Multi-Factor Authentication

Multi-factor Authentication (MFA) is a widely used method of authentication where users are required to provide two or more types of verification factors to gain access to a system, application or account. This is usually done in order to make it harder for unauthorized individuals to access sensitive resources, even if they have compromised the user's password.

Now, IAM, which is responsible for handling the signing in of accounts to the AWS Console and granting access to AWS services, provides us with out-of-the-box MFA integration as one its key features, allowing us to add an additional layer of security to our AWS account in the form of an One-Time-Password (OTP) from a mobile app, a hardware token, or an SMS.

In fact, not utilizing MFA when using IAM credentials as the primary method of accessing the AWS Management Console or CLI is generally frowned upon, with AWS designating Multi-Factor Authentication as an **IAM Best Practice**.

It is accepted as an IAM best practice for system administrators to utilize MFA (Multi-Factor Authentication) for more secure access to AWS Services.