Configuring Google Workspace with the Domain

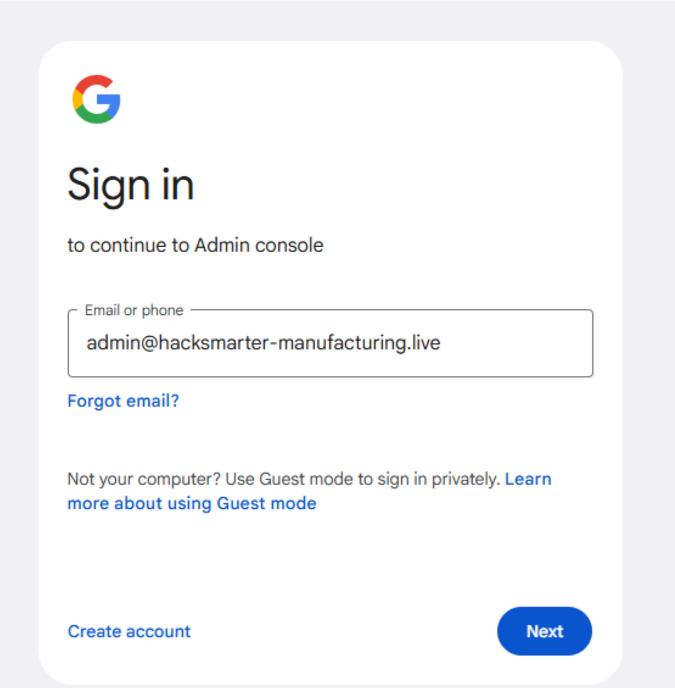
▨ Created	@August 25, 2025 2:29 AM

Overview

This lesson demonstrates how to configure **Google Workspace (formerly G Suite)** to send phishing emails from a trusted and reputable infrastructure. By routing emails through Google's mail servers using a custom domain, attackers can significantly increase deliverability and bypass common spam filters.

The setup involves registering for a Google Workspace trial, verifying domain ownership, and configuring DNS records for Gmail functionality.

hacksmarter1

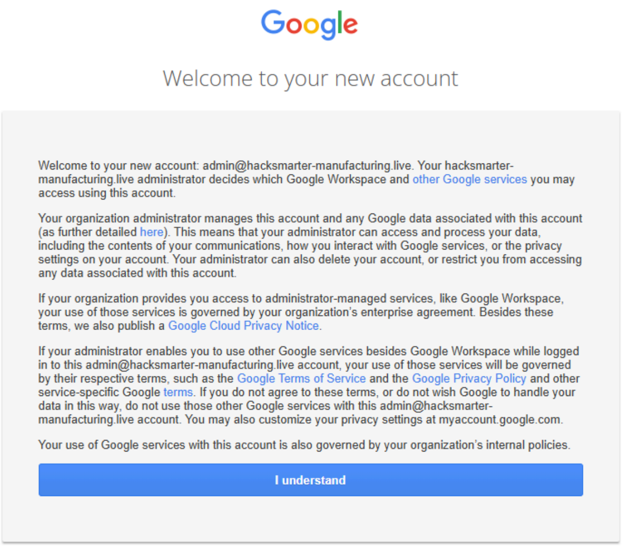


Sign in

to continue to Admin console

Email or phone: admin@hacksmarter-manufacturing.live

Not your computer? Use Guest mode to sign in privately. Learn more about using Guest mode



Welcome to your new account

Welcome to your new account: admin@hacksmarter-manufacturing.live. Your hacksmarter-manufacturing.live administrator decides which Google Workspace and other Google services you may access using this account.

Your organization administrator manages this account and any Google data associated with this account (as further detailed here). This means that your administrator can access and process your data, including the contents of your communications, how you interact with Google services, or the privacy settings on your account. Your administrator can also delete your account, or restrict you from accessing any data associated with this account.

If your organization provides you access to administrator-managed services, like Google Workspace, your use of those services is governed by your organization's enterprise agreement. Besides these terms, we also publish a Google Cloud Privacy Notice.

If your administrator enables you to use other Google services besides Google Workspace while logged in to this admin@hacksmarter-manufacturing.live account, your use of those services will be governed by their respective terms, such as the Google Terms of Service and the Google Privacy Policy and other service-specific Google terms. If you do not agree to these terms, or do not wish Google to handle your data in this way, do not use those other Google services with this admin@hacksmarter-manufacturing.live account. You may also customize your privacy settings at myaccount.google.com.

Your use of Google services with this account is also governed by your organization's internal policies.

Key Concepts

- **Trusted Infrastructure** Using Gmail to send phishing emails (via Google Workspace) allows messages to come from a reputable source. This helps evade many email filters that would otherwise flag messages from lesser-known or self-hosted SMTP servers.
- **Temporary and Disposable Setup** Google Workspace provides a **14-day free trial**. It is recommended that the student completes the phishing course within this period to avoid charges. A calendar reminder should be set to cancel the subscription before the trial ends.

