

**PROFESSIONAL & FINANCIAL RISKS //**  
**CYBER // RISK MANAGEMENT // ASIA PACIFIC**

## Cyber security series: Multi-factor Authentication

JUNE 2023



The following paper is the first in a series of topics on common cyber security challenges organisations are facing, alongside regulatory changes for which organisations require awareness.

# TRENDING TOPICS

ASIA PACIFIC

## Acronym list and defined terms

### Cyber security terms

<b>MFA</b>	Multi-factor authentication
<b>SFA</b>	Single-factor authentication
<b>2FA</b>	Two-factor authentication
<b>U2F</b>	Universal 2nd Factor
<b>PIN</b>	Personal identification number
<b>AiTM</b>	Adversary-in-the-middle
<b>OAuth</b>	Open authorisation
<b>TOTP</b>	Time-based one-time password
<b>SSPR</b>	Self-service password reset
<b>TPM</b>	Trusted Platform Module
<b>IP</b>	Internet Protocol
<b>HTTP</b>	Hypertext Transfer Protocol
<b>IT</b>	Information Technology
<b>URL</b>	Uniform Resource Locator
<b>API</b>	Application Programming Interface
<b>Phishing</b>	An attempt to acquire sensitive data through fraudulent solicitation by an attacker
<b>Keylogging</b>	Recording a users keystrokes through malware placed on a device to gain further access to information e.g., cleartext passwords.

### Cyber security protocols and products

<b>SS7</b>	Signalling System No.7 protocol suite
<b>POP</b>	Post Office Protocol
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>IMAP</b>	Internet Messaging Access Protocol
<b>TLS</b>	Transport Layer Security
<b>FOB</b>	Also known as a hardware token. Typically, a small security hardware device used during authentication e.g., small LCD screen generating random code.
<b>RSA SecurID</b>	A mechanism designed by security company RSA Security that is used to protect network services.
<b>FIDO U2F</b>	A second factor authenticator designed by the FIDO Alliance as an alternative to passwords.
<b>CTAP</b>	Client To Authenticator Protocol – CTAP 1 and CTAP 2 are differing versions, with CTAP 2 being the updated version.
<b>WebAuthn API</b>	A web standard published by the World Wide Web Consortium (W3C). It provides an API for accessing Public Key Credentials and is a core component of the FIDO2 Project.

### Agencies mentioned

<b>ACSC</b>	Australian Cyber Security Centre
<b>NIST</b>	National Institute of Standards and Technology
<b>NCSC</b>	National Cyber Security Centre
<b>CISA</b>	Cybersecurity and Infrastructure Security Agency

In this paper we explore the increasingly used control of multi-factor authentication; why it is used, some of the techniques used by adversaries to bypass it, and recommendations that organisations can adopt to enhance their cyber defence strategy.

**Multi-factor Authentication (MFA)** is an essential cyber security control to prevent trivial account compromise, and something that many organisations rely upon to help secure access to critical systems. Liberty Specialty Markets (Liberty) along with cyber security advisers NCC Group, aims to provide an overview of MFA and discuss

common pitfalls and challenges that an organisation should be aware of when choosing to implement an MFA strategy.

This paper provides an insight into the different methods of MFA, highlighting those that have proven resistant to attack and those which have proven less resistant, in order to guide on best practice implementation.

Whilst MFA is undoubtedly superior to single-factor authentication (SFA), it is not a “silver bullet” and not all methods of MFA can be considered equal. Organisations should consider MFA an essential control, but always as a single component of their broader defensive strategy.

## What is MFA?

When implemented in accordance with best practice, MFA is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to its systems and information.

MFA is an authentication mechanism that requires two or more different proofs of identity to grant access to a resource. It's also commonly referred to as two-factor authentication (2FA), where a second factor of authentication is required.

However, in contrast to 2FA, whilst MFA requires at least two it is not limited to this number.

Governing bodies such as the Australian Cyber Security Centre (ACSC) and the National Institute of Standards and Technology (NIST) identify MFA as requiring two or more different factors to achieve authentication. As such, using two of the same factors to access a system would not be considered MFA. Authentication factors that make up a multi-factor authentication

request must come from two or more of the following:

- ▶ Something a user **knows**  
Example: a PIN code or password
- ▶ Something a user **has**  
Example: physical hardware, physical smartcard or a digital certificate stored on their device
- ▶ Something a user **is**  
Example: their fingerprint or facial recognition scan



The Australian Cyber Security Centre (ACSC) identify MFA as one of the eight essential strategies to mitigate a cyber security incident.



