ManageEngine
ADSelfService Plus

Enhancing cybersecurity:

Mastering CISA's

MFA best practices

Introduction

Passwords are no longer considered the best option when it comes to online security.

Password crackers and AI make even the most complex passwords easy for malicious cyber actors to hack. Because digital data has become the backbone of both our personal and business lives, it's imperative to rethink the way this data is accessed and protected. Authentication methods like multi-factor authentication (MFA) have become a necessary part of identity access and management in organizations worldwide.

The Cybersecurity and Infrastructure Security Agency (CISA) is a cybersecurity agency for the United States that works on improving defenses in the digital world and protecting resources and data against hackers. This e-book will cover how your organization can implement and master MFA best practices from the CISA to secure data and enhance your overall cybersecurity.

The passwordless future

The pandemic has initiated a global shift towards remote work, leading to higher chances of hacks and breaches in organizations with a distributed workforce. Employees using easy-to-guess passwords, misconfiguring their credentials, and setting up insufficient security measures have also contributed to the rise in various security incidents. Though organizations have been quick to fix these issues, hackers are usually one step ahead, exploiting other security vulnerabilities to get past the traditional defenses of passwords. It has become critical to reduce the need for passwords while ensuring secure access to data and resources. This is where Zero Trust comes in. With Zero Trust, every action on your network is viewed as a potential threat. MFA plays a crucial role in Zero Trust and helps to decrease dependence on passwords and implement stronger cybersecurity in your organization.

According to Microsoft, using MFA "can block over **99.9%** of account compromise attacks."

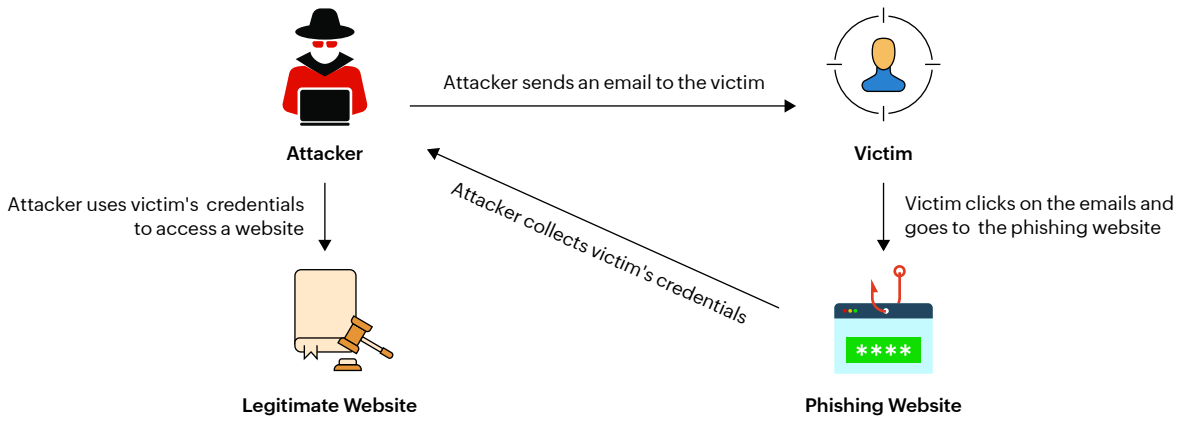
Read on for a quick overview of the most common cyberattacks in today's digital world.

The most common cyberthreats to your organization

The CISA has highlighted the various cybersecurity attacks that pose a threat in today's world, while urging organizations to implement phishing-resistant MFA that can protect against these attacks. The following are some of the most common cybersecurity threats your organization might face:

Phishing

In this cyberattack, attackers deceive their victims into revealing credentials or other information. For example, the target might receive an email that convinces them to visit a site that mirrors the legitimate webpage being targeted. The user might then submit their username, password, and any other authentication keys required to enter the site, thereby giving the attacker the information they require. Most email phishing attacks happen in bulk and are not specifically targeted.



Spear phishing

Spear phishing is a type of phishing attack that targets a specific person or group by sending them counterfeit emails or messages. These will seem to come from a legitimate source and include topics of interest to the target, such as current events.

