ACCOUNTS
DATA STORAGE

LOCKDOWN YOUR: DROPBOX

KEY:
BOLD = CRITICAL

Dropbox's "Security checkup" (click here) covers tasks marked with a: ■

Restrict Access

- ❑ **Turn on two-factor authentication (2FA)** How-To Link
- ■ ❑ **Use a strong, unique password - store securely** How-To Link
- ❑ **Change password if used on other accounts or if you think you've been hacked** How-To Link
- ❑ Restrict access to only those who need it
- ❑ Limit document + folder sharing to view-only; only allow further permission if necessary How-To Link

Reduce Vulnerabilities

- ❑ **Update Dropbox monthly (automate if possible)** How-To Link
- ❑ **Remove unnecessary connected services** How-To Link
- ■ ❑ **Remove unnecessary connected apps** How-To Link
- ❑ Remove unnecessary connected devices How-To Link
- ❑ Only use Dropbox on updated devices & web browsers free of malware

Detect Threats & Breaches

Turn on notifications for when:

- ❑ a large number of files are deleted How-To Link
- ❑ a new browser signs in to your account How-To Link
- ❑ a new device is linked to your account How-To Link
- ❑ a new app is connected to your account How-To Link
- ■ ❑ Review and remove suspicious devices or browsers logged into your account How-To Link

Recover Lost/Stolen Data

- ❑ **Ensure linked email for recovery is valid + protected with 2FA + strong, unique password in order to recover data if locked out of account** How-To Link

Backup Data

- ❑ Backup any data stored solely on Dropbox to a secure device or other cloud account protected with strong, unique password + 2FA if available How-To Link