BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2286

Updated November 2026

The Safe Way to Use AI — What to Never Type Into It

AI is safe to use — as long as you keep a short list of things out of the chat box

Plain-English tech help from:
Bill's Home Tech
Portage County, Ohio

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech
(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3

The Short Version 3

Why This Matters — In Plain Words 4

The Never-Type List 4

The Be-Careful List 5

How to Get Help Without Giving Secrets 6

Photos and Screenshots — a Hidden Trap 6

Watch for Imposters Asking You to Share 7

Setting Up AI More Privately 8

A Special Word on Money and Banking 8

Helping Family Use AI Safely 9

If You Think You Already Shared Something 9

A Simple Monthly Safety Habit 10

When to Call Bill 11

Everyday Cheat Sheet 12

A Note From Bill 13

Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

AI chat helpers are safe to use as long as you remember that whatever you type may be stored and read by the company behind them — treat the chat box like a postcard, not a sealed letter. Never type passwords, PINs, your full Social Security or Medicare number, bank or card numbers, or the six-digit codes texted to you.

You can still ask about any sensitive topic — just ask the how-to or the rule and leave the actual secret out ("What makes a strong password?" not your password). Be careful with photos of documents, which carry numbers and names you forgot were there. And watch for scammers posing as AI: the real tools never call, email, or ask for a code — if a message creates panic and urgency, that pressure is the warning sign.

- Never type passwords, account/card numbers, SSN, or texted codes.
- Ask about the topic without revealing the real detail.
- Real AI never phones or emails you asking for secrets or payment.

1 The Short Version

AI chat helpers like ChatGPT, Gemini, and Copilot are wonderfully useful, and using them is safe as long as you remember one thing: whatever you type into them may be stored and read by the company that runs them. It is a bit like talking to a very helpful clerk at a company you do not entirely know — fine for questions and everyday help, but not the place to read out your bank details.

This guide gives you a short, clear list of what to never type into AI, why it matters, and how to get the help you want without ever handing over a secret. The good news is that you lose almost nothing by being careful — you can ask about sensitive topics without revealing the actual private numbers.

- Treat anything you type into AI as if a company employee might read it one day.
- Never type passwords, full account or card numbers, or Social Security numbers.
- You can still ask about these topics — just leave the actual secret out.

- Being careful costs you almost nothing and protects you completely.

> **WATCH OUT**
> A simple test before you type anything sensitive: "Would I be comfortable if this appeared on a company's screen somewhere?" If the answer is no, don't type it — ask the question a different way, as this guide shows.

2 Why This Matters — In Plain Words

When you type into an AI helper, your words usually travel to the company's computers to be understood and answered. Many companies keep those conversations for a while — to improve their systems, or simply because that is how the service works. That does not make them villains; it makes them like any company that keeps records. But it means the AI chat box is not a private diary or a locked drawer.

So the rule is not "fear AI." The rule is "treat the chat box like a postcard, not a sealed letter." You would happily write a question on a postcard. You would not write your bank password on one. Same idea, and once it clicks, you will use AI with total confidence.

> **GOOD TO KNOW**
> This is the same caution you already use elsewhere without thinking — you do not email your PIN or shout your card number in a shop. AI is just one more place to apply a habit you already have.

3 The Never-Type List

Here is the short list to keep in mind. If something on it comes up, that is your signal to stop and rephrase. Print this and tape it near your computer if it helps.

- Passwords, PINs, and security-question answers (your first pet, your mother's maiden name).
- Full Social Security number or Medicare number.
- Full bank account or routing numbers.
- Full credit or debit card numbers, and the three digits on the back.
- Online banking or login details of any kind.
- One-time codes texted to you (the six-digit verification numbers).

WATCH OUT

Those texted one-time codes deserve special caution. No legitimate helper — human or AI — ever needs one. Anyone or anything asking you to type or share a verification code is a red flag for a scam, every single time.

