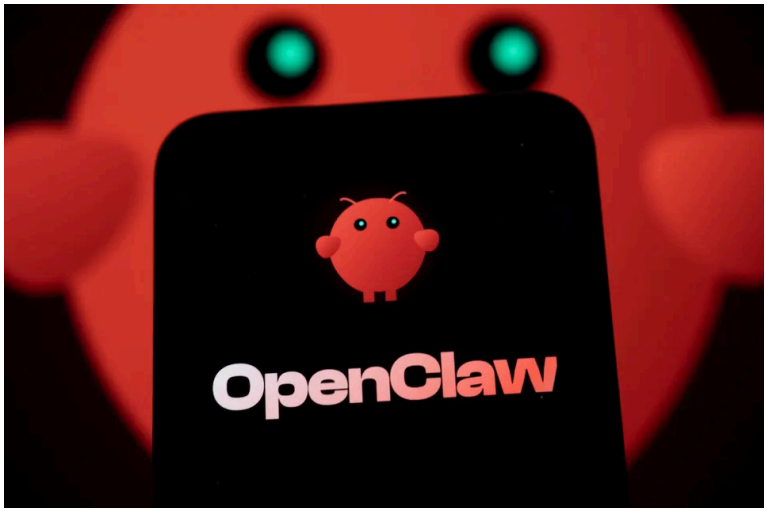
What Is OpenClaw, Formerly Moltbot? Everything You Need To Know

By Kate O'Flaherty, Senior Contributor. Kate O'Flaherty is a cybersecurity...

Follow Author

Published Feb 06, 2026, 09:24am EST, Updated Feb 15, 2026, 11:34am EST



Here's everything you need to know about the viral agent now known as OpenClaw.
NURPHOTO VIA GETTY IMAGES

OpenClaw — the viral AI agent that's already been known by two other aliases, Moltbot and

Clawdbot — is growing in popularity. After bursting onto the mainstream just weeks ago, OpenClaw has earned well over 100,000 GitHub stars.

Then came Moltbook, the Reddit-style social network where AI bots can interact with no humans allowed. Everyone was talking about it, and for good reason.

It's no surprise that concerns about OpenClaw and Moltbook are growing, with worries centring on the security and privacy of the viral bot and in Moltbook's case, the uncontrolled nature of the AI bot-controlled social network.

There are "only a few itty-bitty, teeny-weeny problems" with OpenClaw, says *Computerworld*'s Steven Vaughan-Nichols. "To do useful things like reserving your hotel room, getting your pizza delivered, or cleaning up your e-mail box, it needs your name, password, credit-card number — and all the other things any crook also wants."

Here's everything you need to know about the viral agent now known as OpenClaw.

FORBES

iOS 26.2.1—Update Now Warning Issued To Millions Of iPhone Users

By Kate O'Flaherty

What Is OpenClaw, Aka Moltbot, Formerly Clawdbot?

OpenClaw, aka Moltbot, is an open-source autonomous AI assistant that you can

download and run on a computer. After its setup in November 2025, it was known as Clawdbot, but its creator, developer Peter Steinberger was forced to change the name to Moltbot after Anthropic objected due to similarities with its Claude chatbot. He then changed the name again to OpenClaw.

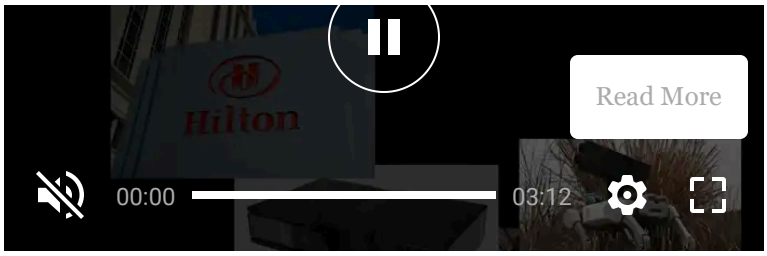
OpenClaw is designed to perform real-world tasks on behalf of users, such as managing calendars, messaging, browsing and other actions that go beyond simple chatbot responses. “OpenClaw runs locally on devices

and in many configurations can read and write files, execute script and interact with external services when given sufficient permissions," Louis Rosset-Ballard, team leader at Pentest People explains.

Nash Borges, SVP of engineering and core AI at security firm Sophos, describes OpenClaw as "more like Jarvis from Iron Man than Siri or Alexa."

You use natural language for every interaction, but can ask it to do things such as conduct research on a topic of your choice, compose a reply to an email summarizing when you're available for a meeting — or even code up any capability that it doesn't already have. "That last part is significant because it means there is almost no limit to what it can do," says Borges.

But does it work? Reddit users describe their experiences as mixed. "Clawdbot is like an Apple product: when it runs it's like MAGIC, until it doesn't," according to one post.



Why Has OpenClaw Blown Up In The Last Couple Weeks?

