

FAMILIAR IS NOT PROOF

Before opening a shared file

Recognise the sender? Still check the request.

FICTIONAL SHARING NOTICE

Alex shared “Updated project documents” with you.

| Expected file?

| Confirm another way

| Unexpected sign-in? Stop

-  **Check the context**
Were you expecting this file, from this person, for this job?
-  **Confirm another way**
Verify unexpected shares through a separate trusted channel, not replies in the same thread.
-  **Open your usual app**
Where possible, open Microsoft 365 or your file-sharing app directly instead of an unexpected email sign-in shortcut.
-  **Stop at surprise requests**
Pause at unexpected login, MFA approval or install-software requests.
-  **Report safely**
Use your organisation’s reporting process. Do not circulate the suspicious link or attachment.

Real SharePoint, OneDrive and Dropbox links can be abused. A familiar sender may be compromised; recognising the person or service is not enough.

Already clicked, signed in or downloaded?

- Clicked: stop interacting and tell IT what happened.
- Entered a password or approved MFA: seek urgent IT account recovery, including reset and session revocation.
- Ran a download or suspect infection: disconnect from the network and contact IT.

osmicro.com.au/printable-guides/sharepoint-file-sharing-phishing-checklist/

Follow your organisation’s security and payment procedures. These checks reduce risk; they do not guarantee a message or transaction is safe.

Checked October 2026 • Sources: [Microsoft \[1\]](#) [Microsoft \[2\]](#) [ACSC \[3\]](#) • More detail and accessible text at the URL above.