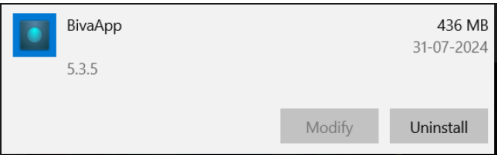


# BivaApp Removal

THREAT SUMMARY	
Name	BivaApp
Threat Type	Potentially Unwanted App
Symptoms	Suspicious startup tasks or background activity. BivaApp listed in "Apps & Features" or Control Panel. Can't uninstall it (error: file not found)
Distribution Methods	Deceptive pop-up ads, free software installers (bundling).
Damage	Hijack browser settings. Inject unwanted ads or popups. Collect browsing and login data. Reinstall itself through startup tasks or hidden folders
Malware Removal	Use a Antivirus to scan the system. Can use the below steps that I made to uninstall malware from the system.

## Incident Summary – BivaApp Removal

During routine maintenance and application cleanup, I identified the presence of an unfamiliar application named **BivaApp** installed on my system. Upon investigation, I determined that the application had been **silently bundled with third-party software** previously downloaded from the internet.



Attempts to uninstall BivaApp via the standard **"Apps & Features" interface were unsuccessful**, as the uninstaller path was either missing or broken. Despite manually deleting the application's files from the system , the application **reappeared upon system restart**, indicating that it had established **persistent startup behavior** likely via scheduled tasks or registry-based autorun entries.

To **permanently remove BivaApp** and prevent reinfection or persistence, I carried out a systematic removal process, as detailed in the following guide.

## Step-by-Step Removal Instructions

### 1. Kill Running Processes

Open Task Manager:

- Look for BivaApp, Bivaji, or unknown tasks
- Right-click → End Task

## 2. Delete Files Manually

Navigate to:

C:\Users\<YourName>\AppData\Roaming\BivaApp

- Delete the **BivaApp** folder
- Also check these paths:
- %APPDATA%
- %LOCALAPPDATA%
- C:\ProgramData

## 3. Remove from Startup

- Press Win + R → type: shell:startup
- Delete any BivaApp.lnk or suspicious shortcuts
- Open Task Manager → Startup tab → disable anything suspicious

## 4. Delete Scheduled Tasks

- Press Win + R → type: taskschd.msc
- Navigate to Task Scheduler Library
- Delete any tasks with names like BivaApp, Update, Startup, or random strings

## 5. Clean the Registry

**Be careful while editing the registry**

1. Open Run (Win + R) → type: regedit
2. Navigate to:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
3. Look for a folder with DisplayName = BivaApp or Visit the keys and look for bivaapp related entries
4. If found: Right-click → Delete
5. Also search:  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

## 6. Scan Your System for Malware

Use one of the following tools:

- Microsoft Defender → Virus & threat protection → Full Scan
- Optionally, run Defender Offline Scan for deep threats

## 7. Reset Browsers (If Hijacked)

### Chrome

- Visit <chrome://settings/reset> → Click "Restore settings to original defaults"

### Edge

- Visit <edge://settings/reset> → Reset settings

### Firefox

- Go to <about:support> → Click Refresh Firefox

## 8. Change Passwords & Enable 2FA

Since BivaApp may steal login data:

- Change passwords for Gmail, Steam, Instagram, Riot, etc.
- Enable Two-Factor Authentication (2FA)

### Note:

- This guide is effective as of July 2025
- **BivaApp may come bundled with pirated or free software — avoid downloading cracked tools or games**
- Always use custom install mode to deselect third-party apps

**Author:** Mahant Deshmukh

**Date:** 10-07-2025

**Version:** 1.0