**What is it?** Multi-Factor Authentication (MFA) requires the user to provide two or more pieces of evidence to verify their identity to gain access to a digital resource. It is used to protect against hackers by ensuring the digital users are who they say they are. MFA is widely used by banking institutions, Social Media pages, and other sites where Personal Private Information (PPI) is stored. A fingerprint, iris or face scans, text messages, phone calls, and codes can all be forms of MFA that can be used to validate your identity.

**Why do I need it?** Online security is everyone’s responsibility. With the rise in phishing attempts, MFA keeps State of New Mexico resources secure by ensuring the intended user is the one accessing the resource.

**Will this make my job harder?** While MFA does take a moment to set up, once that is completed, there is only one extra step when logging in. Re-authentication is NOT required at every log in, but it is required when the user’s environment has changed, e.g., when switching places of work or networks, when adding a device, or when a password is changed.

**How do I set it up?** The Microsoft (MS) Authenticator application is the preferred method, as it turns your phone into a key to prove your identity and unlock your account. You can get the MS Authenticator app by downloading it to your smart device from[**Google Play**](https://go.microsoft.com/fwlink/p/?LinkID=2168850&clcid=0x409&culture=en-us&country=US)or[**Apple App Store**](https://go.microsoft.com/fwlink/p/?LinkID=2168643&clcid=0x409&culture=en-us&country=US)**.** Alternatively, text messages (SMS) and phone calls can be used for those who do not or cannot use the MS Authenticator app (described below).

**Text

Description automatically generated with medium confidence**

**The following example is for an Android device; Apple devices will be similar.**

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated



Graphical user interface, application

Description automatically generated

**FAQ**

**What if I don’t have my phone to authorize my identity?** You can always select *Use a password instead* on the sign-in page to switch back to using your password and initiate a different method of MFA.

**What if I already use the MS Authenticator App?** If you already use the MS Authenticator app for other services, please add your @state.nm.us email address to the account. Select the work or school account.

Graphical user interface, text, application

Description automatically generated

|  |
| --- |
| **Questions?** [Contact the Email Administrative Team](mailto:EnterpriseEmailAdministrators@state.nm.us) for assistance.  For more information regarding the Authenticator app, [click here](https://www.microsoft.com/en-us/security/mobile-authenticator-app). |

*Alternate Instructions - Authenticator Setup (After User is MFA-enabled)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. After downloading and opening Authenticator, tap **Add account** 2. Tap **Work or school account** |  |  | | | |
| 1. Tap **Sign in** 2. Enter your State of NM email address and tap **Next** |  | | | |  |
| 1. Enter your State of NM email password and tap **Sign in** 2. Your phone will receive a code via text message. When ready, enter and tap **Verify** |  | | |  | |
| 1. Tap **Continue** 2. Tap **Register** |  | |  | | |
| 1. Tap **Finish** 2. View your account in the list shown in Authenticator.   MFA is now enabled for your account. |  | | | |  |

**Information for using Text Message (SMS) or Call feature for MFA.**

Graphical user interface, application

Description automatically generated



Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

|  |
| --- |
| **Questions?** [Contact the Email Administrative Team](mailto:EnterpriseEmailAdministrators@state.nm.us) for assistance. |

Informational Awareness

These data points support the need for MFA. (\*source below)

* Identity theft is an easy, low-risk/high-reward type of crime and a threat to all entities. It is the fastest-growing type of crime and is now more profitable than drug-related crimes.
* Weak or stolen user credentials are hackers' weapon of choice, used in 95% of all web application attacks.
* The number of successful breaches is up by 27.5 percent.
* Headlines tend to belong to the household-name companies, but they are not the only companies being targeted. Of all targeted attacks, 31% are aimed at entities with fewer than 250 employees.
* Anti-virus systems and advanced firewalls are necessary security elements, as are vulnerability tests. Without user authentication, however, the front door is wide open to intruders.
* Password theft is constantly evolving as hackers employ methods like keylogging, phishing, and pharming.
* Cyber criminals do more than merely steal data. Often, they destroy data, change programs or services, or use servers to transmit propaganda, spam, or malicious code.
* Employees are already accustomed to authenticating themselves in their personal lives, as providers of online services like banking, gaming, social media, and email have all adopted mobile-based tools to effectively authenticate their users when accessing their systems.

\*(hxxps://techbeacon.com/security/8-reasons-you-should-turn-multi-factor-authentication)