## How does MFA help?






In the event of a password compromise, MFA can safeguard access and prevent an adversary from using the stolen password to gain access to the user's account. The adversary may know the user's password, however, they would also need access to the second authentication factor, such as the person's fingerprint or one-time code to obtain access. Whilst the adversary has access to credentials, they may not have access, or the capability to access the other factor(s).

A common occurrence is that an organisation storing a large set of credentials experiences a data breach, and the adversary uses the obtained credentials to perform "credential stuffing" attacks against other services and organisations.

If a user has reused the same set of credentials for another service – that is the same email address, same password – and has not enabled MFA, then the stolen credentials will grant the adversary access to that service as the user.

When an account or system is protected using only a single factor of authentication – most commonly a password – all an adversary needs to obtain is the username and associated password to access the resource.

The following table outlines examples of large organisations that have had credentials stolen during a breach. In many cases, the breach involved the theft of both usernames and passwords, allowing adversaries to further use these combinations in other locations where they may have been reused.

Organisation	Date of breach	No. of account details stolen
 Yahoo	October 2017	3 billion
 Canva	May 2019	137 million
 Yahoo	January 2021	1.8 million
 Nvidia	February 2022	71 thousand
 Adobe	October 2013	152 million

Source: <https://haveibeenpwned.com/PwnedWebsites>

## Common forms of MFA implementation

MFA can be implemented using a variety of options, including but not limited to:

- ▶ PIN codes or a string of characters, often sent to the user via SMS, email, or voice "call-back"
- ▶ An app on a trusted device (such as those provided by Microsoft or Google)
- ▶ A software certificate installed on a device
- ▶ Biometric details (such as a fingerprint scan, or facial recognition)
- ▶ A physical security device that the user must physically connect to their device (such as via USB)

### Appropriate single-factor authentication scenario

In limited scenarios, the use of single-factor authentication (SFA) may be risk assessed to be appropriate. An example of this could be for device authentication, given modern devices offer brute force protection or hardware-protected storage.

Still, a more secure implementation for a device such as a Windows laptop would be to require both a PIN to unlock the device during boot up and a password to then access the device upon start. MFA is likely to be appropriate when security is of a higher priority than the experience of the user, while SFA may be appropriate when the user's experience is a higher priority than security.

## Are all MFA methods equally effective?

While any form of MFA provides advantages over single-factor authentication, some methods are more effective than others. Notably, MFA is most effective when one of the authentication factors is physically separate from the device initiating the access request. For example, using a physical hardware device provides a higher level of security than using a software certificate, or a “soft” token stored on the same device.

Additionally, some methods of MFA are more resilient to sophisticated phishing techniques designed to bypass MFA controls, such as adversary-in-the-middle (AiTM) phishing and Open Authorisation (OAuth) consent phishing (more about those later).

In the event of MFA being implemented at the perimeter of an organisation, it may not be in place on local workstations or internal web applications and systems. A well-resourced

and motivated adversary may seek to target users with malware to obtain a “reverse connection” and bypass perimeter defences.

In such a scenario, MFA for remote access is significantly better than SFA, but does not negate the requirement for additional security controls such as monitoring and logging, and appropriately hardening systems in accordance with industry best practice.

## MFA methods

The following section outlines popular methods of MFA implementation and techniques adversaries have developed to exploit commonly known weaknesses.

### **SMS messages, emails or voice calls**

MFA that utilises pre-established communication channels, such as phone numbers and email addresses, to send a password to the user. These channels may have been provided during the registration and setup of the user account.

The password is usually a time-based one-time password (TOTP), meaning it expires if not used and works only once, preventing an attacker that finds the password from reusing it.

### **SMS TOTP**

#### **SIM Swapping**

An attack that abuses the legitimate functionality of “porting” a pre-existing phone number from one subscriber identity module (SIM) card to another.

An adversary may have unauthorised access to a mobile operators’ systems, or a method to abuse a legitimate self-service portal and be capable of performing the SIM swap directly. Alternatively, adversaries contact the mobile operator call centre, impersonate a victim, and provide a pretext as to why the “port” is required.

#### **The Signalling System No. 7 (SS7) protocol suite**

A set of protocols that enables phone networks to exchange information needed for setting up calls and sending SMS text messages between telecommunications carriers. Many of the SS7 suite functions largely do not require authentication during transactions and as such, verification of the origin of messaging for certain functions does not occur.

