MFA FAQ

Why do I need MFA?

The purpose of MFA is to provide the strongest possible protection for your identity (user account). It prevents anyone who acquires your password (e.g. through a phishing email) from being able to access your account and your data to commit fraud or a cyber-attack.

What authentication methods can I register for MFA?

You can use the recommended method, the Microsoft Authenticator app, a mobile phone number for SMS codes or another phone number for call back.

Can't I just use my personal email?

Email is not supported as it is not a secure option for MFA.

I don't use a smartphone or have and old device so I can't use the Microsoft authenticator app

The Microsoft Authenticator app will work with most smart phones including those a few years old. Alternatively, you can register the mobile phone method (SMS codes).

I don't have a mobile phone or smart phone. What can I do?

Contact the helpdesk which will be able to advise you on alternative options.

What if I don't register in 14-days it mentions at login?

Any client app or web app will enforce registration before you can access your account if you continue to skip registration for 14 days. The 14 days begins the first time you skip the registration.

What personal data do you collect and how is this used?

The Microsoft Authenticator app does not collect or store any personally identifiable data. Further information can be found here https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-faq

The mobile phone method gathers and stores your mobile phone number exclusively for use with MFA. Only MFA administrators at LTU will be able to access this information.

When will it send me an authentication request or code to my mobile phone?

MFA is an intelligent system it will only send an authentication request or code if it thinks your login is risky. By risky this means an unusual login perhaps from place your rarely visit or from a network it considers to be associated with cybercrime. Both are often associated with cyber criminals who have stolen your password and are trying to access your accounts.

Therefore, you will rarely receive an authentication request or code when you are performing a legitimate login.

What if a cybercriminal tries this and I receive an authentication request on my phone that I didn't ask for?

You can deny the request and we advise you to reset your password.

What if I forget my phone or can't receive authentication requests?

You need data connectivity (Wi-Fi or 4G) to receive an authentication request but you can choose to manually type in the code from the authenticator app which doesn't require this.

If you don't have access to your phone you can also register an alternative phone number via https://aka.ms/mfasetup in advance or contact the helpdesk to reset your MFA registration.

What if I get a new phone?

The recommended Microsoft Authenticator App allows backup on iOS and Android but requires a Microsoft Account. This can be restored to a new phone.

Alternatively, you can setup the app again if helpdesk resets your MFA registration or you have an alternative phone number registered.

I don't have the latest version of Office, MacOS, iOS, Android etc and it won't connect to my email?

Some old applications (e.g. Office 2010) aren't compatible with MFA, we recommend using the latest version of Outlook included with Office 365 which you can download for free for PC and Mac.

The mail app on iOS and Android should work, however you can use the Outlook App available from the app store.

Password less authentication

If you would like to be able to login using an authentication request without even having to type your password, you can enable password less authentication. Find your account in the Microsoft Authenticator app and choose Phone Sign-In.