Learn with OpenClaw

OpenClaw isn't the first AI agent – ??companies have been using automated trading bots and logistics optimization tools for years.

OpenClaw is an open-source AI agent capable of browsing the web, managing files, sending emails, and running code on your computer. Imagine it like ChatGPT , but with added "hands"—it doesn't just answer questions, it performs many tasks.

However, that power also comes with real risks. Researchers have discovered malware injection attacks, login credentials theft vulnerabilities, and instances of AI agents performing actions the user didn't request. This series will teach you how to use OpenClaw effectively and safely – because 'install and see what happens' is not a security strategy.

You'll start by understanding what an AI agent actually is (or isn't) and whether OpenClaw is right for your needs. Then, you'll install it securely – in a Docker container with enhanced security measures that most tutorials overlook.

From there, you'll build practical workflows: a scheduled morning summary, phishing-free email classification, and a system to test community skills before implementing them. The final lesson will create your personal safety manual – rules about what your AI agent can and cannot do.

What you will learn

1. Explain the differences between AI agents like OpenClaw and chatbots like ChatGPT.
2. Assess whether OpenClaw is suitable for your needs, budget, and risk tolerance.
3. Deploying a secure OpenClaw installation based on Docker with enhanced security measures.
4. Use OpenClaw through messaging apps for everyday tasks.
5. Create a scheduled morning summary workflow with cron automation.
6. Designing secure email classification rules prevents Prompt Injection attacks.
7. Assess community skill levels regarding security risks before installing them.
8. Develop a safety manual for personal AI agents with limitations and kill switches.

After this course, you will be able to

1. Run an AI agent to browse the web, manage files, and send emails on your behalf – securely.
2. Installing OpenClaw in Docker with enhanced security flags that most guides completely ignore.

3. Build automated workflows such as morning summaries and email sorting that run on a schedule without supervision.
4. Check community skills regarding security risks before installing them using a structured assessment framework.
5. Demonstrate your ability to use AI agents in your resume – showcase practical experience with automated AI systems that employers value.

What you will build

Secure OpenClaw installation and workflow

A fully documented Docker-based OpenClaw deployment system with enhanced security measures, along with an efficient automated workflow—morning summaries, email sorting, or custom tasks—runs on a schedule.

Safety manual for AI agents

Your personal privacy policy includes agent permissions, skill assessment criteria, incident response procedures, and a weekly review checklist—ready to share with the team or employer.

OpenClaw is for everyone.

Demonstrate that you can install, configure, secure, and build workflows with OpenClaw while adhering to security-first principles.

Prerequisites

1. Basic computer skills (no programming required)
2. I have a ChatGPT, Claude, or Gemini account (for comparison).

Suitable candidates for this course

1. Curious non-technical people often hear about AI agents and want to try one out with the right instructions.
2. ChatGPT users and Claude wanted something that went beyond simple chat functionality and actually performed actions.
3. Developers are exploring open-source AI agents and want a structured introduction before diving into programming.
4. Anyone interested in AI automation and wanting to start with security-prioritizing habits rather than learning them after an incident.

What exactly is (and isn't) an AI agent?

Understand the difference between AI chatbots and AI agents, why agents are the next step, and what you will learn in this course.

You're already familiar with chatbots. Now let's move on to agents!

This is a story that happened to a content creator last month:

She asked ChatGPT for help planning her week. ChatGPT provided her with a beautifully formatted schedule. She copied that schedule into her calendar app. She noticed two conflicts, fixed them herself, and then realized she also needed to reschedule a call with a client. She went to her email, revised the schedule, sent it, went back to the calendar, and updated it again.

Forty-five minutes later, she had a plan for the whole week.

That same week, she tried OpenClaw. She typed a message on WhatsApp: "Check my schedule for next week, identify conflicts, reschedule less important things, and email anyone affected."

Ten minutes later, everything was done. The email had been sent. The calendar had been updated. The conflict had been resolved.

That's the difference between a chatbot and an agent.

By the end of this series, you will understand:

1. What are AI agents and how do they differ from chatbots?
2. What is OpenClaw and why is it generating so much excitement (and concern)?

Things you need to know about this course

This course is designed for those who are familiar with computers and messaging applications but don't know how to program. All technical concepts are explained in easy-to-understand language. When discussing "Docker," the article will explain its meaning before asking you to use it.

You can complete the entire course in one go (~2 hours) or study one lesson per day. Each lesson builds upon the previous one, so please study in order.

The revolution between chatbots and agents.

Let's clarify this distinction, because everything else in this series is based on it.

A chatbot is a conversationalist. You ask a question, and it answers. You copy the answer and do the work yourself. ChatGPT, Claude, and Gemini are chatbots. They are very good at generating text, but they can't do anything in the real world.

An agent is an executioner. You set the goal, and it will figure out the steps, use the tools, and take action. It can send your emails, manage your calendar, book flights, organize files, and browse the web—all without you having to lift a finger.

Scientific American magazine called OpenClaw "artificial intelligence with hands." That's the best summary you can find. A chatbot gives advice. An agent follows it.

