Yo!Gigs

SMTP Email Service

-v3.0 Setup Guide-

Table of Contents

What is SMTP?

SMTP, or Simple Mail Transfer Protocol, is a standard protocol used for sending emails over the Internet. It defines the rules and procedures for email transmission between servers. When you send an email, SMTP is responsible for directing the message from your email client (like Outlook or Gmail) to the email server and then on to the recipient's server.

Here's a basic overview of how SMTP works:

1. **Sending email:** When you compose and send an email, your email client communicates with an SMTP server.
2. **SMTP server:** The SMTP server processes the email and determines the best route to deliver it.
3. **Delivery:** The email is then transferred to the recipient's email server using SMTP or other protocols, such as IMAP or POP3, for retrieval and storage.

SMTP is a text-based protocol and operates over port 25 by default, although other ports like 587 and 465 are also commonly used for secure email transmission.

If you decide to use the SMTP service for sending out system email notifications to all the users including you on the platform, you will need to configure the SMTP feature using the applicable data from an SMTP provider.

Although every type of email service offers SMTP services, we will be using the Google email service to obtain the required SMTP information and configure it on the platform.

Google SMTP service charges

SMTP services provided by Google are not entirely free but have different tiers based on usage and the specific service you're using.

Here's a breakdown:

1. **Gmail SMTP Server:** If you're using a regular Gmail account, you can send emails through Gmail's SMTP server (smtp.gmail.com). However, there are sending limits and restrictions. For instance, personal Gmail accounts have a daily sending limit, and excessive use might result in temporary suspension of the service.

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An asterisk (*) next to a label indicates that the information is mandatory.

2. **Google Workspace (formerly G Suite):** For businesses and organizations using Google Workspace, SMTP services are included as part of the subscription. Google Workspace accounts typically come with higher sending limits and additional features compared to personal Gmail accounts.

3. **Google Cloud Platform (GCP):** Google Cloud offers a more scalable SMTP solution through services like SendGrid, which can be integrated with Google Cloud. These services typically operate on a pay-as-you-go basis, and there may be costs associated with higher usage levels.

In summary, while you can use Gmail's SMTP for free within certain limits, extensive or professional use might require a Google Workspace subscription or a paid service through Google Cloud.

Refer to Google support articles or contact the Google support team to know more.

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

Configure the SMTP Email Service

Configure the SMTP email service under **Admin panel > Settings > System configurations > Email & SMTP** tab.

You can configure these settings from any of the following account types:

- **Third-party email account:** We cannot provide specific steps/SMTP information for any other third-party email accounts, as the data is different for each service provider. For assistance in such a case, please refer to help from Google.

- **Gmail Business account:** You need a Gmail Business account, which typically has an address like *abc@domain.com*, where "**domain**" represents your business or platform name.

- **Gmail account:** You need a simple gmail account; for example, *abc@gmail.com*.

Since email service configurations vary, we will provide setup steps and details specifically for Google-based accounts, including Gmail and Google Workspace (formerly G Suite).

The SMTP configuration settings are the same for all Gmail accounts. For uninterrupted use of the SMTP service, it is advised to enable 2-Step Verification.

