SECURE YOUR ACCOUNTS AND DEVICES WITH MULTI-FACTOR AUTHENTICATION

JUNE 2020

ITSAP.30.030

Organizations and individuals can benefit from using multi-factor authentication (MFA) to secure devices and accounts. With MFA enabled, **two or more** different authentication factors are needed to unlock a device or sign in to an account. Whether accessing email, cloud storage, or online banking services, MFA provides an extra layer of security from cyber attacks like credential stuffing. In credential stuffing, hackers use previously stolen credentials from one website, hoping that you have reused these credentials. If not already doing so, we recommend that you and your organization use MFA where possible to protect high-value business services and data from threat actors.

WHAT ARE AUTHENTICATION FACTORS?

MFA uses combinations of the following factors to authenticate a user:

- **Something you know:** Typically, your passphrase, password, or PIN. This factor can be easily compromised, which is why we strongly recommend adding another factor when possible.
- **Something you have:** This factor can include a hard token (e.g. USB key or access card) or a soft token (e.g. an authenticator App or SMS message).
- **Something you are:** This factor relies on a unique biometric characteristic (e.g. fingerprints, retina, or iris scan).

IS TWO-FACTOR AUTHENTICATION THE SAME AS MFA?

Two-factor authentication (2FA) is a type of MFA and is validated by using a combination of **two different** authentication factors to access a device or system.

WHAT ABOUT TWO-STEP VERIFICATION?

Two-step verification is a process requiring two authentication methods, which are applied one after the other. Unlike two-factor authentication, two-step verification can be of **the same factor type** (e.g. two passwords, two physical keys, or two biometrics). Sometimes two-step verification is known as two-step authentication.

WHAT ARE THE BEST FACTORS TO USE?

Your organization needs to protect its networks, systems, and information. It also needs to ensure that its employees can use systems and access the information required to carry out their job functions. Therefore, the best MFA solution varies for each organization. For example, if your organization does not allow USB keys, then you may not implement a hard token. Instead, you could use a passphrase and a biometric.

Your organization needs to consider which user authentication policies best meet its business and security requirements. And it needs to communicate its MFA approach to all users.

When MFA is implemented, using combinations of any of these authentication factors, your organization is improving its overall cyber security posture.

WHAT ELSE SHOULD BE CONSIDERED WHEN USING MFA?

MFA options on a device or an account can be difficult to find. Often, MFA options are hidden under a service's advanced settings.

Your organization needs a clear recovery plan for lost or compromised authentication factors. For example, if a user misplaces a token, they lose account access. Therefore, users should have access to spare hard tokens that are distributed by a help desk. If that back-up token is used, then a new back-up should take its place in a safe or at the help desk.

When considering the acquisition or renewal of services for your organization, you should look at what MFA options are available for those services. If MFA options are not available, you should encourage employees to **take extra care** when creating passphrases or passwords. See *ITSAP.30.32 Best Practices for Passphrases and Passwords* for additional guidance.

With MFA, you can use a shorter password because the extra authentication adds another layer of protection. However, we recommend that you use a passphrase or a password that is at least 6-8 characters in length.

If you have highly sensitive data on a device or an account, consider using three authentication factors (including one biometric). Keep in mind that although your biometrics are unique to you, threat actors can still mimic, copy, or impersonate them.

The cost and effort required to implement MFA can be high. However, if your organization is compromised, the cost and effort of recuperating from the attack could be higher.

ANY OTHER POINTS TO REMEMBER?

Finally, you should:

- understand the value of your information and where high-value information is stored
- choose services (cloud and Internet-connected services) that offer MFA
- mandate users and administrators to use MFA for cloud and Internet-connected services, especially if sensitive data is involved
- limit the number of services that only allow single-factor authentication
- ensure passphrases or complex passwords are used, especially if only using one-factor authentication

WHERE CAN I FIND ADDITIONAL PUBLICATIONS?

The Cyber Centre has created other publications which support the functions of MFA. These publications include:

- *ITSAP.00.019 Biometrics*
- *ITSAP.30.32 Best Practices for Passphrases and Passwords*
- *ITSAP.00.001 Using Your Mobile Device Securely*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**