIT endorsed storage such as Dropbox, iCloud, public computers, personal computers	
I don't use USB, DVD or other portable media to store or access sensitive RMIT data	
I ensure personal or sensitive information is stored securely in accordance with RMIT Information Management Policy	
I only install applications and software from reputable sources -i.e. Apple store for Apple devices or the Play Store for Android	
I avoid using email to exchange or store sensitive information	
I promptly download the latest software updates to my phone and devices	
I understand that I can contact CISO team to provide data storage guidelines	
I am aware that my role at RMIT should never require me to store credit card numbers	
I follow the data storage, retention and disposal process in accordance with RMIT Information Governance Policy (section 9 Retention and disposal authority)	
SCORE	**_/10**

REMOTE WORKING / TRAVEL	√
When I am working in a public place, I only access RMIT data using MY DESKTOP (RMIT's secure connection) and access RMIT files stored in OneDrive or SharePoint	
I avoid using public or free Wi-Fi (either in the office or working remotely) to download files, access sensitive information and avoid entering my RMIT ID and password	
Before my departure, I arrange for a suitable data plan to ensure I have a secure connection	
I always log off after using a system that requires a password on a public computer	
Before travelling overseas, I update my phone and laptop to have the latest software and I defer any software updates while I am away	
When travelling overseas for work I keep my devices with me and never check them in as luggage	
I keep my devices safely with me rather than leave them in the hotel room or safe	
My mobile devices have the security features turned ON / enabled	
When using public Wi-Fi, I always ask a staff member for the Wi-Fi name to ensure I connect to a legitimate public Wi-Fi (but I would never use this connection to access confidential data or complete financial transactions)	
When I use my own devices for RMIT work, I keep them updated (system and applications) with the latest anti-virus software and plugins to fix any vulnerabilities	
I have up to date virus protection on my home computer or any that I may use in a public place	
I disable Bluetooth and Wi-Fi when not in use on my devices. (Leaving Wi-Fi on leaves me at risk of connecting to untrusted networks. Bluetooth is great for connecting devices and transferring content with trusted devices, but can leave me exposed to transfer of malicious software or data theft)	
SCORE	**_/12**

REPORT & HELP	√
I know the CISO team respond to University Cyber incidents and act on their advice	
I have familiarised myself with the process to get help or report a Cybersecurity incident to the RMIT ITS Services & Support Centre www.rmit.edu.au/its/ithelp	
I know to contact ITS Service & Support Centre immediately if I receive notification that my files have been locked and/ or I receive a demand for money to have information returned to me (ransomware)	
I know that if I receive phishing or a malicious email, I need to always log an Incident with ITS and / or forward the email to reportphishing@rmit.edu.au	
I am aware that I need to report any loss or theft of RMIT mobile devices immediately to the ITS Service and Support Centre www.rmit.edu.au/its/ithelp or +61 39925888	
SCORE	**_/5**