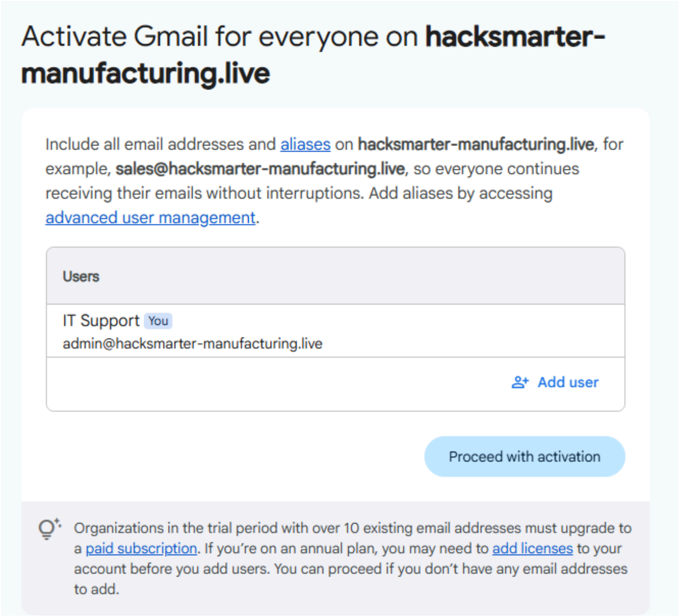
Setup Process

1. **Create a Google Workspace Account**

-
    - Use incognito mode to avoid confusion with personal Google accounts.
    - Navigate to Google Workspace setup and select "For work or business."
    - Enter basic business and contact information (e.g., "Hack Smarter Manufacturing").
    - Provide a valid domain name (purchased previously via Namecheap).

1. **Create Admin User**

   confirm, configure domain and manage



Activate Gmail for everyone on **hacksmarter-manufacturing.live**

Include all email addresses and aliases on **hacksmarter-manufacturing.live**, for example, **sales@hacksmarter-manufacturing.live**, so everyone continues receiving their emails without interruptions. Add aliases by accessing advanced user management.

Users
IT Support You admin@hacksmarter-manufacturing.live

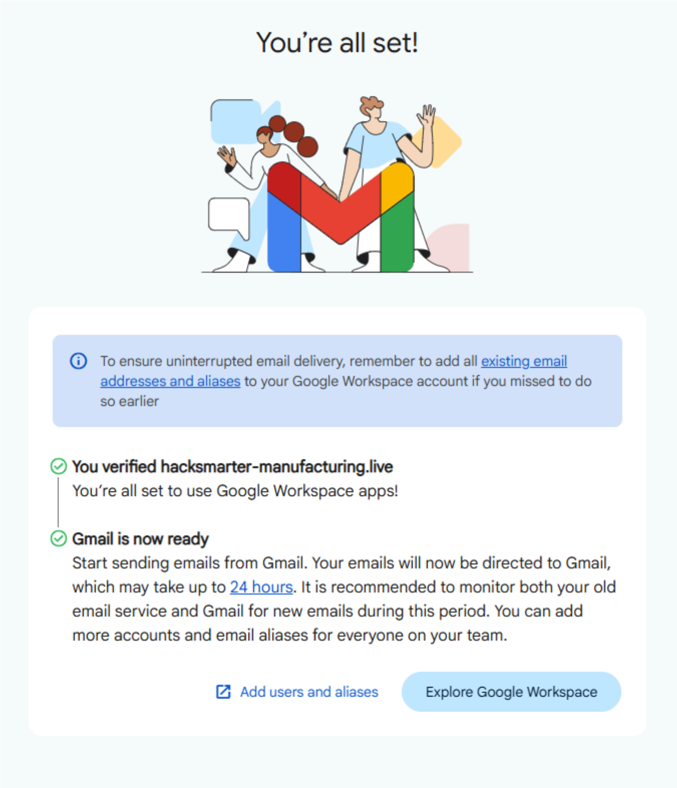
Organizations in the trial period with over 10 existing email addresses must upgrade to a paid subscription. If you're on an annual plan, you may need to add licenses to your account before you add users. You can proceed if you don't have any email addresses to add.

-
    - Configure an administrator account (e.g., `admin@yourdomain.com`).
    - Choose a simple password for lab purposes and record it securely.

1. **Verify Domain Ownership**

-
    - Use Namecheap's Advanced DNS panel to add the TXT and CNAME records provided by Google.
    - Set TTL values to 1 minute for quicker propagation.
    - Confirm domain ownership within Google Workspace.

1. **Activate Gmail**



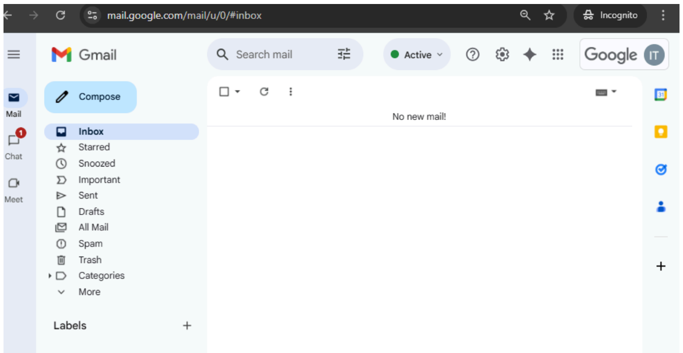
You're all set!

To ensure uninterrupted email delivery, remember to add all existing email addresses and aliases to your Google Workspace account if you missed to do so earlier

You verified hacksmarter-manufacturing.live
You're all set to use Google Workspace apps!

Gmail is now ready
Start sending emails from Gmail. Your emails will now be directed to Gmail, which may take up to 24 hours. It is recommended to monitor both your old email service and Gmail for new emails during this period. You can add more accounts and email aliases for everyone on your team.

-
    - Add **MX records** in Namecheap to route email to Google servers (e.g., `smtp.google.com`).
    - Set MX priority to 1 and TTL to the shortest available.
    - Confirm settings in Google Workspace once the DNS changes have propagated.



No new mail!

Final Outcome

Upon completion:

- You will have a fully functional Google Workspace account linked to your phishing domain.
- Gmail will accept and route email from your custom domain, improving the legitimacy of your phishing messages.

- You can now send emails from addresses like `admin@yourdomain.cam` with high deliverability.