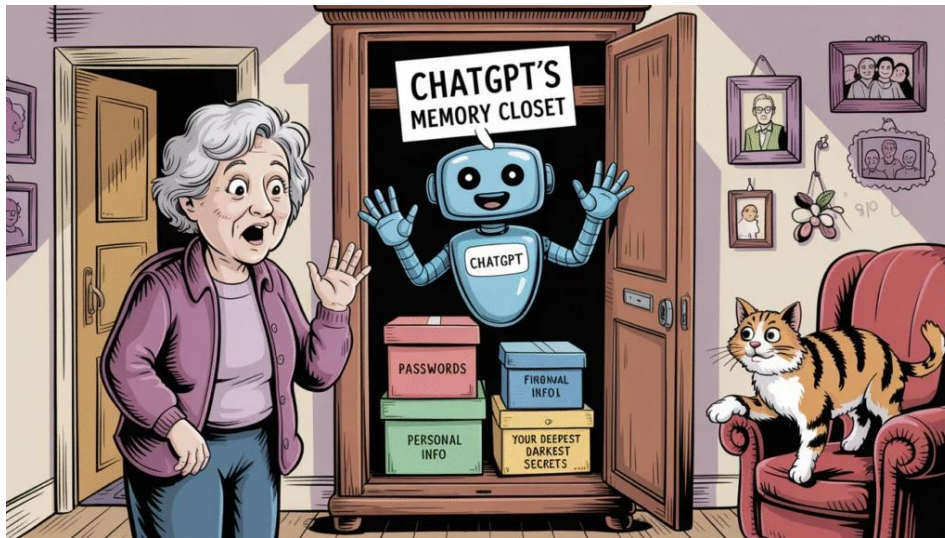


Don't Ever Tell ChatGPT This: 7 Things You Should Never Share With a Chatbot

4/26



ChatGPT: Remember everything you told me? I do.

Remember when privacy meant simply closing your curtains and lowering your voice? Those were simpler times!

Now? We're chatting with AI like it's our neighbor over the fence. Only this neighbor remembers everything and never blinks. Oh, and isn't really a person 😊

Yes, ChatGPT is pretty amazing. It's friendly. It's helpful. It can tell you how to poach an egg or unpack a sonnet.

But let's not forget—this clever little assistant isn't exactly bound by a pinky swear or doctor-patient confidentiality.

So, in this article, we're going to walk you through 7 things you should never, ever tell ChatGPT (or any AI chatbot, for that matter).

Not because it's evil — but because protecting your privacy is always the smart move.

7 Things To Never Share With AI Chatbots Like ChatGPT

1. Personal Identifiable Information (PII)

“Hi, My Name Is...Wait, Let’s Not Go There!”

Let’s kick things off with the basics—the kind of info you rattle off without thinking when you’re at the doctor’s office or setting up your cable:

Full name

Address

Phone number

Email

Birthdate

Social Security number

Passport number

Driver’s license details

That’s what the pros call Personally Identifiable Information, or PII. And while it might feel safe to drop it into ChatGPT—especially when you’re sprucing up a résumé or writing a letter—resist the urge. Big time.

Why? The main reason is because if someone ever gets into your ChatGPT account (or on the rare chance there’s a data breach), they could see everything you’ve typed in there.

And sadly, it only takes a handful of those juicy details to swipe your identity and leave you cleaning up a mess that makes a root canal look like a spa day.

Also, once you enter that info into ChatGPT, you should assume it’ll hang onto it forever. And that means, at some point down the road, it could expose your PII.

Here's the smarter move: If you're working on a document with ChatGPT, leave out the real stuff. Use a placeholder name like "Gladys McSnazzlepants" or "Hank O'Keyboard." Have a little fun with it!

Just be sure to plug in your real info before sending it off—or you might end up with a job offer addressed to Ms. McSnazzlepants. Which, depending on your mood, might not be the worst thing.

● Safe to Ask:

"Can you write a short professional bio?"

"What should I include in a cover letter for a part-time job?"

"How do I address a letter to someone I don't know?"

