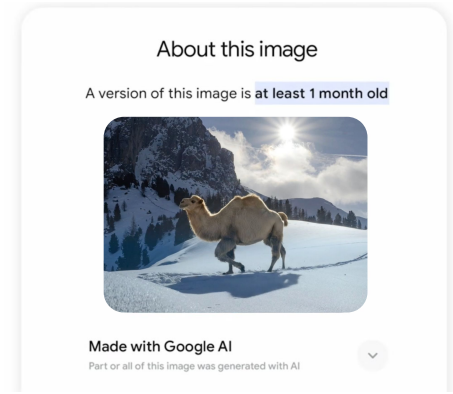


Protect yourself online with Google security tools

Every day, billions of people trust Google and YouTube to find information. We take that responsibility seriously. Throughout the 2026 election cycle, we recognize voters, journalists, and campaigns face new challenges, including sophisticated cybersecurity threats and deepfakes.

We are providing campaigns, officials, and the public with our strongest security tools and AI guardrails—all easily accessible and free. Here are the best resources you can use to protect yourself and your information online.



1. Spot AI-generated content

Verify with [SynthID](#): We add digital watermarks to text, audio, images, and video created with Google AI. You can [easily check](#) if media was made or edited by our tools by uploading it to the Gemini app or using Search or Gemini in Chrome and asking, "Is this AI generated?"

[Likeness Detection](#): On YouTube, government officials, journalists, and candidates can use our privacy tools to find AI-generated content that looks or sounds like them. If found, you can review the content and request its removal under our [privacy guidelines](#).

2. Defend against targeted attacks

[Advanced Protection Program \(APP\)](#): Our strongest level of account security, highly recommended for anyone working in elections. APP defends against phishing and harmful downloads, and it strictly controls which apps can access your data. Sign up for free at google.com/advancedprotection.

[Project Shield](#): Project Shield protects news and election websites from distributed denial of services (DDOS) attacks designed to take them offline or from massive traffic surges. Get protected projectshield.google.

3. Secure your Google account

[Security and Privacy Checkup](#): Get advice to protect your account and enhance your privacy, such as setting up two-step verification. Try it at myaccount.google.com/privacycheckup.

[Password Manager](#): Create and save strong, unique passwords for all your online accounts directly in your Google Account or on your device. Visit support.google.com/accounts.

[Passkeys](#): Sign in securely using your fingerprint, face scan, or screen lock—protecting you from phishing attacks. Learn more at safety.google/authentication/passkey.

4. Control your online presence & browse safely

[Remove personal info](#): Request that Google Search remove your sensitive personal information—like your home address, emails, etc.—from search results using our [removal tool](#).

[Avoid scams](#): Never click on questionable links. Double-check URLs to make sure the website is legitimate (look for "https"), and be cautious when using public Wi-Fi.