CybersecurityGirl

PROTECT YOUR PRIVACY: MANAGING DATA IN *ai tools*

AI tools can make our work faster and easier but they also raise important questions about privacy. The good news is that you can stay in control of your data by choosing the right tools and adjusting a few key settings.

CONSUMER AI TOOLS

Many people use public AI tools like ChatGPT, Claude, or the free versions of Gemini and Copilot. They're convenient and easy to access, but by default, they often use your conversations to improve their models. That means you'll need to tweak a few settings and be mindful of what you share.

AI TOOLS	DETAILS	HOW TO PROTECT YOUR DATA
ChatGPT (OpenAI)	By default, ChatGPT saves your chats and uses them for training.	• Click your profile icon (bottom-left). • Go to Settings > Data Controls. • Toggle off "Improve the model for everyone."
Claude (Anthropic)	As of September 2025, Claude also uses data for training unless you opt out.	• Go to claude.ai. • Click your profile icon (bottom-right). • Open Privacy Settings. • Turn off "Help improve Claude."

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.

SMART HABITS FOR ANY CONSUMER TOOL

- Avoid sharing sensitive information. Don't type in passwords, financial info, or anything you wouldn't say in a crowded room.
- Use a burner email. Keep your main account safe by signing up with a secondary address.
- Check app permissions. If a tool asks for microphone or contact access you don't need, deny it.
- Clear cookies and cache. Especially on shared devices.
- Opt out of marketing/analytics. If the option exists, disable extra data sharing.
- Use a VPN and privacy-focused browsers. These add another layer of security.

TRUSTED (ENTERPRISE-LICENSED) AI TOOLS = MAXIMUM PROTECTION

If you have access to enterprise-licensed versions of tools like Google Gemini, Google NotebookLM, or Microsoft Copilot, you already have strong privacy safeguards.

They're like the "big sibling" of consumer tools more powerful, more secure, and tailored to meet the specific needs of companies.

ENTERPRISE AI TOOLS

With enterprise tools, businesses get more control over how data is handled, stored, and secured. Enterprise tools aren't just private they're also built to meet compliance standards. That means they're safe to use in industries where data rules are strict, like healthcare, finance, or education.

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.

AI TOOLS	DETAILS	HOW TO PROTECT YOUR DATA
Gemini (Google)	Conversations stay within the enterprise domain. Data is not used for model training.	Data is retained for up to 72 hours for security purposes, then deleted automatically. No action required protections are built in.
NotebookLM (Google)	Uploaded documents and interactions are secured under the enterprise agreement.	Data is not used for training. Retained for up to 72 hours only, then deleted. Protections enabled by default.
Microsoft Copilot (Enterprise)	Operates inside your organization's Microsoft 365 environment.	Prompts and responses are not used for training. Data never leaves the Microsoft 365 boundary. Look for the green shield icon to confirm enterprise protection is active.

THE BIG DIFFERENCE? SECURITY & CONTROL

With consumer tools, you're essentially trusting the provider with your data. With enterprise tools, businesses get more control over how data is handled, stored, and secured. So, if you're just brainstorming ideas or writing an essay, consumer tools are fine.

But if you're handling sensitive data or need AI to power your business operations, enterprise tools are the way to go.

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.