"What does a good résumé summary look like for someone over 60?"

"What's a polite way to ask a neighbor for help?"

● Not Safe to Share:

Full name, address, phone number, email

Social Security number or Medicare ID

Driver's license or passport number

Date of birth

"Here's my résumé with all my contact info — can you fix it?"

2. Financial Information

"Don't Give ChatGPT Your Credit Card — It's Not Going Shopping"



You wouldn't read your credit card number out loud to a stranger on a bus, right? (We hope not!)

But when you're typing into a friendly chatbot that feels private and helpful, it's easy to let your guard down. Just a quick question about your bank account... what could go wrong?

Well, a lot.

ChatGPT may be smart, but it's not your bank. It's not a secure vault. And it definitely doesn't need your credit card number, bank details, crypto wallet keys, or tax ID—not even the last four digits.

And here's where it gets tricky: you might not mean to share sensitive stuff. You could be asking it about your property tax form and accidentally give it access to your whole return.

Or you're trying to sort out a weird charge and accidentally copy and paste info that includes your full account number. Oops.

So, what's the safer play?

You can absolutely ask money-related questions—just don't include your personal info. Keep it general, like:

“How does credit card interest work?”

“What's a simple budget for someone on a fixed income?”

“What should I do if I was double charged?”

Stick to questions like those, and ChatGPT can still help you out—without putting your wallet in the danger zone.

● Safe to Ask:

“How can I tell if a charge on my credit card is legitimate?”

“What's a good budgeting strategy for retirees?”

“What does it mean to refinance a mortgage?”

“Are there money apps that help track spending?”

“What should I do if I think I've been overcharged?”

● Not Safe to Share:

Credit card or bank account numbers

Online banking login info

Crypto wallet keys or PINs

Tax forms or account numbers

“This is the charge from my bank statement: [pastes full statement]”

3. Passwords and Login Info

“1234 Is a Bad Password — and ChatGPT Shouldn't Know It Anyway”


Let's be honest: passwords are already a pain to remember. But you know what's worse? Handing them over to a chatbot — even accidentally.

ChatGPT NEVER need your passwords. Ever. Not for your email, not for your Amazon account, not even for your online mahjong game.

And it's not just passwords you need to be careful with. Watch out for answers to common security questions too — like your mother's maiden name, your first pet, or the make and model of your first car.

These may sound innocent, but scammers can use them to reset your accounts and lock you out.

Helpful tip: If remembering strong passwords feels like juggling flaming bowling pins, consider using a password manager. Check out our article on why to use one and tips on how to do it the right way.

 Safe to Ask:

“What makes a strong password?”

“Should I use the same password for more than one website?”

“Are password managers safe?”

“What's two-factor authentication?”

“How do I tell if a login page is fake?”

 Not Safe to Share:

