ESSENTIAL EIGHT BEST PRACTICE GUIDE: MULTIFACTOR AUTHENTICATION

INTRODUCTION

Multifactor authentication (MFA) has grown rapidly over the past several years, with many of today's most-used apps relying on email links, one-time codes, authenticator apps, or other factors. However, implementing MFA in alignment with the Essential Eight framework can be challenging, especially for organisations attempting to achieve higher levels of the maturity model.

This whitepaper aims to demystify this process for small and medium-sized enterprises. By implementing strong MFA solutions tailored to the requirements of the Essential Eight, SMEs can achieve a higher level of security maturity and significantly reduce their risk of falling victim to a cyberattack.

WHAT IS MFA?

Multifactor authentication (MFA), also known as two-factor authentication (2FA) or two-step verification, is any system that requires users to provide multiple forms of verification before granting access to applications or data. By going beyond the traditional username/password pair, MFA makes it significantly harder for unauthorised users to gain access to an organisation's valuable assets.

An MFA solution will combine at least two of the following three categories of authentication factors:

- **Something a user knows**, such as a password, PIN, or the answer to a security question.
- **Something a user has**, such as a hardware token, a phone or other mobile device, or a smart card.
- **Something a user is**, including biometric identifiers like fingerprints, facial recognition, or iris scans – which are nearly impossible for an attacker to replicate.

Requiring authentication factors from different categories means that even if an attacker manages to obtain one factor, such as a password, they still won't gain access without obtaining the other factors.

Today's internet user often has hundreds of passwords, many of which are reused across many applications – making them vulnerable to breaches. A favourite strategy of cybercriminals is to compile and sell massive databases of stolen username/password combinations that can be chained with phishing attacks, social engineering, or password-guessing techniques to gain unauthorised access to corporate systems.

Multifactor authentication plays a crucial role in mitigating this risk by making usernames and passwords on their own much less valuable to cybercriminals.

INTERNAL, THIRD-PARTY, AND CUSTOMER MFA

Any organisation seeking to implement multifactor authentication must consider three distinct types of people who interact with its data and systems: employees, customers, and third parties such as vendors that store, process or communicate data on behalf of the organisation.

Internal MFA

Internal MFA refers to the authentication process used by your organisation's employees. At maturity level one, the Essential Eight requires staff who access internet-facing systems to use MFA. Maturity level three adds the requirement that employees use MFA when accessing any important data, regardless of whether it is internet-facing or not.

Third-Party MFA

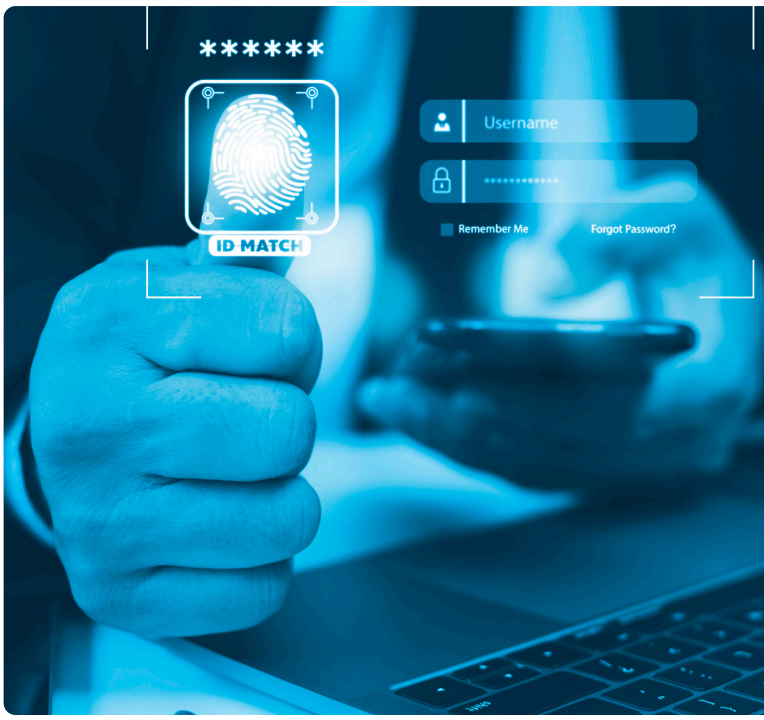
Modern businesses, especially SMEs, often use a variety of third-party services to conduct business, from SaaS accounting packages to marketing tools. Third-Party MFA refers to the authentication that your organisation's employees use when accessing these external services.

While an organisation will not have control over the MFA solution used by outside vendors, it does have control over which third-party services it chooses to use and whether its own employees leverage the MFA available.

