

# CyberPilot

---

**Guide: Whitelisting in Google**

# Intro: Whitelisting guide for Phishing Simulation

- The guide relates to **Google** .
- This guide is for administrators to help whitelist in order to run phishing simulations for the organization's users.

# Step 1: Configure Spam, phishing, and malware in Google

**Step 1.1:** Go to your Google admin <https://admin.google.com/>

**Step 1.2:** Click on Apps

The screenshot shows the Google Admin console interface. At the top, the browser address bar displays `admin.google.com`. A red arrow points to the address bar with the text **(1) Go to https://admin.google.com/**. Below the address bar, the Admin console header includes a search bar with the text "Search for users, groups or settings". On the left side, there is a navigation menu with the following items: Home, Directory, Devices, Apps, Security, Reporting, Account, and Storage. A red arrow points to the "Apps" menu item with the text **(2) Click on Apps**. The main content area is divided into two columns. The left column is titled "Users" and includes a "Manage" link and a list of actions: "Add a user", "Delete a user", "Update a user's name or email", and "Create an alternate email address (email alias)". The right column is titled "Discover" and includes a "See all" link and an illustration of a person and a dog. Below the illustration, there is a section titled "Get the most out of Google workspace" with the text "Learn more about the best features of Google Workspace and make sure everything is set up just right" and a link "DISCOVER GOOGLE WORKSPACE".

# Step 1: Configure Spam, phishing, and malware in Google

## Step 1.3: Click on Gmail

The screenshot displays the Google Admin console interface. On the left, a navigation menu lists various services: Home, Directory, Devices, Apps, Overview, Google Workspace (Service status, AppSheet, Calendar, Drive and Docs, Gmail, Google Chat, Google Meet, Google Voice, Groups for Business, Jamboard, Keep, Sites, Tasks), and a red arrow points to the 'Gmail' link with the text '(3) Click on Gmail'. The main content area is divided into several sections: 'Users' (Manage, 59 Active, Add a user, Delete a user, Update a user's name or email, Create an alternate email address), 'Discover' (See all, Get the most out of Google workspace), 'Product updates' (View all, Google Workspace Updates Weekly Recap - Feb 9 February 9, 2024, Share spaces smart chips in Google Chat - Feb 9, Google Meet hosts can pin multiple tiles for all meeting participants - Feb 5, Google Workspace Updates Weekly Recap - Feb 2 February 2, 2024), 'Alerts' (View alert center, You don't have any open alerts), 'Groups' (Create groups for mailing lists and applying policies), 'Account settings' (Manage your organization's profile and preferences), 'Buildings and resources' (Manage and monitor your buildings, rooms, and resources), 'Apps' (Manage web and mobile app access and settings), 'Organizational units' (Organize users into units for applying policies), and 'Directory sync' (Manage your external directories).

# Step 1: Configure Spam, phishing, and malware in Google

**Step 1.4:** Scroll down to the bottom of the section

**Step 1.5:** Click on Spam, Phishing and Malware

The screenshot displays the Google Admin console interface. On the left, a navigation sidebar lists various services under 'Google Workspace', including Gmail, Google Chat, and Google Meet. A red arrow labeled '(4) Scroll down' points to the 'Gmail' link. The main content area shows the 'Settings for Gmail' page, with a search bar at the top and a list of configuration sections. A red arrow labeled '(5) Click on Spam, Phishing and Malware' points to the 'Spam, Phishing and Malware' section in the list. The sections listed are: 'Configure email and spam safety features', 'Setup', 'End User Access', 'Spam, Phishing and Malware', 'Compliance', and 'Routing'. The 'Spam, Phishing and Malware' section is currently expanded, showing 'Configure spam, phishing and malware features'.

# Step 1: Configure Spam, phishing, and malware in Google

## Step 1.6: Click Edit on Email allowlist

The screenshot shows the Google Admin console interface. On the left is a navigation menu with 'Gmail' selected. The main content area is titled 'Spam, phishing, and malware' and contains several settings sections: 'Email allowlist', 'Enhanced pre-delivery message scanning', 'Inbound gateway', and 'Spam'. The 'Email allowlist' section is highlighted, and a red arrow points to the 'Edit' button next to it. The 'Spam' section contains a table with the following data:

Description	Status	Source	Actions	ID	Values
clients	Enabled	Locally applied	<a href="#">Edit</a> - <a href="#">Disable</a> - <a href="#">Delete</a>	b9796	Aggressive spar Bypass internal Bypass approve Bypass approve Bypass spam fil Quarantine mes Aggressive spar Bypass internal

(6) Click Edit on Email allowlist

# Step 1: Configure Spam, phishing, and malware in Google

**Step 1.7:** Type our IP address: 3.75.105.111. If you have other IPs, make sure to separate them with commas

**Step 1.8:** Click Save

The screenshot shows the Gmail Admin console interface. On the left is a navigation menu with options like Service status, AppSheet, Calendar, Drive and Docs, Gmail (highlighted), Google Chat, Google Meet, Google Voice, Groups for Business, Jamboard, Keep, Sites, Tasks, Additional Google services, Web and mobile apps, Google Workspace Marketplace apps, and Security. The main content area is titled 'Spam, phishing, and malware' and includes a 'GOT IT' button. Below this is the 'Email allowlist' section, which is applied to 'lab08.com'. It contains a text input field with '3.75.105.111' entered. A red arrow points to this field with the text '(7) Type our IP address: 3.75.105.111'. Below the input field is a 'SAVE' button, which is also pointed to by a red arrow with the text '(8) Click SAVE'. Other settings visible include 'Enhanced pre-delivery message scanning' (OFF) and 'Inbound gateway' (ON).