



UnHacked - AI Productivity Series

Connecting AI to Microsoft 365

Quick-start guide for Claude (Cowork) and ChatGPT • Episode 90 Resource

⚠ SECURITY DISCLAIMER — READ BEFORE CONNECTING

Connecting an AI platform to Microsoft 365 grants that platform access to your email, calendar, contacts, OneDrive files, and SharePoint data. Understand the following risks before proceeding:

- **Data exposure:** AI providers may process and temporarily store your M365 content on their servers. Review the provider's data-retention and privacy policies.
- **Credential risk:** Never store passwords or credit card numbers in your browser if the AI has browser access — agents can act on saved credentials autonomously.
- **Scope creep:** AI agents will attempt to access anything they can reach. Use least-privilege permissions — grant only what the task requires.
- **Admin approval required:** M365 connector apps require IT/Global Admin authorization. Do not attempt to bypass this step.
- **Compliance:** If your business is subject to HIPAA, SOC 2, or similar frameworks, consult your MSP or compliance officer before enabling any AI–M365 integration.
- **Autonomous actions:** Read-only mode is the safest starting point. Write/send access should only be added after thorough testing and with a human-in-the-loop review step.

What You'll Need Before You Start

Requirement	Claude (Cowork)	ChatGPT
App/Platform	Claude Desktop App (mac/Win)	chatgpt.com or ChatGPT desktop
M365 Account	Business or personal M365	Business or personal M365
IT/Admin access	Required for first authorization	Required on business tenants
Permissions level	Mailbox, calendar, OneDrive, SharePoint (read)	OAuth scope — choose read-only first
Recommended starting point	Daily inbox summary prompt	Email summary in a Custom GPT

Best Practices for Both Platforms

Start with read-only access and a single task. Build complexity one layer at a time — confirm each step works before adding the next.

Always keep a human in the loop for outgoing communications. Review drafts before anything is sent, posted, or saved.

Test with 'what can you see?' first. Ask the AI what it has access to before building any workflow. If it describes your actual data, the connection is live.



Watch for AI 'scope creep.' Agents naturally try to be helpful — and will explore anything they have access to. Limit folder and data access explicitly.

Questions? Visit unhackmybusiness.com to find this resource, episode transcripts, and request a free 30-minute consult with the UnHacked hosts.



Claude (Cowork) + Microsoft 365

Using the Claude Desktop App and Claude Cowork to connect your M365 mailbox, calendar, and files

Setup Steps

1	Install the Claude Desktop App Download from claude.ai/download . The desktop app (not the browser tab) is required for M365 connector access and Claude Cowork.
2	Open Customize → Connectors In the Claude Desktop App, click Customize (top-right), then select Connectors. You will see a list of available integrations.
3	Select Microsoft 365 and click Connect Find the Microsoft 365 plugin and click Connect. A Microsoft login/authorization window will appear.
4	Get IT/Admin approval You will not have Global Admin access — nor should you. Have your IT department or M365 Admin authorize the app. They will see exactly what Claude is requesting access to (mailbox read, calendar read, OneDrive, SharePoint based on your existing permissions).
5	Confirm the connector is active Return to Connectors and verify Microsoft 365 shows as connected. Claude can now see your mailbox and calendar.
6	Open Claude Cowork and set folder permissions In Cowork, start a new task. When prompted for file access, choose Limited Access — do NOT grant full system access. Select only the specific project folder(s) needed. This prevents Claude from browsing sensitive areas of your computer.
7	Test with a read-only prompt Start simple: "What are the top 5 emails in my inbox right now?" Confirm Claude can see your data before building any automation. If it returns an error, permissions have not yet propagated — wait a few minutes and retry.
8	Build your automation incrementally Once access is confirmed, add complexity one layer at a time. Example: "Create a daily inbox summary at 7:55 AM Monday–Friday." Then add calendar. Then add ticket triage. Each addition should be tested before the next is layered in.