<u>DISCLAIMER:</u> The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

If you prefer not to enable 2-Step Verification, you can skip directly to **configuring the SMTP service** on your platform.
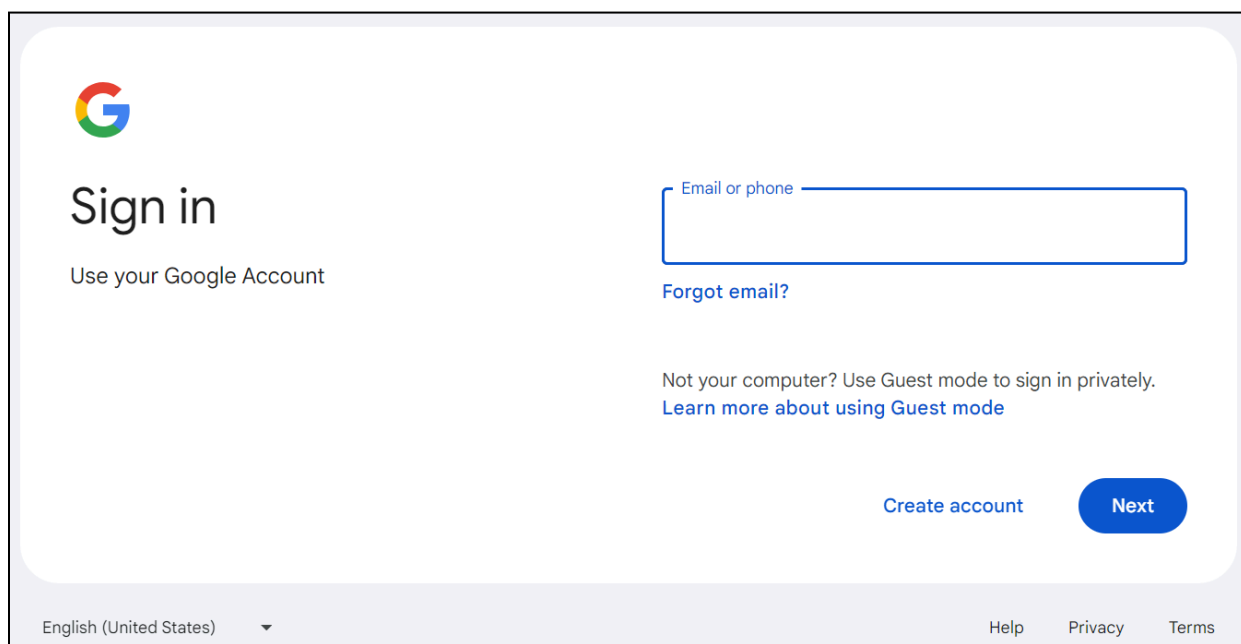
Steps to enable 2-Step Verification

If you decide to enable the 2-steps authentication, follow the steps shared below:

Step 1: Visit the Google My Account page

Visit https://myaccount.google.com/.

If you are not already logged in, you will be taken to the login page. Sign in to your Gmail Business or Gmail account using your credentials.
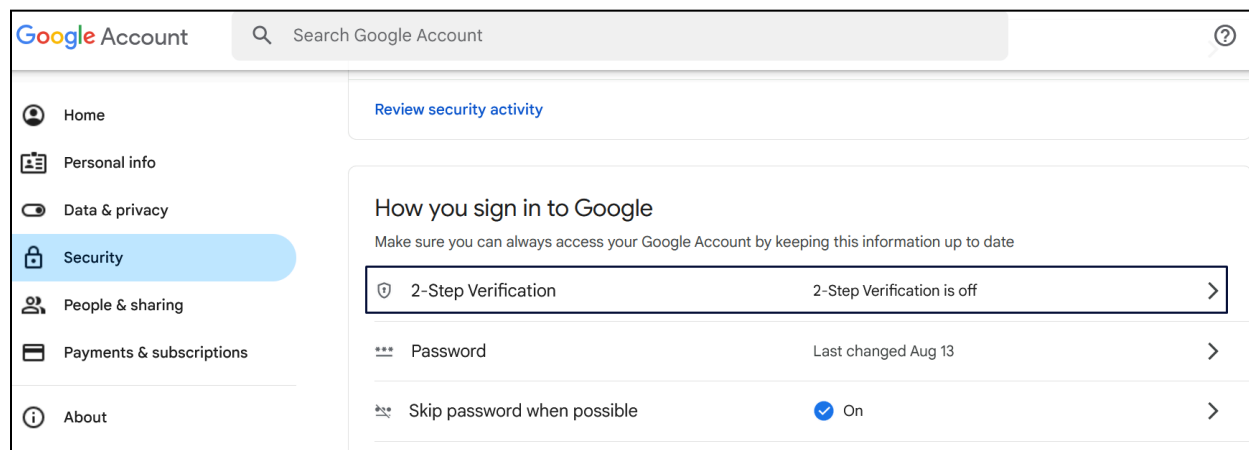