To achieve any level of Essential Eight maturity, MFA must be used for access to all third-party services. The only exception is when MFA is not available, and the data stored, processed or communicated by the service has been analysed and classified as non-sensitive.

Customer MFA

Customer MFA refers to the authentication process your customers use to access your applications. This might be services such as online banking or e-commerce platforms, portals, reports or other digital means of connecting with customers.
The Essential Eight requires MFA to be offered to customers and enabled by default; however, it does allow customers to opt out if they choose.



TYPES OF MFA

Before implementing an MFA solution, an organisation should evaluate the most suitable options based on its unique security requirements, user groups, and business needs. There are a wide range of MFA technologies available, and each offers different levels of security and user experience.

One-Time Passcodes

One-time passcodes (OTPs) are unique, time-sensitive codes generated by a hardware device or software application. Users receive the OTP via SMS, email, or an authenticator app and must enter it during the authentication process. Due to their simplicity and ease of use, OTPs are one of the most common MFA methods in use today.

Advantages	Disadvantages
Easy to use Widely supported Cost-effective	Vulnerable to SIM swapping, phishing, and man-in-the-middle (MITM) attacks May be less accessible for users without a mobile device or internet connection

Hardware Tokens

Hardware tokens are physical devices, such as key fobs or smart cards, that require physical interaction (e.g., a swipe or button press) to approve authentication.

Advantages	Disadvantages
Resistant to phishing and MITM attacks Does not rely on internet connectivity Provides a clear separation between user credentials and MFA factors	Higher cost Risk of loss or damage Less convenient for users to carry and use

Software Tokens

Software tokens are applications installed on a user's mobile device or computer that generate OTPs or push notifications for MFA. Users must have the app installed on their device to authenticate their identity.

Advantages	Disadvantages
More convenient than hardware tokens Cost-effective Supports various authentication methods, such as push notifications and biometrics	Vulnerable to device compromise Often relies on internet connectivity May be less accessible for users without a compatible device

Biometrics

Biometric MFA uses unique physical characteristics, such as fingerprints, facial recognition, or iris scans, to verify a user's identity. It always relies on specialised hardware, such as fingerprint scanners or cameras equipped with facial recognition technology; however, most modern laptops and smartphones include facial and/or fingerprint recognition.

Advantages	Disadvantages
Highly secure Resistant to phishing and MITM attacks Offers a convenient and seamless user experience	Potentially higher cost Potential privacy concerns May be less accessible for users with disabilities or incompatible hardware

LOGGING OF MFA

Logging is an important component of any multifactor authentication implementation. By recording MFA-related activities, organisations can monitor and review access attempts and detect potential security incidents early.

Maturity level two of the Essential Eight requires logging both successful and unsuccessful MFA events. For level three, these events must be logged centrally, protected from unauthorised modification and deletion, monitored for signs of compromise and actioned when those signs are detected.

PRIVILEGED USERS

At maturity level two, the Essential Eight specifies additional requirements for privileged users. Any user with additional system privileges, such as administration rights, must authenticate with MFA – regardless of the classification of the data within a system or whether the system is internet-facing or not.

PHISHING-RESISTANT MFA

Phishing attacks are a common method employed by cybercriminals to obtain user credentials, such as usernames, passwords, and even one-time passcodes. With this in mind, the Essential Eight introduces the requirement to implement phishing-resistant MFA methods at maturity level three.

In general, for an MFA method to be considered phishing resistant, it must

reduce or remove user activity from the authentication process. For example, an OTP could be intercepted or coerced from a user; however, a tap of a smart card or scan of a fingerprint is much harder for an attacker to replicate.

It's important to recognise that phishing-resistant MFA is not completely phishing-proof. For example, if a scammer calls a user pretending to be from their bank, and encourages them to open their banking app using their fingerprint and press allow on a push notification, they can possibly bypass even phishing-resistant MFA methods.

While no solution is completely secure, MFA is exponentially better than relying on username/password combinations alone, and phishing-resistant MFA is better still than other MFA methods.

CONCLUSION

In today's ever-evolving threat landscape, implementing robust security measures is more critical than ever. Multifactor authentication (MFA) is a proven and effective method for enhancing any organisation's cybersecurity by providing additional protection against unauthorised access to sensitive data and systems. By aligning its MFA implementation with the Australian Cyber Security Centre's Essential Eight framework, organisations can ensure they are following best practices and further strengthen their security posture.

CONTACT INFO

+61 8 8238 6500

sales@advance.net.au

www.LinkedIn.com/company/advance-business-consulting