

# USE MULTI-FACTOR AUTHENTICATION



Creating a strong password is the first crucial step in safeguarding your account against hackers. However, even robust passwords can be susceptible to cyberattacks. Utilizing multi-factor authentication ensures that a hacker who obtains your password cannot access your account without an additional authentication factor. The most prevalent form of multi-factor authentication involves receiving a verification passcode via text message or email.



## ENABLE MFA ON ALL CRITICAL ACCOUNTS

Activate Multi-Factor Authentication (MFA) for crucial accounts like emails, banking, and work-related systems to enhance security. MFA requires a second form of verification, like app code, fingerprint, or facial recognition, reducing unauthorized access and protecting sensitive information.



## USE DIFFERENT TYPES OF AUTHENTICATIONS

Diversify your authentication methods, including apps, hardware keys, and biometric authentication, to improve security against various attacks. Avoid relying solely on SMS codes, as they are susceptible to interception or SIM-swapping attacks.



## REGULARLY UPDATE AUTHENTICATION METHODS

Regularly updating your authentication methods, such as changing your phone number or using a different device for MFA, is crucial for maintaining strong security. This ensures that your accounts remain secure and lessen the risk of account lockout or potential threats.



## REGULARLY UPDATE AUTHENTICATION APPS THAT YOU USE

Regularly check for app updates and double-check your authentication app settings to ensure they are up to date with the latest security features. Review and validate your verification settings to ensure they meet your current security requirements, thereby reducing the risk of security issues.