Push bombing

This type of MFA fatigue attack, also known as MFA bombing, helps attackers gain access to the victim's account by triggering multiple MFA requests in hopes that the victim will accept a request.

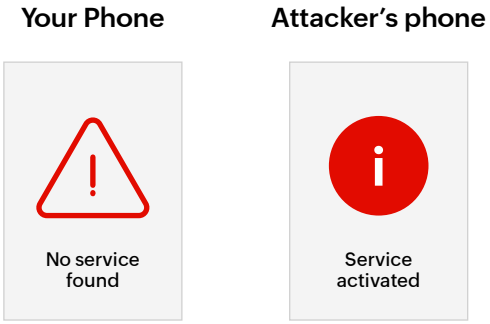
This kind of attack works especially well for employees that access many different apps and might have to re-authenticate into these apps on a daily basis. This repetition can cause a muscle memory that triggers them to approve an errant push notification.

Exploitation of SS7 protocol vulnerabilities

Signaling System № 7 (SS7) is a set of telephony signaling protocols, and it is the leading protocol for connecting network communication worldwide. But its outdated security concepts make it an attacker's best friend. An SS7 attack takes advantage of a weakness in the design of SS7. This can lead to data theft, location tracking, and text interception.

SIM swap

SIM swapping is a technique used by threat actors to get control of a victim's phone number. They do this by tricking and convincing the mobile carrier to transfer the victim's phone number to a SIM card they own. They obtain personal information through phishing, which enables them to answer the security questions asked by the mobile carrier. Once the connection is made, every phone call, message, and more will be transferred to the fraudster's phone.

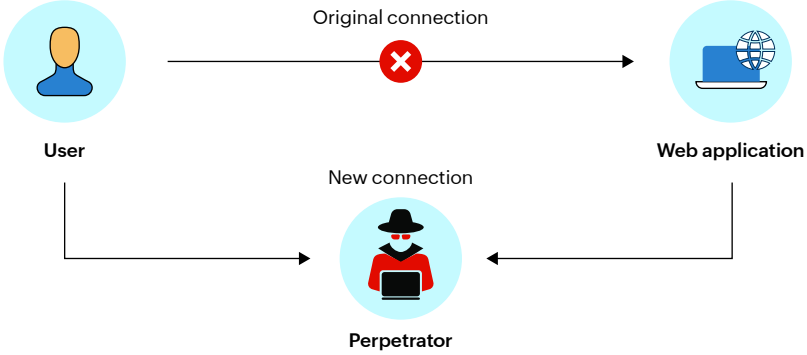


Credential stuffing

This is a cyberattack that uses a set of compromised credentials to attack a system. The attacker uses automation bots, assuming that most people are reusing their usernames and passwords across apps and services.

Man-in-the-middle (MiTM) attack

This kind of cyberattack is used when the perpetrator positions themself in between a user and an application to steal personal information like credentials and credit card numbers.



Forms of MFA to fight attacks

CISA recommends various MFA forms that organizations can implement to protect against cyberattacks that could put their data and business at risk. These include phishing-resistant MFA and app-based authentication systems. Organizations can also use SMS or voice authentication, but this form of MFA is not recommended as it can easily be breached by bad actors.

Phishing-resistant MFA	App-based authenticators	Other MFA methods
Phishing-resistant MFA includes FIDO/WebAuthn authentication and Public Key Infrastructure (PKI)-based authentication.	You can use app-based authenticators that either generate an OTP or send a push notification to the user's smartphone to verify their identity.	Other forms of MFA include mobile application push notification, but without any number matching, and SMS or voice MFA.
System administrators and other high-value targets are recommended to implement such forms of MFA to protect themselves against attacks.	If you are implementing the push notification authentication form, then CISA recommends that you also deploy number matching. This adds an additional step between the prompt and approval.	With mobile application push notification without any number matching, the user is prompted to approve a login request without entering any number. This means that there is no additional step between the prompt sent to the user and the user approving the request.
CISA strongly suggests that all organizations implement phishing-resistant MFA as part of their plan to apply Zero Trust principles.	Token-based authenticators generate OTP codes that the user is asked to enter to verify their identity by proving they have the token. Such app-based authenticators are best for small to medium-sized businesses that cannot implement phishing-resistant MFA methods.	In SMS or voice MFA, a code is sent to the user's phone or email. The user then uses this code to complete their login request. CISA recommends that this form of authentication should be used only as a last resort.

