Multi-Factor Authentication

Multi-factor Authentication (MFA) is a way of establishing and confirming a user's identity on a system. It consists of a unique ID such as a username, account number, or email and a password; then another piece (or multiple pieces) of information that are unique and preferably dynamic or changing.

Many systems only use a user ID and password that can be stolen and used by others. MFA uses separate repositories of information, so there is no single data source. If an online service provider, for instance, has your username and password secured in their database, the next factor could be a code sent to your email that you key in. This code might only be valid for five minutes, so it is very temporary and worthless once it expires. By using MFA, the user must have access to both factors to sign in.

There are several types of factors:

- **Knowledge factors** like your user ID and password
  - PINs
  - Secret questions, which should be obscure and hard to figure out like, "What did I call my second car?" instead of something easy to figure out like, "Where was I born?"
- **Possession factors** which are similar to your car key. These are often called security tokens.
  - A disconnected token might be a keychain type of device with a display that shows a code that changes every minute
  - A connected token might be a USB key or ID card that you plug into the computer
  - A software package that is installed on your computer or mobile device
- **Inherent factors** are identifiable traits associated with the account owner
  - Biometrics like fingerprints or eye/face/voice recognition. Biometrics can make mistakes or be spoofed, so use caution here if using them as a complete authentication method!
  - Behavior biometrics like intelligent keyboard or mouse usage dynamics

A few examples of authentication tools:

Software Key Apps: Google Authenticator, Authy, LastPass Authenticator, Microsoft Authenticator

Hardware Keys: RSA, Duo, YubiKey, ShoBadge, HID Global

Biometrics: Apple Touch ID/Face ID, Samsung Pass, Microsoft Windows Hello, Voice Biometrics Group

Possession Keys: Email code, text message code, automated phone call to mobile phone with code

The best solutions for your situation will vary depending on the level of security needed, costs involved, employee training, etc. We're here to help you make the best decisions for your company's security and IT needs. ***We welcome your questions!***

You can contact us at **385.312.9030** or submit your questions at https://sanityworx.com anytime.