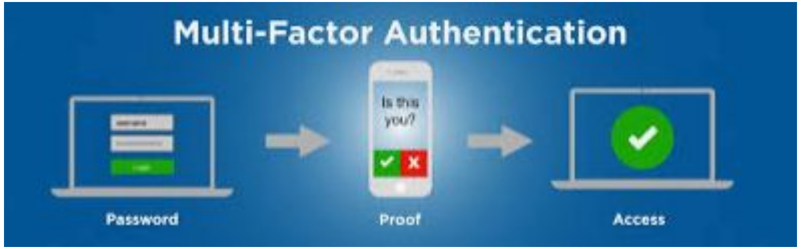
Overview of MFA best practice

V1.0

LOCAL DIGITAL Cyber

Objective

Outline guidance and approach to best practice design features for the use of Multi Factor Authentication (MFA) options for use within Local Authority Information Systems.



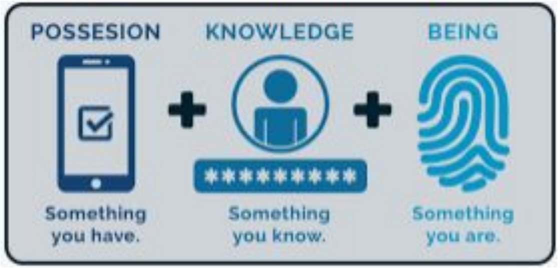
MFA helps prevent attackers from accessing your systems even if they obtain your username and password.
For example, if you create a multi-layered mechanism, an unauthorised user would have to defeat all layers to gain access

How does Multi Factor Authentication work ?

Multi Factor Authentication works on the principle of requiring more than one of these items:

- Something you have (such an authentication application on your phone)
- Something you know (such as your username and password)
- Something you are (such as fingerprint or iris recognition)

For remote system access MFA is usually built up of the first two items, but the authentication applications can also require the third item.



LOCAL DIGITAL Cyber

Best practices

Best practices for the usage of MFA are :-

- Protection of Online Administrative Accounts (Such as M365 Global Administrators)
- Protection of Internal Domain Privileged Accounts (Such as Domain Administrators, SAN Administrators, Backup Server Accounts)
- Protection of User Accounts for Remote Access
- Protection of Regular M365 User Accounts when not in ‘Whitelisted’ locations

Best practices (cont.)

Best practices for the usage of MFA are :-

- NCSC Guidance on MFA explicitly states that “All users, including administrators, should use multi-factor authentication when using Cloud and Internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data.” and “Administrators should, wherever possible, be required to use multi-factor authentication” when using any service.

Why are these practices important?

Using MFA for VPN Remote Access:

- Stops unauthorised access if a stolen username and password is used.
  A VPN is, after all, a direct link into your network.

Using MFA on M365 Global Administrator Accounts :

- A M365 Global Administrator Account is an incredibly important account, and if compromised you can find yourself locked out of your entire organisation. It should be treated as ‘The Keys to the Kingdom’ and protected with an extremely secure password, and **at least** one other form of Authentication.

Why are these practices important? (cont.)

Using MFA on On Premise Privileged User Accounts:

- These accounts are extremely important and unauthorised usage can result in significant damage to internal systems. As with other items listed, requiring additional authentication will help protect the accounts even if a valid username and password are used to access key services such as Domain Controllers, Storage Systems, etc.

Using MFA on M365 User Accounts when not onsite:

- By using a specific type of Conditional Access Policy you can require a user to use MFA when accessing their emails or Microsoft 365 located files when they are not connected to your local network, or trusted locations. This will reduce user impact by allowing them to connect with just usernames and passwords when working internally.

How to implement MFA

- For Microsoft 365 Accounts the most common implementation model is to use the Microsoft Authenticator App on a users Mobile Device.
  - This application is Free, and is designed to be integrated with M365
- For On Premise Domain accounts (privileged or not) you can use any number of MFA systems, some are Free, others are chargeable. Suitability should be assessed before selecting one.
  - Options include but are not limited to Microsoft Authenticator App, Google Authenticator App, Cisco Duo, RSA.
- For Standalone Systems check with the system manufacturer for compatibility with MFA Solutions.

How to implement MFA (cont.)

- Overview:
  https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authentication
- On Premise Options (No Integration with Azure AD)
  - Manageengine ADSelfService Plus:
    https://www.manageengine.com/products/self-service-password/windows-logon-two-factor-authentication.html?lhs
  - Cisco Duo:
    https://duo.com/blog/protecting-windows-servers-and-remote-desktops-with-duo
- Where Active Directory is Integrated into Azure AD (M365):
  - Azure MFA
    https://docs.microsoft.com/en-GB/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

Final considerations*:

- You will need to consider how administrators can gain access to the service if multi-factor authentication is unavailable. This could be caused by a service configuration or the loss of an authentication token.
- Creating an emergency ('break glass') account would give you the capability to log in to a server which has administrative accounts protected by MFA in the event of an MFA service failure. These accounts should have hyper-complex passwords and known only to a small number of high level administrators, ideally in a Password 'Safe' product, so the passwords are not easily viewed.
- Accounts such as an emergency or 'break glass' accounts that use a single authentication factor should be the subject of increased protective monitoring so that its misuse can be easily detected.

* https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber