CyberDefense Firm FREE CHECKLIST

Five Questions Before You Install Any AI Tool

You don't need to read code to ask these. Put them to the company that makes the tool, your IT person, or the AI assistant itself. Popular isn't the same as safe.

1 What can it reach?

Your files, your email, the passwords saved in your browser? Give it only the access it needs for the job.

A good answer: "Only what this job needs, and you can see and change that list."

2 Where does it keep my logins, and are they locked?

"Saved in a file on your computer" is not the same as "locked." A backup or a lost laptop shouldn't hand someone your accounts.

A good answer: "They're scrambled, and the key is held by your computer's own password vault."

3 What leaves my computer?

Look for settings named sharing, usage reports, or "help us improve," and check whether they start out on or off.

A good answer: "Nothing leaves unless you turn it on."

4 How does it update?

Automatic updates are great from a company you trust. From a stranger's free project, an update can change the tool without anyone checking it first.

A good answer: "Updates come from us, and you can choose when to install them."

5 Who checked it besides the person who built it?

Stars, downloads, and five-star reviews measure popularity, not safety.

A good answer: "An outside reviewer checked it, and here's what they found."

> **The risky part is usually a default.** Most trouble starts with a setting someone accepted without reading it. Slow down at the install screen.

CyberDefense Firm
A 501(c)(3) nonprofit helping schools, churches, and small businesses stay safe online.
Questions? 760-874-8729
cyberdefensefirm.org