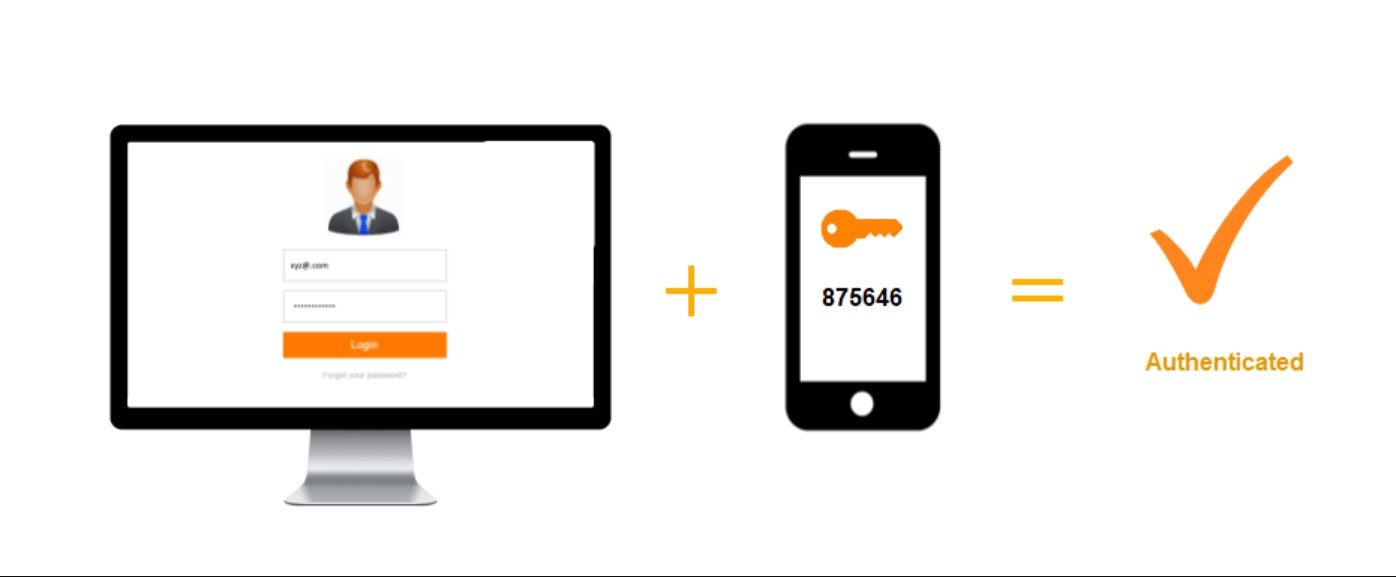
**Multi-factor authentication for web app**

**Purpose of multi-factor authentication**

* The main benefit of MFA is it will **enhance your organization's security by requiring your users to identify themselves by more than a username and password**. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties.

## How Does MFA work?

* **Multi-Factor Authentication (MFA)**is an authentication method that requires the user to authenticate themselves for two or more factors, in order to gain access to company resources, applications, or a VPN. Enabling [Multi-Factor Authentication (MFA)](https://www.miniorange.com/products/multi-factor-authentication-mfa) means that users need to provide additional verification factors apart from their username and passwords. These second-factor methods can range from OTP over SMS, OTP over Email, Push notification, Google/Microsoft authenticator, and many more.
* Having this extra layer of security ensures that the information being accessed is well protected from activities such as phishing, malware, hacking, and many more. Having a strong MFA setup ensures a robust Identity and Access Management (IAM) for your organization and secures your resources.



### ****Multi-Factor Authentication Methods****

MFA Authentication is based on various authentication factors. Multi-Factor Authentication takes the help of these factors to authenticate a particular individual.

* **Knowledge Factor**is something that a user remembers like “First Password”, “First School Name”, “A Pin” etc.
* **Possession Factor**is something the user has, such as a mobile device, smartphone app, or security token to approve authentication requests.
* **Inherence Factor** mainly referred to as a biometric factor, is something different in the user’s physical self. These could also be personal attributes like fingerprint, retina, or voice
* **Location factor** usually denotes the location from which an authentication attempt is being made. Location-based MFA methods can limit user access when a user breaks out from the given location. Location-based MFA can also limit the authentication attempts made by the user to specific devices by tracking their Internet Protocol (IP).
* **Time factor**restricts user authentication to a specific time panel in which logging on is granted and restricts access to the system outside of that window. In simpler terms, we called it Time based OTP (TOTP). Mobile Apps like Microsoft Authenticator, Google Authenticator provide a key code that’s time-dependent up to limited seconds.

