July 2026

Dear Member,

In 2018, the General Service Board of Alcoholics Anonymous in Ireland (GSBAA) introduced official AA email addresses (mailboxes) for use by the fellowship. Under the GDPR personal data regulation it allows AA service levels to communicate AA business within the Structure and eliminates the need for AA members to use personal email addresses. It also reduces unnecessary postage costs as the mailboxes can be used to email minutes etc. within the Structure.

Our email provider, Microsoft, has a policy that ensures that mailboxes stay active. An email account stays active when at least one email is sent in a 90-day period.

If you decide not to send any emails in a 3-month period, your allocated email address will go into a non-active state. Should this happen, you will no longer be able to access it to send and receive emails and any emails contained in your mailbox will be permanently deleted after a 1-month period. If you decide to reactivate your account, you will need to contact GSO to request this.

Microsoft granted Charity Licences to the GSBAA for each account. They informed us that we need to ask you to take the above action if you wish to enjoy uninterrupted use of your email address.

We thank you for your cooperation and hope that this will encourage the level of usage as is required by Microsoft.

Kind regards

General Service Board of AA

Included in this document is a useful User Guide which will help you to access and use the new official AA mailbox.

Please be aware that certain functions in your new mailbox have been disabled, this includes 'Auto-Forwarding' to external email addresses. These functions are not available in the mailbox.

If you need any help accessing the mailbox, please contact GSO on 01 8420700 during office hours, or email gso@alcoholicsanonymous.ie.

HOW TO ACCESS AN OFFICIAL AA EMAIL ACCOUNT

USER GUIDE FOR AA MEMBERS

The General Service Office has issued this step-by-step technical guide for AA members.

PROCESS FOR THE OBTAINING THE OFFICIAL LOGIN INFORMATION FOR THE AA EMAIL ADDRESS/MAILBOX

a) How to obtain the login and password for your group:

- **New Groups:** The email address for your group will automatically be issued to the nominated member of your group, by phone text message, on receipt of a Group Information Sheet (GIS), sent via the Structure, to GSO.

- **Existing Groups:** A group member can fill a GIS for an already registered group here to request the login information If access has been lost, or a new person has been nominated to take over the mailbox.

- Once GSO receives the GIS, we will text the nominated member with their details.

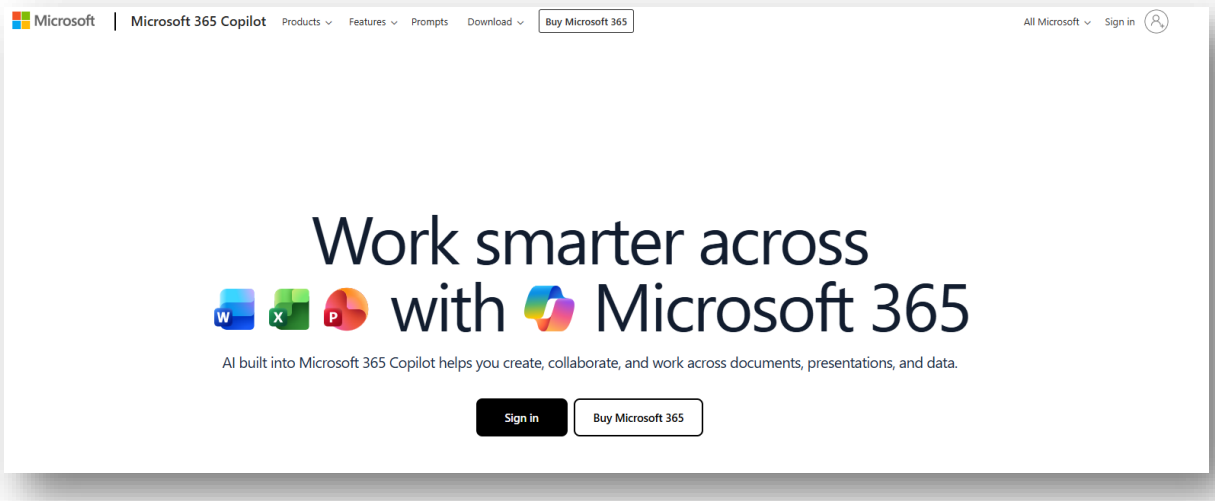
- Password reminders may be given to the designated contact by phone, once verified. GSO are available on 01 8420700

b) How to access the AA mailbox:

The setup of the new account is processed by GSO, via Microsoft Office 365, and like any email account e.g., Gmail, Hotmail, Yahoo etc., you must first access their website to login.

