

BEST PRACTICES TO PREVENT MFA BYPASS ATTACKS

1

Set push notification limits

Limit or disable MFA push notifications per login attempt to prevent attackers from overwhelming users with fraudulent requests.



2

Switch on number matching

Enable number matching in the MFA settings to ensure only legitimate users can authenticate by requiring them to input a code from their browser onto their device.



3

Use hardware security keys

Use hardware security keys for secure, passwordless authentication to reduce risks of session-based MFA and man-in-the-middle attacks.





Change human cyber security behavior with

security[®]
quotient.

Singapore | India | Malaysia