Once logged in, you will be directed to the My Account page.
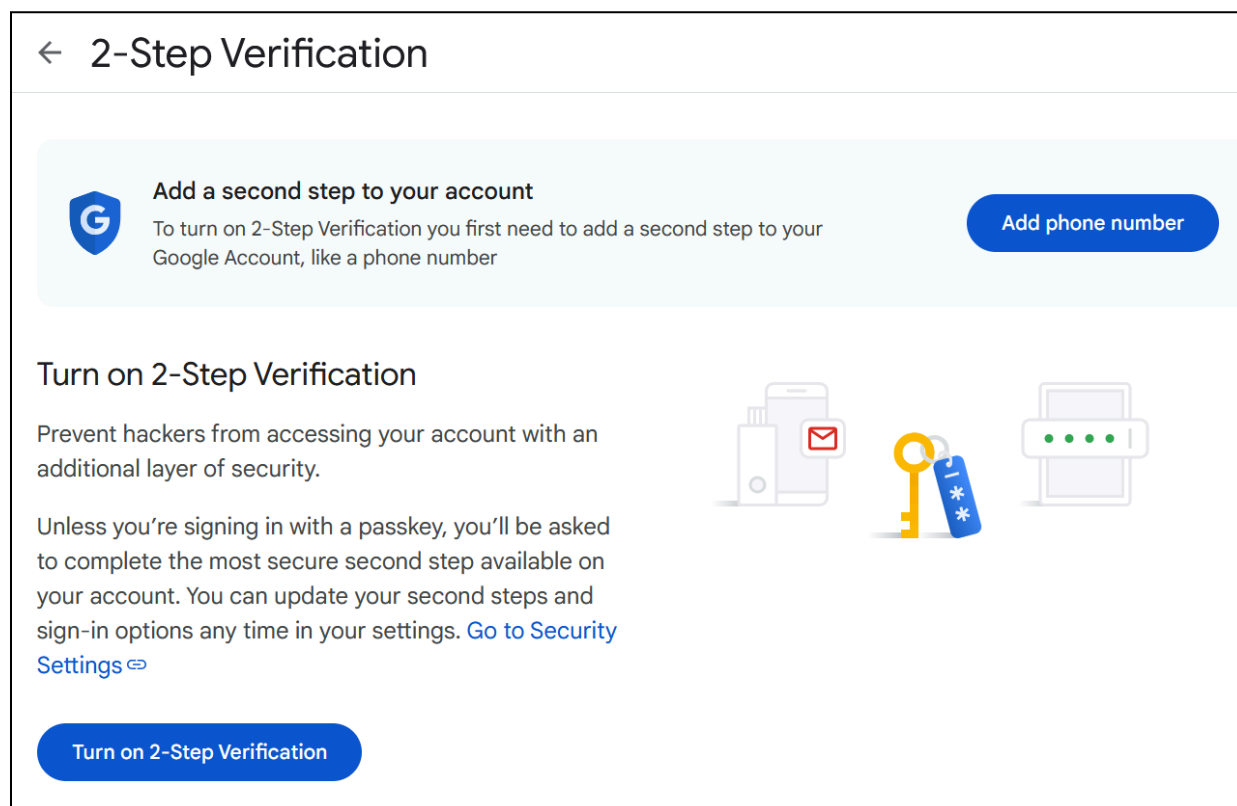
Step 2: Set up 2-Step Verification for your account

To enable 2-Step Verification for your account, select **Security** from the left-side navigation panel on your **My Account** page.

Scroll down to the "**How you sign in to Google**" section.

You will be asked to verify your identity by entering your password again.

Once entered, you will be directed to the 2-Step Verification page.

Click **Turn on 2-Step Verification** to proceed to the next step, or click **Add phone number**.

In both situations, the **Add a phone number for 2-Step Verification** pop-up form will appear.

