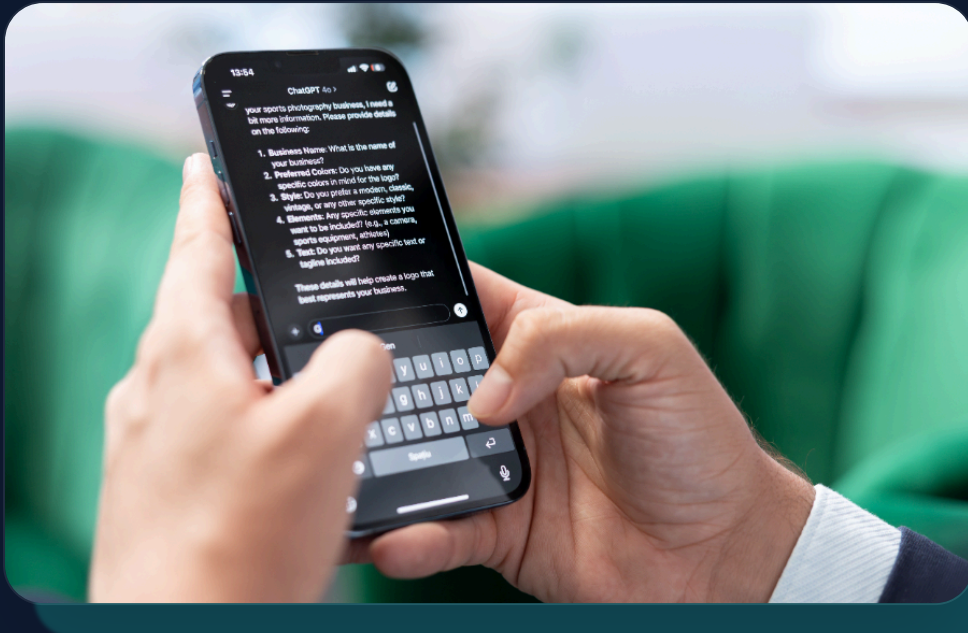


INFOGRAPHIC

# Safe AI Usage at Work

AI can boost productivity, but your prompts may be stored or used to train AI. Share only approved information in approved tools.



THE RISKS

## AI Risks You Should Know



### Uploading Sensitive Data

Pasting customer records, financial data, source code, or confidential documents into AI tools can permanently expose them.



### Unapproved “Shadow AI” Tools

Random AI apps or browser extensions that IT hasn't vetted can leak data outside company control.



### Risky Prompts

Asking AI to process passwords, contracts, or internal strategy documents creates records you can't take back.



### Excessive Permissions

Some AI extensions and connected apps request broad permissions to read your webpages, emails, files, calendars, and internal systems.

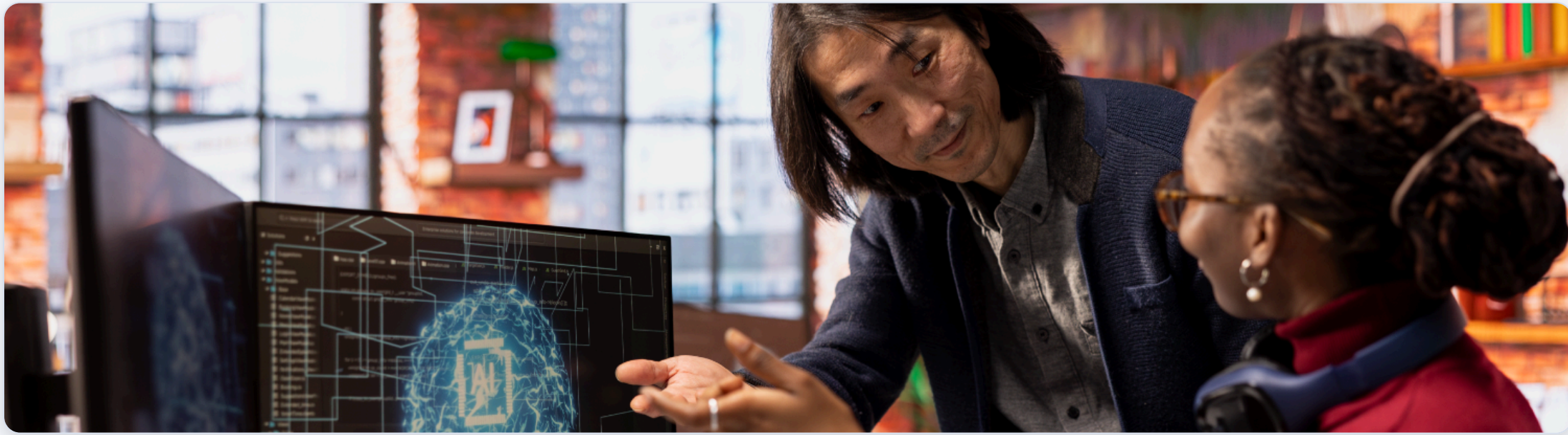


### Third-Party Data Sharing

Many free AI tools reuse your inputs to train their models or share them with partners.

THE RESPONSE

## How to Stay Safe When Using AI



1

### Use Only Approved Tools

Stick to AI platforms your company has reviewed and authorized. Check with IT if you're unsure.

3

### Think Before You Prompt

If you wouldn't post it publicly, don't paste it into an AI tool.

5

### Limit Data Retention

Turn off model training in your AI tool's settings, or use tools that disable it by default.

2

### Check Extension Permissions

Before installing any AI browser extension, review what data and access it's requesting.

4

### Remove & Protect Sensitive Details

Strip names, numbers, and identifiers first, and never save AI outputs with company data outside approved systems.

QUICK CHECKLIST

## Before You Paste

- ✓ Is this tool approved by my company?
- ✓ Does this contain customer, financial, or confidential data?
- ✓ Have I removed names, IDs, or sensitive details?
- ✓ Would I be comfortable if this became public?
- ✓ Am I using company-sanctioned access, not a personal account?