atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

WHAT IS MULTIFACTOR AUTHENTICATION (MFA)

When securing access to sensitive IT infrastructure, professionals must consider what security authentication method is going to be implemented to protect the data and content stored within. With the prominent and growing concerns of cybercrime and internet security in the computing industry, a simple single factor authentication process with a standard user name and password to access online accounts, computers, servers or even banking services is insufficient.

To maintain security, it is essential that only approved users or authorized personnel are granted privileged access onto IT solutions and services. Most organizations choose to implement a security standard that uses either Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). 2FA and MFA share similar security techniques which require the user to prove their identity; however, there are fundamental differences between them, and although you may not realize it, it is quite likely that you already use these methods in your day-to-day lives.

WHAT IS TWO FACTOR AUTHENTICATION (2FA)

2FA is a security practice wherein access is granted to a user upon provision of **something only they know** (usually a password) with a **security item they have.** This item is usually a physical device provided by an organization or 3rd party, such as a mobile phone, a PKI security card or an RSA Secure Token. These secured items often display a changeable code or pin number. The user must enter their Username and Password, as well as the pin code to access or login. 2FA is extremely popular on the internet and is used by organizations like Amazon and for Google Services like Gmail and YouTube.

As most of the population carry smart phones, many organizations opt to send SMS text codes to users when either accessing secure sites and services or when conducting sensitive transactions, such as removing funds from digital financial services like PayPal or Skrill. Applications have also been developed, like One-Time Password (OTP) Authentication, which generate secure codes that only you and the provider share. Timed One-Time Password (TOTP) apps add a further level of security, as the pin codes TOTP generates will change at a predefined timed interval.

Many business compliance standards, such as Healthcare HIPAA standards, or SOC1/SOC2/SOC3, demand that at least 2FA is implemented for protection of sensitive data and transactions. This is because it is a much more difficult authentication practice to compromise. Server-side authentication devices and those of the user need to be aligned, which makes security breaches unlikely.

WHAT IS MULTIFACTOR AUTHENTICATION (MFA)

MFA is a security practice like 2FA but with an additional layer of complexity to secure logon access. A user is required to provide **something only they know** (again usually a password) with a **security item they have** and **something unique to the user** (such as a fingerprint or retina scan). In extremely secure environments, there may be even more additional security layers required to gain access.

atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

WHAT IS MULTIFACTOR AUTHENTICATION (MFA)

MFA is favoured by Managed Service Providers (MSPs) as it offers significant protection to enterprise files and applications. Besides verifying the identity of each user, the systems can diagnose the health of each MFA device. By establishing the presence of vital security controls and checking for out-of-date software, MFA can easily block high-risk or infected machines or devices.

SFA VS 2FA VS MFA

Both 2FA and MFA are significantly more secure that single factor authentication (SFA). In SFA, only a single password needs to be compromised or cracked to gain unauthorized access. There are password cracking tools available online which can breach low quality or common passwords in a matter of seconds. In SFA, it is the user's responsibility to ensure that a strong password is created, and IT infrastructure administrators cannot always guarantee an employee is not going to use low standards or share their simple passwords. 2FA and MFA enforce additional layers of protection which the user must adhere to in order to gain appropriate system access. Warnings can be flagged if an incorrect part of the 2FA or MFA are entered, and often IT systems will email the user stating that a failed log in attempt has been monitored.

Ease of use must be balanced with security in authentication practices. While strong security is a core concern in IT, it is important to consider the user and how security impacts the user. Not everyone is technically skilled and 2FA and MFA can create barriers within a system that less savvy users will have difficulty surmounting. Best practice should achieve a balance where the system is secure while not hindering the user experience.

2FA and MFA cannot be used in every scenario and are not a full proof answer to a good password policy; for example, consider a scenario where a user has a mobile phone device which acts as a pin code generator to access a system. If the user has no signal or if the mobile phone was in the repair shop, then the user will not get access. To counteract these problems, 2FA and MFA are often only required at first logon or when accessing sensitive data from a new terminal. Once initial trust is established through the use of cookies, SFA is often acceptable for future use for a certain period of time.

Contact Atlantic.Net today and we will be happy to help you strengthen your data security!

Find Out More?

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at www.atlantic.net, call 888-618-DATA (3282), or email us at sales@atlantic.net.