Multi-factor Authentication
Frequently Asked Questions

Q: What is MFA protecting?
A: MFA adds an extra layer security to keep your data and VU networks more secure. Even if a hacker has your username and password, MFA places an additional barrier to stop the hacker from accessing your account. You may not think your account has sensitive information in it but someone which access to your account could potentially gain access to information about you held on VU systems such as:

- Your address and contact details
- Banking details
- Health records
- Emergency contact information
- Academic records

Q: Do I have to register for MFA?
A: Yes. MFA will be the only way to access your email, OneDrive, SharePoint and other O365 applications when working on or outside of the VU network, including on laptops and mobile devices such as smart phones and tablets. Even if you do not work remotely or access O365 on your phone you still need to register for MFA as this will make your account more secure and protect VU's information and data from cyber criminals.

Q: Do I have to download the Authenticator app to use MFA?
A: Although you can authenticate through other methods, the Authenticator app is the preferred and most secure method for MFA. It is also the easiest way and will make authenticating more seamless than other authentication methods. If it is not practical to use the authenticator app, the following options are available to use MFA:

- Receive an SMS to a register mobile phone
- Receive a call to a registered mobile phone
- Receive a call to a registered landline
- Use a physical token (this is the most difficult option for MFA and is not recommended)

Q: I haven't registered for MFA – can I still access O365?
A: No, if you're not registered for MFA you will be unable to access and you have not registered you will be prompted to register for MFA at that point.

Q: How will MFA affect the way I work on a day to day basis?
A: MFA should not affect the way that you work on a daily, the change will include the way you log in to the systems. MFA will also not challenge you if you are accessing other applications such as Finance 1, VUPortal or HRZONE.

Q: Will I need to use MFA if I use VPN?
A: Yes. When you are logged in using VPN, your computer is logged in to the VU network remotely, which will occasionally prompt an MFA challenge.

Q: Will I be challenged by MFA if I am sitting at my office desk?
A: Yes. Occasionally, whether you are connected to the VU network, or an external network when accessing O365 systems, you will be prompted to verify your identity through the MFA challenge.

Q: How do I know if I am connected to the VU network?
A: If you are on a VU campus, signed into your account and connected to the internet via VPN or eduroam Wi-Fi you are connected to the VU network.

Q: Why do I have to set up a passcode on my phone?
A: To prevent a criminal from accessing your personal information and VU's sensitive information from a lost/stolen phone, a passcode is required on the device being used for MFA. These guides show you how to easily set up an iPhone passcode or an Android lock screen.

Q: I need to travel interstate/overseas for work – will MFA still work to access O365?
A: Yes. You'll need to set up the below before you travel so that you can access O365 and your email securely while overseas:

- Register the Microsoft Authenticator App on your phone while at your computer in Australia by going to click here and follow the registration guide
- You'll need access to an internet connection to receive the challenge, we recommend buying a cheap SIM card with a small amount of data so that you can work uninterrupted
- If you can't get a SIM card you can elect to turn data roaming on to receive the challenge, this may incur costs depending on your carriers policy OR you can connect to the hotel wifi – we recommend connecting to the VPN first before accessing a public wifi (VPN instruction here)

Q: I don't have access to my mobile phone or it's been stolen/lost – can I still use MFA?
A: Yes. We recommend when you register for MFA you will set up a secondary verification method. If you are not able to use/access any of your registered verification methods, you will need to contact IT service desk for assistance.

Q: I use WhatsApp when I travel overseas – can MFA use WhatsApp to verify me when travelling if I change my SIM card?
A: No. MFA cannot send challenges through other apps like WhatsApp. MFA needs to use the Authenticator app to send you challenges to verify your identity. The Authenticator app will continue to work, even if you are using a local SIM while travelling overseas, so long as you have data or access to a Wi-Fi network.

Q: If someone steals my phone will they be able to access my email and OneDrive because I have the MFA authenticator app on it?
A: To access your account, a thief would need your username, password and the phone you have registered to receive an MFA challenge. If your phone is stolen you should contact the IT service desk immediately.

Q: I have changed the SIM card in my phone with the Authenticator App installed – will it still work?
A: Yes – provided that you still have data or can access Wi-Fi your Authenticator app will still work. However, if you have chosen to authenticate through your mobile number then MFA will not be able to challenge you through your new SIM unless you have transferred your pre-existing mobile number to the new SIM card.

Q: I have bought a new phone and the Authenticator App no longer works. What should I do?
A: If you have a new phone and experience problem setting up the authenticator app, please contact the IT service desk for help.

Q: What if I don't have a mobile phone or don't want to use my mobile phone for MFA?
A: You can register to receive a call to a landline for MFA or you can be issued with a physical token that will validate your identity when you receive an MFA challenge.

Q: Can I change my authentication method after I've set it?
A: Yes – you can go to https://aka.ms/mfasetup and sign in to change, or add backup, authentication methods. Avoid "office phone" field as this is not configurable.

Q: Why do I need to download an app on my phone?
A: The MFA app is the fastest, most reliable and secure option of verification. The app ensures you do not need to carry around an extra piece of hardware plus there are no charges to yourself by using this method. The app also uses very minimal data on your device.

Q: What if I don't have a smart phone?
A: If you don't own a smart phone you can use the text or call option to verify your identity.

Q: What if I don't own a mobile phone?
A: If you don't own a mobile device you can chose to authenticate through a home or work landline phone number

Q: I don’t wish to download an app, what are my options?
A: MFA can send a text message, or phone call, to a smart-phone, cell phone, land line (such as your office or home phone) or a tablet. We recommend that users use the app as this is the most secure and convenient option.

Q: Does the app track or use my location?
A: No, the MFA app does not use or request your location.

Q: Does MFA see my password?
A: No, the MFA system will verify your password with the internal system and will not send it to MFA. MFA is only used for the second factor authentication which is the “something you have”. It is used to verify, not store.

Q: Why does MFA need to have access to my smart phone camera?
A: When you are registering for MFA for the first time, the app will use your camera to scan a QR code that will be displayed on your screen. After you have setup MFA, you can disable the app permission to access your device camera.

Q: What if my question hasn’t been answered in these FAQs?
A: If you have a question that hasn’t been answered please contact the ITS Service Desk on 9919 2777 (option 1)