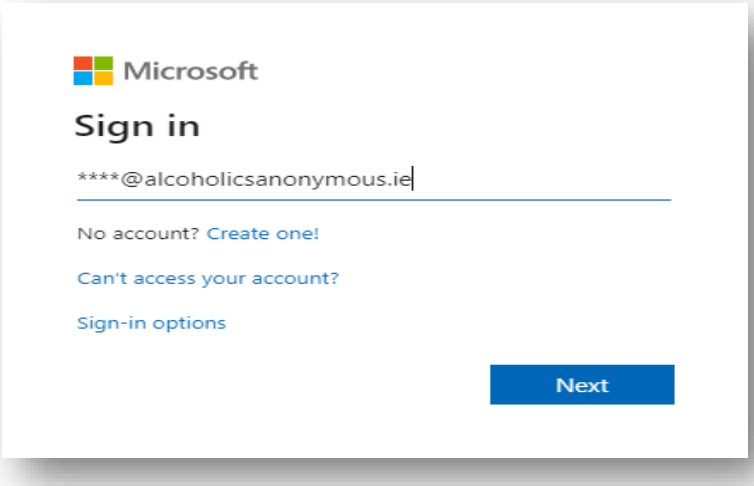
When you receive the login and password from GSO follow these steps:

- Go to www.office.com where you will see Microsoft's homepage:



- You can either click on the main 'Sign In' button on the screen or click on the 'sign in' option in the circle on the top right of the screen.

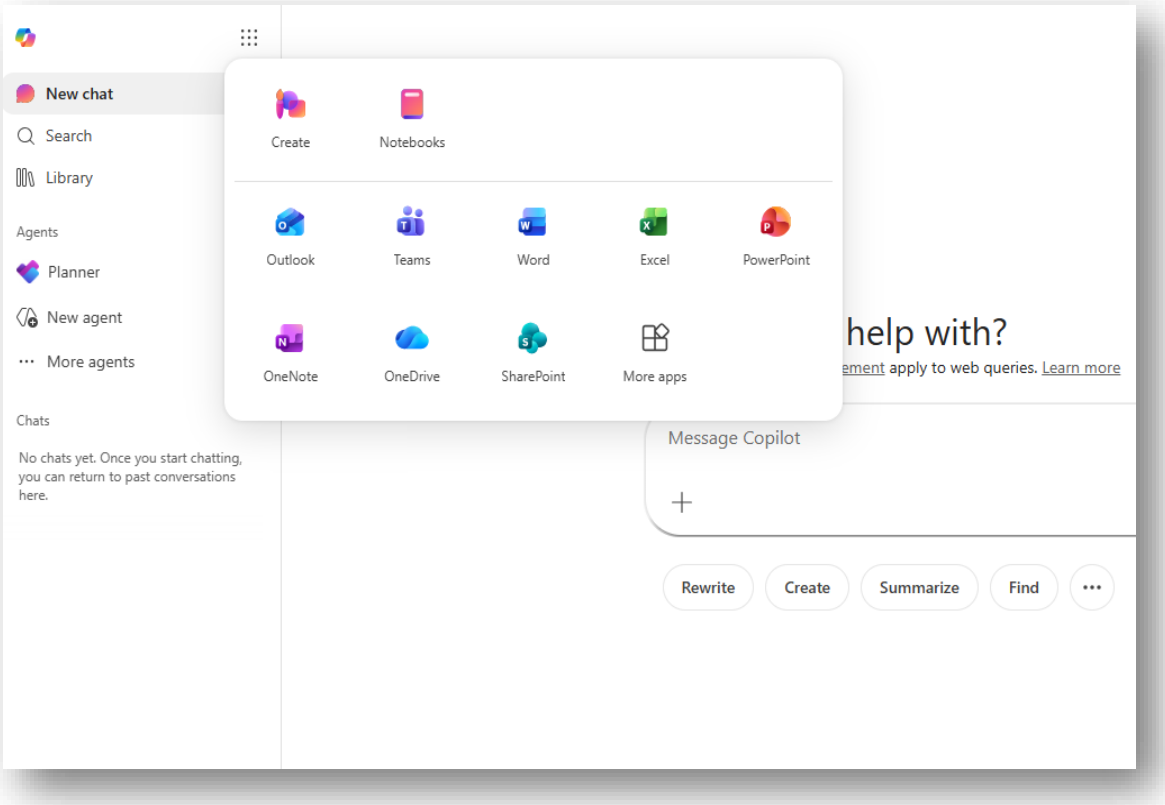
Enter the group's designated email address listed below and click 'Next':



