

I dieci controlli di sicurezza

L'AI di casa tiene i dati sul tuo PC. Ma «sul tuo PC» è sicuro quanto il tuo PC. Spunta i controlli uno per uno.



DA FARE UNA VOLTA

I dieci controlli

☐

1

Il PC ha una password, o un PIN, e si blocca da solo quando ti allontani.

☐

2

Windows è aggiornato: Impostazioni > Windows Update.

☐

3

I programmi dell'AI sono aggiornati: LM Studio, Ollama, Jan e AnythingLLM avvisano quando c'è una versione nuova.

☐

4

Programmi solo dai siti ufficiali: lmstudio.ai, ollama.com, jan.ai, anythingllm.com. Diffida dei nomi simili (capitolo 7).

☐

5

Modelli solo da fonti note: i modelli verificati di LM Studio, la libreria di Ollama, i produttori ufficiali su Hugging Face.

☐

6

Il cloud spento dove non serve: in Ollama l'interruttore **Cloud** (capitolo 9).

☐

7

Il web spento negli agenti che lavorano su dati riservati: AnythingLLM, Abilità dell'agente (capitolo 16).

☐

8

Il server chiuso alla rete: in Ollama **Expose Ollama to the network** spento, in LM Studio **Serve on Local Network** spento, salvo quando ti serve (capitolo 19).

☐

9

Gli agenti con una cartella sola (capitolo 18).

☐

10

Una copia di sicurezza dei documenti importanti, su un disco esterno o dove la fai di solito.

CAP. 20

Dove i dati possono uscire di casa

DOVE	CHE COSA ESCE	COME LO CONTROLLI
Download di programmi e modelli	che cosa scarichi, e da dove	inevitabile, ma non contiene le tue domande
Cloud di Ollama	le domande ai modelli cloud	interruttore Cloud spento
Agenti con il web	le parole della ricerca	abilità web spente (capitolo 16)
Statistiche d'uso anonime	dati d'uso, non le chat, secondo i produttori	Jan: Impostazioni > Privacy; al primo avvio abbiamo scelto Deny
Questionari al primo avvio	quello che scrivi tu	AnythingLLM: sono facoltativi, lasciali vuoti
Server aperto alla rete	domande di altri dispositivi al tuo PC	resta chiuso (capitolo 19)
Estensioni del browser	il contenuto delle pagine	solo dagli store ufficiali, indirizzo localhost

La prova del nove: rifai la missione Wi-Fi del capitolo 8 con il programma che usi di più. Questa lista non è una consulenza legale: per l'uso al lavoro leggi il capitolo 20 e, per il tuo caso, chiedi a un professionista.