Securing Our World Through Multi-Factor Authentication

A Vital Layer of Security

Cybersecurity Awareness Month

Office of Information Technology / Division of Information Security

Multi-Factor Authentication (MFA) is a security process that requires users to provide two or more verification factors to gain access to a system, application, or account. Instead of relying solely on a password, MFA combines various elements: knowledge-based factors (like a password or PIN), possession-based factors (such as a smartphone or security token), and/or inherit traits (such as biometric verification with a fingerprint or facial recognition).

MFA typically involves the following three types of authentication factors:

1. Knowledge Factor (a personal possession): This is the most common form of authentication and includes passwords, PINs, or answers to security questions.

2. Possession Factor (an item you possess): This factor requires something that only the user possesses, such as a smartphone, security token, or PIV card.

3. Inherence Factor (an asset you possess): This refers to biometric verification, which leverages the unique characteristics of the user such as fingerprints, facial recognition, or voice recognition.

When MFA is enabled, users must provide at least two of these factors to access their accounts.

The Importance of MFA.

1. Increased Security: By requiring multiple forms of authentication, MFA reduces the risk of unauthorized access even if one factor (such as a password) is compromised.

2. Compliance Requirements: MFA is often mandated as part of compliance with data protection laws.

3. Protection Against Identity Theft: MFA ensures that even if an attacker gains access to login credentials, they still cannot access the account without the additional verification factor.

4. User Trust: Customers are more likely to trust a company that takes their security seriously and implements robust measures.