

Samuel Opoku Afriyie

Technical Writer

Two-Factor Authentication (2FA)

Explanatory Guide with User Instruction Elements

Version: 1.0

Last Updated: June 2026

Applicable For: General Users / Employees / Customers

Document Purpose

This guide explains **Two-Factor Authentication (2FA)**, its importance, and how to use it to secure your account.

Key Topics Covered

- What is 2FA?
- How 2FA Works (SMS, Email, Authenticator Apps)
- Why 2FA is Important
- Step-by-Step Setup & Verification

Notes

- For support, contact: gids@gmail.com
- © 2026 | Gidsind Company . All rights reserved.

1. Introduction

1.1 What is Second-Factor Authentication (2FA)?

Second-Factor Authentication (2FA) is a security management system that enhances account protection by adding a second security identification. While the primary security measure is the username and password, 2FA provides an additional layer of defence. This guide aims to explain 2FA to general users.

1.2 Examples of 2FA

- Google Authenticator
- Email verification
- Biometric verification: Face recognition, fingerprint

2. How Does 2FA Work?

Login processes vary depending on the platform. However, 2FAs follow a similar procedure:

A. First Factor

The user is required to log in by entering the login credentials which are:

- **Username/ Email**
- **Password**

B. Second Factor

If the credentials are recognised, the user is requested to authenticate the account using:

- **SMS code:** A one-time code is sent via text.
- **Email verification:** A link or code is sent to the user's email.
- **Google Authenticator:** User enters a code from their Authenticator app.

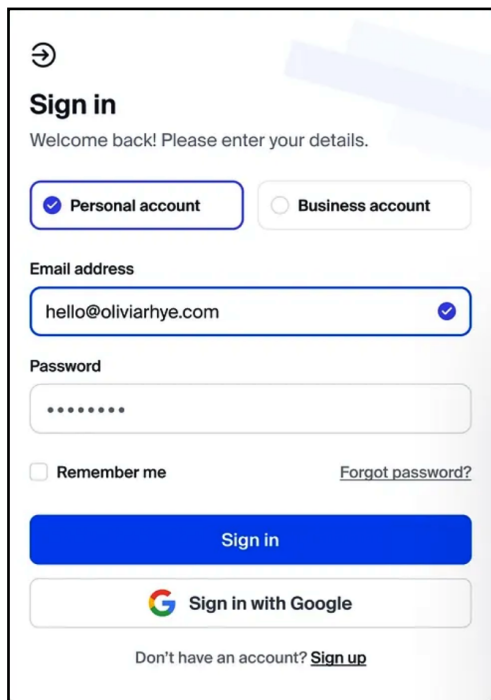
- **Device lock:** Biometric or device unlock method (e.g., fingerprint or PIN).

C. Verification

The user's account is verified and is granted access. This only takes a few seconds.

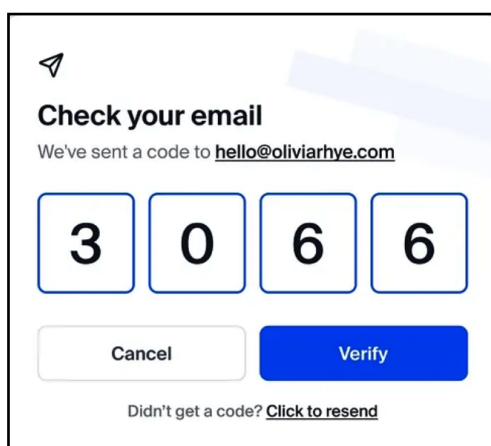
An example of 2FA using an email would progress like this:

1. The user enters their name and email, then taps **Sign in**



A mobile app sign-in screen. At the top is a back arrow icon. Below it is the title "Sign in" and a subtitle "Welcome back! Please enter your details." There are two radio buttons: "Personal account" (selected) and "Business account". Below these is an "Email address" field containing "hello@oliviarhye.com" with a checkmark icon on the right. Below the email field is a "Password" field with masked characters ".....". To the left of the password field is a "Remember me" checkbox, and to the right is a "Forgot password?" link. Below the password field is a large blue "Sign in" button. Below that is a "Sign in with Google" button with the Google logo. At the bottom is a link: "Don't have an account? [Sign up](#)".

2. The user receives an email containing a **code** that they type into the space.

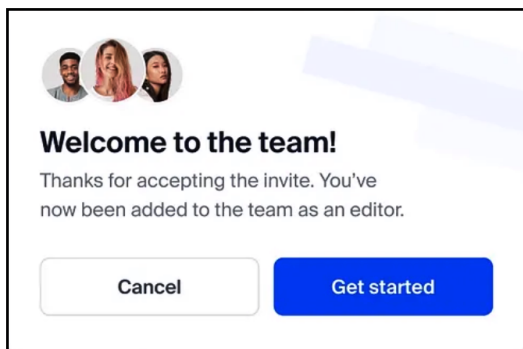


A mobile app screen for checking email. At the top is a paper plane icon. Below it is the title "Check your email" and a subtitle "We've sent a code to [hello@oliviarhye.com](#)". Below the subtitle are four input boxes containing the numbers "3", "0", "6", and "6". Below these boxes are two buttons: "Cancel" and "Verify". At the bottom is a link: "Didn't get a code? [Click to resend](#)".

3. The account is verified



4. The user is granted full access.



You can find more 2FA image examples [here](#).

3. Why is 2FA Important?

- **Enhanced Security** – Even if a password is compromised, the second factor blocks unauthorized access.
- **User Confidence** – Users are assured of better protection against hacking attempts.

4. Summary

Two-Factor Authentication (2FA) is a reliable security management procedure that involves a few steps to provide an additional layer of defence for accounts and ensure a secure login for all users