What Claude Can Access (Once Connected)

M365 Service	Default Access	Notes
Email (Inbox)	Read	Summarize, triage, draft responses — never auto-sends
Calendar	Read	Daily agenda, meeting prep summaries



OneDrive	Read (your files only)	Find files, review folder structure
SharePoint	Read (your permissions)	Access limited to what your account already has
Send/Write	Not enabled by default	Must be explicitly added; human review recommended

Sample Starter Prompts

Daily summary: *"Create a daily inbox summary that runs at 7:55 AM, Monday–Friday. Include my top 5 emails by priority, my calendar for the day, and flag anything time-sensitive."*

Folder audit: *"Look at my OneDrive folder structure. Are there duplicate or disorganized folders I should clean up?"*

Test prompt: *"What are the top 5 emails in my inbox right now?" — Use this first to confirm the connection is live before building any automation.*

Security reminder: When setting up Cowork, always choose Limited Access and select only the specific folder(s) needed. Do not grant full computer access. Keep Claude Desktop App open for scheduled tasks to run — but close any browser tabs with saved passwords or payment info.



ChatGPT + Microsoft 365

Connecting ChatGPT to your M365 mailbox, calendar, and files via OAuth and Custom GPTs

Setup Steps

1	Log in to ChatGPT and go to Explore GPTs Visit chatgpt.com. From the left sidebar, click Explore GPTs, then search for Microsoft.
2	Find and open the Microsoft 365 connector Search for "Microsoft 365" in the GPT store. Anthropic-published connectors are labeled clearly. You can also access integrations directly inside a custom GPT's settings.
3	Connect your Microsoft account Click Connect to Microsoft 365. A Microsoft OAuth window will open. Sign in with your work account. Carefully review the permissions list — accept only what your task requires.
4	Admin consent (enterprise accounts) On M365 business tenants, the first-time connection may require Admin Consent from your IT department. Send them the authorization link that Microsoft provides. This is required for your organization's data to be accessible.
5	Choose your access scope When possible, use read-only permissions first. Only enable write permissions (e.g., send email, edit files) if the task explicitly requires it — and only after testing thoroughly.
6	Test access with a simple query In a new chat with the connected GPT, ask: "Summarize my last 5 emails." If the connection is working, ChatGPT will return actual email data. A failed connection returns a generic error or hallucinated content.
7	Use within a Custom GPT (recommended) For recurring workflows, build a Custom GPT (My GPTs → Create) and connect M365 there. This lets you give the GPT a specific system prompt and scope, reducing the chance of it wandering outside its intended task.
8	Set a human review checkpoint Do not let ChatGPT auto-send emails or auto-modify files without a human reviewing first. Configure your workflow so ChatGPT drafts content that you review and approve before anything is sent or saved.

What ChatGPT Can Access (Once Connected)

M365 Service	Default Access	Notes
Email (Inbox)	Read	Summarize emails, draft replies — do not auto-send
Calendar	Read	View events, meeting prep
OneDrive / SharePoint	Read (if authorized)	Access depends on OAuth scope granted at setup



Contacts	Read (if authorized)	Available but use cautiously — PII risk
Write / Send	Not recommended initially	Enable only with human review checkpoint in place

Sample Starter Prompts

Test connection: *"Summarize my last 5 emails." — Run this first. If ChatGPT returns real email data, the connection is live. Hallucinated content means the connection failed.*

Custom GPT workflow: *"Draft a reply to the most recent email from [client name] summarizing our conversation and next steps." — Best used inside a Custom GPT with M365 connected at the GPT level.*

Calendar prep: *"What meetings do I have tomorrow and what should I prepare for each one?"*

Security reminder: ChatGPT's M365 integration uses OAuth — your credentials are never shared with OpenAI directly. However, the content of emails and files you ask about is sent to OpenAI for processing. Do not use this integration if your business handles PHI, PCI data, or other regulated content without first confirming your compliance posture with your MSP or attorney.