SECURITY: THE POWER OF MULTI-FACTOR AUTHENTICATION

Your accounts, data, and systems are more secure when you add layers of authentication.

In a security setting, authentication means proving your identity. Additionally, you regularly authenticate. The information you enter while logging into accounts and systems is used to verify that you are an authorized user. Single-point authentication, such as using passwords and PINs, has the drawback of being a single point of failure. If the only security measure is a password, and that password is stolen, then everything is compromised.

In order to access a resource, a user must first submit two or more verification factors (known as multifactor authentication, MFA, or 2FA). This security solution is more efficient in an identity and access management (IAM) strategy than a single password.

Before accessing company resources, applications, or VPNs, users must authenticate themselves using two or more factors according to the multifactor authentication (MFA) approach. When Multi-Factor Authentication (MFA) is implemented, users are forced to input additional verification factors in addition to their login and password. These second-factor methods could include push notifications, Google/Microsoft authenticator, OTP by SMS, OTP via email, and many others.

"PASSWORD THEFT AND THE RISE IN SUCCESSFUL CREDENTIAL COMPROMISE ATTACKS ARE WHAT ARE DRIVING MFA ADOPTION" - RICHARD LUNA

Three Primary MFA Authentication Techniques

One of three additional forms of information serves as the foundation for most MFA authentication methods:

1. Things you know (knowledge)

A passphrase, PIN, or password.

2. Things you have (possession)

A timely, individual verification code. Typically, a mobile app or security token will produce these authentication tokens and send them to you through text message.

3. Things you are (inherence)

These are biometrically a part of you, such as a speech pattern, iris scan, or fingerprint.

Why always opt for MFA?

MFA is mandatory in some situations. Employees are frequently required to provide several types of authentication for resources like virtual private networks (VPNs) and cloud-based services by organizations.

In order to access a resource, a user must first submit two or more verification factors (known as multifactor authentication, MFA, or 2FA). This security solution is more efficient in an identity and access management (IAM) strategy than a single password.

1. It's Simple to Add

Yes, you have to do something to make MFA for your logins available. However, the procedure is simple. In general, websites and applications offer clear, step-by-step instructions explaining when to expect an MFA prompt and how to finish a login.

2. It's Simple to Use

An organization can implement MFA in various ways. However, MFA only lengthens the login procedure by a few seconds, regardless of the technology used for the additional authentication factor(s). (And it's worth the extra few seconds.)

3. It's Far Safer Than Just Using a Password

Cybercriminals can access billions of stolen usernames and passwords on darknet forums. What if a compromised password is the only thing preventing a criminal from accessing your data, money, and files? If a threat actor steals (or purchases) account credentials, the damage that can be done is reduced because of MFA.

MFA in Cloud Computing

MFA is becoming more critical now that cloud computing has evolved. Businesses that shift their systems to the cloud may no longer rely on security measures like a user being physically on the same network as a machine. More security must be implemented to prevent malicious actors from accessing the systems. MFA can help establish that users are whom they claim to be by requesting extra authentication parameters that are more difficult for hackers to duplicate or crack using brute force techniques. Users can access these systems from anywhere at any time.

PROTECTED HARBOR