Multi-Factor Authentication FAQ's

20210325_V1.0

1. What is Multi-Factor Authentication (MFA)?

   A = Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

2. Why is MFA important?

   A = The main benefit of MFA is it will enhance the state of Alaska's security by requiring our staff to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

3. Can Alaska state employees use our personal cell/mobile devices for MFA and not be subjected to seizure of the mobile device?

   A = Per Alaska statue 12.35.020 and 12.35.025, warrants may be issued for search and/ or seizure of any property, personal or work, if used in conjunction with the commission (or the intent of commission) of a criminal act. However, the use of MFA alone (without a warrant) on a personal device does not make it subject to search and seizure.

4. Will MFA on my personal cell phone disrupt configuration?

   A = If text-back or call-back MFA is used, no changes are made to your cell phone.

   If the MFA application is installed on your device, then your mobile device will utilize the application. The application is the most secure and easiest MFA method to use, and it should not disrupt your mobile phone configuration.

5. How is MFA handled with a shared mailbox accessed by more than one person?

   A = When using a correctly configured shared mailbox, employees authenticate as themselves using MFA and then access the shared mailbox. This is the same security process as accessing a shared network folder.

   It is against good security practices and state policy (ISP-178) to share passwords. Shared mailboxes that provide access to multiple employees using their own credentials are available to any group who needs them.

6. Which MFA option is the lowest impact to my personal cell/mobile device?

   A = Text-back and call-back do not require any changes to your device. Of the two, text-back is the more secure method since call-back MFA can be easily forwarded to another number.

7. Well, I'm not sure what to do. My cell phone is ancient, and I have constant space issues so I'm not sure I will be able to download an app.

   A = Use the text-back or call-back option which does not require you to install an app.

8. Does MFA only apply if the Office 365 user is using a VPN?

A = No it does not. MFA applies to all O365 applications such as email/outlook, Teams, Word, Excel, PowerPoint, etc. regardless if logged in to VPN or not.

9. Does a user need to setup MFA if they only access their state O365 applications from a State laptop/desktop?

   A = O365 MFA is required regardless of device used for work.

   A state PC or Smart Phone is recognized as a trusted device after you successfully authenticate the first time so you will not be prompted for MFA every time you run the O365 application.

10. Are there plans to implement O365 MFA to log into laptops?

   A = Yes. OIT is exploring the use of O365 MFA to login to laptops.

11. How is the requirement for MFA by end of February within DOA impacted by the availability of SOA-provided or subsidized smart phones?

   A = As indicated in the announcement on 2/5/21 a state provided/subsidized device is not required.

   Employees can setup call-back MFA to their work phone number and answer it remotely with a Cisco soft phone installed on their work laptop.

12. I have no work cell phone, no work desk phone, no work soft phone, or I use a shared work phone in the office… how do I access work email after Feb?

   A = MFA is required for all DOA staff. If you are uncomfortable with the option of using a personal cell phone with call-back or text-back MFA please consult your administration team for a solution.

13. MFA asks for multiple authentications whenever I change from Teams to Outlook and back to Teams. Is this just a bug or will this always happen?

   A = That is a bug on your PC. Submit an incident ticket with AlaskaNow and it will be worked by OIT. Correctly functioning work PCs and smart phones only prompt you once for MFA each time you change your password (every 90 days).

   Non-work/personal devices may prompt you more than once (i.e. every time when accessing email through a web browser).

14. Can a report be provided to agencies for users who have not gone through the steps to activate MFA?

   A = Yes, management can receive reports for who has and has not enabled O365 MFA.