Supplemental Guidance on Passwords and the use of Password Managers

July 22, 2021
Version 1.0

Revision History

Date	Action	Notes	Approved by
7/22/2021	Initial Draft		Chip Stewart

Contents

Introduction

Validating the identity of users is a keystone of security. The use of memorized secrets continues to be the primary mechanism to validate the identity of a user. Memorized secrets can take many forms, including:

- Passwords
- Passphrases
- Passcodes
- PINs

Additional corroboration of a user identity is achieved through multi-factor authentication, which uses two or more "authentication factors" in the transaction. These factors are:

- Something you know (e.g., a password)
- Something you have (e.g., a cell phone that receives a text message)
- Something you are (e.g., a biometric authenticator, such as a fingerprint)

As users interact with a growing number of systems, they are required to remember an ever-growing list of passwords. This frequently incentivises these users to engage in poor password management practices. For these reasons, DoIT is publishing guidelines to help users balance security and usability.

Key Takeaways

- Maryland uses the guidance from NIST to set the requirements for passwords, but must also meet certain regulatory requirements (e.g., IRS Pub 1075)..
- Password management tools can provide a balance between security and usability
- Multi-factor authentication, when available and optional, should be used

General Guidance

Choosing a secure password:

There are several guidelines for ensuring that the password you select is secure and appropriate.

1. Length is the predominant factor in determining password strength (i.e., longer is better)
2. Use a mixture of uppercase and lowercase letters, numbers, and special characters
3. Do not use pattern-based passwords that would be easy for someone to guess (e.g., SpringPassword2021 followed by SummerPassword2021)
4. Don't use the same password on more than one site, or derivations of the same password across sites (e.g., TargetPassword2021 and WalmartPassword2021), as described in control IA-5 of the Maryland IT Security Manual.

These are best summarized as "Make it long", "Make is complex", "Make it unique", and "Make it easy for you to remember but hard to guess."

Protecting your passwords:

Every day, websites are compromised, and password databases are stolen. In many cases, the passwords are not hashed to protect them from disclosure. Hashing is a one-way cryptographic function that converts plaintext into a value. For example, the password "ThisIsMyMostSecretP@55w0rd!"

would become “953331DC325BF66C963E157CF029E233” when hashed using the MD5 algorithm. When a website compromise occurs and plaintext passwords are stolen, cybercriminals will use them in combination with other user identity information to perform credential stuffing attacks.

Some web browsers and other tools will use these stolen password lists to identify passwords on these compromised password corpuses, and will display a warning message that your credentials were compromised. If you see this message, you need to change that password.

For passwords on systems used for work purposes:

When accessing systems that are used for State business purposes, there are several key considerations for how to handle this sensitive information.

Users must:

- Take reasonable measures to ensure that their passwords are secured
- Notify the security team and system owner if they believe their password has been compromised
- Follow the directives of the system owner for password composition and changes

Users should:

- Consider the use of a password manager or password vault for storing passwords
- Choose a unique password for every site
- Ensure that the password is adequately complex
- Use a password vault or privileged access management tool for administrative login activities
- Ensure that their credentials are transmitted over secure connections (e.g., using HTTPS in a web browser)
- Utilize multi-factor authentication if available, preferably with an authenticator app or hardware key

Users must not:

- Use any password that is currently or previously used on a Maryland State System
- Disclose their password to anyone, excluding certain unusual circumstances
    - Your Agency Chief Information Security Officer (A-CISO) can help you better understand these situations
- Disclose shared administrative password with anyone unless authorized by the system owner

Users should not:

- Use knowledge-based questions as a second-factor of authentication
- Write their password down in a location where it could be accessed by anyone
- Re-use old passwords, no matter how long ago they were used
- Select password hints with easy to guess or discover information (e.g., name of your elementary school)

If any of this information is unclear or you require additional guidance, please contact your agency cybersecurity leadership or the Maryland Security Operations Center at soc@maryland.gov.

Using a password manager:

With the ever growing number of passwords that users must remember, password managers offer a reasonable balance between security and usability when properly configured. There are several important considerations when using a password manager to ensure that adequate protection is provided.

1. Ensure that the master-password is unique
2. Select a strong master-password for access to your password manager, and utilize a second factor if you can reasonably do so
3. Consider purchasing hardware security key for additional protection, or use a key-file
4. Select a passphrase that is easy to type, especially on a cellphone keyboard since you will be typing this passphrase many times throughout the day/week.
5. Do not mix personal passwords, user-level work passwords, and administrative credentials
6. Maintain a backup of your password database in a safe location
7. If your password manager is compromised, all of your passwords must be changed
8. Do not use well-known lyrics or phrases such as “To be or not to be” as a starting point
9. Do not forget your master password. You will have to reset the passwords on all sites/areas you used the password manager to store. It is very important to remember your “master” password

DoIT authorizes the use of KeePassXC as a password manager, provided the conditions of this guidance are met.

1. **Enable -** Check for updates at application startup once per week
2. **Enable -** Clear Clipboard after 10 seconds
3. **Enable -** Clear Search Query after 5 minutes
4. **Enable -** Hide Passwords in the entry preview panel
5. **Disable -** Enable Browser Integration
6. When generating a password, use at least uppercase characters, lowercase letters, and numbers. Use special characters if supported by the site.
7. Select a maximum supported password length
8. Do not store second-factor information within the application

Definitions

1. **MUST** - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. **MAY** - This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)