MINNESOTA STATE UNIVERSITY MOORHEAD

Information Technology

Multi-Factor Authentication

About this article

This article includes the steps involved in configuring multi-factor authentication (MFA) for Microsoft Office 365. It is intended for all MSUM students, faculty, and staff.

What's Office 365 Multi-Factor Authentication (MFA)?

In order to better protect you, your data, and our campus network from increasingly sophisticated phishing and other social engineering attacks, Minnesota State University Moorhead has implemented an Office 365 (O365) security feature called Multi Factor Authentication (MFA). Your password alone (which someone could have stolen from you) will not be enough to prove your true identity when you log into O365. In addition to your username and password, O365 will ask for more proof before it lets you in the door. Think of it as a special knock or a secret handshake. O365 will not request your special handshake every time you log in from your office or other "trusted" computers, only when it detects something has changed or your account is being used someplace new.

MFA Options

You can choose from several MFA options and can use different options in different situations, depending on what's most convenient for you. The type of handshake or knock you choose can have an impact on how and where your account can be used, so we want you to be well-informed before you decide what is best for you.

Option 1: Smartphone Notification App

This is generally the easiest option for people who have a smartphone and is presented as **"Notify me through app"**. When the system needs additional assurance to verify your password was really entered by you, a number will display on the on-line service's login page and you will receive an Authenticator application notification on your cellular device. You will be required to enter the number shown on the login page into the Authenticator application to approve the login request. Once you enter the matching number and approve the request, you will be logged into your account. This application is easy to configure, easy to monitor and consumes very little data and battery. The upside of this option is that it makes your O365 account accessible to you wherever you bring your smartphone. The only downside to this option is that not everyone has a smartphone or is willing to use their smartphone for anything work-related. This is why there are other options.

Option 2: Cell Phone Text

This is the next easiest way for people who either don't have a smartphone or don't want the overhead of the application to verify their identify when the need arises. The **"text a code to my phone"** option will simply text you a seemingly random 6-digit number that you will be prompted to enter after your password. When you enter the correct numbers it sent, the system is relatively certain it is you and not a hacker with a stolen password and will let you in. This option is again very easy to set up, requires very little configuration, and relies on only basic texting service. While it isn't quite as easy as the notification app, it does provide people with the ability to access their account while not at work or on a work laptop, which can be important to some people. While not required,

leveraging a personal cellular device does provide you the most flexibility in accessing your work account when not at work.

Option 3: Smartphone Code Generating App
Similar to the 6-digit codes sent via text to your cell phone, the code generator app is a way to verify your identity, but without the data requirements of Option 1 or even the cellular text requirement of Option 2. It will work in the basement of a fallout shelter. Though not as easy as pressing Y or N, it does provide users a good option if they are frequently in a location where cellular service is poor, but they have Internet access through a different provider.

Option 4: Call My Personal Phone
This option is for anyone who wants to be able to access their O365 account from off-campus but doesn't have a smartphone or cell phone capable of receiving a text. This option works on any home phone or basic cell phone. When the system doesn't recognize you logging in, you will receive a phone call with an automated voice asking you to approve this logon attempt. If you weren't expecting this call you would obviously not approve it, but if you had just typed your password into your home computer you would press a number to finish the logon process. This isn't an ideal option for most people because it is much slower and less mobile that the others, but it can be very helpful in a pinch.

Option 5: Call My Office Phone
Just like Option 4, O365 has your university office phone number pre-populated and can call you to confirm your logon. If you forgot your cell phone at home, or dropped it in the river over the weekend, this option is a fail-safe that will allow you to get logged in when you return on Monday morning. Again, this option can be cumbersome and will not facilitate access on a home computer or anywhere that isn't within arm's reach of your work desk phone, but it does ensure that you can get your work done on your work computer when you are at work.

Setup Trust Account

If you see other choices you may have set something up previously. Office 365 personal or security and privacy settings contain some of this info so it may have been added previously.

1. Go to https://aka.ms/mfasetup
2. Sign into your account and configure MFA

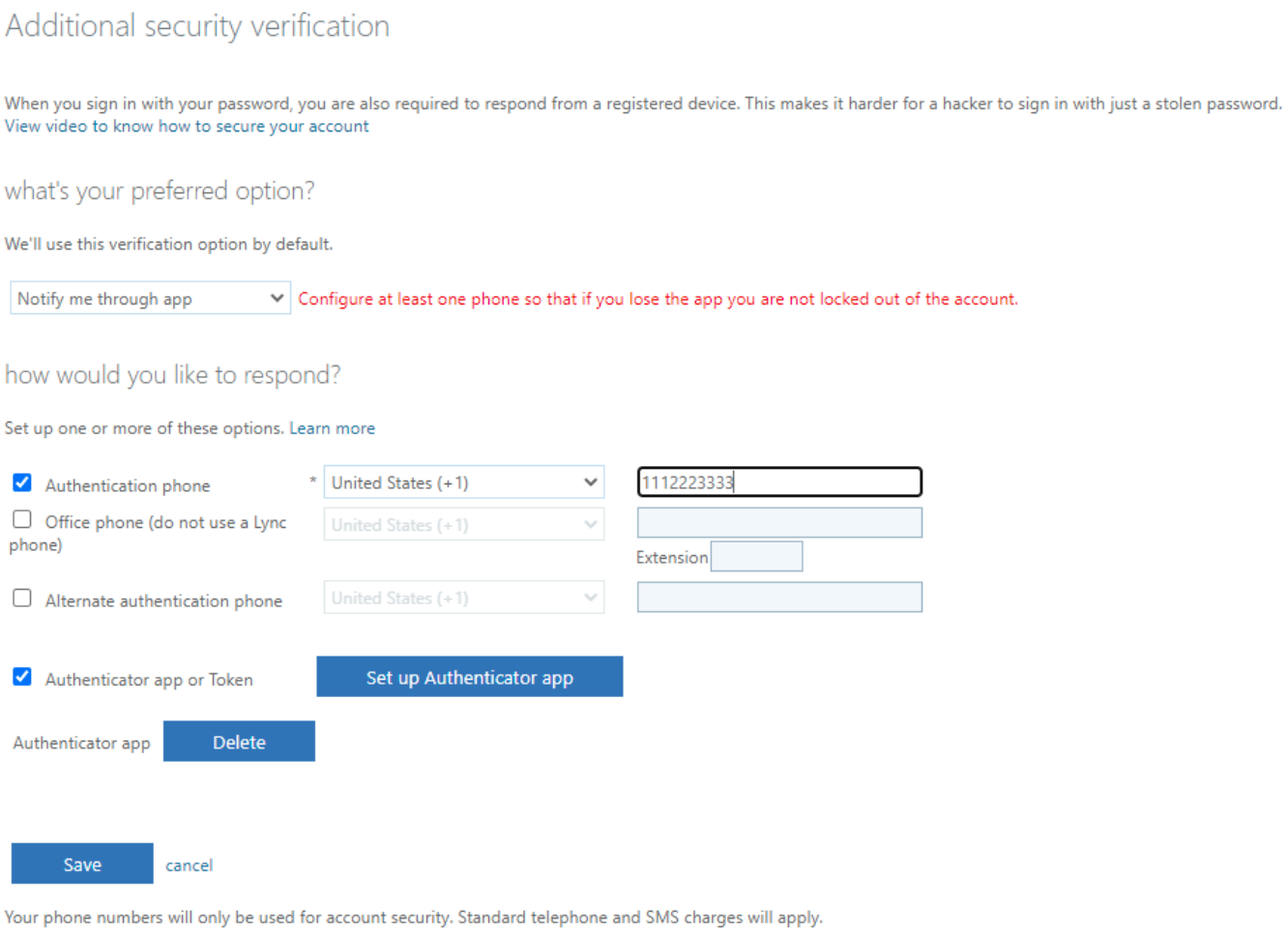
Our Recommendations

Provided you have a smart phone, we highly recommend using the Notify Me through app using the Microsoft Authenticator app as your #1 choice; followed by a backup text. This notification process makes it super easy when your account is finally tripped.

