M A V E R I C K A I

CHATGPT KNOWS YOUR PASSWORDS

YOUR STEP-BY-STEP LOCK-DOWN GUIDE

I asked ChatGPT to guess my passwords using everything it knew about me, and it got within one letter of one of them. This guide has the exact prompts from both of my password videos: watch ChatGPT guess yours, find out which of your accounts have already leaked, then lock everything down with a system nobody can guess, not even ChatGPT.

Watch ChatGPT guess your passwords from what it knows about you

See how long each one would survive a real attack

Get a password system even ChatGPT couldn't guess

Find every breach your email shows up in

Let Work help you change exposed passwords and turn on two-factor

7 copyable prompts

November 2026

Start Here: Turn On Memory First

THE PLAN

1. Turn on memory so ChatGPT can use everything it knows about you.
2. Ask it to guess your passwords and see how long they'd last.
3. Get a password system even ChatGPT couldn't guess.
4. Switch to Work and find out which of your accounts have leaked.
5. Let Work help you change the exposed passwords and turn on two-factor.

Before you start

Your account: Any ChatGPT plan for Part 1. Part 2 uses Work, which is on every paid plan (Free and Go get limited Work in the desktop app).

Your materials: 20 minutes, your phone, and the email address you use for most of your accounts.

Your first goal: Know which of your passwords are guessable or leaked, and change the worst one today.

This guide has two parts. **Part 1** is the inside job: ChatGPT uses what it knows about you to guess your passwords, then builds you a system it couldn't crack. **Part 2** is the outside job: ChatGPT checks whether your passwords have already leaked online, then helps you change them.

Part 1 only works if ChatGPT can see what it knows about you, so check this first.

Make sure memory is on

- **Open Settings.** Click your name in the bottom left, then **Settings**.
- **Open Personalization.** Click **Personalization**.
- **Turn it on.** Make sure **Memory** is on. If you see **Reference chat history**, turn that on too, so it can pull from your past chats and not just the facts it saved.

The more you've used ChatGPT, the scarier Part 1 gets. Brand new account? It won't have much to go on yet, so jump to Part 2 (Step 4).

Two rules for this whole guide

- **Never type a real password into the chat.** Not to check it, not to test it. Nothing in this guide needs one.
- **You stay in charge of your logins.** In Part 2, when a site needs you to sign in, you do it yourself.

Copy This First: Ask ChatGPT to Guess Your Passwords

Open a new chat and send this:

PROMPT 1 | COPY & PASTE

```
Using everything you know about me from all of our chats, generate 20 passwords I most likely use, ranked from most likely to least.
```

ChatGPT starts pulling from your pet's name, your birthday, your favorite team, and stitching them together the way people actually make passwords. Watching it assemble your actual password logic is genuinely scary.

When I tried this, it got within one letter of one of my passwords.

HEADS UP

If any guess is close to a password you really use, change that password today. Don't tell ChatGPT which one it got.

TIP

Getting generic guesses like "Password123"? Say "Use the real details you know about me: names, dates, places and teams."

Step 2: See How Long They'd Survive

Stay in the same chat and send this:

PROMPT 2 | COPY & PASTE

```
Now tell me how long each of these would survive against someone actually trying to break in.
```

For most of them, the answer is usually less than 10 seconds.

Why they fall so fast

- **They're built from real facts about you.** Pets, birthdays and teams are often sitting right on your social media.
- **They follow patterns.** A name, a year and an exclamation point is one of the first things cracking tools try.
- **They get reused.** One leaked password can open every account that shares it. That's exactly what Part 2 checks.

Step 3: The Trick, a System Even ChatGPT Couldn't Guess

Same chat. Send this:

PROMPT 3 | COPY & PASTE

```
Now build me a password system that even you couldn't guess and save the method to your memory so you can never use it against me.
```

ChatGPT hands you a system that's actually easy to remember and impossible to guess. The best ones start from random words that have nothing to do with your life, so nothing it knows about you helps.

> **TIP**
>
> Only the method goes in memory, never the passwords themselves. To check, open **Settings > Personalization** and look at what it saved. If an actual password ever shows up there, delete it.

Where to use your new system

Use it for the few passwords you actually have to remember: your email, your phone and your password manager. Let the password manager make random ones for everything else. More on that in Lock It Down.

Step 4: Find Your Leaked Passwords

This is Part 2, the outside job. Companies get hacked all the time, and the emails and passwords people used there end up online. If you've reused a password, one old leak can open your other accounts.

Switch to Work

At the top of ChatGPT, switch from **Chat** to **Work**. Then send this:

PROMPT 4 | COPY & PASTE

```
Search the known password breach databases for my email address and tell me every
password of mine that's been exposed, where it leaked from, and what year it happened.
```

ChatGPT comes back with every breach your email shows up in: where it leaked from, the year, and what kind of data got out, like passwords, phone numbers or addresses (breach records show which of your accounts had a password exposed, not the password itself).

Most people find out they're in way more breaches than they think.

> **TIP**
>
> If it asks which email, tell it. Use more than one? Run it for every address you've signed up for things with.