Add a phone number for 2-Step Verification

A phone number can be used as a second step, to help you sign back in if you lose access, and to receive alerts if there's unusual activity

| 🇺🇸 ▼ | Enter phone number |

You can use a Google Voice number, but you won't be able to receive codes if you lose access to your Google Account. Charges from your carrier may apply. Learn more about how Google uses this info ⓘ

Cancel   Next
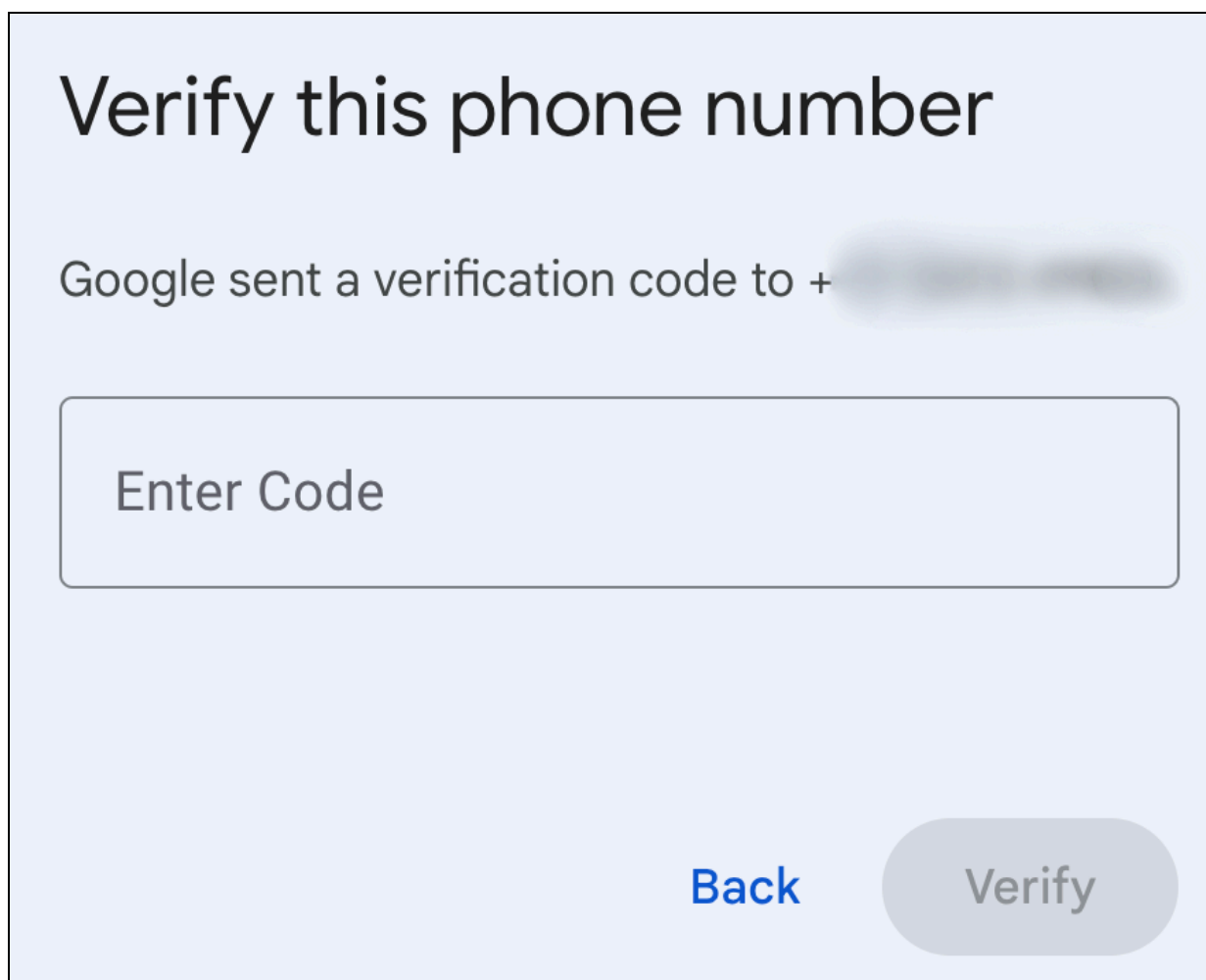
Start by selecting your country code.

Next, enter the phone number in the following field.

Click **Next**.

A verification code will be sent to the phone number you provided.

