Multi-Factor Authentication

Fact Sheet for Partners with P#'s

What is Multi-Factor Authentication?

Multi-factor Authentication (MFA) is a security system that requires more than one method of authentication to verify the user's identity to log into services or applications.

A user is prompted for at least two pieces of identification:

- Something you know (typically a password).
- Something you have (a trusted device that is not easily duplicated, like a cell phone or a hardware token).
- Something you are (biometrics like facial recognition or a fingerprint).

MFA is offered by many online services, including most email providers and banks.

MFA also creates a layered security defense and makes it more difficult for an unauthorized person to access a computer, network, or database.

Why do we need MFA?

Under the 2019 Statewide Information and Cyber Security Standards, MFA:

- Protects client and employee data from being compromised.
- Is essential to help safeguard access to critical systems.
- Is the most effective way to stop hacking through phishing, guessing or theft.
- Is much stronger insurance that your information is only accessible to the intended people.

What will be affected by MFA changes?

To access M365 apps in the ODHS|OHA environment (Teams, Outlook, OneDrive, OWL, etc.), you will need to provide a second authentication method.

For example, if you need to access Workday to enter time, you will need to MFA.

You will also soon be asked to use MFA to access Citrix. To access the new Citrix URL, you will enter your UPN, rather than your P#, and use the same password. Your UPN will usually be your <name>@dhsoha.oregon.gov email address. You will be provided the new URL when testing is complete and you have been scheduled.

What are the approved methods for authenticating?

There are two approved methods for partners with P#'s to authenticate:

- The Microsoft Authenticator app on your smartphone, or
- A partner purchased YubiKey.

Either method may be used by partners with P#'s to access M365 apps in the ODHS|OHA environment, Workday, and soon Citrix.

If you are blocked from registering one of these methods, please contact the OIS Service Desk (503-945-5623) when you are ready to register to get temporary access to the registration page.

How do I set up an authentication method?

Microsoft Authenticator App

The Microsoft Authenticator app instructions help you register an iPhone, but the process isn't much different for an Android device.

The following documents show how to register and use the Microsoft Authenticator app for MFA.

Register for MFA Using the MS Authenticator App

How to Use the MS Authenticator App for MFA

YubiKey

For YubiKeys, you will need to install the Yubico Authenticator app on any computer you will be using to access M365 apps, Workday, or Citrix in the ODHS|OHA environment. Once the Yubico Authenticator app is installed, you will then need to register your YubiKey against your account.

Download the Yubico Authenticator app here: https://www.yubico.com/products/yubico-authenticator/

The following documents how to register and use a YubiKey for MFA.

Register for MFA Using a YubiKey

How to Use a YubiKey for MFA

Video for Registration/Use of YubiKeys