MULTI-FACTOR AUTHENTICATION

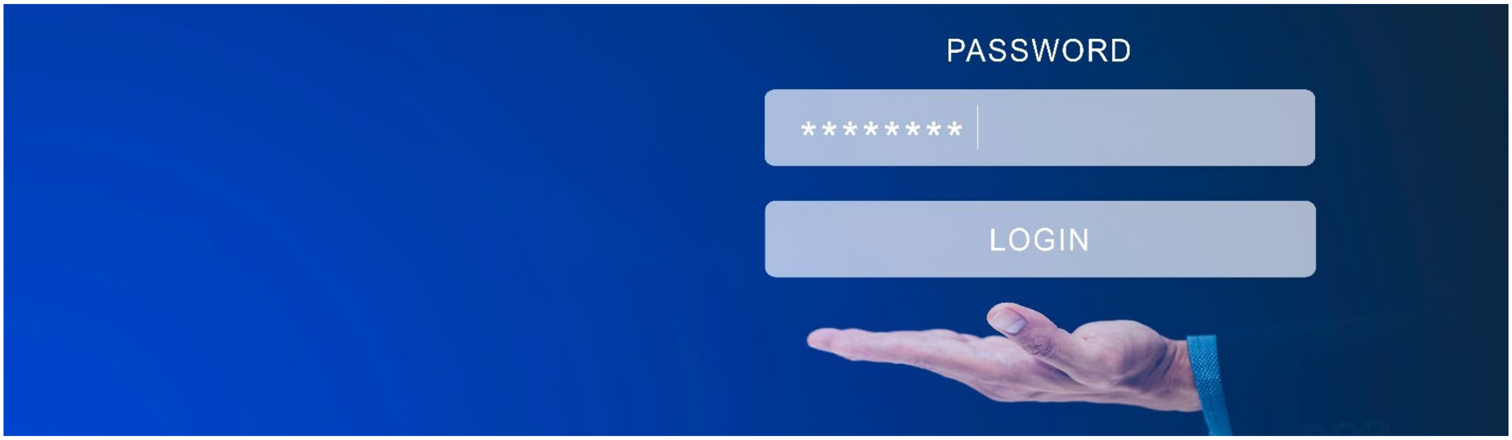
Introduction

Multi-Factor Authentication (MFA) is an authentication method that requires more than 1 piece of evidence for verification before access is granted, such as a password and a fingerprint scan. It’s an important layer in your security strategy, but many people are still resistant. Funnily enough, most people are already using MFA and may not even realize it. ATMs need both your banking card and your pin. The college computer lab needs your student ID and account credentials.

Nowadays, many organizations are offering MFA to their users, and some are even requiring it. This additional layer of security can be annoying, but the extra few seconds it takes can save you hours of pain. Here we’ll talk about the types MFA, the types of attacks, how to prevent them, and see what method could be better.

Passwords Aren’t Enough Anymore

Gone are the days where passwords were considered the cornerstone of security. Hackers have learned that people tend to use weak passwords, and those weak passwords are often reused for other accounts. The more security conscious person uses a strong password, but perhaps after an 8-hour workday, accidently clicks a malicious link. Hackers have a wide arsenal of tools and endless amounts of time to steal your credentials. Passwords simply aren’t enough anymore. Enabling MFA on your accounts gives you that extra peace of mind in the event you get compromised.



Types of MFA

There are many forms of MFA, ranging from your typical passwords to something more advanced such iris scanners. MFA methods can typically be broken into 3 categories.

Something You Know

This category of authentication is the most well-known and widely used. This relies on something that only you should know such as passwords or pins. Though this method has been the de facto way to protect your accounts and devices in the past, this is no longer the case. Hackers have been more sophisticated in their methods and technology has advanced far enough that passwords can be easily acquired.