Think of it this way: A chatbot is like calling a friend to ask for directions. An agent is like having a driver take you there.

? **Quick check** : If you ask ChatGPT to "reschedule my 3 PM meeting to Thursday", what happens?

Answer : Nothing. It can tell you how to reschedule, but it can't access your calendar or send emails. An agent can.

What makes OpenClaw different?

OpenClaw isn't the first AI agent – ??companies have been using automated trading bots and logistics optimization tools for years. But it's the first agent that ordinary users can run on their own computers.

This is what makes OpenClaw different:

1. **It's open source** . Anyone can check the code, modify it, or contribute. OpenClaw has over 250,000 stars on GitHub – making it the most-starred software project on the platform, even surpassing React. Jensen Huang (CEO of NVIDIA) called OpenClaw the "next ChatGPT" at GTC in March 2026.
2. **It uses your messaging apps** . Instead of learning a new interface, you chat with OpenClaw through WhatsApp, Telegram, Signal, or Discord—the same apps you use to message your friends.
3. **It runs locally** . Unlike cloud-based AI assistants, OpenClaw runs on your computer (or a small server). The data remains on your computer—in theory.
4. **It has memory** . OpenClaw remembers your past conversations, interests, and interactions using a file-based memory system. Over time, it learns how you work.
5. **It connects to an AI brain** . OpenClaw itself doesn't generate text—it connects to Claude, GPT-5.4, Gemini 3.1 Flash, DeepSeek , or other AI models to perform the thinking. It's the hands; the AI ??model is the brain.

The story of naming (brief history)

You may have heard many different names mentioned. Here's the story:

The project was originally called Clawdbot – a playful play on words based on "Claude," Anthropic's AI. Anthropic raised concerns about the trademark, so its creator changed the name to Moltbot. That name was also rejected (it was associated with shedding one's old skin). The final name is OpenClaw – "open" meaning open source, "claw" as a nod to its origins.

Its creator, Peter Steinberger, is a renowned developer who previously built PSPDFKit. He retired but returned to build OpenClaw and has been making over 6,600 code changes per month using multiple AI agents working in parallel. In February 2026, Steinberger joined OpenAI, and the project is now transitioning to an independent 501(c)(3) open-source organization to ensure future community governance.

? **Quick check** : Name two differences between OpenClaw and ChatGPT.

The possible answer is: OpenClaw performs actions, not just generates text. It runs locally. It uses messaging applications as its user interface. It has persistent memory.

Why should you be interested in OpenClaw?

You might be thinking, "That sounds great, but do I really need this?"

That's a valid question. And here's the straightforward answer:

AI agents are the industry trend. Gartner predicts 40% of enterprise applications will integrate AI agents by the end of 2026. Apple, Google, and Microsoft are all building their own AI agents. OpenClaw is just the first to do so for individual users.

Those who learn this early will have an advantage. When smartphones first appeared, early adopters who understood the app had a head start. The same is happening with AI agents. Understanding how they work—even if you decide not to use them—will give you a greater advantage in an AI-driven world.

But there are real risks. Security researchers have found hundreds of vulnerabilities. Admittedly, "no setup is completely secure," so this course is specifically designed to help you understand that reality.

Key points to remember

1. Chatbots answer questions. AI agents perform actions. That's the fundamental change.
2. OpenClaw is an open-source AI agent that runs on your computer and communicates with you through messaging applications.
3. It connects with AI models (Claude, GPT-5.4, Gemini 3.1 Flash, DeepSeek) to process thought – OpenClaw provides the execution software.
4. It has real potential AND real risks - this course will address both honestly.
5. Understanding AI agents is becoming a core skill, regardless of whether you use OpenClaw or not.

1. Question 1:

   Which statement about OpenClaw is TRUE?

   1. A. It was built by a major technology company like Google or Meta.
   2. B. It is a closed-source commercial product with a monthly fee.
   3. C. It is an open-source project with over 250,000 stars on GitHub.
   4. D. It only works with ChatGPT

   EXPLAIN:

   OpenClaw is free, open-source software originally created by Peter Steinberger (who joined OpenAI in February 2026). It connects with various AI models (Claude, GPT, DeepSeek) and is currently the most-starred software project on GitHub.

2. Question 2:

   What user interface does OpenClaw use?

   1. A. A desktop application you install
   2. B. A web browser extension
   3. C. The messaging apps you have used (WhatsApp, Telegram, etc.)

4. D. Voice commands via smart speaker

EXPLAIN:

OpenClaw uses your existing messaging apps as its interface. You chat with it via WhatsApp, Telegram, Signal, or Discord—no need to learn any new apps.

3. Question 3:

What are the main differences between chatbots and AI agents?

1. A. Agent is more expensive.
2. B. Chatbots answer questions; agents perform actions on your behalf.
3. C. Agent only works on Mac computers.
4. D. Chatbots are an outdated technology and no longer work effectively.

EXPLAIN:

The core difference is the action. A chatbot tells you what to do. An agent does it—sending emails, scheduling meetings, managing files—with tangible consequences.

Submit your work

Training results

You have completed **0** questions.

-- / --

Review the lesson