4 The Be-Careful List

These are not forbidden, but they are worth a pause. You can share them if you truly need to for the task, but ask yourself first whether the AI really needs the real detail or just the general picture.

- Your full home address and daily routine.
- Detailed medical history with your name attached.
- Photos of documents — IDs, bills, statements — that show numbers and addresses.
- Other people's private information (a family member's health or finances).
- Anything a workplace or client told you in confidence.

GOOD TO KNOW

You can almost always get the same help by blurring the specifics. "Explain this type of bill" works as well as uploading the bill with your account number on it. The AI helps with the shape of the problem; it rarely needs the identifying details.

5 How to Get Help Without Giving Secrets

This is the liberating part: you can ask about every sensitive topic on earth without ever typing the private number. The trick is to ask about the situation, not to hand over the data.

Instead of typing this…	Type this…
My password is Rover123, is it strong?	"What makes a strong password? Give me rules."
Here's my bank statement [photo]	"How do I read a bank statement? What do these terms mean?"
My card number is 4111… is this charge normal?	"I see an unfamiliar charge. How do I dispute it with my bank?"
My SSN is 123-45-6789	"How do I protect my Social Security number from fraud?"

WATCH OUT

Notice the pattern: ask for the how-to, the explanation, or the rule — never paste the secret itself. You get all the knowledge and give away nothing. This one habit covers almost every situation.

6 Photos and Screenshots — a Hidden Trap

It is easy to forget that a photo carries information you are not thinking about. Snap a picture of a letter to ask what it means, and you may have just shared your full name, address, account number, and a barcode along with it. The AI reads everything in the image, not just the part you care about.

1. Before sharing a photo of any document, look at everything visible in it.

2. Cover or crop out account numbers, full names, addresses, and barcodes you don't need help with.
3. Better yet, just type your question in words rather than sharing the image at all.
4. Never share a photo of an ID, a card, a check, or a medical record.

WATCH OUT

A check shows your bank account and routing numbers right along the bottom. A photo of a check is one of the most dangerous things to share anywhere online, including with AI. Describe it instead; never picture it.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

7 Watch for Imposters Asking You to Share

The most important safety point is not about the real AI tools at all — it is about scammers who pretend to be them, or who use AI language to sound convincing. The genuine ChatGPT, Gemini, and Copilot will never phone you, never email you asking for a password, and never demand payment in gift cards.

- A real AI tool does not call you, text you, or email you out of the blue.
- No legitimate service ever asks for your password or a verification code.
- "AI" in a pop-up or email demanding urgent action or payment is a scam dressed up.
- If a message creates panic and urgency, that pressure itself is the warning sign.

WATCH OUT

Scammers now use AI to write very convincing emails and even to clone voices. If you get an urgent call or message — even one that sounds like family — asking for money, codes, or secrets, hang up and call the person or company back on a number you already trust. This is one of the most important habits I teach, and I'm always glad to talk it through.

8 Setting Up AI More Privately

Beyond watching what you type, you can tell most AI tools to keep less of your conversation. It is a few taps in the settings, and it is worth doing once.

1. In the AI app's settings, look for a Privacy or Data section.
2. Find an option like "improve the model for everyone" or "use my chats for training" and turn it off if you prefer.
3. Look for a way to delete your chat history, and clear old conversations you don't need.
4. Some tools offer a "temporary" or "incognito" chat that isn't saved at all — use it for anything slightly sensitive.

> **GOOD TO KNOW**
>
> There is a companion guide, "Keep AI From Learning Your Private Information," that walks through these settings for each major tool. Turning off training and using temporary chats are the two simple moves that do most of the work.

9 A Special Word on Money and Banking

Because money scams are the ones that hurt most, they deserve their own moment. AI can be a fine helper for understanding money — explaining a term, comparing options, drafting a letter to the bank. It is never a place to conduct your banking or reveal your account details.

