



Counter
Terrorism

Cyber Incident
Response Team

Andrew M. Cuomo
Governor



Something
you have



Something
you are



Something
you know

Multi-Factor Authentication (MFA)

Multi-factor authentication creates a layered defense that combines two or more independent credentials: what the user knows (passwords), what the user has (security token) and what the user is (biometric verification).

- Only 28% of people are using multi-factor authentication
- 67% of people share their passwords with friends, family, or colleagues
- Around 81% of data breaches have been the result of weak or stolen passwords

Multi-factor authentication makes it difficult for an unauthorized person to gain access to your data even if your password is compromised.

- Data breaches involving disclosure of passwords are commonplace
- If your password has been compromised through a data breach or other means, a second factor such as a physical security token or mobile device push notification may be all that stands between a would-be attacker and your data

Common multi-factor authentication methods:

- Hardware authenticators (Smart Cards, YubiKey, Titan)
- Time-based tokens (physical or app-based RSA token)
- Mobile application push notifications
- SMS/text message code notifications

You should use MFA whenever possible, especially when it comes to your most **sensitive** data!

If you suspect a cyber incident, immediately contact:

CIRT is an initiative of the New York State Division of Homeland Security and Emergency Services.
For additional information, visit dhses.ny.gov/oct/cirt