There are several attacks that can be leveraged against SS7, all with different levels of severity and complexity. A successful attack against the SS7 suite can result in all incoming services for the affected phone number – including inbound SMS services containing MFA TOTP – being intercepted.

## Email TOTP

### Weak passwords

An adversary can exploit a weak password of an email account that is not protected by MFA. Upon gaining access, the attacker can generate an email-based TOTP for other services that provide an email-based TOTP and authenticate to the service.

### Credential stuffing

The adversary uses known leaked credentials to authenticate to likely email providers, enabling the same TOTP exploitation as above.

### Forwarding rules

Having gained access to a target's email inbox, an adversary may set up forwarding rules to forward all emails, or potentially all emails that match a certain criteria – for example, MFA code emails – to an inbox it controls. Although detection opportunities exist, and the method is somewhat crude, it remains a feasible and effective method of attack.

### Legacy cleartext protocol

An adversary exploits email infrastructure that is configured to still use a legacy authentication protocol that travels across networks in cleartext (unencrypted) e.g. POP, SMTP, IMAP.

Such an attack requires the adversary to be in a position to 'eavesdrop' on the target, e.g. via a compromised home network, hotel or airport lounge wireless network. Combined with ability to eavesdrop, further email TOTPs are generated by the attacker on the target's inbox to authenticate to further services impersonating the target.

Additionally, a sophisticated and well-resourced adversary with appropriate network access may be capable of intercepting many cleartext protocols and extract TOTPs at scale.

## Voice call-back TOTP

### Attacks against voicemail

If a target's voice mailbox is either not password protected, or uses a default, weak and guessable password such as '0000', '1234', an adversary can gain access.

The attacker then changes the voice greeting message to an audio message of the dial tone used to approve the MFA request, commonly "#". An attacker then calls the victim's phone to ensure it is engaged, initiates a logon request and asks the service to send the MFA challenge using the voice call-back service.

The TOTP is sent to the victim's voicemail inbox, at which point the attacker accesses the TOTP and completes the MFA challenge response. Given the frequent maximum voicemail PIN of 4 digits 0000 through 9999, security researchers have identified weaknesses in voicemail password protection controls that enable brute forcing of all possible password combinations. Combined with an SS7 attack, a voice call-back TOTP could also feasibly be intercepted.



When implementing MFA, it is essential that it does not create a false sense of security.

It is important to remain aware and vigilant in the face of potential threats.



## Mobile apps

Multiple mobile applications exist to provide secure MFA solutions, each with their own various approaches. All rely on the principle of using a secure channel, for example, TLS, to communicate the MFA proof to the user.

Users download the application – for example, Google Authenticator or Microsoft Authenticator – from a trusted application store and configure them on a mobile device. Configuration commonly involves account setup, where the user enrolls the application using a QR code or other means.

The following are examples of three common solutions. Although more secure than SMS, email and voice calls, it should be noted that they are not without vulnerability.

### 1. Push notification TOTP

A TOTP is sent to the user using the pre-established mobile application channel in the form of a push notification.

### 2. Push notification approval

Like the above, but in place of a TOTP, a push notification provides the user the option to approve or decline the login attempt.

### 3. Push notification approval challenge

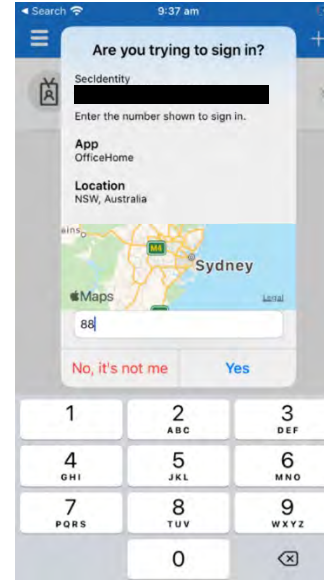
Following a rise in “MFA bombing” attacks, push notification approval challenge requires the user to not only approve an MFA request, but also confirm a further piece of information, for instance, a random number generated by the resource the user is attempting to access.

## What is MFA bombing?

In the event of an adversary obtaining a set of credentials but lacking the sophistication to perform an adversary-in-the-middle (AiTM) attack, they may resort to a technique known as “MFA bombing”.

This involves repeatedly authenticating a service, causing the legitimate user’s device enrolled for MFA to continuously request login confirmation.