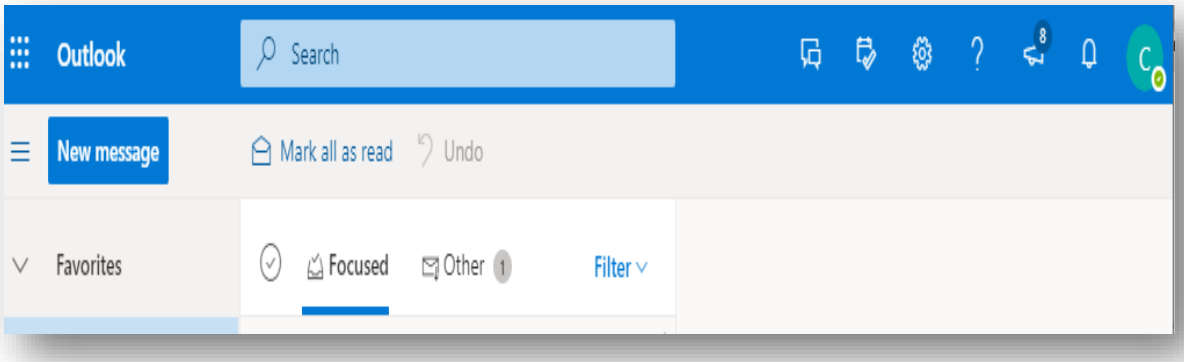
- Enter the password on the next screen and click 'Sign In'

- **At this point, a pop-up box usually appears on your device asking you if you want to stay signed in,* ***we recommend choosing 'No'*** *to avoid replacing any personal email account you already have set up. If you choose 'Yes' the AA email account will become the Primary Email Account on your device*.*

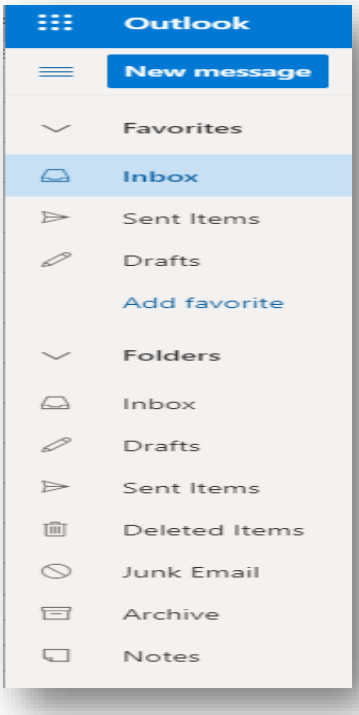
- You will see a screen with a Apps tab, which is a 'square' of 9 dots on the left-hand side



