

**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](mailto:gids@gmail.com)
- © 2026 | Gidsind Company . All rights reserved.

## 1. Introduction

### 1.1 What is Two-Factor Authentication (2FA)?

Two-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:

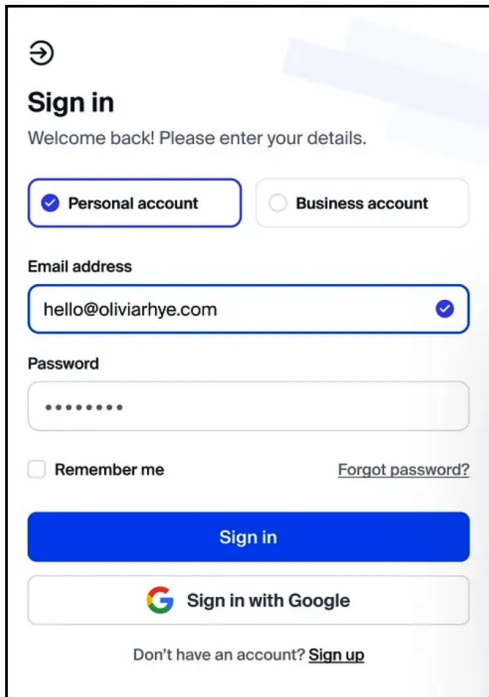
- **SMS code:** A one-time code is sent via text.
- **Email verification:** A link or code is sent to the user's email.
- **Google Authenticator:** User enters a code from their Authenticator app.
- **Device lock:** Biometric or device unlock method (e.g., fingerprint or PIN).

### C. Verification

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

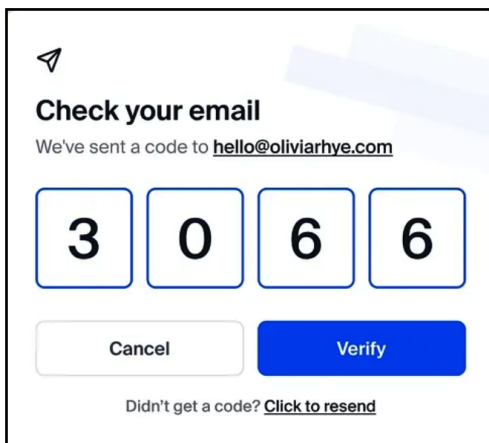
An example of 2FA using an email would progress like this:

1. The user logs in using a username and password.

A screenshot of a web application's sign-in page. At the top left is a circular arrow icon. Below it is the heading "Sign in" and a subtext "Welcome back! Please enter your details." There are two radio buttons: "Personal account" (selected) and "Business account". Below these is a text input field for "Email address" containing "hello@oliviarhye.com" with a blue checkmark on the right. Underneath is a "Password" field with masked dots. To the left of the password field is a "Remember me" checkbox, and to the right is a "Forgot password?" link. A large blue "Sign in" button is centered below the password field. Below that is a "Sign in with Google" button featuring the Google logo. At the bottom, it says "Don't have an account? [Sign up](#)".

*Screen prompting the user to enter email address and password.*

2. The system emails the user a one-time code.

A screenshot of a "Check your email" screen. At the top left is a paper plane icon. Below it is the heading "Check your email" and subtext "We've sent a code to [hello@oliviarhye.com](#)". In the center are four square boxes containing the digits "3", "0", "6", and "6". Below these boxes are two buttons: "Cancel" and "Verify". At the bottom, it says "Didn't get a code? [Click to resend](#)".

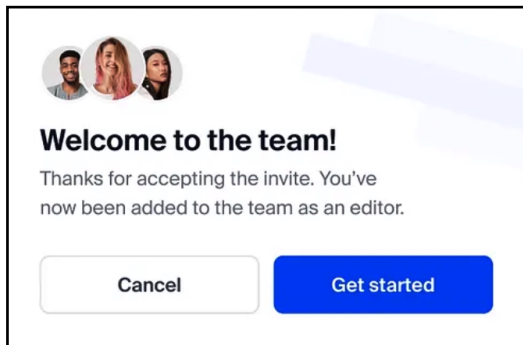
*A screen displaying spaces for verification code input.*

3. The system verifies the account.



*A screen displaying a successful account verification.*

4. The user gains full access.



*A screen displaying a successful login.*

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. Setup & Troubleshooting

### A. How do I enable 2FA on my account?

1. Go to **Account Settings** → **Security**.

2. Select **Enable 2FA** and choose your method (SMS, app, etc.).
3. Follow the prompts to verify.

## **B. What if I don't receive my 2FA code?**

- Check your spam/junk folder (for email codes).
- Ensure your phone has signal (for SMS).
- Use a backup method (e.g., authenticator app).
- Click "**Resend Code**" or contact support.

## **C. Can I use 2FA without a phone?**

Yes! Use an **authenticator app** (works offline) or **email-based 2FA**.

---

## **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