The user may assume there is an error with the application and confirm the login. There also exist many plausible scenarios within which the user mistakes the alert for a legitimate request or accidentally confirms the login while distracted by another task. Although the technique is crude, it has been seen to be effective and leveraged by real-world adversaries to breach high-profile organisations.



Source: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context>



### Software certificates

A software certificate is installed locally on a device as a second factor, and when a user performs an authorisation request, the system presents the certificate. The certificate may be stored within a file on the system, within the system registry or within system hardware, for example, on a TPM, which is the more secure option. Although this method removes the need for a user to provide a time-bound PIN, if an adversary can compromise the device storing the certificate and private key, the adversary can likely replay legitimate requests to gain access, or depending on the level of access required, extract the certificate and install this on a device they control.

Furthermore, the device storing the certificate is likely the same device within which the initial factor is provided, feasibly enabling an adversary with access to the device to obtain both factors through use of this extraction technique.

When mutual authentication is correctly configured, the use of certificates can protect a user from an AiTM attack. Although the user would still be able to connect to a malicious proxy, it would not be possible for the proxy to further authenticate to the target service.

### Biometrics

A fingerprint, facial recognition pattern or iris scan are examples of biometrics that can be used as a second factor and would be enrolled during account setup. Due to the limitations of some biometric technology,

some users may not be able to successfully enrol, and it is likely an alternative form of MFA may also be required.

Biometric matching is probabilistic, as opposed to deterministic, with the process only being as strong and effective as the algorithm that determines the likely match. A well-resourced and motivated adversary is likely capable of obtaining biometric data, and biometrics cannot be revoked – unless resorting to extreme measures. Security researches have also identified instances in which a biometric reader can be fooled e.g. similar-looking relatives able to unlock phones using biometrics, or even printing 3D masks of a target user to bypass biometrics.

### Physical hardware devices

Physical hardware-based MFA can be implemented in several ways, including the use of:

- ▶ PIN-generating key FOB: PIN codes generated by a physical device Example: RSA SecurID
- ▶ A physical device that contains a mechanism to secure storage of a private key Example: smartcard, FIDO U2F – now renamed to Client to Authentication Protocol version 1 (CTAP1)

In the case of a hardware device that generates a time-bound code, a separate physical device is used which is already pre-synced to the code generation mechanism. As a result of this pre-synchronisation, a significant vulnerability remains in that if the

code is intercepted, it provides the capacity for an MFA bypass such as AiTM phishing to occur.

An alternative approach to physical hardware-based MFA is that of a smartcard or other USB-style hardware providing secure storage of a private key that, when combined with a password, authenticates a request for access.

The private key stored within the physical device is used to sign a challenge-response request from a service, which then verifies that the response is signed by the valid and correct private key of the requesting user. To access the private key, the user may be required to enter a PIN to unlock the smartcard, press a button on the device, provide biometric data to the device, or authenticate via another method involving physical interaction with the device.

Where smartcards require a software-based PIN to unlock them, this PIN is likely entered via the same device that provides the other factor (e.g. password). This creates a scenario similar to that of software certificates stored locally on a device.

An adversary with sufficient access to the device could use a variety of techniques – for example, keylogging or memory dumping – to obtain both the password and PIN required to interact with the smartcard and bypass MFA access controls.

A more effective practice involves physical interaction with the smartcard or a U2F key



in the form of a button on the device, or a code physically entered onto the keypad of the device. Physical attacks are however still possible for these devices, as an adversary with sufficient physical access could observe the PIN being entered into a device and later steal the device, or steal an unattended U2F token.

In that scenario, the adversary would still require the other factor – a password, for example – and could use a variety of techniques to obtain this.

Furthermore, it is still feasible for an adversary operating AiTM tooling to intercept the signed challenge response issued by a CTAP1/U2F key and impersonate a user.



## Common techniques used to bypass MFA

In addition to the individual weaknesses outlined against particular MFA methods, there exists a number of techniques used by adversaries to bypass MFA. These are usually as a result of poorly implemented controls associated with MFA registration, or logic flaws in associated processes. The following are some important considerations to be mindful of.

### New users

When a new user is onboarded into an organisation, they are frequently required to set up MFA upon joining. Given modern ways of remote working, users may never physically visit an office and have their device(s) shipped directly to their home.

Under such a circumstance, if an adversary were able to obtain the user's credentials ahead of them, it would be feasible that they could register a device they control and bypass MFA. Combined with weak and

common passwords for all users (e.g. all new users have a password of "Welcome1" that requires changing on first use), and password spraying attacks, this scenario is easily exploited.