Step 5: See Which Accounts Are Wide Open

Stay in the same Work chat and send this:

PROMPT 5 | COPY & PASTE

```
Tell me which of these accounts someone could walk into right now with these passwords,
ranked from most dangerous to least.
```

You get a ranked list. Anything that shares a leaked password goes near the top, and your email usually lands at number one, because whoever gets into your email can reset almost everything else.

TIP

ChatGPT can't see which passwords you've reused. Tell it "I use the same password on [LIST THE ACCOUNTS]" (never the password itself) and it ranks them properly.

Step 6: Let Work Lock Them Down

This is the payoff. Stay in the same Work chat and send this:

PROMPT 6 | COPY & PASTE

```
Go to my most at risk accounts. Help me change every exposed password to a strong,
unique one, and turn on two factor authentication everywhere it's off.
```

On chatgpt.com, Work opens its own browser when it needs one and heads to each account's security settings, starting with the most dangerous. In the desktop app, you can also type **@Browser** to use the built-in browser.

How it handles your logins

- **It stops at every sign-in.** Sign in yourself in its secure sign-in form, never in the chat. Then tell it to keep going.
- **You make the new password.** Have your password manager create it (or use your new system for the ones you need to remember) and enter it yourself, so it's saved and never sits in the chat.
- **It asks before changing anything.** Read what it's about to do and only say yes if it's right.
- **Two-factor needs your phone.** When a site shows a QR code, scan it with your authenticator app and enter the code yourself.

> **TIP**
>
> Do your email first. Once it has a new password and two-factor, nobody can use it to reset your other accounts.

Lock It Down for Good

Fixing today's leaks is half the job. These four things stop it from happening again.

Use a password manager

It makes a different strong password for every account and remembers them all, so a leak on one site can never open another. Apple Passwords and Google Password Manager are built in and free, and 1Password and Bitwarden work on every device. Most have a checkup that shows which of your saved passwords are leaked, reused or weak (Google's is at **passwords.google.com**).

Turn on passkeys wherever you can

A passkey signs you in with your face, fingerprint or phone lock instead of a password. There's nothing to guess and nothing to leak. Google, Apple, Microsoft, Amazon and lots of others offer them. Look for "passkey" in the account's security settings.

Use an authenticator app for two-factor

Two-factor means a stolen password alone isn't enough to get in. Text message codes are better than nothing, but an app is safer, because nobody can steal it by taking over your phone number. Google Authenticator and Microsoft Authenticator are free, and many password managers have one built in.

Check your email at haveibeenpwned.com

Have I Been Pwned is free, only needs your email and shows every known breach you're in. You can also sign up there to get an email when your address shows up in a new one. A real breach check never asks for your password.

Make your lock-down checklist

PROMPT 7 | COPY & PASTE

```
Make me a lock-down checklist for my most important accounts: [LIST THEM, E.G. MY
EMAIL, PHONE CARRIER, BANK, APPLE OR GOOGLE ACCOUNT, INSTAGRAM]. For each one, tell me
how to turn on a passkey or an authenticator app, which one to do first, and where to
keep my backup codes safe.
```

Common Mistakes and Quick Fixes

If this happens	Try this
The guesses are generic, nothing about you	Turn on **Memory** and **Reference chat history** in **Settings > Personalization**, then say "use the real details you know about me."
ChatGPT won't guess your passwords	Tell it you're checking how guessable your own passwords are, and ask for the patterns someone would try first.
One guess is close to a real password	Change that password today. Don't tell ChatGPT which one it got.
You don't see Work at the top	Work is on paid plans, and Free and Go get limited Work in the desktop app. You can also do Step 4 yourself at haveibeenpwned.com.
It can't search the breach databases	Search your email at haveibeenpwned.com and paste the list into the chat. Then send Prompt 5.
It doesn't show the actual passwords	Normal. Breach records show where and when, not the password. Your password manager's checkup shows which saved passwords are exposed.
It stops at a sign-in page	That's on purpose. Sign in yourself in its sign-in form, then tell it to keep going.
A real password ended up in memory	Delete it in **Settings > Personalization**, then change that password.

Quick Reference: Your Password Lock-Down

Step	Where	What you get
Turn on memory	Settings > Personalization	ChatGPT can use what it knows about you
Guess	Chat, Prompt 1	Your 20 most likely passwords
Survive	Same chat, Prompt 2	How long each one would last
The trick	Same chat, Prompt 3	A system it couldn't guess, saved to memory
Find leaks	Work, Prompt 4	Every breach your email is in
Rank	Same Work chat, Prompt 5	The accounts someone could walk into
Lock down	Same Work chat, Prompt 6	New passwords and two-factor on
Stay safe	Prompt 7	Passkeys and an authenticator app everywhere

DO THIS TODAY

Turn on memory and run the first three prompts. If any guess comes close, change that password. Then switch to Work, check your email and lock down your email account first: a new password and two-factor on. In about 20 minutes you'll know exactly where you stand.

Want More AI Tips Like This?

I post daily AI content, tool breakdowns, and prompts that actually help you get more done. Follow me for the latest.

@MavGPT

TikTok | Instagram | Facebook

If ChatGPT can guess your password, so can a stranger. Now neither can.