Office of the
Chief Information
Security Officer
State of Texas

Multi-Factor Authentication (MFA) Best Practices

What is MFA?

MFA is a security enhancement used when logging in to a digital resource. It requires the user to validate their credentials by providing two or more pieces of evidence (authentication factors) to gain access.

Why Use MFA?

A common authentication used is a password. While using a complex alphanumeric password offers extra security it is difficult to remember. Using password managers can help but they are geared towards tech savvy users and typically charge a subscription fee.

Using MFA adds an additional layer of security making it harder for attackers to take over your devices and online accounts. So, even if your credentials are hacked or leaked, the password alone will not be enough to gain access.

82% of hacking-related breaches are due to compromised, reused, or weak passwords*.

How To Use MFA?

Log in with your traditional username and password. You'll be prompted to provide an additional authentication factor (see list below). Depending on the additional factor, you may be asked to enter a One-Time Passcode (OTP). Upon verification of additional factor, access is granted.

Three Types of Authentication Factors:

1. Something you **know** (password, PIN etc.).
2. Something you **have** (a physical object such as a smart phone, laptop, USB hard token etc.).
3. Something you **are** (biometrics such as thumbprint, face ID etc.).

*2022 Verizon Data Breach Investigations Report

What is One-Time Passcode (OTP)?

An OTP is an automatically generated number for a single login session. It's only valid for a short time before it expires so it cannot be reused. The OTP can be delivered via:

Email (Easy to Use)

- If your email account is already compromised, or doesn't have MFA enabled itself, then any account that uses it for OTP delivery will also be compromised.
- Not a recommended method but still better than username/password only.

Authenticator App (Best Security and Ease of Use)

- Available for free from Microsoft, Google, and others.
- Push notification options can be vulnerable to "prompt bombing".
- Recommended method because attacker cannot intercept the OTP.

SMS or Phone Call (Easy to Use and Very Common)

- Vulnerable to "SIM swapping" through social. engineering targeting your cell phone service provider (out of your control).
- Not a recommended method but still better than username/password only.

Hard Token (Most Secure)

- Least convenient as it requires the token (a device) to be physically present when you login.
- If lost or stolen, replacement is complicated.
- Recommended method because attacker would need to have the token physically in their possession.

⚠ **Never share the OTP with anyone or enter it outside of the login prompt.**