Cybersecurity
Be empowered

2018

Your guide to staying safe at RMIT

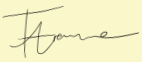
Be safe

The digital world continues to evolve at a fast pace, delivering innovation and interconnectivity. Today's proliferation of the Internet of Things, smart devices and growing adoption of cloud services, to name a few, is revolutionising the way we live, learn and work.

Whilst these technology advances are delivering tangible benefits and opportunities, it also exposes us to potential cyber threats. The complexity of our systems and our constant need to be online is creating a world of opportunities for threat-actors to exploit our weaknesses.

The dependency and trust we place on technology to manage our work, finances and social life has never been so high. To stay safe, we must adopt good security practices, be vigilant and proactive in protecting ourselves and RMIT's reputation.

To support your enjoyment of all the benefits of participating in today's connected world, we have prepared this simple guide. In these pages, you will find information on some common cyber threats, the basics of good cybersecurity and a summary of our collective responsibilities contained in RMIT policies and processes that aim to keep both you and RMIT cybersafe.



Tony Aramze
Chief Information Security Officer, RMIT

CISO Office

ITS Help & Support

Have a question or want to report inappropriate conduct?

Contact the RMIT IT Service and Support Centre:
www.rmit.edu.au/its/ithelp
+61 3 9925 8888

The RMIT Cybersecurity website contains further useful information and links to current IT and security policies:
www.rmit.edu.au/students/support-and-facilities/it-services-for-students/cyber-security

Be involved

Be part of a safe university by complying with university policy

4

Social Media

Use social media as the amazing information resource it is; discover new resources, learn about others' opinions and respect the differences and similarities of your various connections.

Don't share personal information (e.g. credit card details, real time locations or passwords) over social media, even in private messages, including on messaging apps like WhatsApp.

Make sure you check your privacy and security settings regularly, so you can manage who sees your posts and when. If you see or hear of someone impersonating, or being impersonated, on social media, report this to the social network ASAP. Consider contacting iDcare, Australia and New Zealand's national identity support service, at http://www.idcare.org.

1

Facebook sessions per day on the RMIT network

60,0

in 5

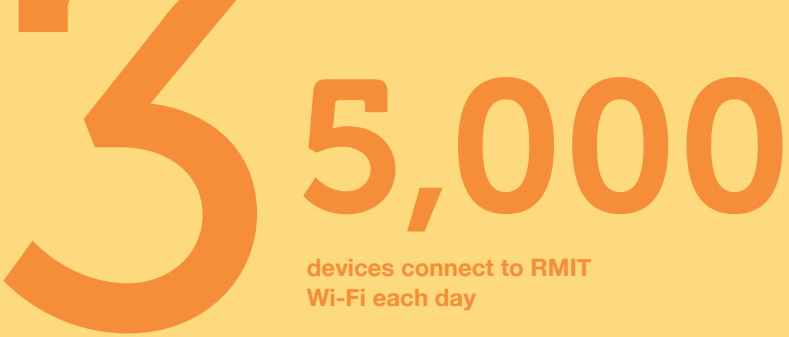
RMIT emails received each day are rejected as they are malicious

Email Communications

Accessing personal and university email is allowed on the university network, but be secure. Regularly check the email addresses you are sending to; ensure you are sending to the right recipient.

Phishing email is a type of cyber scam, where the sender usually poses as a trusted source and wants recipients to open malicious links or files, or supply personal information such as a password, credit card details, etc.

Phishing email is common and should be deleted. Protect yourself by reporting and deleting suspicious emails and not clicking on links from unknown senders. RMIT will occasionally send test phishing emails to ensure you don't reply or open files and links.



RMIT WiFi & Internet

The primary purpose of the on-campus Wi-Fi and network services are for learning, teaching and research, enabling you to maximise the benefits and learning from your university work.

These facilities can also be used for reasonable amounts of personal use, including online banking, personal browsing and streaming. Illegal streaming and gambling is not permitted on the network.

Using the RMIT university network to access inappropriate materials including anything depicting violence, medical procedures, pornography, sexual acts or discrimination is not permitted, unless part of legitimate university work.

For more information as to what is and is not allowed please visit the RMIT Cybersecurity website.

Password & Data Security

The longer and more complex a password is, the stronger it is. Do not duplicate passwords across platforms. Change your passwords regularly and make sure you log out at the end of your session.

Adopt a password that is complex, but easy for you to remember, e.g. '43carBROKEONARAINYDAY!#'.

Many RMIT applications will log you out after a period of inactivity and you may lose unsaved data. Please try to save any forms or work before leaving your computer.

werty football
ncess 1234567890
sw0rd loveme
bc123 admin

These are eight of the top most common passwords. If yours is similar to any of these, change it!

Source: SplashData, 2016

Be organised

Social Media

Consider what you are sharing online and who is able to view it

Email

Be on the lookout for phishing emails, these should be deleted

Online Network

Ensure you use trusted networks, such as RMIT University's Wi-Fi

Passwords

Adopt long passwords and do not duplicate across platforms

Copyright

Illegal downloading and streaming are a breach of RMIT policy/copyright

Data & Privacy

Know the value of the data you utalise and send out