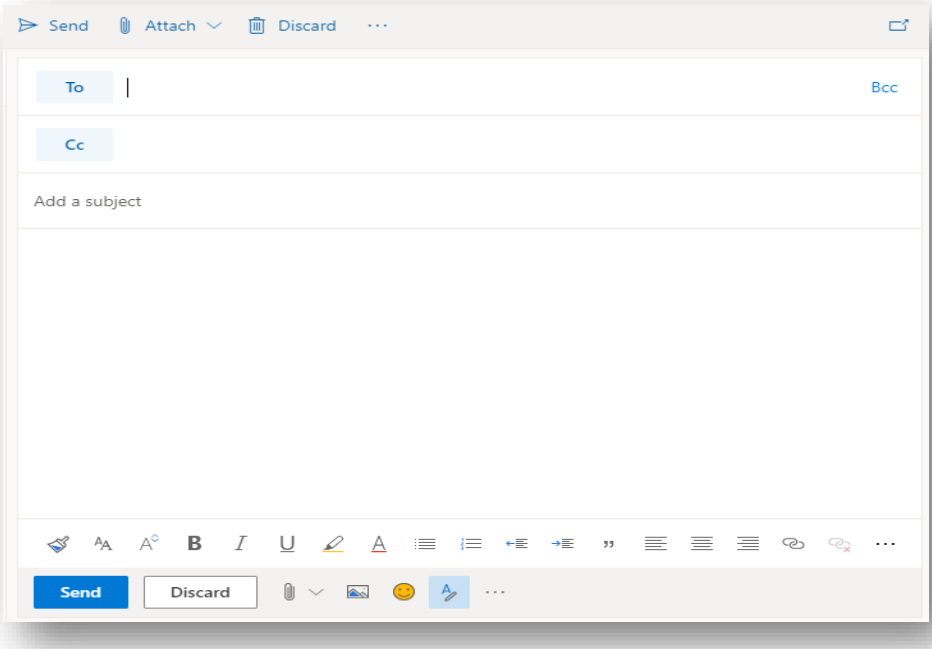
- Choose the 'Outlook' button/icon, this is the email account:



➢ On the left-hand side, you will see all the folders:



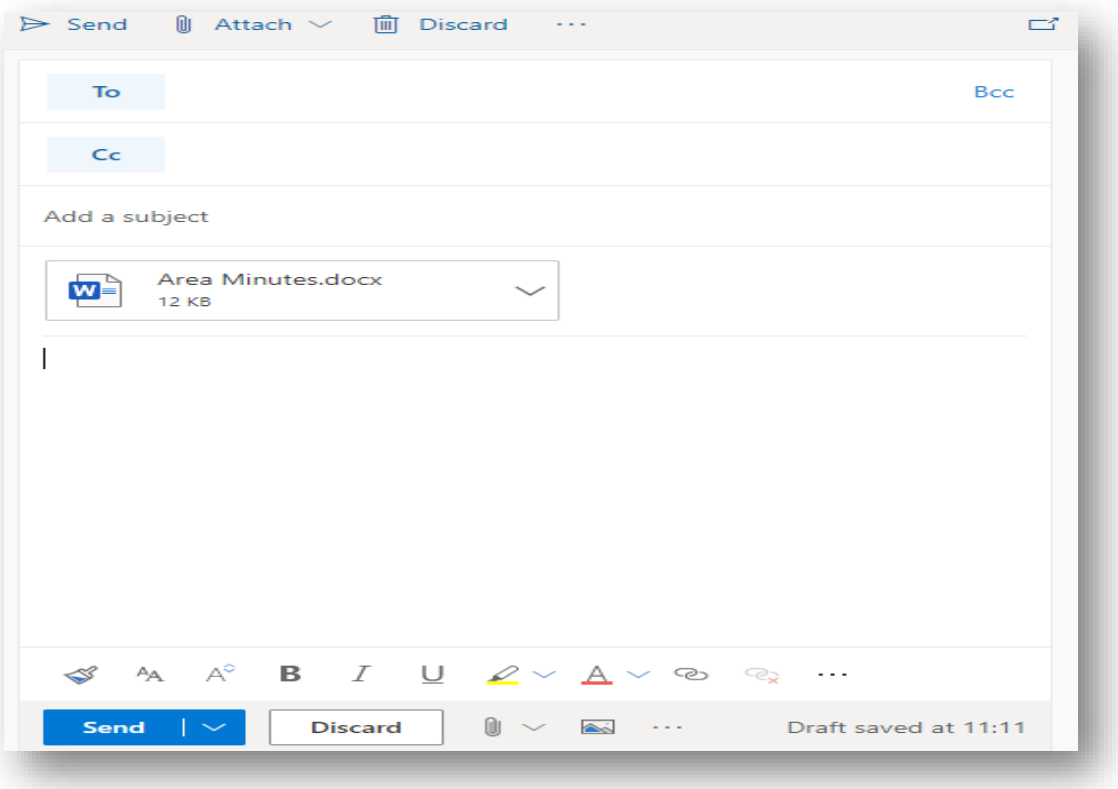
➢ To send a NEW Email, click on 'New message'