If you didn't know about OpenClaw a week ago, you must at least have heard about it now. The whole development journey has been "insanely fast," and this explosion of interest is "just the latest gear shift," says Borges.

OpenClaw's rapid adoption is driven by demos showing extreme productivity gains — automating tasks that normally require human interaction, says Stefan Dasic, threat researcher at cybersecurity outfit Malwarebytes. "The promise of a powerful, locally run AI agent without obvious limits has resonated strongly within developer and AI enthusiast communities."

But things that grow so fast often come with risks. "It seems that in just a couple of days, everybody doing anything with AI, and even many who don't, have installed and raved about this new agentic product," says Erich Kron, CISO advisor at KnowBe4. "The almost feverish rush to use this product is frankly a little disturbing."

Check Your iPhone Now—These Models Will No Longer Receive Updates

By Kate O'Flaherty

Why Is OpenClaw A Risk To Security And Privacy?

Uncontrolled AI is a concern more generally, and OpenClaw is no different to other products that have shot into the mainstream, such as ChatGPT.

A concern with OpenClaw is how much information it can have access to when using it the way people are showing, says Kron. “For example, giving it full access to all of your emails may seem fine and might make sense since you want it to act as your personal assistant. However, there is real danger, not just from malicious use but accidental when giving AI agents this type of access. In the blink of an eye, it could be deleting your emails, or taking malicious actions such as siphoning off data to attackers.”

Security issues are already starting to happen. Researchers found hundreds of exposed Moltbot instances online with “zero protection,” says Denis Romanovskiy, chief AI officer at SOFTSWISS, a provider of tech solutions for iGaming. This included API keys, private messages, the ability to send messages as the user and root shell access.

OpenClaw is a security threat “on multiple levels,” says William Thackray, IT and cybersecurity expert and operations director at

AGT. “Firstly, the platform’s GitHub repository reveals a troubling accumulation of unaddressed security vulnerabilities, from an exposed database, creating a direct pathway for unauthorised access to user information, to dangerous plugins. Koi Security, documented 341 malicious skills uploaded to ClawHub, OpenClaw's extension marketplace.”

Granting an AI agent full system control creates a single point of failure, says Dasic. “If compromised, OpenClaw can access saved passwords, personal documents, browser sessions, and financial data."

OpenClaw poses risks to privacy, too. These stem from its access to and storage of sensitive user data, says Rosset-Ballard. “Because the agent may retain long-term memory, store credentials and tokens in plain text, and process external inputs without robust guardrails, it can inadvertently expose personal information."

At the same time, the AI agents post on social networks without asking permission. “Screenshots of agent conversations spread across Twitter,” Romanovskiy points out. “Your entire digital life sits one vulnerability away from exposure.”

I have contacted OpenClaw creator Peter Steinberger and will update this article if he responds.

Here's How To Turn It On

By Kate O'Flaherty

What Is Moltbook?

Moltbook is a social network built exclusively for AI agents, launched in January 2026. "Unlike traditional forums where users interact and share content, Moltbook is a space where OpenClaw agents autonomously post content, comment, argue, joke and upvote or downvote each other," says Dasic.

Human users can observe agent interactions, but cannot directly participate.

Moltbook "further amplifies" the risks associated with OpenClaw, says Professor Katerina Mitrokotsa, chair of cybersecurity at the University of St. Gallen. "Although it gained attention for showcasing AI-to-AI interactions, early findings revealed that it exposed entire databases, including secret API keys that could let attackers impersonate any agent on the platform. This creates clear threats for users: Identity spoofing, unintentional data exposure, and reduced control over their digital environment."

The risks of Moltbook "became very clear very quickly," adds Daniel dos Santos, head of research at Forescout.

"There is no moderation on the content, so bots can post instructions for other bots to execute ultimately on a victim machine, can use prompt injection attacks or generate offensive content."

Should I Use OpenClaw?

OpenClaw might have some cool capabilities, but for now, the risks outweigh the benefits, especially if you aren't techy. OpenClaw's creator Steinberger has warned users that the tool requires careful configuration and is not yet meant for non-technical users.

If you're technical, curious and willing to sandbox everything carefully, it's "a fascinating glimpse of the future," says Romanovskiy.

But if you handle sensitive data or need reliable security, stay away for now, he advises. "The project moves faster than its security can keep up. Treat it as an experiment, not a production tool."

If you do choose to use the viral AI agent, be careful that you are discovering the real deal. "When searching for a product like this to download and install, it's very important that people are careful not to end up in an unofficial repository that contains malware or other dangerous programs," Kron warns.

OpenClaw is growing at an alarming rate, making it important that you treat it with caution. Unless you are an expert, leave it well alone for now.

Find Kate O'Flaherty on LinkedIn and X.

Join The Conversation

Comments 1

One Community. Many Voices. Create a free account to share your thoughts. Read our community guidelines here.

See All Comments (1)

Forbes