TimeBinder.io

timebinder.io
Free guide, 11 November 2026

A GUIDE FOR EVERYONE

How to protect yourself from AI forgeries, deepfakes and backdating

A plain-English 2026 guide for the US, UK, Europe, Australia and Canada

TimeBinder adds a layer of protection against AI and human fraud and disputes.

- Voice-clone scam calls
- Deepfakes and fake nudes
- Fake documents and screenshots
- Backdating in disputes
- Identity theft
- AI phishing
- Where to report

Read it online: https://timebinder.io/guides/protect-yourself-from-ai-forgeries/
General information, not legal advice. Every link was checked on 11 November 2026.

SHORT ANSWER

You protect yourself from AI forgeries by relying on **process, not your eyes and ears**. Agree a family safe word. Hang up and call back on a number you already have before you act on any urgent request. Never pay a blackmailer. Keep original files and date them when you create them. Lock down your accounts with a password manager, two-step login and, where you can, a credit freeze.

No tool can tell you for certain whether a photo, video, voice or document is fake. Detectors give a score, not proof. This guide shows what works, which free tools are real, and exactly where to report in the US, UK, Europe, Australia and Canada.

Contents

1. Voice-clone scam calls 5
How do AI voice-clone scam calls work, and how do I stop them?

2. Deepfake video and photos 7
How can I tell if a video, photo or voice note is a deepfake?

3. Sextortion and fake nudes 8
What do I do if someone threatens me with fake nude images (sextortion)?

4. Fake documents, screenshots and chats 9
How do I protect myself from fake documents, receipts, screenshots and chat logs?

5. Backdating in disputes 10
What is backdating, and how do I protect myself in a dispute?

6. Fake IDs and identity theft 12
How do I protect myself from fake IDs and identity theft?

7. AI phishing 13
How do I spot AI phishing emails, texts and fake websites?

8. Protect your own work and records 14
How do I protect my own work and records, and date my files when I create them?

9. What to do if it happens to you 15
What should I do if I am hit by an AI scam, deepfake or forgery?

10. Verified tools 17
Which tools can I trust, and which are free?

11. FAQ 19
Frequently asked questions

12. Quick link directory 21
Every link in this guide, in one place

The 60-minute protection checklist

Do these eight things first. They stop most AI-assisted scams.

- [ ] Agree a **family safe word** this week, in person. Do not text it or post it.
- [ ] Make a rule: for any urgent request for money, codes or secrets, **hang up and call back on a saved number**.
- [ ] Turn on **two-step login** for email, banking and your phone account, and use a **password manager**.
- [ ] Check your email addresses at **Have I Been Pwned** and change any reused passwords.
- [ ] **Freeze your credit** where that is available to you (free in the US). See the country table in section 6.
- [ ] Keep **original** photos, files and receipts. Work on copies. Date the original when you create it (section 8).
- [ ] Limit how much of your **voice and video** is public. Make social accounts private where you can.
- [ ] Save the **reporting links** for your country (section 9) in your phone's notes now, not mid-crisis.

Your family safe-word plan

Fill this in together, in person. **Do not write the safe word itself on this page.**

Who is included (children, grandparents, partner, close friends)

Our backup question (something only the real person would know)

What we do if the caller cannot say the word: hang up and call back on a saved number. Date we agreed this:

1. How do AI voice-clone scam calls work, and how do I stop them?

SHORT ANSWER

Scammers copy a voice from short audio clips, then phone you as a relative in trouble or as your boss asking for an urgent payment. The fix is the same every time: **hang up, then call the person back on a number you already have**, and use a family safe word. Never send money, gift cards, crypto or codes on the strength of a call, voice note or video alone.

The FBI warns that criminals generate short audio clips of a loved one's voice to pose as a relative in a crisis and ask for immediate money, and use AI video in real-time calls to pose as executives or officials (FBI IC3 alert, 3 Dec 2024). The US Federal Trade Commission has warned about the same family-emergency pattern. The Canadian Anti-Fraud Centre describes emergency and grandparent frauds, and Australia's Scamwatch explains how scammers use technology and AI.

What do these scams usually sound like?