### MFA rollout not choreographed

When an organisation has "turned on MFA" and requires existing users to enrol when prompted, opportunities for exploitation emerge.

For example, an organisation requires MFA to access corporate resources from home, but not the office. If the credentials are stolen from an employee who only works full-time from the office, the adversary can register the mobile number to receive the MFA code. The likely outcome is the employee would not be aware of the MFA enrolment, and unless the organisation had the appropriate logging and monitoring controls, may be unaware of the unauthorised access.

### Self-service password reset (SSPR)

Due to flawed logic in the process flow of an authentication service, it may be possible to reset a password by answering easy-to-guess security questions.

### Weak conditional access policy

An organisation may have configured a conditional access policy to require MFA for users "not accessing resources via a trusted IP address" (the office IP address).

Where guest Wi-Fi is available, an adversary with access to credentials may be able to use the stolen credentials to authenticate to services from the guest Wi-Fi and bypass MFA requirements.

Under the right conditions, or through the use of specialised antennas, the adversary could even gain access to a guest Wi-Fi remotely. Provided they are able to send and receive traffic on the network, it would be feasible to obtain an external IP within the allow list of the conditional access policy.



## MFA bypass attack (adversary-in-the-middle)

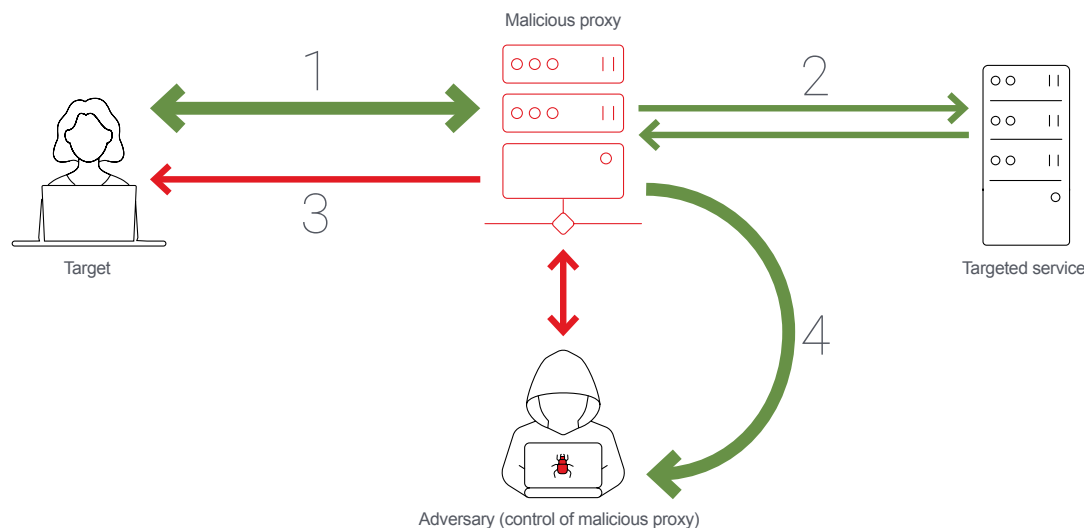
Due to the increased prevalence of MFA usage, competent adversaries have developed techniques and tooling to bypass MFA controls, most notably AiTM tooling.

Such tooling enables an adversary to deploy a proxy between the target user and the legitimate service they wish to access. A common means of deploying the access would be traditional phishing techniques and requesting the user visit a URL and perform an action – for example, “log in to a Microsoft 365 account to access a time-sensitive email or voicemail” or other lures.

If the adversary is successful in having the user visit the link and perform the required authentication, the following steps occur:

1. Adversary supplies user with a request to log in to a targeted service via a proxy server, into which they enter their account username and password.

2. Upon successful authentication, the proxy relays this information to the targeted service, which in turn sends back a legitimate MFA request.
3. The MFA request is forwarded to the user as the second factor of authentication – this could be a request for a code, or push of a U2F button.
4. At this point, if a correct MFA code or challenge response is provided, the proxy will relay this to the legitimate service, granting access to the adversary and not the target. The target is redirected to another page, for example, a “failed login page”, or potentially redirected to the legitimate service and no longer passed through the proxy. In most cases, the user will assume they have entered either a password or code incorrectly.



An example of this technique is featured below.

Depending on the sophistication of the tooling used, it is likely that, except for the URL, there will be no visible difference between the phishing site and legitimate service.

