KEEPYOUREAL

Deepfake protection checklist

Protect your face, voice, photos, videos, and social posts before AI misuse happens - and know what to save if a fake appears.

START WITH ONE ORIGINAL

Keep this sheet with your media records

01 Before you share

- Keep the original camera file, full recording, or finished export.
- Create a protected version and keep its dated ownership record.
- Choose the audience: public, followers, close friends, or private.
- Save the official post URL and publication date.

02 Protect the accounts

- Use a unique password for every email, social, and cloud account.
- Turn on multifactor authentication and store recovery codes safely.
- Review signed-in devices, recovery contacts, and connected apps.
- Keep your official profile links consistent and easy to verify.

03 Verify urgent requests

- Pause requests for money, passwords, codes, or secrecy.
- Call back through a number or account you already trust.
- Use a private family or team verification phrase.
- For payments, follow the usual approval process every time.

04 If a fake appears

- Save the exact URL, username, date, screenshots, and context.
- Find the closest original and its ownership record.
- Report the content and impersonating account through the right route.
- Keep report numbers and replies together; warn likely targets privately.

Free tools to help you act

Protect an original	keepyoureal.com/deepfake-protection/
Record evidence	keepyoureal.com/deepfake-evidence-log/
Read the full guide	keepyoureal.com/guides/how-to-protect-yourself-from-deepfakes/

Use the official reporting route for the platform or service involved. For immediate danger, threats, blackmail, fraud, or intimate-image abuse, contact the appropriate specialist service or authority in your location.

OFFICIAL SOURCES

FBI online safety | FTC voice-cloning guidance | C2PA Content Credentials

keepyoureal.com

Educational checklist - not legal, financial, medical, or emergency advice.

Published 1 November 2026