Configuring Microsoft Multi Factor Authentication (MFA)
Cybercriminals are increasingly targeting businesses to get access to company information through the practice of phishing.

Multi Factor Authentication (MFA) adds a layer of security to mitigate the risk of credentials being stolen. MFA is also sometimes referred to as Two Step Verification (2SV) or Two Factor Authentication (2FA).

It's easier than you think for someone to steal your password

Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help keep bad guys out, even if they have your password.

Source: google 2-step verification
An extra layer of security

Most people only have one layer – their password – to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account.

Sign in will require something you know and something you have

With 2-Step Verification, you'll protect your account with something you know (your password) and something you have (your phone or Security Key).

Source: google 2-step verification
You need to make a choice

The most convenient way to access your passwords and authenticator code is through the authenticator app on your smart phone.

If you do not have a smart phone, you can have a verification code sent by text message to your mobile. If you do not have a mobile phone at all, or do not want to use your smart phone, you can opt to receive a call to your landline.

Authenticator app
Text message
A phone call
Set up MFA – go to ecu.edu.au/infosec

LastPass Password Manager

Microsoft Multifactor authentication (MFA)
Set up MFA

We recommend you select the mobile app. The text to mobile phone or landline option can also be selected from this drop down menu.

Read the instructions

Press Microsoft Multifactor Authenticator
If you want to receive the codes through your the landline or desk phone

1. Select the Authentication phone option
2. Select "Call me"
3. Select the country code and put in Your landline number (without the 0)
If you want to receive the codes via a text message on your mobile phone:

1. Select the Authentication phone option.
2. Select “Send me a code by text message.”
3. Select the country code and put in your mobile number (without the 0).
4. Press Save.
Configure a backup phone number

As a backup configure your desk phone as the Alternate authentication phone.

Select “Send me a code by text message” if your backup phone is a mobile number. Select “Call me” if your backup phone is a desk phone (land line).

Press Save.
Once your MFA has been activated, you will need to go to the Microsoft website to select your preference for receiving verification codes.

Install one of the three authenticator apps onto your mobile phone. This procedure refers to the configuration of the Microsoft authenticator, however other authenticators are configured in a similar manner.
Get started with the Microsoft Authenticator App

We recommend you select the mobile app.

Press ‘Select’.
Set up MFA

First time users might get this message. Press continue

Select “Work or School account”

Press “Add account”

Your Camera will open in the authenticator app to scan a QR code
Scan the QR code with your mobile phone

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

- How do you want to use the mobile app?
  - Receive notifications for verification
  - Use verification without notifications

To use these verification methods:

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

Configure app without notifications

If you are unable to scan the image, enter the following information in your app.
Code: 12345
Url: https://bn1pfpad10.phonefactor.net/pad//12345

If the app displays a six-digit code, choose "Next".

Next  cancel
Set up MFA

1. Additional security verification
   Secure your account by adding phone verification to your password. View video to know how to secure your account.

   **Step 1: How should we contact you?**
   - Mobile app
     - How do you want to use the mobile app?
       - Receive notifications for verification
       - Use verification code
   
   To use these verification methods, you must set up the Microsoft Authenticator app.
   - Set up
   - Checking activation status.

2. Additional security verification
   Secure your account by adding phone verification to your password. View video to know how to secure your account.

   **Step 2: Enter the verification code from the mobile app**
   Enter the verification code displayed on your app.

3. Additional security verification
   Secure your account by adding phone verification to your password. View video to know how to secure your account.

   **Step 3: In case you lose access to the mobile app**
   Select your country or region
   
   Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

   Done
Configure your settings

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.

View video to know how to secure your account

what’s your preferred option?

We’ll use this verification option by default.

- Use verification code from app or token
- Call my authentication phone
- Text code to my authentication phone
- Call my office phone
- Notify me through app

Set up Authenticator app

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Review your settings and press ‘Save’
Configure your settings

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. View video to know how to secure your account.

What's your preferred option?

We'll use this verification option by default.

- Use verification code from app or token
- Call my authentication phone
- Text code to my authentication phone
- Call my office phone
- Notify me through app

Set up Authenticator app

Review your settings and press 'Save'.

Repeat the previous steps to configure a backup (2nd) device for the Microsoft authenticator app.
The InfoSec Team

Enabling safe digital business is our goal

Karen Owens
Yvonne Wallwork
Andy Tilbury
Allan Cantlay
Wade Hams
Ronald van Erven

Contact the IT Service Desk:
+61 8 6304 6000 or itservicedesk@ecu.edu.au

or find us at ecu.edu.au/infosec