

Forum:[Hack Forums](#)

Thread: [Clawdbot AI Assistant](#)

Omniscient - January 26, 2026, 9:37 am

Let's have a sticky for Clawdbot talk. We need to really dig into this.

<https://clawd.bot/>

<https://github.com/clawdbot/clawdbot>

AI Quote: Clawdbot is an open-source, self-hosted personal AI assistant that runs entirely on your own hardware—whether that's a Mac, Linux machine, Windows via WSL, Raspberry Pi, or even a dedicated VPS. Launched in early January 2026 by developer Peter Steinberger (founder of PSPDFKit/Nutrient), it has rapidly gone viral in the AI community, amassing thousands of GitHub stars and a dedicated Discord. Unlike cloud-based chatbots from big tech, Clawdbot keeps all your data, conversations, and context private and local, with no uploads to external servers. It integrates seamlessly into the messaging apps you already use—like WhatsApp, Telegram, Discord, Slack, Signal, or iMessage—turning it into a contact you can text naturally, making it feel like chatting with a super-capable teammate or "AI employee" rather than switching to yet another app.

What sets Clawdbot apart is its ability to actually perform real-world actions instead of just responding with text. It can clear your inbox by unsubscribing from spam, send emails on your behalf, manage your calendar (rescheduling conflicts autonomously), check you in for flights, browse the web to fill forms or extract information, run shell commands and scripts, control smart home devices, handle code tasks like debugging or opening GitHub PRs, fetch health stats from apps like WHOOP, generate summaries from meetings or notes, and even spawn background sub-agents for research. It supports persistent memory across sessions (often stored in local Markdown files), learns your preferences over time, and can be proactive—sending morning briefings with weather, objectives, reminders, trending topics, or personalized content suggestions without you asking first.

Powered by leading LLMs like Claude (Anthropic), GPT models, or fully local ones via Ollama (for complete offline use), Clawdbot is highly extensible through community-built "skills" and plugins, allowing it to connect to services like Gmail, GitHub, Todoist, Spotify, Obsidian, and more. Users describe it as the closest thing yet to a true "Jarvis"-style personal AI OS or butler—hackable, autonomous, and transformative for productivity, with many running it 24/7 on dedicated hardware like a Mac Mini. While it's still early and can require careful setup for security (e.g., sandboxing tools, avoiding full access to sensitive accounts), its open-source nature (MIT license) and rapid community momentum make it a standout in the shift toward owning and controlling your own AI agents. ?

Who has one of these setup? I am trying to decide if I want to build a PC from old parts, use an old server I have laying around, or buy something cheap for \$200.

This guy has a nice thread about cheap hardware options.

Omniscient - January 26, 2026, 9:59 am

btw, I like this wording from their Github.

Quote: Clawdbot is a personal AI assistant you run on your own devices. It answers you on the channels you already use (WhatsApp, Telegram, Slack, Discord, Google Chat, Signal, iMessage, Microsoft Teams, WebChat), plus extension channels like BlueBubbles, Matrix, Zalo, and Zalo Personal. It can speak and listen on macOS/iOS/Android, and can render a live Canvas you control. The Gateway is just the control plane — the product is the assistant.

If you want a personal, single-user assistant that feels local, fast, and always-on, this is it.

newQuery - January 27, 2026, 8:40 am

Rebranded as Moltbot after Anthropic claims trademark

Omniscient - January 27, 2026, 9:26 am

(Jan 27, 2026 09:40 AM)newQuery Wrote: [\[CITE\]](#) Rebranded as Moltbot after Anthropic claims trademark

Of course. I was wondering about the brand confusion. MoltBot it is then.

SIM-2470866 - January 28, 2026, 2:29 pm

Any idea how I can upgrade to moltbot? Mine still says Clawdbot (did the clawdbot update, also did a rerun of the package installer)

It still says Clawdbot?

Do I need to uninstall first and re-install it?

Omniscient - January 28, 2026, 2:42 pm

(Jan 28, 2026 03:29 PM)SIM-2470866 Wrote: [\[CITE\]](#) Any idea how I can upgrade to moltbot? Mine still says Clawdbot (did the clawdbot update, also did a rerun of the package installer)

It still says Clawdbot?

Do I need to uninstall first and re-install it?

Ugh, no idea. He may not have updated the package yet. It's a new rebranding.

skull - February 6, 2026, 6:49 am

And its now named Openclaw. What a shitshow.

But it is quite fascinating what it can do. I did a factory reset on a old Macbook, plugged it into a isolated network and gave it admin access to the computer. It can basically do anything we could, sometimes not the best on application interactions, nor gaming...

The guardrails are quite limited, I would recommend to monitor the "openclaw logs" with automated systems to ping you when something seems off, and to not run it on a computer you use yourself - make it a clean machine with no accounts setup or anything - only provide it the access that it needs to be able to run your tasks.

