



What you should **never** type into an AI chatbot

Tools like ChatGPT, Claude, and Gemini are great for writing, learning, and brainstorming. But the moment you hit enter, your words travel to outside servers — and may be used to train future AI or seen by human reviewers.



Treat every prompt as if it could become **public and permanent**.

5 things to keep to yourself



NEVER SHARE

01

Government & legal IDs

If your account is hacked or data leaks, these numbers are a direct route to identity theft.

DON'T TYPE

Social Security number

Driver's license

Passport details

Tax ID



NEVER SHARE

02

Financial & account info

AI doesn't need real account details to help you budget or do math. Keep your money separate.

DON'T TYPE

Card numbers

Bank accounts

PINs

Crypto private keys



NEVER SHARE

03

Work secrets & code

Pasting confidential work into AI can leak company secrets and break your employment agreement.

DON'T TYPE

Unreleased plans

Financial reports

Internal emails

Proprietary code



NEVER SHARE

04

Medical & therapy details

General health questions are fine — but your actual records and deeply personal crises are not.

DON'T TYPE

Medical records

Named conditions

Mental-health crises



NEVER SHARE

05

Passwords & security answers

An AI is not a password manager. Never ask it to "store" or "remember" your credentials.

DON'T TYPE

Email passwords

Wi-Fi keys

Security-question answers

Mother's maiden name

Smart habits that keep you safe



Anonymize first

Reviewing a resume or contract? Swap real names, numbers, and addresses for placeholders like **[John Doe]**.



Turn off chat history

Under **Privacy** or **Data Controls**, disable history & training so your text isn't reused.



Don't trust it blindly

AI can "hallucinate" convincing nonsense. Double-check medical, legal, and money facts with a real expert.



THE GOLDEN RULE

If you wouldn't post it publicly on a billboard, don't paste it into an AI.