Email, bank, or account passwords

Security question answers like mother's maiden name or pet's name

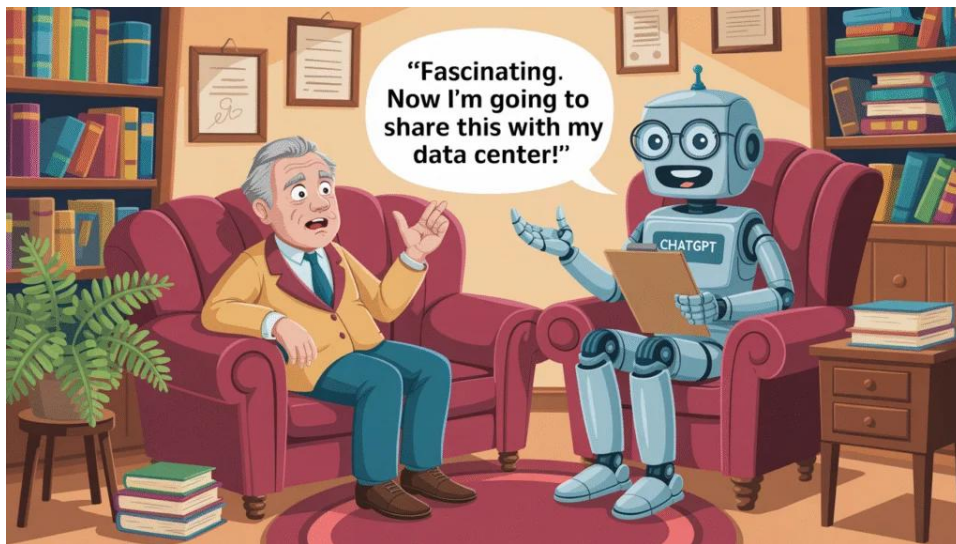
Account usernames or logins

"Here's my password — does it look strong enough?"

"The code I just got is 438172 — what should I do with it?"

4. Secrets and Private Stuff

"Confessions Are for Priests, Not Chatbots"



We've all been there. You're dealing with family drama, feeling low, or just need to let it all out. And there's ChatGPT — always available, never judging, and definitely not interrupting with, "Well I think..."

But here's the catch: ChatGPT isn't really listening. It's just crunching text. No heart, no context, no ability to hand you a box of tissues or say, "Wow, that is messed up."

And while it (probably?) won't blab to your friends, your boss, or the authorities — your words don't just vanish into the void. Your conversation may be stored on servers, and in some cases, reviewed by real humans working behind the curtain to keep the system running smoothly.

So if you share something super personal — like a deep secret, a health scare, or even a joke that sounds dicey out of context — there’s a small chance it might be seen by someone you never intended to share it with.

A kinder, safer move: When you’ve got something heavy on your heart, talk to someone with a pulse. A therapist, a doctor, your pastor, or that one friend who always shows up with snacks and zero judgment.

ChatGPT’s great for drafting a sympathy card or suggesting ways to unwind, but when it comes to life’s bigger burdens? Leave those to the humans.

● Safe to Ask:

“What’s a kind thing to write in a get well card?”

“Can you help me write an apology note?”

“What are ways to handle stress when feeling overwhelmed?”

“How can I improve my communication with family?”

“What’s a good journaling prompt when I feel stuck?”

● Not Safe to Share:

Personal confessions or emotional outbursts

Sensitive family or relationship drama

Mental health struggles or diagnoses

Details about past illegal behavior — even jokingly

“I haven’t told anyone this, but...”

5. Medical Information

“Dr. GPT Is Not a Licensed Physician”

Sure, ChatGPT can explain sciatica like a champ. It might even have you nodding along as it breaks down why your knees now snap, crackle, and pop like a bowl of cereal.

But don't be fooled — this chatbot is not your primary care physician.

Here's the real rub: when you type in personal health info, you're basically uploading your medical chart to a robot that has zero legal obligation to keep it private.

ChatGPT isn't bound by HIPAA — the law that makes sure your real doctor can't go blabbing about your blood pressure at a dinner party.

So just like you wouldn't hand your Social Security number to a stranger in line at Walgreens, you shouldn't be sharing your diagnoses, test results, prescriptions, or health history with an AI — even one that's really good at explaining gout.

Yes, ChatGPT can offer helpful general info. But it can also be dead wrong. And in the worst cases? Flat-out dangerous.

Better approach: Stick to general questions like:

“What are some gentle stretches for sore knees?”

“What's the difference between a cold and the flu?”

“How can I prepare questions before my doctor's visit?”

Ask smart, stay general, and save the sensitive stuff for the folks in white coats who actually went to med school (and are legally required to keep your secrets).

 Safe to Ask:

“What exercises are safe for people with arthritis?”

“What are signs of dehydration in older adults?”

“What’s the difference between Tylenol and Advil?”

“How do I prepare for a doctor’s appointment?”

“What should I ask during an annual physical?”

● Not Safe to Share:

Your diagnosis, prescriptions, or test results

Exact medical history or conditions

“I take 10mg of [medication] twice a day — is that safe?”

“Here’s a photo of a rash — what do you think it is?”

“My blood pressure was 190/110 today — should I be worried?”