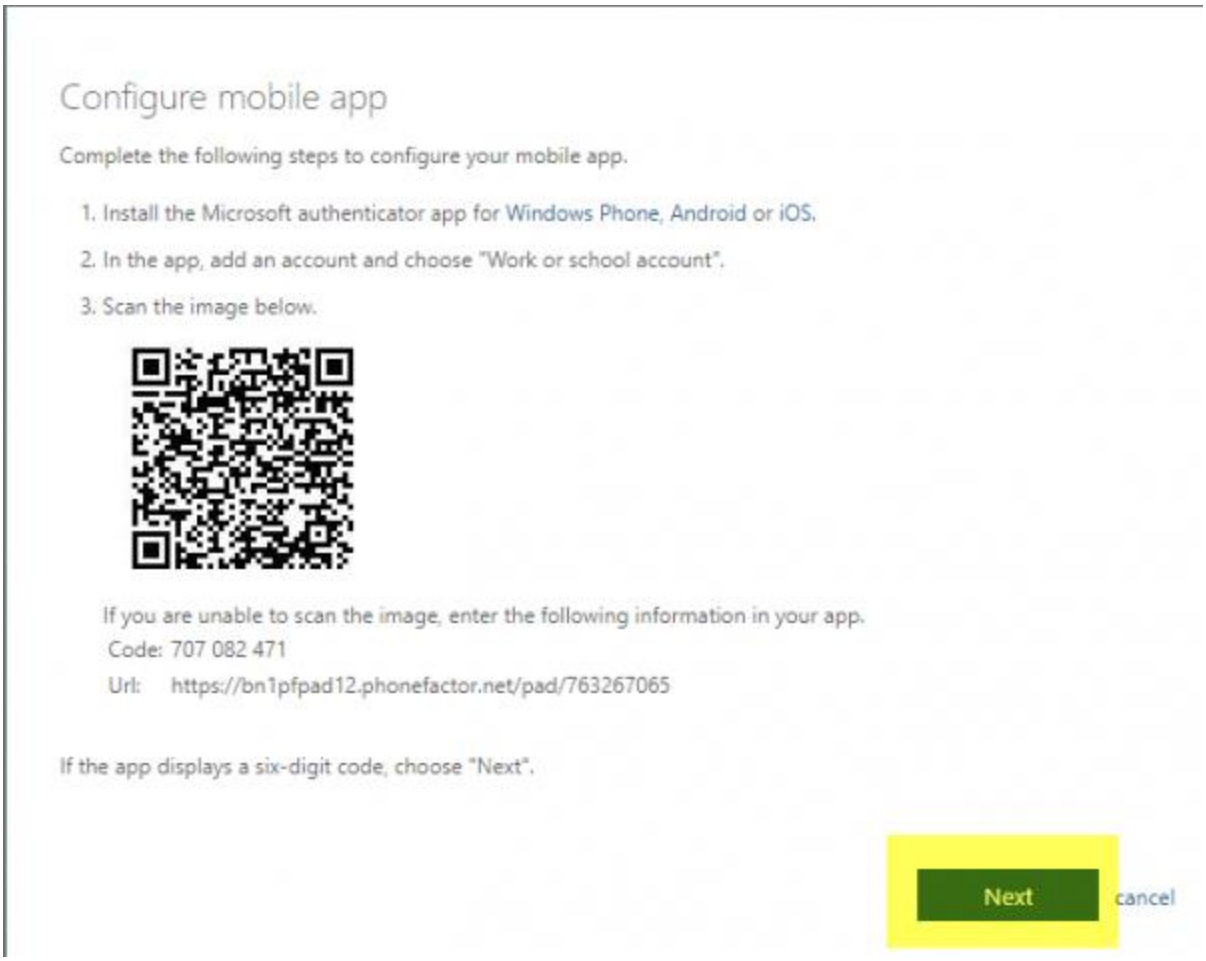
A regular cell phone without smart capabilities use text.