- Use AI to understand: "What's the difference between a credit freeze and a fraud alert?"
- Do your actual banking in your bank's own app or website, or by calling the number on your card.
- Never let AI, or anything online, talk you into moving money, buying gift cards, or sharing codes to "protect" your account.

WATCH OUT

A real bank will never ask you to move your money to "keep it safe," and neither will any legitimate helper. That request is always a scam, no matter how official it sounds or how much it knows about you.

10 Helping Family Use AI Safely

If you are the one in the family others turn to, or if you worry about a relative, these habits are worth sharing gently. The goal is confidence, not fear — AI is safe to use well.

- Share the never-type list; it is short and it sticks.
- Agree on a family "safe word" to confirm a call for help is really from family.
- Remind each other: real companies don't demand codes, passwords, or gift cards.
- Make it normal to say "let me check on that and call you back" — pausing defeats most scams.

TIP

The single most protective habit for anyone is the pause. Scams and bad ideas rely on urgency. "I'll think about it and get back to you" is a complete, powerful answer to any pressure, online or off.

11 If You Think You Already Shared Something

If you realize you typed a password, a card number, or another secret into an AI tool — or into anything online you now doubt — don't panic, and don't be hard on yourself. It is a common mistake and it is fixable. The key is to act calmly and promptly to close the door.

1. If it was a password, change that password now, and change it anywhere else you used the same one.

2. If it was a card number, call the bank using the number on the back of the card and ask them to watch for fraud or reissue it.
3. If it was your Social Security number, consider a free credit freeze with the credit bureaus to block new accounts.
4. Delete the conversation in the AI tool's history so it is not sitting there.
5. Keep an eye on your statements for anything unfamiliar over the next few weeks.

> **GOOD TO KNOW**
>
> Sharing something once rarely leads to immediate harm, and taking these steps closes off nearly all the risk. The worst thing you can do is nothing out of embarrassment — and there is genuinely nothing to be embarrassed about.

12 A Simple Monthly Safety Habit

Safety is easiest when it is a small, regular habit rather than a worry you carry constantly. A few minutes once a month keeps everything tidy and catches problems early, whether or not you use AI much.

- Glance at your bank and card statements for charges you don't recognize.
- Clear out old AI conversations you no longer need.
- Check that your important passwords are still strong and not reused.
- Remind yourself of the never-type list — a quick re-read keeps it fresh.

> **TIP**
>
> Pin it to a day you'll remember — the first of the month, or the day you pay a regular bill. Ten minutes, once a month, is enough to keep you well ahead of almost any online trouble.

13 When to Call Bill

Using AI safely is mostly about a few simple habits, and this guide gives you all of them. But it helps to have someone set your privacy options with you, look over the tools you use, and talk through the scam warning signs on your own screen — especially if a message has already rattled you.

I come to you, set up your AI tools the private way, go over the never-type list until it feels like second nature, and show you exactly how to spot an imposter asking for secrets. If you have had a suspicious call, email, or pop-up, bring it to me — I will tell you plainly whether it is a scam and help you shut the door on it. There is never any judgment, only help.

- You want your AI privacy settings set up the safe way.
- You received a suspicious message and want to know if it's a scam.
- You'd like the never-type habits shown and practiced on your own device.
- You want to help a family member use AI safely and want a hand setting it up.

CHEAT SHEET

Everyday Cheat Sheet

Tape this near your computer. Treat the chat box like a postcard, not a sealed letter.

I want to...	Do this...
Know the hard rule	Never type passwords, PINs, SSN/Medicare, bank or card numbers, or texted codes
Get help on a secret topic	Ask the how-to or the rule — leave the actual number out
Share a document safely	Don't photo it — describe it; crop out numbers, names, barcodes
Spot an imposter	Real AI never calls, emails, or asks for a code or password
Beat the pressure	"Let me check and call back" — the pause defeats most scams
Keep less stored	App settings Privacy turn off training, use temporary chats
Get help	Call Bill: (330) 200-8042

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.