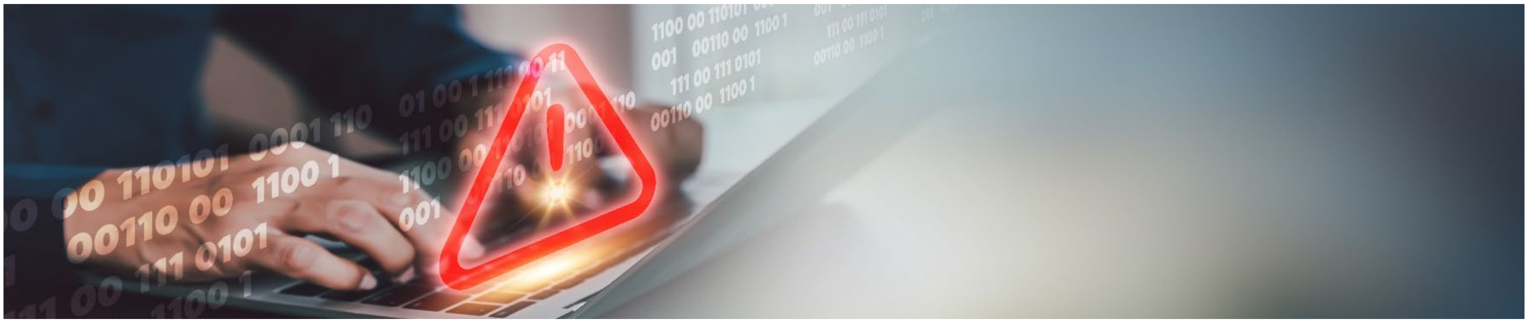
Something You Have

This category typically involves a physical item you own, such as a smartphone, phone number, hardware token or a Timed One-Time Password (TOTP) generator. This method is usually the easiest to use as a second factor because most people already have a smartphone, but if they don't a hardware token doesn't cost too much. Some methods in this category are:

- You can receive a TOTP over a phone call or text message.
- An authenticator app on a smart device to retrieve a TOTP.
- A hardware token plugged in via USB that sends a challenge response to the service.
- A smart card used to scan on a card reader.

Something You Are

With the integration of biometrics into smart devices, this category of authentication has gained popularity. This uses biometric data such as fingerprints, facial recognition, or iris scans to authenticate the user. This is thought to be one of the most secure and convenient methods of authentication. However, it is important to note that your physical characteristics are typically unchanging, so you it will be difficult to "reset your password" with this method.



MFA Attacks & Preventions

MFA is a powerful security measure, providing significant protections for user accounts and devices. However, nothing is infallible and attackers have a wide array of methods at their disposal. Here are a few that attackers use and what you can do against them.

Brute Force

Like passwords, attackers can attempt to brute force your TOTP codes.

What Can You Do?

- If you are an organization, enable adaptive MFA features that will block anomalous activity.
- Enable login attempt limits or account lockouts.
- Use MFA methods that are brute force resistant such as hardware tokens.
- Set up security alerts for unusual activity.

MFA Fatigue

An MFA fatigue attack involves the attacker repeatedly sending MFA push notifications until the target either accidently approves one attempt or intentionally approves an attempt to stop the notification spam.

What Can You Do?

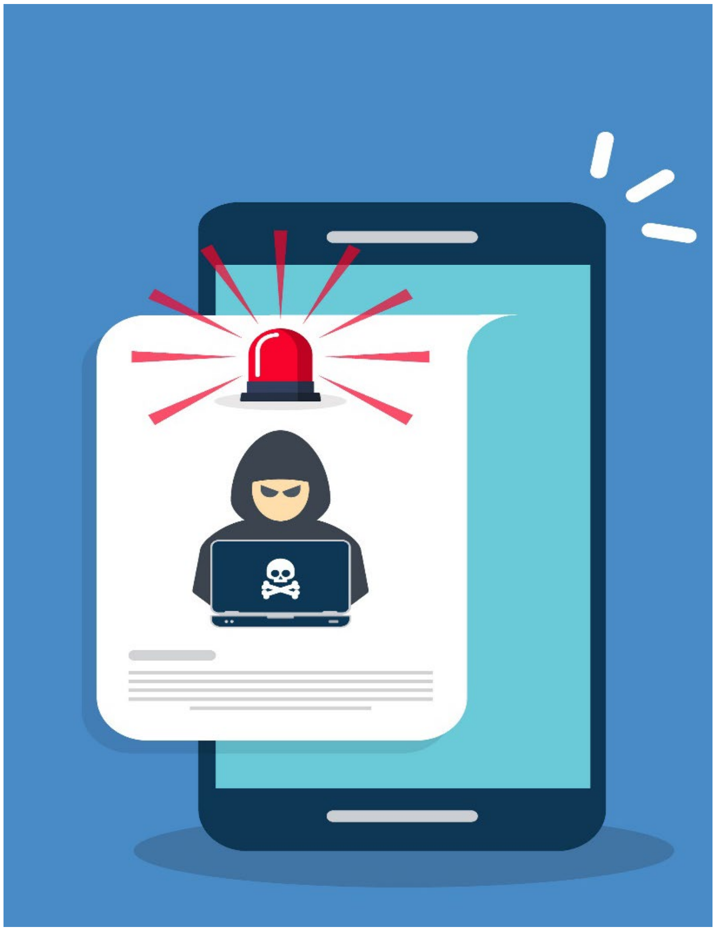
- Limit push notifications for your authenticator app on your device or system.
- Use MFA methods that are unaffected by this attack, such as hardware tokens.
- If you are an organization, enable adaptive MFA features that will block anomalous activity.