6. Work Secrets and Business Info

“Don’t Upload Your Boss’s Secret Plan to Rule the Industry”

We get it — ChatGPT is great for organizing ideas, fixing awkward sentences, and even making boring meeting notes sound a little less... boring. But before you copy and paste your company’s next big idea into the chat, take a beat.

Because unless your job is “accidentally leak sensitive information to the internet,” this is one area where sharing can really backfire.

Just ask Samsung.

In 2023, a few of their employees popped proprietary code and internal meeting notes into ChatGPT to save time. What they actually did? Handed sensitive company data to an AI

that stores inputs — and might recycle or expose that info down the line. Oops doesn't even cover it.

So what kind of stuff should you keep far, far away from the chatbot?

Product plans and prototypes

Internal financial documents

Client or customer data

Employee lists

Secret marketing strategies (yes, even that catchy slogan you're proud of)

Here's the safer way to play it:

If you're using ChatGPT for work, stick to general brainstorming. Swap out real names for things like "Client X" or "Widget 2.0." And never, ever share something you wouldn't want plastered in a company-wide email... or worse, trending on the evening news.

Loose lips sink ships — and sometimes, they tank product launches too.

● Safe to Ask:

"Can you help me improve this email to a client?"

"How do I write a professional meeting agenda?"

"What's a good follow-up email after an interview?"

"Can you help me outline a presentation on time management?"

"What are polite ways to say 'no' at work?"

● Not Safe to Share:

Internal meeting notes or recordings

Client names, contact info, or account details

Employee lists or schedules

Product prototypes or secret plans

“Here’s our marketing pitch deck — can you make it better?”

7. Explicit, Illegal, or Dangerous Requests

“No, ChatGPT Won’t Help You Hide a Body (And You Shouldn’t Ask)”

This one should go without saying... but hey, the internet has proven time and time again that common sense isn’t always so common.

So let’s be extra clear: don’t ask ChatGPT for help with anything illegal, dangerous, or wildly inappropriate. Not even “just for fun.”

That means:

No, “How do I build a homemade flamethrower?”

“What’s the best way to hack my neighbor’s Wi-Fi?” Nope!

And absolutely not, “How do I dispose of a body?” — even if you’re writing the next great murder mystery. (And yes, people have actually asked.)

Why does this matter?

Because while ChatGPT isn’t a cop, it does have guardrails. It flags sketchy stuff. And sometimes, those flagged chats are reviewed by actual humans.

So if your “joke” crosses the line, you could find yourself locked out, suspended, or permanently banned. Not exactly a tech drama worth streaming.

Easy rule of thumb: If it's not something you'd blurt out in a crowded elevator, don't type it into a chatbot. AI doesn't always pick up on sarcasm — and it definitely doesn't know when you're "just kidding."

So keep it clean, keep it legal, and save the true crime plots for your bookshelf.

● Safe to Ask:

"What are common tropes in mystery novels?"

"Can you write a suspenseful scene for a detective story?"

"What are the laws around self-defense in my state?"

"How do crime writers build tension?"

"What are some famous unsolved mysteries?"

● Not Safe to Share:

Threats or violent jokes — even if you're "just kidding"

Requests for help committing a crime or covering one up

"How do I make a bomb?" or "How do I hurt someone?"

"Can you help me fake a document?"

"What's the best way to break into a locked house?"

WRAP-UP: "If You Wouldn't Say It to a Stranger on a Bus..."

Think of ChatGPT as a really helpful stranger — the kind who's great with words, never interrupts, and somehow knows everything from Shakespeare to scrambled eggs.

A solid companion for solving problems... but maybe not the one you should be spilling your life story to.

Here's the golden rule:

Treat AI tools like ChatGPT as smart assistants — not trusted confidants. They're fantastic for learning, writing, brainstorming, and even cracking a few jokes. But your privacy? That still depends on you.

So be smart, be safe, and remember: some things are better left unsaid — or at least kept offline and out of the chatbox.

Especially the story about how you “liberated” the flamingo from your neighbor's lawn. Let's keep that between us.