

Avoid Accidental Data Leaks: A Simple Employee Checklist

Quick guidance for safer sharing across apps, cloud, and AI tools



Sensitive data moves through chat, email, SaaS apps, cloud workflows, AI tools, and more. Most exposure starts with normal work habits, not bad intent, so a quick check in the moment helps prevent accidental data leaks.

The Four High-Risk Moments

Sharing and collaboration

If you are about to: share a link broadly; change link access or add collaborators; share a screenshot with customer data or internal tools

Do

- Share to the smallest audience necessary
- Check access first: view vs. edit, internal vs. external
- Check what the link grants access to (file vs. folder)

Avoid

- Using “anyone with the link” access for sensitive files
- Posting sensitive links or screenshots in large channels
- Sharing from “recents” without confirming the contents

Quick Check

If anyone external can access it, tighten permissions first.

Storage and file transfers

If you are about to: upload to a new app, workspace, plugin, or connector; consider using a personal account for a work task; move files between accounts or workspaces

Do

- Use approved tools and corporate accounts
- Verify the destination (correct tenant, workspace, folder)
- Confirm who will have access after the upload or share

Avoid

- Personal storage “just for a minute”
- New plugins or applications without admin approval
- Uploading while signed into multiple accounts

Quick Check

If anyone external can access it, tighten permissions first.

AI tools and assistants

If you are about to: use an AI tool or assistant; ask it to summarize a customer case, ticket, or contract; include identifiers (names, emails, IDs)

Do

- Remove identifiers first (names, emails, IDs)
- Describe the problem rather than pasting raw records
- Use the minimum text needed to get the result

Avoid

- Pasting customer records, tickets, or contracts
- Sharing credentials, secrets, or internal links
- Pasting unique details (order numbers, case IDs)

Quick Check

If it could identify a person, account, or customer, delete it.

Moving data between tools

If you are about to: export a report with customer, employee, or financial info; copy data into spreadsheets or documents; compress, zip, encrypt, or package files to transfer them

Do

- Export only what’s needed for the task
- Check for hidden columns, extra tabs, and embedded data
- Open and review before you send, zip, or encrypt

Avoid

- Exporting full datasets by default
- Assuming renamed or reformatted data isn’t sensitive
- Sharing a spreadsheet that includes hidden sheets

Quick Check

If you wouldn’t want it forwarded, share only what’s needed.

Steps If You’re Unsure or Something Went Wrong

If you are unsure:

Pause. Minimize. Verify. Ask.

- ▶ **Pause:** Stop before you send, paste, upload, or export
- ▶ **Minimize:** Limit to critical data only
- ▶ **Verify:** Confirm destination and who can access it
- ▶ **Ask:** Check with Security or IT if still unsure

If it already happened:

Stop. Contain. Report.

- ▶ **Stop:** Cancel the action or revoke access if possible
- ▶ **Contain:** Remove external access and limit viewers
- ▶ **Report:** Share what data, where it went, when it was shared, and who might have access

Want to reduce accidental data leaks? See how CrowdStrike Falcon® Data Protection can help.

[Learn more](#)