Two common voice-clone scripts

Script	What you hear	What the scammer wants
Family emergency	A panicked voice that sounds like your child, grandchild or partner. An accident, an arrest, a hospital bill, "I lost my phone", sometimes a "lawyer" or "police officer" who takes over the call.	Money now, often by bank transfer, crypto, gift cards or a courier collecting cash. You are told not to tell anyone (a "gag order").
Boss or supplier payment	A voice or video call, or voice note, from your manager, director or a supplier. "I am in a meeting. Pay this invoice today. Keep it between us."	A payment to a new bank account, a change of bank details, gift cards or access codes.

Red flags that should stop you

- **Urgency and secrecy.** "Do it now, don't tell anyone." Real emergencies survive a two-minute call-back.
- **An unusual way to pay.** Gift cards, crypto, wire transfers, cash pick-up or a courier. The Canadian Anti-Fraud Centre notes that Canadian courts do not let anyone be bailed out with cash or cryptocurrency.
- **A new number or a "broken phone" story** from someone claiming to be family.
- **A call that moves you somewhere else.** A "lawyer", "officer" or "bank" takes over and tells you not to call anyone.
- **Caller ID that looks right.** Numbers can be spoofed, so a familiar name or number proves nothing.
- **The voice is good but the questions are not.** The caller cannot answer something only that person would know.

How do I set up a family safe word?

The FBI's advice is to create a secret word or phrase with your family to verify identity. Make it work in real life:

1. **Choose it together, in person.** Pick two or three unrelated words. Avoid pet names, birthdays, street names or anything on social media.
2. **Never put it in writing online.** Do not text it, email it or save it in a shared note that others could read.
3. **Include everyone who might be called**, especially older relatives and teenagers. Practise it once so it feels normal.
4. **Agree what happens if the caller cannot say it:** you hang up and call back on a saved number. No exceptions, even if the voice is crying.
5. **Change it after it has been used or if you think it leaked**, and keep a backup question that only the real person could answer.

What should I do during a suspicious call?

1. **Stay calm and slow it down.** Say you will call back. Scammers need you to stay on the line.
2. **Hang up.** Do not press buttons or call the number they give you.
3. **Call the real person** on a number you already have, or ask another family member to reach them.
4. **Ask for the safe word.** If the caller cannot give it, treat the call as a scam.
5. **If they say they are police, a lawyer or your bank**, hang up and call that organisation using a number from its official website or the back of your card.
6. **Tell someone.** Scams rely on you acting alone.

How do I protect my workplace from boss and supplier payment fraud?

- **Two-person rule.** No new payee, changed bank detail or urgent payment without a second person approving.
- **Call back on a known number**, never one from the email, voice note or video request.
- **Treat video as unproven.** A face on a video call is no longer proof of identity. Ask a question only the real person would know, or move the request to a second channel.
- **Tell finance staff the script.** Scamwatch covers business email compromise, a close cousin of the fake-boss payment request.

> **If you already sent money**
>
> Call your bank or card issuer **straight away** and ask them to recall or block the payment. For gift cards, contact the card company. Then report it using the table in section 9. Keep the phone number, any messages and payment receipts. Banks act fastest in the first hours, so do not wait until you feel sure.

2. How can I tell if a video, photo or voice note is a deepfake?

SHORT ANSWER

You often cannot tell by looking or listening, and detection tools can be wrong in both directions. Check the **source**, the **context** and any **provenance data**, run a reverse image search, and confirm with the person through a **second channel**. Treat a detector result as one clue, never as proof.

Older advice said to look for odd hands, teeth or shadows. The FBI still lists signs like distorted hands or feet, irregular faces, inaccurate shadows and lag in video calls, but good fakes have none of them. Use these checks in order.

1. **Ask where it came from.** Who first posted it, and is there an original source you can reach? A shocking clip with no source is a warning sign.
2. **Check the context.** Does it match what the person would really say or do? Does a trusted news source report the same thing?
3. **Run a reverse image search.** Google Lens and TinEye can show where an image appeared before, or whether it is a recycled photo.
4. **Look for Content Credentials.** Upload the file to the free Content Credentials verify tool. If the file carries signed provenance data, it can show who made it and how it was edited. Most files carry none, and a missing credential does not mean a file is fake.
5. **Check metadata** with ExifTool or an online viewer such as exif.tools. Metadata can be edited or stripped, so it is a clue only.
6. **Try a detector, if you must.** See the tools table in section 10. Remember that each gives a probability, and each can miss a fake or flag a real file.
7. **Verify with a human.** Call the person on a saved number. For something that matters, ask for a fresh photo or video that includes a detail only they could supply right now.