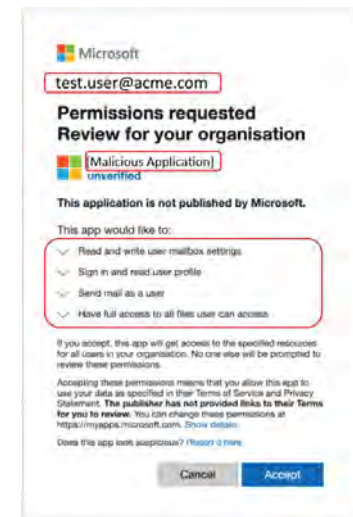
The legitimate service is transparently provided through the malicious proxy, with the HTTP requests being decrypted, inspected, altered, and re-encrypted as the proxy relays traffic between both the target and legitimate service on the fly.

As far as the targeted service is aware, the authorised user has successfully authenticated with a source location e.g. IP address of the malicious proxy.

## OAuth consent phishing

As a result of the continual arms race between those tasked with designing MFA methods, and those tasked with identifying weaknesses and bypasses and exploiting them, a new class of attack has been developed.

Consent phishing is designed to be capable of bypassing the use of passwords, MFA, and even passwordless solutions. This attack exploits services that support OAuth 2.0 authorisation – for example, Microsoft and Google – and through the use of a malicious application masquerading as an alternative service, attackers send phishing emails to targets and request that they provide consent for the malicious app to make API requests on their behalf.



In the example above, if “test.user” accepts the request for “Malicious Application”, that has a Microsoft Logo to disguise it, the Malicious Application can then authenticate to Microsoft as test.user and gain the ability to access files, read and send emails on their behalf.

It is important to understand this attack technique is capable of completely bypassing MFA, because the adversary would have permissions granted on behalf of the target once the malicious application is installed. At this point, an incident response investigation would be required to identify malicious applications and revoke the permissions granted to each.

Microsoft provides guidance on how to best protect from consent phishing [here](#).

### Notable threat actors using MFA bypass

The weaknesses outlined in this paper are well-known by threat actors. Notable examples of MFA bypasses and attacks include:

- ▶ **Chimera**  
Registered alternate numbers of compromised victims to intercept SMS MFA codes.
- ▶ **LAPSUS\$**  
Performed SIM swapping attacks and used MFA Bombing.
- ▶ **Yanluowang**  
MFA Bombing attacks.

- ▶ **APT29 (CozyBear)**  
Self-registration for MFA for new/unused accounts, in addition to MFA Bombing.
- ▶ **SEABORGIUM**  
AiTM to phish user's credentials and session tokens, bypassing MFA.

In addition, there exists a rise in "Access Brokers" who specialise in obtaining access to multiple targets, and sell "access as a service" to threat groups who may themselves be incapable of bypassing perimeter defences, but willing to purchase access to enable their objectives.

## The future – passwordless?

A common theme of weakness in MFA methods is forming a workaround mechanism to support the use of passwords.

FIDO2 is a set of standards, designed to provide a secure alternative to using passwords, based on public key cryptography.

FIDO2 is an evolution of U2F, and includes W3C Web Authentication specification (WebAuthn API), and CTAP2.

**In the following example "Bob" wishes to sign up for a new service, "ACME Service".**

During registration, Bob used a FIDO2 capable device e.g. mobile device, to generate a new "pair of keys", public and private. The FIDO2 device retains the private key and provides the public key to ACME Service.