Ask these questions

When your organization is on the path to implement phishing-resistant MFA, CISA recommends that you ask the following questions:

1. What resources should you protect?

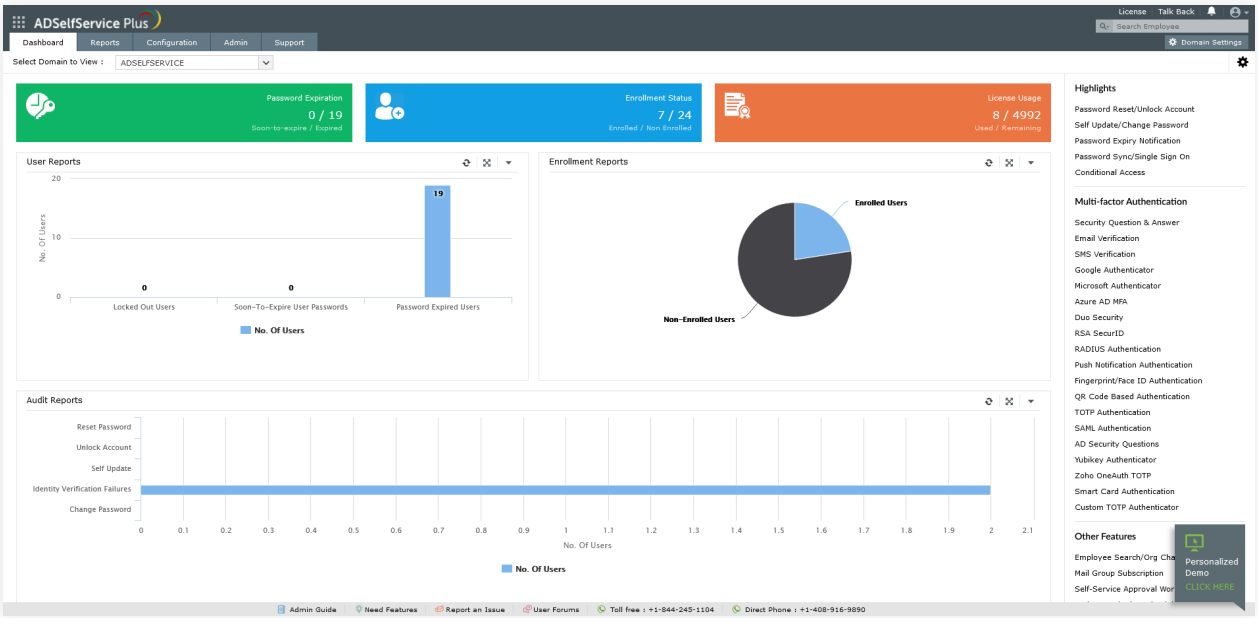
While implementing or migrating to a phishing-resistant MFA format, the organization needs to decide which resources it wants to protect from being compromised. For example, cyberthreat actors might focus on gaining access to certain resources that can help them gain more control over the organization. In such cases, these resources need to be closely protected in order mitigate the risk of their access falling into the wrong hands.

2. Which users classify as high-value targets?

While the compromising of any user account in your organization is a security issue, there could be certain user accounts that have additional access or privileges. This makes them more valuable to threat actors. Such users can include system administrators, HR staff, and the legal team. These user accounts might need an additional layer of security.

