MFA - What is MFA and Why it is Important

For every business – big or small – security is of paramount importance in today's hyper-connected digital space. Because nothing tanks your bottom line more than an intrusion due to a security lapse. There are thousands of security tools deployed to protect cyber attack vectors, including multi-factor authentication.

Multi-factor authentication is important for every commercial establishment because it is the most cost-effective method of protecting assets – usually at little to no cost.

The premise behind multi-factor authentication is simple: users have to provide at least two pieces of verification factors to gain access to an account. This is because passwords and usernames are relatively easy to acquire. But a third verification factor, such as fingerprints, mobile phone, or keycard, is virtually impossible to gain access to.

Multi-factor authentication stops the vast majority of petty criminals in their tracks. In fact, nearly 80% of breaches are caused by stolen or weak passwords. One survey by the Digital Shadows Photon Research found that a whopping 15 billion credentials are available on the dark web, including usernames with their relevant passwords for online banking!

How Multi Factor **Authentication Works**

Multi-Factor authentication works by identifying one or several of the following factors:

Knowledge Factor

Multi-Factor authentication works by identifying one or several of the following factors:

Possession Factor

These are credentials based on items that the user is likely to possess, such as a security key, Google Authenticator app, or a mobile phone

Inherence Factor

Metrics that authorized users own. They take the form of biometrics such as fingerprints, facial recognition, and eye patterns.

Location Factor

Access is granted to devices based on their IP address or geographic location. This can ward off bad actors from attempting to breach data from different geographical origins.

Businesses can combine a few or all of the above authentication methods to grant access to individuals.

Why Passwords Are **No Longer Enough**

Passwords no longer offer the desired level of security because of two reasons:

01 Brute forcing attempts can eventually break passwords and grant access to accounts

02 Multiple data breaches have provided bad actors with access to passwords (you can check if your account has been compromised at haveibeenpwned.com)

One outdated security advice involved changing the password and using complex characters would provide a sufficient level of security. That is no longer the case – even if the password is extremely complex. This doesn't mean you shouldn't change the password every few months - it means you should add an extra layer of protection.

And given the fact most people use the same password across different account makes it all too easy for hackers to break into an account. For example, let's say you used the same password for your Google account and your employee account.

Suppose someone gains access to the credentials you use for your employee account. They now have access to your Google account – and with, access to vital pieces of personally identifying information and financial data.

However, you can completely nullify unauthorized access by rolling out multi-factor authentication across your accounts.

The Value Of **MFA**

Multifactor authentication is inconvenient, because it takes longer to sign in – but the tedious signing-in process is a good tradeoff for security. You can never put a price on security.

Many employees express their frustration when dealing with a second factor every time they sign in. It also goes without saying that MFA is time-consuming and expensive to set up.

The extra inconvenient steps you and your employees have to go through are worth the security features. MFA makes your networks, accounts, and databases impervious to breaches and hacks.

Bulletproof Solutions for Remote Working

Businesses have pivoted to a hybrid working model (work from home and office). This has increased the need for increased cybersecurity measures – and multi-factor authentication is one of the simplest ways of adding more protection.

Many businesses are now rolling out adaptive MFA, which uses contextual information to determine which identifying factors should apply to a particular user or account. Adaptive MFA looks at various details such as the user's device and location to provide more context.

For example, a user signing in from their office in a trusted location won't be asked to provide additional security factors. But if they log from their home or personal mobile, they may be asked to provide an additional factor because they are using an untrusted device or connection.

Adaptive MFA also solves the problem of inconvenience for most users as long as they are working from a trustworthy connection.

Adaptive MFA makes it easy to gain access to accounts without disrupting the user experience. Moreover, it avoids weighing down the IT team with frequent password resets.

MFA secures a digital environment and the people in it – and the best part is that it also meets regulatory requirements. For example, regulatory frameworks such as the Payment Card Industry Data Security Standard (PCI-DSS) require MFA to be implemented in certain situations to prevent unauthorized users from accessing payment processing systems.

The Risk of **Not Using MFA**

The vast majority of data breach attempts can be stopped with MFA. It is an effective means of protection from social engineering, phishing, and brute force attacks and prevents hackers from using stolen credentials or exploiting weak passwords.

Adding MFA is the most cost-effective security feature that enterprises can add to prevent cyber security incidents. It is useful even in industries that don't require MFA for regulatory compliance.

If someone with the resources wants to discover your credentials, they most likely can, especially now that more businesses are working remotely. However, MFA stops them with an extra layer of protection, with little to no effort required on your end.

Ready to secure your workforce and roll out cybersecurity measures? Get started today and use multi-factor authentication to protect your employees, your business, and your reputation from cybersecurity incidents.

You can also talk to our experts to thoroughly evaluate the security features for your organizations.

Click here to start a security audit!