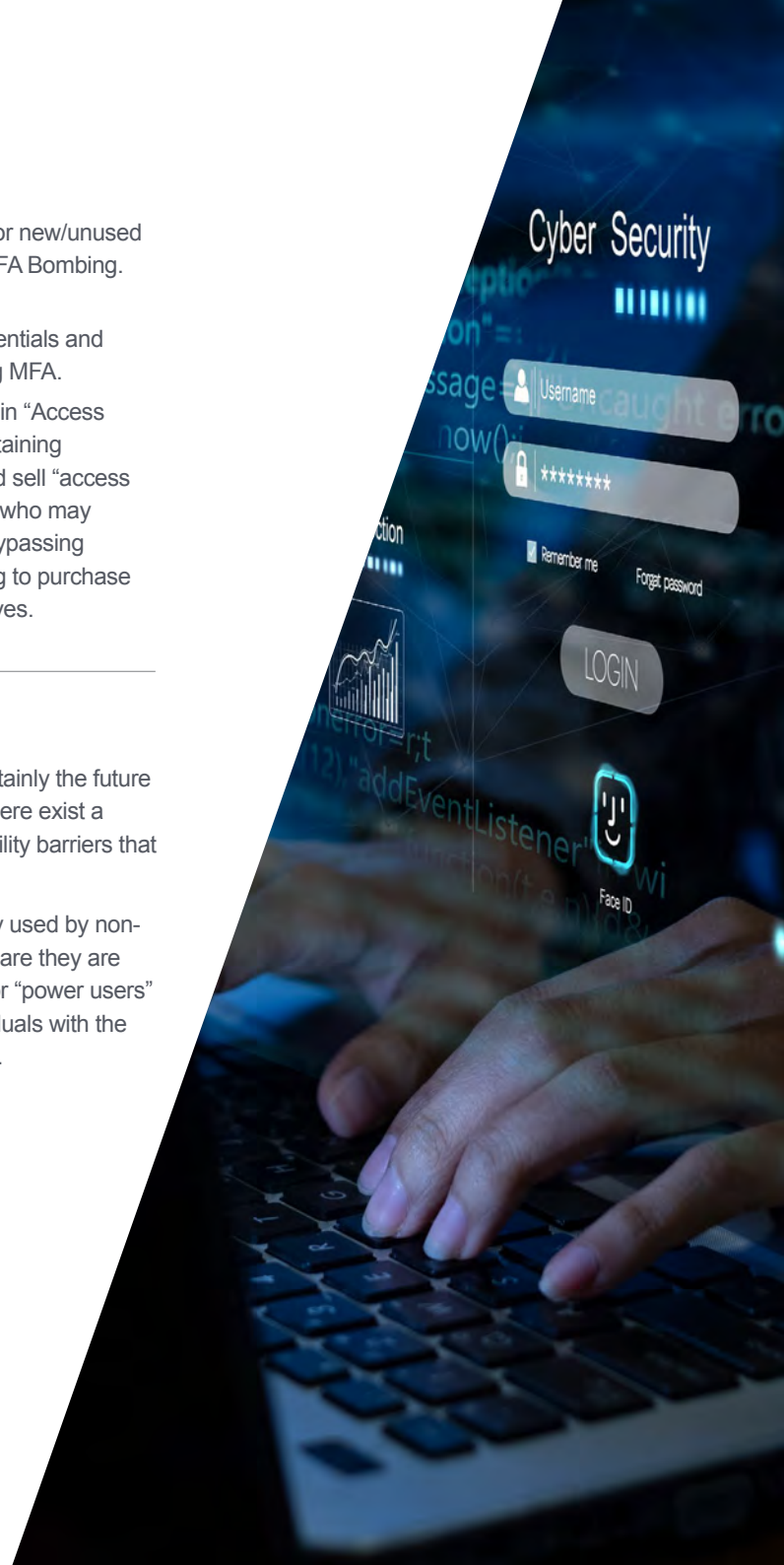
In the future, to authenticate to the service, the FIDO2 authenticator (mobile device), can sign a challenge-response using the private key to prove Bob is Bob. The authenticator protecting the private key can also be configured e.g. to require the use of a PIN, Password or Biometric measures.

Although designed to support passwordless authentication, FIDO2 can also be used in addition to a password to achieve MFA.

One of the challenges of FIDO2 is that the loss of the token would result in loss of access to the service. Lost tokens require revocation within each individual service it was used, a new token to be purchased, and backup authentication mechanisms used to authenticate to services to register the new token.

Although FIDO2 is almost certainly the future standard for authentication, there exist a number of technical and usability barriers that prevent easy mass adoption.

Currently, FIDO2 is commonly used by non-technical users who are unaware they are using FIDO2 authentication, or "power users" and security-conscious individuals with the required technical capabilities.





## In summary: MFA implementation best practices

MFA is an essential complement of any business's approach to cyber security, and it is essential that it's implemented and managed in a strategic and well-thought-out way. While any form of MFA provides advantages over single-factor authentication, with evolving threats some methods have proven less effective than others. Notably, MFA is most effective when one of the authentication factors is physically separate from the device, and resistant to communicating to illegitimate authenticators.



### The following guidance is offered to enhance the MFA strategy of an organisation

#### Choreograph the rollout of MFA in a planned fashion and consider process requirements and weaknesses

For example, enabling users to enrol in MFA from anywhere globally may be a requirement for a geographically dispersed workforce, but if additional controls are not in place an adversary may be able to enrol a device for MFA usage with the user unaware.