Session Hijack

When you successfully authenticate, you’re given a timed session token. This token if not yet expired, allows you to access other resources without having to sign in again. It’s convenient for you and attackers. Because these tokens can be stored your device, a proxy server, or even in some logs, attackers can steal these tokens and impersonate you. This can range from using malicious sites to steal your tokens to compromising your device.

What Can You Do?

- If you are an organization, require that only org-managed devices can access resources or implement Zero-Trust.
- If you are an organization, enable adaptive MFA features that will block anomalous activity.
- Implement security controls such as antivirus and credential protection settings.
- Set up security alerts for unusual activity.
- Avoid using functionality that let you stay signed in.



Phishing

MFA makes phishing a more difficult task, but not impossible. The attacker can use the same phishing tactics such as impersonation, clone emails/websites, and appeals to psychology to trick you into disclosing your TOTP. Other common tactics include tricking the target into registering MFA under the attacker or impersonating you and calling the service provider’s helpdesk to reset MFA.

What Can You Do?

- Security awareness and training. Be cautious for phishing attempts as always, but even more so if another person is requesting your code.
- If you are an organization, enable adaptive MFA features that will block anomalous activity.
- Never register MFA using someone else’s information. MFA is based on something YOU know, something YOU have, or something YOU are.
- Implement security controls that block malicious or spammy websites, emails, messages, and calls.
- Set up security alerts for unusual activity.

Sim Swapping

Sim swapping involves the attacker either tricking the target’s mobile carrier or having an accomplice working under the mobile carrier into transferring the target’s phone number to the attacker’s SIM card. This grants them access to MFA or recovery methods that use a phone number. This is a complicated attack that has gained popularity in the recent years.

What Can You Do?

- Call your mobile carrier and create a pin that must be entered before changes can be made. This isn’t a guarantee to prevent this attack, but great reduces the chances.
- Avoid MFA using phone numbers where possible.
- Set up security alerts for unusual activity.

Is One Better Than the Other?

Any MFA is better than no MFA; plain and simple. However, they all have their own strengths and weaknesses. Let’s talk about a couple of them.

The Hardware token such as the Yubikey, is considered one of the most secure MFA methods. This is because it is tied to a physical device the user must possess, making it immune to phishing and brute-force attempts. It cannot be infected with malware and can be further reinforced with MFA on top of the token itself.

Authenticator apps that generate TOTPs or push notifications provide powerful security. They don’t rely on a mobile carrier, are resistant to phishing, and function without internet or cellular connection. Though this method is phishing resistant, it is not phishing immune as hackers can still trick the user into providing the TOTP or push approval. However, If you choose to use a software TOTP generator, keep it on a separate from your main computing device because if that device gets compromised, that method can be compromised. If you must keep them together, make sure you have a strong password or another method of authentication to prevent access to it.

Biometric authentication is generally considered one of the most secure MFA methods, however there are many factors that can affect how secure it is. Depending on the vendor, the false acceptance rate and false rejection rate may not be optimally tuned, or the biometric scanner is using outdated technology that is easier to fool. Another consideration is that biometrics rarely change, so your fingerprint will typically always be your fingerprint, so you can’t easily “change your password.” In terms of security, iris scanning is considered to be the most secure.

You should not use phone numbers as an MFA method if you can avoid it. Phone numbers were never meant to be used as an ID, but here we are. Phone numbers can change hands willingly and unwillingly, they can be deactivated, they can be disrupted, and spoofed. You may put your phone number on a website when you register for an account, or you may have written it down when you wait for a dinner table. Your phone number is out there, so don’t make it easier for hackers to steal your information.

Despite what method is better, please use MFA.