MFA Recovery & Lockout Communication Guide

The following document outlines the steps users should take in the event they are locked out of their account due to lost or inaccessible Multi-Factor Authentication (MFA) devices. It also provides guidance for secure recovery and best practices to prevent future incidents.

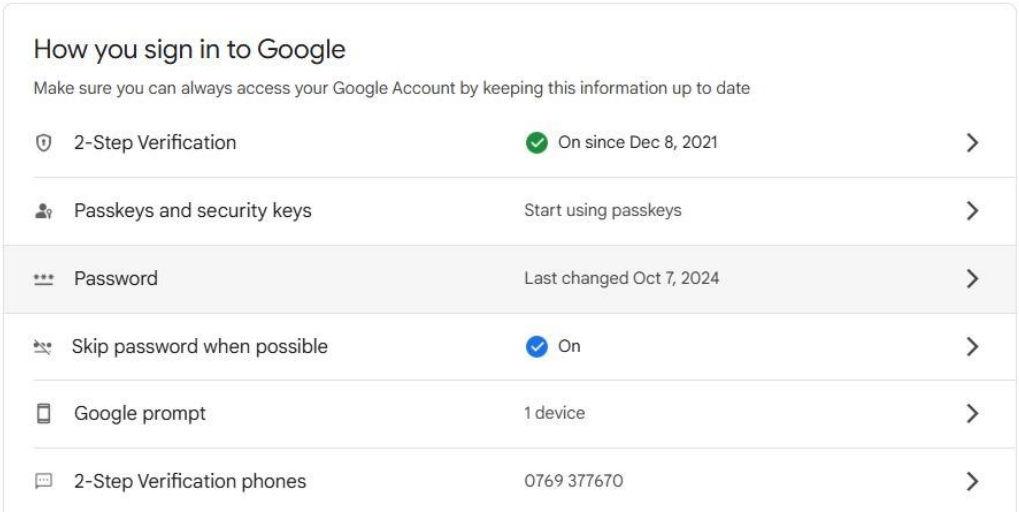
1. Purpose of MFA

Multi-Factor Authentication (MFA) is a security mechanism that enhances account security by requiring users to verify their identity using more than one method, such as a password and a mobile app code. It plays a big role in ensuring that even if a password is compromised, unauthorized access is prevented.

2. Recovery Process (Lost or Inaccessible Device)

Follow these steps if you lose access to your MFA device:
1. Notify IT Support immediately.
2. Verify your identity through secondary email or security questions.
3. IT Admin resets your MFA registration.
4. Re-register your MFA on a new phone using Google Authenticator or another approved method.
5. Test your login to ensure MFA is functioning correctly.

3. Screenshots.



Google

Google Verification Code

Dear Google User,

We received a request to access your Google Account [redacted] through your email address. Your Google verification code [redacted]

If you did not request this code, it is possible that someone else is trying to access the Google Account [redacted]. **Do not forward or give this code to anyone.**

Sincerely yours,

The Google Accounts team

4. Preventive Recommendations

Add a secondary verification method such as SMS or backup email.
Review your MFA settings quarterly to ensure accuracy.
Avoid approving unknown MFA requests.

5. Support Contact

If you cannot complete recovery, contact your system administrator or IT support desk.

Email address: *trsttch.IT@gmail.com*

Or Call:+254 76393300