- ▶ The onboarding process could involve the user providing a mobile number to the helpdesk, which restricts enrolment to that number.
- ▶ Where a corporate mobile device is provided for use as the second factor, ensure that the provided device is the device used and not a device owned by the employee. The corporate mobile device should be managed and hardened in accordance with industry best practice.

#### Harden all devices involved in the authentication process

This includes laptops and mobiles, in accordance with industry best practice, and could be informed by:

- ▶ Vendor-specific guidance.
- ▶ Australian Cyber Security Centre (ACSC) guidance.

- ▶ Other regionally appropriate cyber security centres. For example, National Cyber Security Centre (NCSC), Cybersecurity and Infrastructure Security Agency (CISA).

#### Set the expiry times of time-bound PINs to the lowest practical values

Ensure they are configured for single use only and only communicated over secure encrypted protocols.

#### Educate users on the importance of protecting MFA hardware

Example: users know that they should never provide details (such as the serial number) of their physical hardware, unless they have initiated a call to the IT helpdesk.

#### Require access controls to access authentication applications on mobile devices

Example: require use of the device password or a user biometric to open the device.

#### Instruct users to report lost or missing hardware involved in any MFA process as soon as possible

Example: lost mobile device with authenticator app, lost smartcard etc.

#### Implement logging and monitoring with detection rules to detect and respond to stolen authentication factors

Example: turn on "impossible travel" anomaly detection that alerts when authentication/simultaneous sessions occur from geographically impossible locations that a user could not travel between or exist in at the same time.

#### Ensure all users have been provided with a basic level of incident response training

Example: know how to report a suspicious email or suspicious request and ensure the security team or incident response team knows how to respond in the event of MFA compromise.

#### Plan for the capability to revoke MFA hardware

Example: remotely wipe a lost device, and revoke a private key.

MFA is not a "silver bullet" and should rather form a component of an organisation's broader cyber defence strategy. In addition to MFA, it is important that organisations have the ability to patch security vulnerabilities, deploy and use hardened applications and operating systems, have a tested incident response plan and perform regular backups of key and critical systems, with backup and restoration capabilities regularly tested and proven.



## Global reach. Financial strength. Local authority.

Distinct, complex and constantly evolving – every business is as unique as its insurance needs. To confidently progress in the face of risk and uncertainty requires a level of security you can only achieve through working with specialists.

Liberty Specialty Markets offers a breadth of world-class insurance and reinsurance services to brokers and insured clients. We bring value and solutions to more than 26,000 of Asia Pacific's most significant business and government organisations – helping protect what they earn, build and own.

We're part of the global Liberty Mutual Group, a Fortune 100 company that's been in business since 1912 with a Standard and Poor's 'A' (strong) rating.

This is a summary of a comprehensive Liberty Trending Topic. To learn about this topic in greater detail and access the full version, please contact your Liberty Professional & Financial Risks underwriter.

 [View our office locations](#)

 [Meet our Cyber team members](#)

Liberty is not authorised to provide financial product advice. The information in this document does not take into account your objectives, financial situation or needs. Always consider the applicable policy wording and other relevant documents before deciding to acquire a financial product. © Liberty Mutual Insurance Company 2023. This information is current as at July 2023. Liberty means Liberty Specialty Markets, a trading name of Liberty Mutual Insurance Company, Australia Branch (ABN 61 086 083 605) incorporated in Massachusetts, USA (the liability of members is limited); Liberty Specialty Markets Hong Kong Limited (No. 2400200); Liberty Specialty Markets Singapore Pte Limited (UEN 201538069C); and Liberty Specialty Markets Singapore Pte Limited, Labuan Branch (Company No. LF12903), a licensed insurer under the Labuan Financial Services and Securities Act 2010 (Licence No. IS2016162).

## About NCC Group

Liberty Specialty Markets engages NCC Group as a cyber security adviser to support clients underwriting Professional and Financial Risk policies.

NCC Group is trusted by more than 15,000 clients to protect their most critical assets from cyber threats. With NCC Group's knowledge, experience and global footprint, they are well placed to help clients identify, assess and treat risks. NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

NCC Group has more than 1,800 colleagues in 12 countries. NCC Group's Technical and Risk Consulting, Incident Response and Managed Services have significant market presence in North America, Europe and Asia Pacific.



Connect and join the Liberty conversation

