# Melbourne University Data Breach - Staying cyber-safe at University

Dear colleagues,

Many of you would now be aware of the recent Melbourne University data breach. Personal details of students and staff going back as far as 19 years were accessed in a "sophisticated" breach that was detected on 1 April 2020.

While we, random University, have technical controls in place, careless behaviour and user errors remain the weakest links in cyber security. Breaches of security can occur through social media, emails or visiting websites infected with malware. Cyber criminals can infiltrate your computer and university IT systems to steal personal and other sensitive information.

There are several things that you can do to protect your data both at work and at home:

**Tips for staying safe online from Stay Smart Online**

- **Avoid being scammed. Stop and think before you click.** The university will never ask you for your username or password. Before you click on links and attachments, always check the sender's address and verify any links as trusted. If in doubt, contact the sender via other means to check.
- **How safe is your computer? Don't let the bugs in!** Install and update anti-virus software and set it to scan regularly. Click here to get a free copy of Symantec Antivirus, available to all current staff members and currently enrolled students.
- **One small step for you, one giant leap for your online safety.** Keep your software, operating systems and applications up to date. Always lock your computer when unattended.
- **Don't put your system at risk. Buy from a trusted source.** Ensure you download apps from reputable publishers and read all permission requests before you commit.
- **You don't share your toothbrush so why share your passwords?** Be smart. Don't share your passwords. Choose complex passwords and keep them secure.

More information can be found at Stay Smart Online: https://www.staysmartonline.gov.au/

How do I report anything suspicious?
Act fast. Report any suspicious activity to the **Service Hub for Information Technology on +61 13 27 46** or via **ServiceHubInfoTech@randomu.edu.au.**

If the suspicious activity is specific to an email you have received in your university Outlook, you can click the 'Report Phish' button in Outlook.

**Further information**

If you have any questions regarding cyber security, please contact the university Service Hub for IT.