- Enter the email address you want to send to in the 'To' box and do not forget to 'Add a subject'. This is helpful when emailing i.e., gso@alcoholicsanonymous.ie.

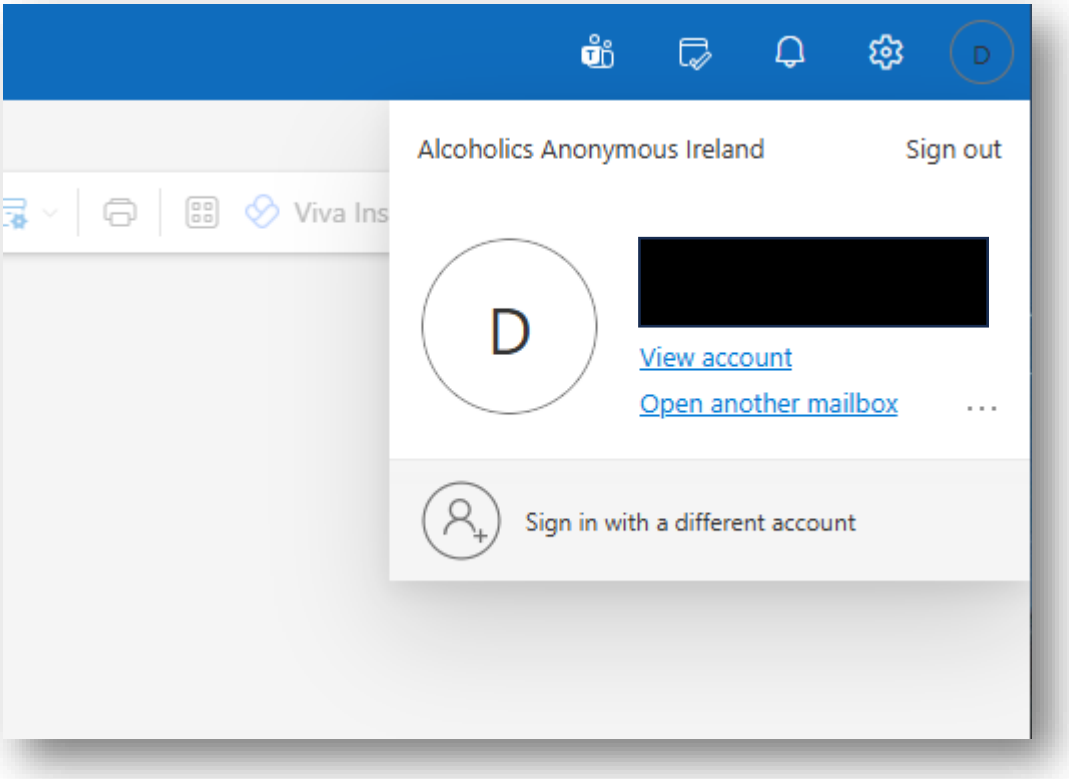
- *In the interest of GDPR and Data Protection, personal email addresses should not be included on emails to other recipients.

