MULTI-FACTOR AUTHENTICATION (MFA)

Every individual within an organization, from the CEO to the intern, has an identity within that organization's networked environment. Organizations use identities to control who may have access to particular networks, systems, services, databases, and files.

The claiming of an identity is known as *authentication*. This is traditionally performed by the user providing a username and password. While passwords have been the most common authentication security control in use for decades, they have also proven to be vulnerable to compromise. Passwords can be stolen or guessed and then used by another individual for malicious purposes. Account holders also have a tendency to re-use passwords for different accounts, which could allow a malicious actor to use one compromised password to access numerous different systems or applications.

What Is Multi-Factor Authentication?

In its simplest form, *multi-factor authentication (MFA)*, which is sometimes referred to as two-factor authentication (2FA), is the use of two ways to authenticate an individual. With MFA implemented, one must provide the first factor (usually a password, but it could also be a fingerprint or face scan) and then a second factor (such as SMS code or physical token) to access a network or service. Factors within an MFA system can take many different forms, which are commonly categorized as:

- **Something you know:** (passwords, PINs, and security question answers)
- **Something you are:** (a physical characteristic or biometric of a person, such as a fingerprint, facial mapping, iris or retinal mapping, or voice print)
- **Something you possess:** (smartcard, banking card, Bluetooth token, a physical security key, or a one-time password or code sent via text message (SMS) or email. Another option is an algorithmically generated, time-based, one-time password (TOTP) through an authenticator application)

To qualify as a true "multi-factor" authentication, the two authenticating factors should be from different categories. Authentication requiring a password as well as the answer to a security question is not a true MFA system as both are "something you know" that could be discovered by a threat actor and used to remotely access a resource.

MULTI-FACTOR AUTHENTICATION (MFA)

Why Should An Organization use MFA?

1. MFA is an added layer of security to protect your organization's networks, operations, and data.
2. Your organization is a target for malicious actors. Yes, no matter its size or operational purpose, disrupting your operations or stealing your data has value to a threat actor.
3. Your cyber insurance may require it. Insurers are requiring that their insureds harden access controls as a part of an overall effort to mitigate cybersecurity threats.
4. Integrating a form of Single Sign-On (SSO) with MFA could actually make your employees more efficient and less frustrated by allowing one authentication to grant them access to all resources and applications that they should have access to, while at the same time increased security.

What are the benefits of implementing an MFA System?

1. **Reduced Helpdesk costs:** Fewer password-related issues, such as resets, mean fewer calls to the IT helpdesk. This translates to reduced operational costs and allows IT personnel to focus on more pressing matters.
2. **Regulatory Compliance:** Many industries have regulations and standards that require enhanced security measures. MFA can help organizations stay compliant and avoid potential legal and financial penalties.
3. **Customer Trust:** If customer data is protected by MFA, you can build and maintain trust with your customer base, which can lead to more profit.
4. **Flexibility:** MFA solutions can be tailored to fit the needs of organizations, whether it's a large corporation or a startup. As your company's needs change, so can the MFA solution.
5. **Supports Remote Work:** This is the era of work-from-home, which can lead to greater security concerns. MFA allows employees to access company resources security from any location.
6. **Analytics:** MFA solutions offer insights into authentication attempts, which can help an organization identify potential threats, patterns and vulnerabilities much more easily.
7. **Ease of Implementation:** Modern MFA solutions are user-friendly, which reduces the burden on both the end-users and the IT department.