Additionally, a **Verify this phone number** pop-up will appear.

Verify this phone number

Google sent a verification code to +

Enter Code

Back   Verify

Enter the code you received on your mobile phone in the designated field.

Then, click **Verify**.

Another pop-up will confirm that the process is complete and that 2-Step Verification has been added to your account.

You're now protected with 2-Step Verification

When signing in you'll be asked to complete the most secure second step, so make sure this info is always up to date

💬 Phone number   ✓ ⬛⬛⬛⬛

Done

Click **Done**. This will direct you back to the 2-Step Verification page.

Google Account

← 2-Step Verification

Your account is protected with 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. Go to Security Settings 🔗

Turn off 2-Step Verification

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

Step 3: Generate the Google App Password

Since you have enabled 2-Step Verification on your Google account, you now need to generate a Google App password for SMTP access.

This password serves as a secure alternative to your regular account password for applications that don't support 2-Step Verification. Using an App password ensures that the enhanced security of 2-Step Verification is maintained while allowing your SMTP service to function properly without exposing your primary password.

To obtain this password, visit:

https://security.google.com/settings/security/apppasswords

You will be asked to re-enter your email password again. And you will be directed to the **App passwords** page.

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

Enter a name for your app password and then click **Create**.

This will create your app password.

Copy and save this password, as you will need it in place of your Google password when entering the SMTP details.

⊕ *Note that you won't be able to retrieve this same app password again; if needed, you will have to generate a new one.*

Then, click **Done**.

Now, go to your platform's admin panel and enter the SMTP details.

Instead of your Gmail account password, use the app password you generated (since 2-Step Verification is enabled).
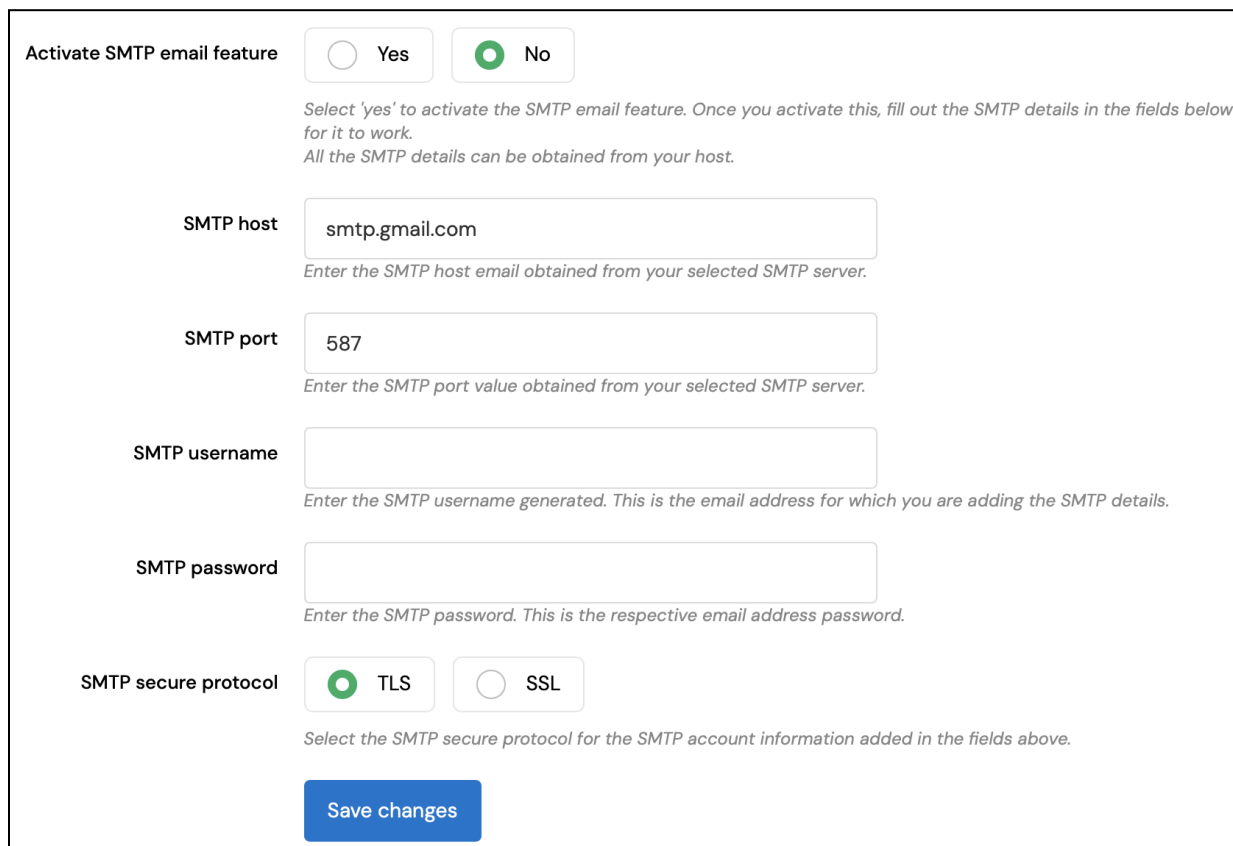
DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