### ****Multi-Factor Authentication Vs Two Factor Authentication****

* The major difference between 2FA and MFA is: In 2FA there are only two authentication methods: one traditional username-password and another one like (OTP, Push notifications). While in MFA there are no such restrictions, you can opt for multiple authentication methods according to your way.

## How can Cybercriminals Bypass Multi-Factor Authentication?

* Hackers can bypass MFA in much the same way as they would for two-factor authentication, where there is just a username and password. Below are some of the most common ways that MFA can be bypassed:

### Social Engineering

* Social engineering techniques, such as phishing is a common way for attackers to obtain credentials. For example, in some cases, they will try to login to an organization’s cloud service provider, which sends an SMS message with the verification code to the account owner. The hacker will then send an email to the account owner asking them for the verification code. Of course, in order for this to work the hacker must convince the user that they are a trusted entity. In some cases, the hacker will send an email to an unsuspecting employee in order to obtain some basic personal information. Using this information, they might then try to call the service provider and explain that they have been locked out of their account, and they want help getting back in.

### Consent Phishing

* Another social engineering technique that is becoming popular is known as “consent phishing”. This is where hackers present what looks like a legitimate OAuth login page to the user. The hacker will request the level of access they need, and if access is granted, they can bypass MFA verification.

### Brute Force

* One of the main benefits of multi-factor authentication is that it makes it a lot harder for hackers to brute-force-guess account passwords. Although it makes it harder, it doesn’t make it impossible. For example, hackers may look for photos of the user on social media, which can they can use to bypass MFA that uses facial recognition as an additional factor. In some extreme cases, they may try to find the fingerprints of the user by dusting a smooth or non-porous surface with fingerprint powder and then taking a photograph of the prints using a high-resolution camera.

### Exploiting Generated Tokens

* Many online services use authentication apps, such as Microsoft Authenticator and Google Authenticator, to generate temporary tokens which can be used as an authentication factor. In some cases, these services will keep a list of authentication codes, which are used by the service provider in the event of an account lock-out. Hackers will try to obtain this list by exploiting poor data security practices in order to bypass MFA.

### Session Hijacking

* Session hijacking is where an attacker steals session cookies, which contain a user’s authentication credentials. Session cookies are used by many web applications to provide a customized browsing experience and track the user’s activity. These session cookies remain active until the user logs out, and are sometimes sent to the server over an insecure connection. Hackers can easily find out if the session cookies are not secure, and are able to steal these cookies via a man-in-the-middle attack. Once they have access to a session cookie, they can bypass MFA.

## How to Strengthen Multifactor Authentication

### Choose your authentication methods wisely

* If you want to be extra secure, it’s probably a good idea to avoid SMS-based authentication altogether, as SMS OTPs are easier to compromise than other methods. If you do want to use SMS verification, consider setting up a SIM card lock, which means that a PIN number is required to modify your SIM card. Try to use biometric authentication whenever possible. After all, few hackers will bother to dust your door knobs with powder in order to get a copy of your fingerprint.

### Use adaptive multi-factor authentication

* Consider using adaptive multi-factor authentication (AMFA), which is a more contextual approach to MFA. With AMFA, each request is validated by examining the user’s geo location, IP reputation, device, and login behaviors.

### Use complex passwords, restrict access and monitor logon attempts

* Make sure that your users are using strong and unique passwords. Passwords should either be long alphanumeric strings with upper and lower case characters, or a passphrase that is difficult to guess.
* For example, If x number of logon attempts occur within a given time-frame, a custom script can be executed to disable a user account, shut down the affected server, and anything else that will help to contain the threat. These solutions can also work on cloud-based environments.

**Top 10 Multi-Factor Authentication (MFA) Software**

* Microsoft Authenticator.
* Google Authenticator.
* Duo Security.
* LastPass.
* Authy
* IBM Security Verify.
* SecurID.
* OneLogin.
* Okata MFA for Fortinet VPN
* Auth0

.