Does AI Take Your Data? AI and Data Privacy

Generative AI, including platforms like ChatGPT, DALL-E, Google Gemini, Apple Intelligence, has revolutionized our relationship with technology. Maybe these tools have completely changed how you work and engage with the internet. There seems to be endless ways to use these platforms, many of which are called large language models (LLMs). These chatbots can assist with brainstorming, writing, and even coding—but they also can be significant risks when used carelessly. One of the biggest concerns? Employees inadvertently exposing sensitive company information.

Our 2025 Oh Behave report found that 65% of us are concerned about AI-related cybercrime, and most people (58%) haven't received any training about using AI securely. Let's change that!

First and foremost, when you're using an AI tool, think about what you're sharing and how it could be used.

Think intelligent about AI

AI models process and store data differently than traditional software. Public AI platforms often retain input data for training purposes, meaning that anything you share could be used to refine future responses—or worse, inadvertently exposed to other users.

Here are the major risks of entering sensitive data into public AI platforms:

- **Exposure of private company data** – Proprietary company data, such as project details, strategies, software code, and unpublished research, could be retained and influence future AI outputs.
- **Confidential customer information** – Personal data or client records should never be entered, as this could lead to privacy violations and legal repercussions.

Many AI platforms allow you to toggle off the use of what you enter for training data, but you shouldn't trust that as an ultimate failsafe. Think of AI platforms as social media: if you wouldn't post it, don't enter it into AI.

CHECK BEFORE YOU USE AI AT WORK

Before integrating AI tools into your workflow, take these critical steps:

1. **Review company AI policies** – Many organizations now have policies governing AI use. Check whether your company allows employees to use AI and under what conditions.
2. **See if your company has a private AI platform** – Many businesses, especially large corporations, now have internal AI tools that offer greater security and prevent data from being shared with third-party services.
3. **Understand data retention and privacy policies** – If you use public AI platforms, review their terms of service to understand how your data is stored and used. Specifically look at their data retention and data use policies.

HOW TO PROTECT YOUR DATA WHILE USING AI

If you're going to use AI, use it safely!

- **Stick to secure, company-approved AI tools at work** – If your organization provides an internal AI solution, use it instead of public alternatives. If your workplace isn't there yet, check with your supervisor about what you should do.
- **Think before you click**—Treat AI interactions like public forums. Don't enter information into a chatbot if you wouldn't share it in a press release or post it on social media.
- **Use vague or generic inputs** – Instead of inputting confidential information, use general, nonspecific questions as your prompt.
- **Protect your AI account with strong passwords and MFA** – Protect your AI accounts like all your other ones: use a unique, complex, and long password (at least 16 characters). Enable multi-factor authentication (MFA), which will add another solid layer of protection.

Increase your AI IQ

Generative AI is powerful! But you are wise. Use AI intelligently, especially when sensitive data is involved. By being mindful of what you share, following company policies, and prioritizing security, you can benefit from AI without putting your company at risk.

You can learn more about AI safety and many more cybersecurity topics by signing up for our newsletter!