Update the SMTP Settings on the Yo!Gigs admin panel

On another tab, open the admin panel of your platform.

Go to **Settings > System configurations > Email & SMTP tab.**

Activate SMTP email feature	○ Yes ● No

Select 'yes' to activate the SMTP email feature. Once you activate this, fill out the SMTP details in the fields below for it to work.
All the SMTP details can be obtained from your host.

SMTP host

smtp.gmail.com

Enter the SMTP host email obtained from your selected SMTP server.

SMTP port

587

Enter the SMTP port value obtained from your selected SMTP server.

SMTP username

Enter the SMTP username generated. This is the email address for which you are adding the SMTP details.

SMTP password

Enter the SMTP password. This is the respective email address password.

SMTP secure protocol   ● TLS   ○ SSL

Select the SMTP secure protocol for the SMTP account information added in the fields above.

Save changes

Enter the following information in the fields provided:

- **Activate SMTP email feature:** Select 'Yes' to activate the SMTP email feature. Once you activate this, fill out the SMTP details in the fields below for it to work.

- **SMTP host:** Enter – smtp.gmail.com – in this field.

- **SMTP port:** There are two options for this:

  - **TLS:** If you are choosing this port, enter 587 in this field. Use this port for SMTP with TLS (Transport Layer Security). It's the most commonly used port for secure email communication and is **recommended** for most email clients and applications.

<u>**DISCLAIMER:**</u> The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

- ○ **SSL:** If you are choosing this port, enter 465 in this field. Use this port for SMTP with SSL (Secure Sockets Layer). While it is also secure, it's less commonly used compared to Port 587.

- **SMTP username:** Enter your valid Gmail address or Gmail business account address.

  *Ensure this same email address is added in the '**From email**' field at the top of the Email & SMTP tab page.*

- **SMTP password:** Enter your Gmail account password in this field.

  If you have enabled 2-Step Verification, use the app password you generated instead of your regular Gmail password.

- **SMTP secure protocol:** Depending on the port entered, select either 'TLS' or 'SSL' as needed:

  - ○ **Port 587:** Select TLS (Transport Layer Security), if you are using this port.

  - ○ **Port 465:** Select SSL (Secure Sockets Layer), if you are using this port.

Click **Save changes** to update the information.

Working of the SMTP email service

Instead of using the PHP system embedded into the platform system, all the platform emails will be sent via the SMTP service you configured.

You can edit all the email templates sent by the platform under **CMS > Email templates**.

Yo!Gigs - Online Service Marketplace Solution

Visit https://www.yo-gigs.com/ to know more!

www.fatbit.com | sales@fatbit.com

[Contact us](#)

+91 95555 96666 / +91 73075 70707

Copyright ©FATbit Technologies (Ably Soft Pvt. Ltd). All Rights Reserved.

The information contained in this document represents the current views, requirements as interpreted by FATbit Technologies for its clients. All information contained within this document is proprietary to us, unauthorized disclosure, distribution of the information contained either in part or as a whole shall not be accepted and shall be considered a breach of Copyright and Intellectual rights.