

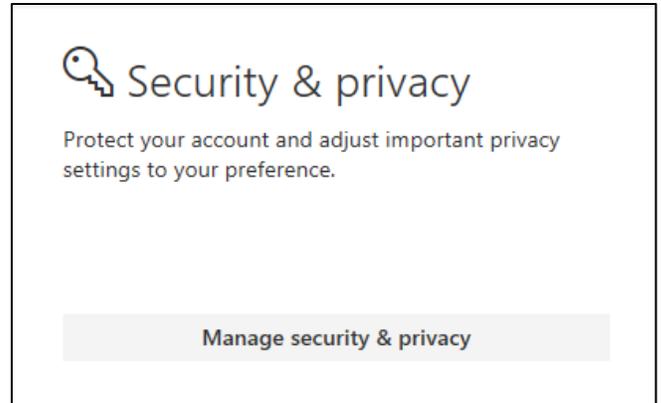


# Introduction to Multi-Factor Authentication

## What is Multi-Factor Authentication?

Multi-Factor authentication (MFA) is a security mechanism in which authentication requires the use of more than one verification method. MFA adds a second layer to the normal user id and password sign-in, it relies on two forms of authentication:

1. Something you know, like your user ID/password, and
2. Something you have, like your phone or mobile device

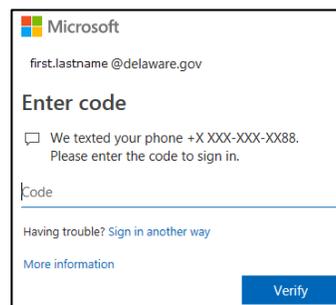
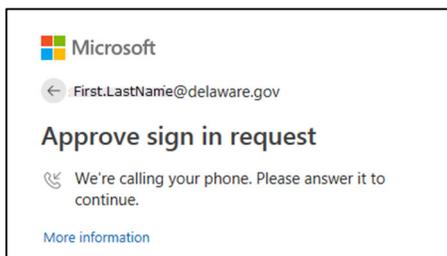


## Why use Multi-Factor Authentication

Our jobs now require a mobile and diverse environment. We are increasingly connecting by complex scenarios; e.g. moving from enterprise to personal devices, on and off the state network, using smart phones, tablets, PCs, and laptops, often on multiple platforms. Using only passwords as an authentication factor can be susceptible to brute-force and phishing attacks. Adding an additional authentication factor layer lessens our risks associated with these types of attacks. In order to protect your Office 365 account from malicious hackers, the State of Delaware is requiring all Office 365 accounts to be MFA enabled.

## MFA User Experience

Here is an example of Multi-Factor authentication. When opening an application in your web browser, you will be prompted to sign in using your existing user ID and password. The system validates your credentials and then performs the Multi-Factor Authentication (MFA) by calling or texting your phone (based on how you initialized MFA). You are directed to perform a verification task and then the application will launch.



You may be wondering how often you can expect to be prompted to enter the second factor authentication when accessing Office 365 resources.

**For desktop applications** such as Outlook and Skype for Business, you can expect MFA prompts under the following conditions:

- First-time setup
- Logging into a new device and performing first-time setup
- After 90 days of inactivity

Simply opening or closing the application on your desktop will not require you to re-authenticate with MFA

**For web-based clients**, such as Office Web apps (Outlook Web App), you can expect MFA prompts under the following conditions:

- Logging into Office 365 web-based apps such as Outlook Web App
- Closing your web browser and logging back into Office 365 web-based apps
- After 6 hours of inactivity in Outlook Web App

**For the Outlook mobile app**, you can expect MFA prompts under the following conditions:

- First-time setup on a mobile device
- Deleting and re-installing the Outlook mobile app

Note: Simply opening and closing the Outlook mobile app will not require you to re-authenticate with MFA.