Omniscient - February 6, 2026, 10:47 am

(Feb 6, 2026 07:49 AM)skull Wrote: [\[CITE\]](#) And its now named Openclaw. What a shitshow.

But it is quite fascinating what it can do. I did a factory reset on a old Macbook, plugged it into a isolated network and gave it admin access to the computer. It can basically do anything we could, sometimes not the best on application interactions, nor gaming...

The guardrails are quite limited, I would recommend to monitor the "openclaw logs" with automated systems to ping you when something seems off, and to not run it on a computer you use yourself - make it a clean machine with no accounts setup or anything - only provide it the access that it needs to be able to run your tasks.

I think I plan on running it on a rented VPS.

Dirty - February 6, 2026, 12:00 pm

(Feb 6, 2026 07:49 AM)skull Wrote: [\[CITE\]](#) And its now named Openclaw. What a shitshow.

But it is quite fascinating what it can do. I did a factory reset on a old Macbook, plugged it into a isolated network and gave it admin access to the computer. It can basically do anything we could, sometimes not the best on application interactions, nor gaming...

The guardrails are quite limited, I would recommend to monitor the "openclaw logs" with automated systems to ping you when something seems off, and to not run it on a computer you use yourself - make it a clean machine with no accounts setup or anything - only provide it the access that it needs to be able to run your tasks.

this would seem common sense but sadly alot of people ran it straight from their computer with admin rights only to cry that it's completely insecure duh

haven't used it yet myself since I have not had the time but I'm planning on doing the same also with the mentioned logging mostly so that when it does something wild I can track what it's doing.

skull - February 7, 2026, 12:40 am

(Feb 6, 2026 11:47 AM)Omniscient Wrote: [\[CITE\]](#) I think I plan on running it on a rented VPS.

Makes sense. It's isolated then ?

(Feb 6, 2026 11:47 AM)Omniscient Wrote: [\[CITE\]](#) I think I plan on running it on a rented VPS.

Yes, there are crazy stories out there where it had access to everything, even credit card details etc ?

Hackers - February 7, 2026, 3:57 am

Highly recommend looking into it. If not this one, pick another like it. This will be the norm of telecomms in our lifetimes.

Omniscient - February 7, 2026, 8:14 am

(Feb 7, 2026 01:40 AM)skull Wrote: [\[CITE\]](#) Makes sense. It's isolated then ?

Yes, there are crazy stories out there where it had access to everything, even credit card details etc ?

Some of the crazy stories are engagement click-bait.

Oh_Well - February 16, 2026, 11:24 pm

The creator just joined OpenAI - interesting turn.

OpenClaw, OpenAI and the future

Published:

14 Feb, 2026

I'm joining OpenAI to work on bringing agents to everyone. OpenClaw will move to a foundation and stay open and independent.

Spoiler ([Click to View](#))

OpenClaw, OpenAI and the future

Published:

14 Feb, 2026

•

3 min read

| [Edit on GitHub](#)

tl;dr: I'm joining OpenAI to work on bringing agents to everyone. OpenClaw will move to a foundation and stay open and independent.

The last month was a whirlwind, never would I have expected that my playground project would create such waves. The internet got weird again, and it's been incredibly fun to see how my work inspired so many people around the world.

There's an endless array of possibilities that opened up for me, countless people trying to push me into various directions, giving me advice, asking how they can invest or what I will do. Saying it's overwhelming is an understatement.

When I started exploring AI, my goal was to have fun and inspire people. And here we are, the lobster is taking over the world. My next mission is to build an agent that even my mum can use. That'll need a much broader change, a lot more thought on how to do it safely, and access to the very latest models and research.

Yes, I could totally see how OpenClaw could become a huge company. And no, it's not really exciting for me. I'm a builder at heart. I did the whole creating-a-company game already, poured 13 years of my life into it and learned a lot. What I want is to change the world, not build a large company and teaming up with OpenAI is the fastest way to bring this to everyone.

I spent last week in San Francisco talking with the major labs, getting access to people and unreleased research, and it's been inspiring on all fronts. I want to thank all the folks I talked to this week and am thankful for the opportunities.

It's always been important to me that OpenClaw stays open source and given the freedom to flourish. Ultimately, I felt OpenAI was the best place to continue pushing on my vision and expand its reach. The more I talked with the people there, the clearer it became that we both share the same vision.

The community around OpenClaw is something magical and OpenAI has made strong commitments to enable me to dedicate my time to it and already sponsors the project. To get this into a proper structure I'm working on making it a foundation. It will stay a place for thinkers, hackers and people that want a way to own their data, with the goal of supporting even more models and companies.

Personally I'm super excited to join OpenAI, be part of the frontier of AI research and development, and continue building with all of you.

The claw is the law.

Omniscient - February 17, 2026, 11:08 am

Not actually a fan of this move by him to join Open AI.

