Secure your accounts and devices with multi-factor authentication

CANADIAN CENTRE FOR CYBER SECURITY

February 2024| 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. During credential stuffing, hackers use previously stolen credentials to access an online service, hoping that you used the same credential for other services. 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.

Authentication factors

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

- **Something you know:** Typically, your passphrase, password (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 (such as a USB key or access card) or a soft token (such as an authenticator app or SMS message).
- **Something you are:** This factor relies on a unique biometric characteristic (such as fingerprints, retina, or facial structure).

Two-factor authentication and two-step verification

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.

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**, such as, 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. It also 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.

MFA vulnerabilities

While MFA helps protect your accounts, it is not without its vulnerabilities. Threat actors have been able to bypass MFA protection using techniques such as **MFA fatigue**, **token theft** and **machine-in-the-middle** attacks (MitM).

- MFA fatigue: When a threat actor continuously bombards the user with MFA push notifications until the user accepts one.
- Token theft: Tokens allow for data to be shared between user and a system. Once stolen, the threat actor has access to protected data within the session.
- MitM: A threat actor positions themselves between the user and the platform to intercept and modify data. This is often achieved through false URL links or SMS texts which made to look like they are coming from the legitimate system.

Cat. No. D97-1/30-030-2024E-PDF ISBN 978-0-660-68431-4

Protecting against MFA vulnerabilities

There are measures you can take to mitigate vulnerabilities from MFA fatigue and phishing attacks.

Activate number matching feature of MFA configurations: This feature prompts the user to input an approved number(s) from the identity platform to successfully complete the authentication process. This can help protect you from MFA fatigue attacks.

Implement phishing-resistant MFA technology: For example, fast identity online (FIDO) based-solutions are strongly recommended to secure online accounts. To learn more consult the Cybersecurity and Infrastructure Security Agency's publication on phishing-resistant MFA.

Limit the number of MFA authentication requests per user: Leverage this feature if available on your selected MFA solution as it can help protect your account from MFA fatigue attacks.

> 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.

Considerations when using MFA

Often MFA options are hidden under a service's advanced settings and are difficult to find. Organizations should provide training or information to their users on how to locate MFA settings and how to implement them in line with their Organizations MFA policy

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 password that is a minimum of 12 characters and if possible, a passphrase that is at least 4 words and 15 characters long.

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.

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

Learn more

The Cyber Centre and its partners have created other publications which support the functions of MFA:

- Biometrics (ITSAP.00.019)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Using your mobile device securely (ITSAP.00.001)
- Using authentication guidance for information technology systems (ITSP.30.031 v3)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Authentication methods: choosing the right type (NCSC)
- Implementing number matching in MFA applications (CISA)

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada