The modern workplace today is not the same as it used to be a couple of years ago. With technological advancement and better chances of mobility, it is easier for organizations to collaborate with team members. Moreover, team members can access information regarding projects anytime and anywhere. Cloud computing has made it possible for organizations to give their employees flexibility.

Moreover, the software has made it possible for employees to choose their working hours and work remotely as well. This new advancement has made it convenient for organizations to function as a whole and share data but at the same time, it has left company data vulnerable. With every passing year, there is a surge in the number of cyberattacks taking place. There is also an increase in data breaches taking place.

With the alarming increase in the number of cyberattacks, businesses are constantly working on methods to improve their cyber security. Among many other ways to improve cybersecurity, multi-factor authentication is one of the most tried and tested solutions to make data more secure for organizations.

## What is Multi-Factor Authentication?

Multi-factor authentication is a system that enforces users to make multiple login criteria to be able to access the system. A system that uses Multi-Factor Authentication will most likely use more than static credentials. It will also require the user to authenticate their identity through real-time sources like a smartphone or other hand-held devices. The extra layer of security minimizes the chances of a system to be hacked. The two-layer security is similar to the two-man rule in military operations where two keys are required to access warfare materials.

## What are Authentication Factors?

## There are several ways to implement Multi-Factor Authentication. Almost all authentication methods are based on authentication factors. These factors can be either passwords, possession factors, or something else. Let's find out the different authentication factors below:

1. **Knowledge factor:** A knowledge factor can be a factor that is only in the knowledge of the user. It can be a PIN, password, or a secret shared.
2. **Possession factor:** A possession factor can be the user's ID card, [smart cards](http://www.cardzgroup.com/ContactSmartCard.html), cellphone, or another mobile device that is under use.
3. **Inherence factor/biometric factor:** A biometric factor or an inherence factor is the personal attributes of the user such as fingerprints. They can also be attributes like facial and voice recognition factors. More advanced technology also supports speech patterns, behavior biometrics, etc.
4. **Location factor:** The system uses the location from which the login attempt was made. The location factor uses the geographical location of the user and registers the IP address of the user to monitor the login attempts made. In case a login attempt is made from a different location, the system generates an error.
5. **Time factor:** If the authentication system is using the time factor then they will give the users a certain amount of time to enter the password. With a limited time window, the system can restrict any hackers from making forceful attempts to log into the system.

## What are the benefits of 2-factor authentication?

Maintaining security standards is extremely important for an organization's well-being. Here are some benefits of 2-factor authentication:

1. Creating a secure and reliable work-environment

For a lot of people signing into multiple places to access one account is a nuisance. No matter how difficult the multi-factor authentication is it should be noted that the standard password procedure becomes less effective and more dangerous.

1. Fewer chances of identity theft

Identity theft has become a common crime even in the most developed systems of the world. Using adaptive measures like 2-factor authentication is a good way to protect users from having their systems hacked and leaking confidential data.

1. In compliance with regulatory authorities

Protecting customer data is the responsibility of companies. There are several legal liabilities that the companies have to undergo if they are not able to protect the data of their clients.

Multi-factor authentication is a great way to ensure that companies can keep their customer data safe and be in compliance with regulatory authorities as well. If you have still not implemented multi-factor authentication on your company systems,it is high time that you pay attention to this aspect of security in your organization.