How ADSelfService Plus can help secure your organization

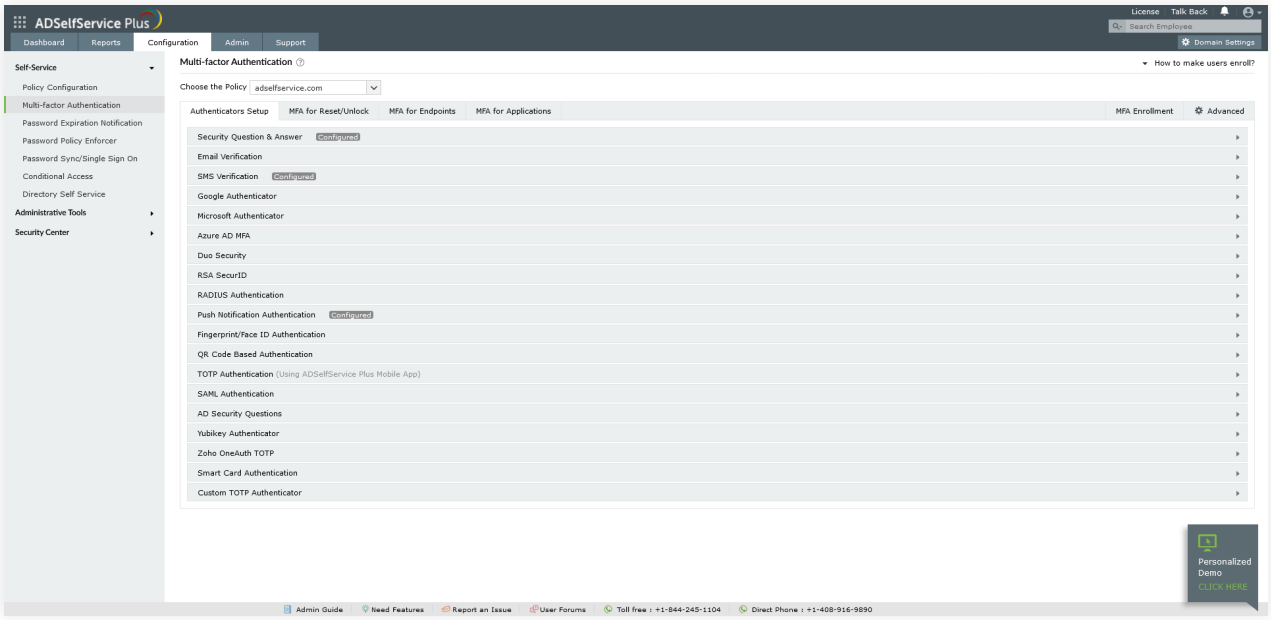
ManageEngine ADSelfService Plus is an identity security solution that can help you guard your organization against various cyberattacks and start your Zero Trust journey. With adaptive MFA and a wide range of authenticators to choose from, you can secure your organization's resources and user accounts and gain visibility across your on-premise, cloud, and hybrid environments.



Enhancing protection: Various MFA methods in ADSelfService Plus

ADSelfService Plus can take care of all your MFA needs with its 19 different authenticators, single-sign on (SSO) feature, and self-service password management. The different types of authentication techniques available in ADSelfService Plus include:

1. Fingerprint/Face ID authentication
2. YubiKey Authenticator
3. RSA SecurID
4. Duo Security
5. Azure AD Multi-Factor Authentication
6. RADIUS authentication
7. Google Authenticator
8. Microsoft Authenticator
9. SMS-based verification code
10. Email-based verification code
11. Time-based one time password (TOTP)
12. Custom TOTP authenticator
13. Zoho OneAuth TOTP
14. Push notifications
15. QR code-based authentication
16. SAML authentication
17. Smart Card authentication
18. Security questions and answers
19. AD-based security questions



Streamline identity security with MFA, SSO, and conditional access

Most users find themselves having to enter more and more passwords every day because their organizations use various applications and services. ADSelfService can help you effectively manage and secure user accounts with its SSO feature.

This feature gives users one-click access to all SAML-, OAuth-, and OIDC-enabled cloud-based applications with only one set of credentials. With ADSelfService Plus, you can choose to enable SSO for a number of pre-configured applications. You can also create custom applications for SSO. With SSO enabled, your organization can save money by eliminating multiple user logins and reducing IT costs, streamline user experience with one-click access, and perform faster IT integration by allowing users to log in and access multiple apps and services with a single sign-on.

Additionally, ADSelfService Plus offers a self-service password management feature. Users can reset their passwords and unlock accounts for various platforms such as Microsoft 365, Active Directory, and other enterprise applications. You can also enforce a custom, granular password policy over your organization's built-in Active Directory password policies to tighten your security measures.

Download ADSelfService Plus today and enhance MFA in your organization!

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

ManageEngine
ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

$ Get Quote Download Support