Dear <firstname>,

Education is a prime target for cyber-criminals, and as a result, student accounts are frequently compromised. To protect your data and the University, UQ is activating Multi-Factor Authentication (MFA) for student accounts through a staged rollout beginning in August 2022.

MFA provides an extra layer of protection to ensure that the person logging in to your UQ account is you. MFA requires two items to identify you:

1. Something you ‘know’ (your username and password).
2. Something you ‘have’ (such as a mobile phone or a physical token).

How will this impact me?
You will be required to use MFA in addition to your UQ username and password when logging in to most UQ applications, services, and websites.

What do I need to do?
The MFA rollout will occur in stages, so not all student accounts will be activated at the
same time. You will be notified over the coming months via email with more information, instructions and key dates for when MFA will be activated for your account.

Most students will use their smartphones to utilise MFA however there are also alternative options available. If you do not have a smartphone or have accessibility requirements or concerns, please complete the [MFA student accessibility request](#).

**Why is this happening?**
The number one cause of privacy breaches and compromised records in large organisations is stolen credentials (login information). MFA will provide an extra layer of security, significantly reducing the risk of your account being compromised.

**Where can I find help and support?**
For more information and FAQs, visit the [MFA Website](#) or contact [AskUs](#) for support.

Kind regards,

**Dr David Stockdale**

Director, Cyber Security

Information Technology Services
The University of Queensland
Brisbane Qld 4072 Australia

[stockdale@its.uq.edu.au](mailto:stockdale@its.uq.edu.au) [its.uq.edu.au](https://www.its.uq.edu.au)