CHECKLIST · SCAMS & SECURITY

1Password and Todoist hacked through their code systems: what to do

Published 26 November 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/1password-todoist-breaches-november-2026/

- [ ] **Don't act on unexpected 1Password emails.** Ignore invitations or account recovery requests you didn't start, and open the 1Password app or type its address yourself instead.
- [ ] **Keep your 1Password Secret Key and account password to yourself.** 1Password will never ask for them by email, text or phone.
- [ ] **Check for a Todoist incident email.** Look for a message from no-reply@notify.todoist.com and follow the steps it lists for your account.
- [ ] **Change reused Todoist passwords.** If Todoist emailed you about your password and you use that password anywhere else, change it on those services too.
- [ ] **Replace secrets stored in Todoist.** If Todoist's email says your content was searched, revoke any API keys, access tokens or recovery phrases kept in tasks or comments with the service that issued them; deleting the task isn't enough.
- [ ] **Update Todoist API tokens in your scripts.** If Todoist revoked your API token, get the new one in Todoist on the web under Settings, then Integrations, then Developer.
- [ ] **Reconnect Slack or Outlook if Todoist disconnected them.** On a work or school account, your organisation may block the Outlook add-in until Microsoft's verification is complete.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.