Hackers - February 17, 2026, 12:56 pm

(Feb 17, 2026 12:08 PM)Omniscient Wrote: [\[CITE\]](#) Not actually a fan of this move by him to join Open AI.

With the salaries going around it's hard for anyone to say no I'm sure, no matter how honest their intentions are for OSS

But it's rough, this is what will happen at a bigger scale too... AI companies swoop up the talent and we have a handful of "monopoly" AI companies running services for every industry we have today, but with automations.

OSS communities will be decimated because people will be able to generate what they need for so cheap & reliably.

laksor - February 20, 2026, 12:20 pm

I have clawdbot setup, its amazing, i set it up and gave it granular access so it can organize my life and thoughts for me, I deal with so much stuff and its very easy to forget and too inconvenient to open apps to write and shit so i just send it voice notes. i rented a vps for 40\$ a month and made a user specifically for it.

however make sure to not let it install skilss on itself. the skills market is infestedddd with malware

Omniscient - February 20, 2026, 12:26 pm

(Feb 20, 2026 01:20 PM)laksor Wrote: [\[CITE\]](#) however make sure to not let it install skilss on itself. the skills market is infestedddd with malware

Interesting. Tell us more about that. Does the Malware basically provide root level access to the server or is it just AI Agent takeovers?

laksor - February 20, 2026, 12:29 pm

(Feb 20, 2026 01:26 PM)Omniscient Wrote: [\[CITE\]](#) Interesting. Tell us more about that. Does the Malware basically provide root level access to the server or is it just AI Agent takeovers?

level, it runs with normal user permissions and can excute anything, its basically python code that the llm executes blindly and trusts by whatever is written inside the SKILL.MD file which describes the skill and how it should be used to the llm

more over depending on the llm you decide to use, if its crappy

all it takes me is a single email to your inbox that you gave access to clawdbot to so you it can read ur emails and note out anything important and respond for you

this email can have very simple prompt injection that makes clawdbot not only run on server commands

but also extract all it knows about you, all auth keys, all passwords you may have given it, and send it over to a webhook of mine.

so far with a simple scan 100s of top ranking skills turned out to be malware, the skills market for clawdbot is free for all and community ran with zero monitoring or scanning

s0lo - February 24, 2026, 10:11 am

You have to pay for tokens while using Clawdbot, correct? Since i'm kinda broke, i've been running both Claude and Codex on a PC of mine, meaning they live on the PC, control the PC and use the PC, I just run them using the 20/month subscriptions, meaning, log in with the account and use it, but maybe i'm missing out.

psickophant - February 24, 2026, 7:54 pm

(Feb 24, 2026 11:11 AM)s0lo Wrote: [\[CITE\]](#) You have to pay for tokens while using Clawdbot, correct? Since i'm kinda broke, i've been running both Claude and Codex on a PC of mine, meaning they live on the PC, control the PC and use the PC, I just run them using the 20/month subscriptions, meaning, log in with the account and use it, but maybe i'm missing out.

There are a ton of options that can reduce the cost of AI models/interaction. Most of the decent

choices run locally. I have had wonderful success using Deepseek via Openrouter. The model is actually completely free to use. I started off using it on a Raspberry Pi4 but found it to be a little sluggish. I have had a much better result with running on an old Macbook. As some of the posts above address security is a major concern. There is some documentation to assist with securing the model but I would warn everyone to pay close attention to security principals.

ModernEHustle - August 7, 2026, 2:43 am

(Feb 20, 2026 01:29 PM)laksor Wrote: [\[CITE\]](#) level, it runs with normal user permissions and can execute anything, its basically python code that the llm executes blindly and trusts by whatever is written inside the SKILL.MD file which describes the skill and how it should be used to the llm more over depending on the llm you decide to use, if its crappy all it takes me is a single email to your inbox that you gave access to clawdbot to so you it can read ur emails and note out anything important and respond for you this email can have very simple prompt injection that makes clawdbot not only run on server commands but also extract all it knows about you, all auth keys, all passwords you may have given it, and send it over to a webhook of mine. so far with a simple scan 100s of top ranking skills turned out to be malware, the skills market for clawdbot is free for all and community ran with zero monitoring or scanning I've seen prompts hidden in all kinds of different file types, there is a website called black swan that is a community of people training doing exactly this.

The Pact - August 29, 2026, 10:04 am

(Jan 27, 2026 09:40 AM)newQuery Wrote: [\[CITE\]](#) Rebranded as Moltbot after Anthropic claims trademark

Ah I was wondering about that. And with the issue of Claud watermarking I think a lot of people might want to stay away from Claud right now anyway. I was confused and wondered if it was an Anthropic product.

issagi - August 30, 2026, 6:40 pm

I'm new to this and don't have powerful hardware

What is the minimum setup to run Clawdbot?

Will it work on:

- An old desktop PC?
- An old laptop?
- Raspberry Pi?

I want to try it but don't want to buy new hardware. Any advice for beginners?

Thanks.