- To attach a document i.e., Area Minutes, click on the 'Attach' option at the top (this shows a paperclip image), and select 'Browse this computer'. You can find the document that you have already saved on your device and when you click on it, it will add itself to your email:



- Type the message into the blank 'body' of the email and press 'Send'

- To sign out of the email account, click on the circle on the top right of the email account and 'Sign out':



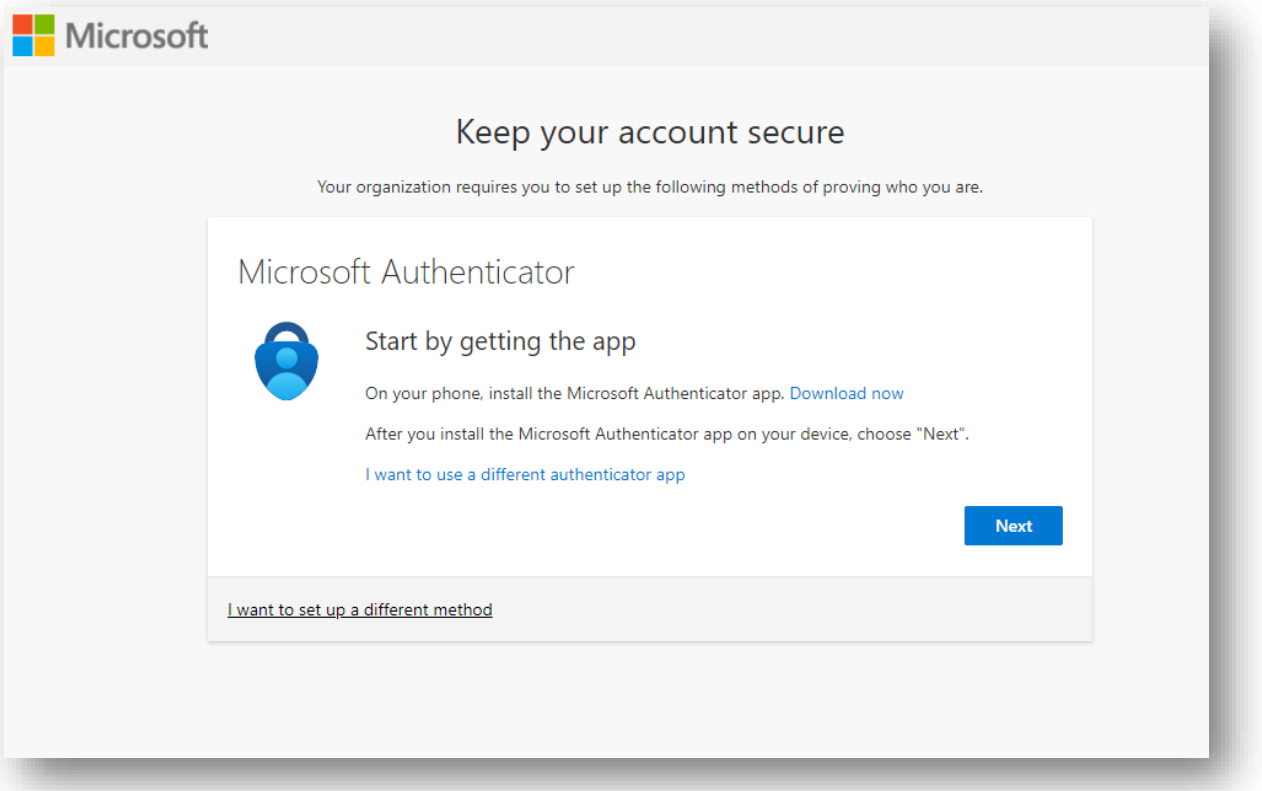
Multi-Factor Authentication

Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their mobile phone or alternative email address.

If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate.

Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
- An alternative email address.



Available verification methods

When users sign in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. Users can access My Profile to edit or add verification methods.