If no cell phone your options are to use your office phone or home phone if working remotely.

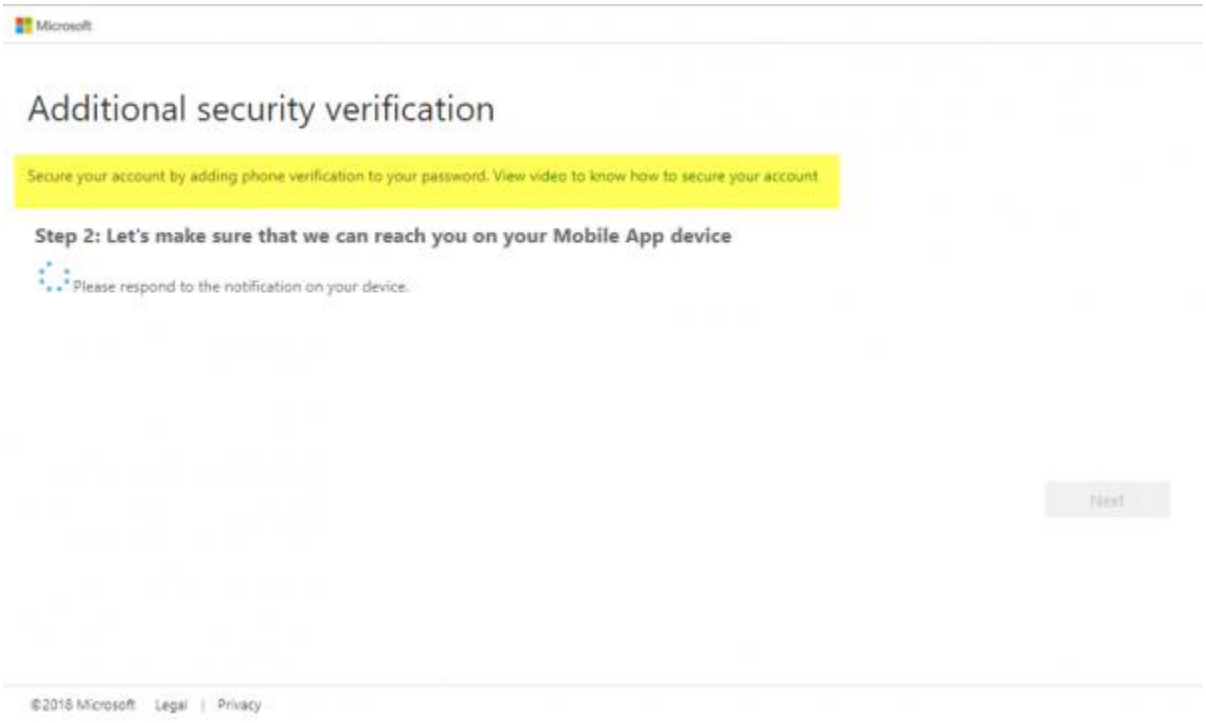
Setup Process



- Click on Setup Authenticator app
- On the next screen read through the instructions, install the app and click on Next



- A message will be sent to you phone



- When you get the verification message click on Approve

Activation

- Activation consists of scheduling your account to have Multifactor
- You will get a popup - Within an hour you will need to validate your account
- Type in your StarID password once and click approve (or enter text option)

You can also contact the MSUM IT Helpdesk by email, phone, or stopping by the office.

MSUM IT Helpdesk
218.477.2603
support@mnstate.edu
Livingston Lord Library LI122