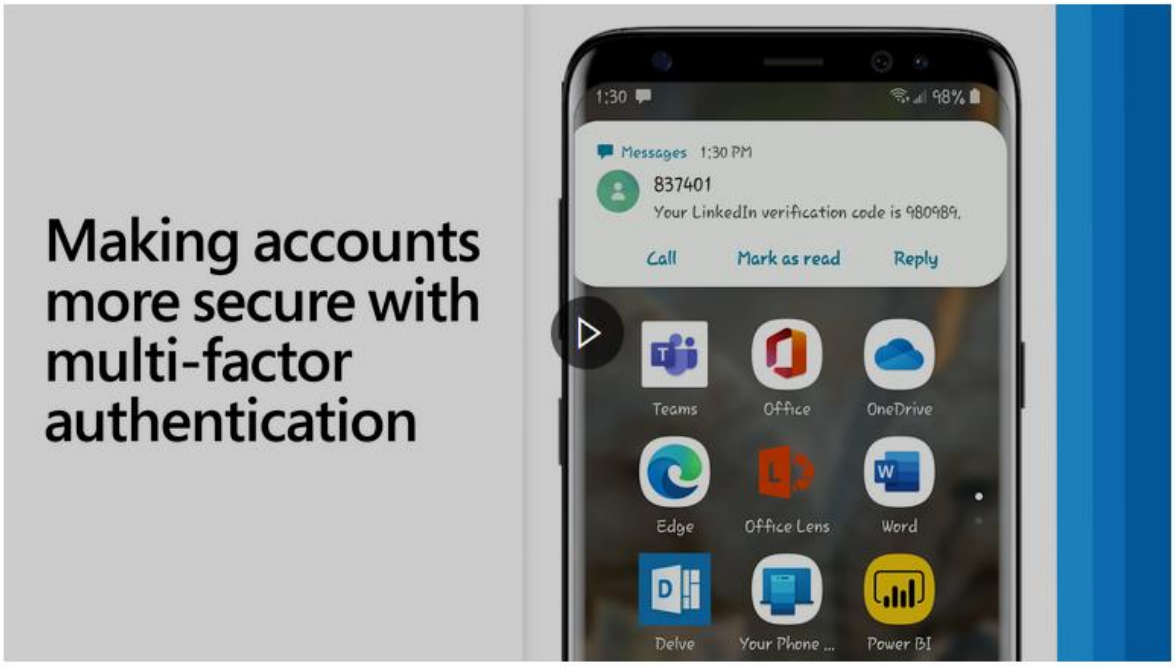
What is: Multifactor Authentication

Security

When you sign into your online accounts - a process we call "authentication" - you're proving to the service that you are who you say you are. Traditionally that's been done with a username and a password. Unfortunately, that's not a very good way to do it. Usernames are often easy to discover; sometimes they're just your email address. Since passwords can be hard to remember, people tend to pick simple ones, or use the same password at many different sites.

That's why almost all online services - banks, social media, shopping and yes, Microsoft 365 too - have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multifactor Authentication" but the good ones all operate off the same principle. When you sign into the account for the first time on a new device or app (like a web browser) you need more than just the username and password. You need a second thing - what we call a second "factor" - to prove who you are.



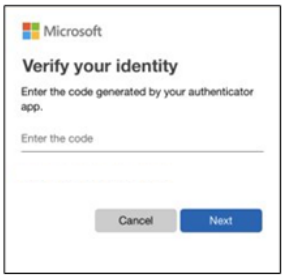
A factor in authentication is a way of confirming your identity when you try to sign in. For example, a password is one kind of factor, it's a thing you know. The three most common kinds of factors are:

- Something you know - Like a password, or a memorized PIN.
- Something you have - Like a smartphone, or a secure USB key.
- Something you are - Like a fingerprint, or facial recognition.

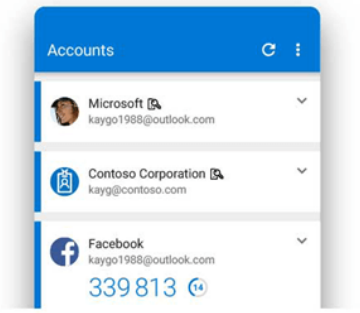
How does multifactor authentication work?

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. Learn more and get it here.

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.

Multifactor authentication is not just for work or school. Almost every online service from your bank, to your personal email, to your social media accounts supports adding a second step of authentication and you should go into the account settings for those services and turn that on.

- Click here to turn two-step verification on for your personal Microsoft Account
- Click here if you're an IT Pro or administrator and you want to know how to enable multifactor authentication for Microsoft 365

Compromised passwords are one of the most common ways that bad guys can get at your data, your identity, or your money. Using multifactor authentication is one of the easiest ways to make it a lot harder for them.

Source

https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661