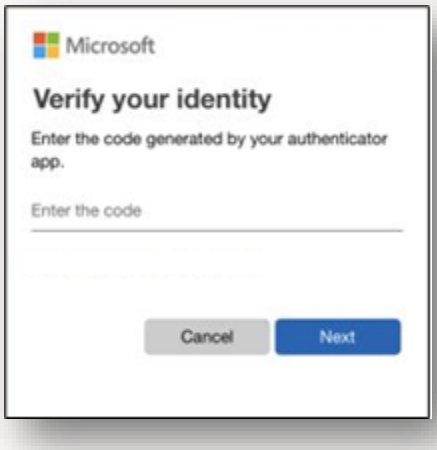
The following additional forms of verification can be used with Azure AD Multi-Factor Authentication:

- Microsoft Authenticator
- Authenticator Lite (in Outlook)
- Windows Hello for Business
- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call

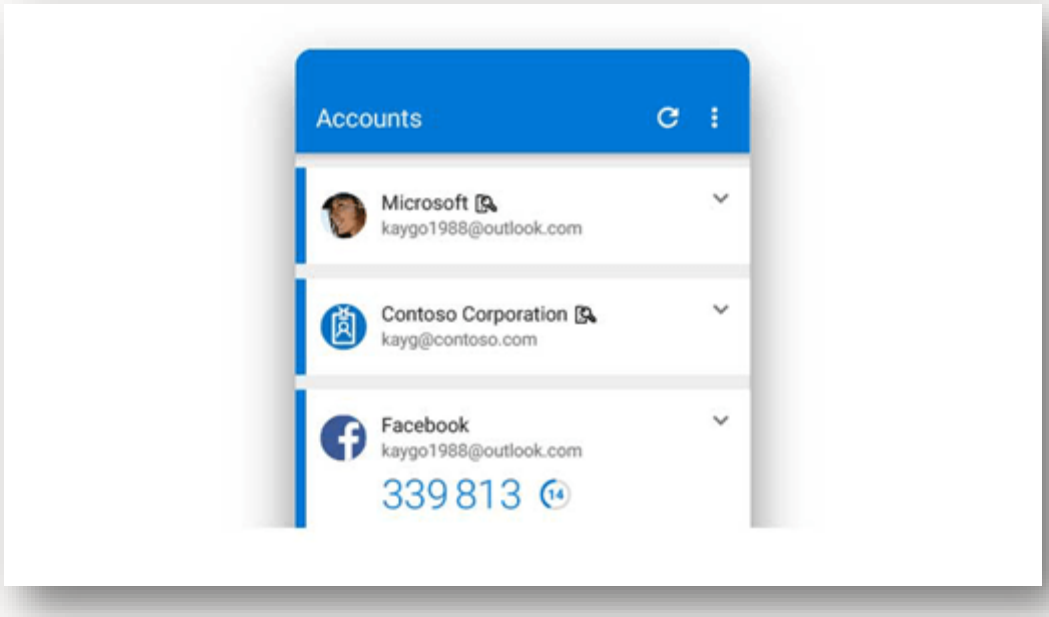
How does multifactor authentication work?

Let's say you're going to sign into your work or school account, and you enter your username and password. If that's all you need then anybody who knows your username and password can sign in as you from anywhere in the world!

But if you have multifactor authentication enabled, things get more interesting. The first time you sign in on a device or app you enter your username and password as usual, then you get prompted to enter your second factor to verify your identity.



Perhaps you're using the free Microsoft Authenticator app as your second factor. You open the app on your smartphone, it shows you a unique, dynamically created 6-digit number that you type into the site and you're in.



If somebody else tries to sign in as you, however, they'll enter your username and password, and when they get prompted for that second factor they're stuck! Unless they have YOUR smartphone, they have no way of getting that 6-digit number to enter. And the 6-digit number in Microsoft Authenticator changes every 30 seconds, so even if they knew the number you used to sign in yesterday, they're still locked out.

- **Get the free Microsoft Authenticator app**
- Microsoft Authenticator can be used not only for your Microsoft, work, or school accounts, you can also use it to secure your Facebook, Twitter, Google, Amazon, and many other kinds of accounts. It's free on iOS or Android.

Important things to know

You won't have to do the second step very often. Some people worry that multifactor authentication is going to be really inconvenient, but generally it's only used the first time you sign into an app or device, or the first time you sign in after changing your password. After that you'll just need your primary factor, usually a password, like you do now.

The extra security comes from the fact that somebody trying to break into your account is probably not using your device, so they'll need to have that second factor to get in.