# Office 365 – security and overview

**Authentication to gain access to email and the portal**

**What is 2 FA – Terminology**

Users must go through two layers of security before being granted access to an account or system. 2FA increases the safety of online accounts by requiring two types of information from the user, such as a password and PIN. 2FA is designed to prevent unauthorized users from gaining access to an account with nothing more than a stolen password. Users may be at greater risk of compromised passwords than they realize, particularly if they use the same password on more than one device or website.

This requires users to set one of 3 different methods to authenticate. When you first login it will ask for a 6 digit pin this is so that it can install a certificate on the device so when you login in next time it knows you and the device are linked. If you then login from a device at home it will do the same for the first time and install a certificate, then the certificate will expire after 60 days, it will then ask you to reconfirm the pin. It works the same way as telephone banking.

# IMPORTANT

If you receive a text or call from Microsoft and you have

1. not opened outlook “Email”,
2. its within 56 days of you already entering a code,
3. there is no login prompt on your screen asking for a code,

this means that its possible someone else trying to login from elsewhere and is asking you to let them in. Ignore the call or the text in these instances.

**Which method should I use to authenticate**

|  |  |  |
| --- | --- | --- |
| User type | Authentication method | Restrictions |
| Sit at the same desk every day | Use deskphone method | If we go into Disaster Mode and have to work remotely there is a chance that the authenticator will ask you to authenticate and ring the desk phone and you will not be there to approve access. The code will not be asked for 56 days so it would be unlucky if we vacate the site during this time |
| Remote worker different sites everyday. | Use mobile text, or Microsoft authenticator app.  If you are in an area of bad reception use the app as this still proves you with a code, whereas a text may not be received | If you forget or loose your mobile you will not receive the code to enter. |
| Sit at same desk but sometimes go to other sites and I don’t have a company mobile | Use deskphone or setup Microsoft authenticator app on your mobile (it is fee) |  |
| I am a static user sit at the same desk but I want to use another computer at home to access email | Use the mobile text or app service | If at home and you setup to use the work deskphone when you try and login at home it will be ringing your desk phone to authenticate, if you use a mobile it will be on your possession |
| I share a computer, I use a hot desk machine | Use the deskphone next to the hotdesk computer | If you try to login to another machine in the office the deskphone next to the original computer you logged into will ring and this could be at the other end of the office ! |

If someone was trying to access the O365 account from a foreign device or location, a message would be sent to the users mobile and would say approve or deny access. If the user isn’t accessing O365 or didn’t login then they know its a compromise attack and click deny.

Staff who do not have company mobile can either have the app installed or text sent to their personal mobile or alternatively have an automated call to their desk phone providing them with the 6 digit pin to enter. If they do not have a company mobile it is assumed they are static desk users and therefore their desk phone is sufficient

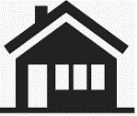
Approve or Deny foreign device

Text to mobile every time compromised



 pin code   pin code 

 60 days  60 days

**Verification code from mobile app**

A mobile app like the Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The mobile app option can be used whether or not the phone has a data or cellular signal.

**Call to phone**

An automated voice call is placed to the user. The user answers the call and presses **#** on the phone keypad to approve their authentication. Call to phone is a great backup method for notification or verification code from a mobile app.

**Text message to phone**

A text message that contains a verification code is sent to the user, the user is prompted to enter the verification code into the sign-in interface.