Do not upload private or intimate images to a detector

Most online checkers send the file to a company's servers. Never put intimate images, children's images, ID documents or confidential papers into a detector. If an intimate image of you is being shared or threatened, use the services in the next section instead.

Can a detector prove something is AI-made?

No. Detectors estimate a likelihood. Google's Gemini app can check for **SynthID** watermarks, but it can only recognise content made by Google's own AI tools, and a "not detected" answer does not mean a file is real (Google's help page). The same limit applies to every detector: a miss does not make a file genuine, and a hit does not make it fake.

3. What do I do if someone threatens me with fake nude images (sextortion)?

SHORT ANSWER

Do not pay, and stop contact. Block the person, keep the evidence, and report it. Ask each platform to take the images down, use **StopNCII.org** (adults) or **Take It Down** (images of anyone under 18 at the time), and report to the police and your national centre. It is not your fault, and a fake image of you is still abuse.

Sextortion is when someone threatens to share an intimate image, real, edited or AI-made, unless you pay or send more. The US Federal Trade Commission notes that these images may be real, digitally altered, or deepfakes created with artificial intelligence, and that the victims can be adults or minors.

What should I do first?

1. **Do not pay and do not send anything more.** Paying rarely ends the threats. The FTC and Australia's eSafety Commissioner both advise against it.
2. **Cut off contact.** Block the person and stop replying. Do not give access to your accounts or devices.
3. **Keep evidence.** Screenshot threats, usernames, profile links, payment demands and dates. Do not delete the conversation. **If the image shows someone under 18, do not copy or forward it**; report it instead.
4. **Ask the platform to remove it.** In the US, the Take It Down Act requires covered platforms to remove reported intimate images, including AI-made ones, within 48 hours of a request. If a platform does not, report it at TakeItDown.ftc.gov.
5. **Use the hash tools to stop it spreading.** Adults: StopNCII.org makes a digital fingerprint of the image on your own device and shares that with participating companies, so they can detect copies. Images of someone under 18 at the time: NCMEC's Take It Down.
6. **Report to the police and your national centre.** Use the table below.
7. **Talk to someone you trust.** Many people feel shame. You are the victim of a crime.

Where to get help with sextortion and fake nudes, by country

Country	Report and get help
United States	TakeItDown.ftc.gov (platform failed to remove), FBI tips.fbi.gov or 1-800-CALL-FBI, NCMEC CyberTipline for anyone under 18, CCRI Safety Center, your local police.
United Kingdom	Revenge Porn Helpline (adults), Report Harmful Content, Report Fraud if money was demanded, your local police (999 if you are in danger).
Europe	Your national police, and Europol's report-a-crime page for where to report in your country. StopNCII.org and Take It Down can be used from anywhere, though participating platforms vary.
Australia	eSafety: report image-based abuse and dealing with sexual extortion, ReportCyber, your local police.

Country	Report and get help
Canada	Cybertip.ca (reports about children and teens), NeedHelpNow.ca (under 18), report cybercrime and fraud to the Canadian Anti-Fraud Centre, your local police.

> **Beware of paid "removal" and "blackmail help" services**
>
> The FTC has sued one company that allegedly charged thousands of dollars to stop sextortion and remove images but did not deliver (FTC consumer alert). The real routes above are free. Search any paid service's name with "scam" or "complaint" first.

What if it is a child or teenager?

- **Stay calm and do not blame them.** Fear of getting in trouble is what keeps children silent.
- **Use NCMEC's Take It Down** or Cybertip.ca in Canada, and report to the police.
- **Do not copy, forward or screenshot the image itself.** Keep threats and account details instead.

4. How do I protect myself from fake documents, receipts, screenshots and chat logs?

> **SHORT ANSWER**
>
> Assume any screenshot, PDF, receipt or chat export **can be made or edited in minutes**. If one is used against you, ask for the original from the source system, do not argue from memory, and keep your own originals safe. If you may need to rely on your own records, keep the originals and make a dated, checkable record of them early.

AI tools can now draw a convincing invoice, fabricate a conversation in the style of a real chat app, or edit a photo of a receipt. A screenshot only shows pixels. It does not show that the conversation ever happened. See also: can screenshots be used as evidence?

What if someone shows me a document or screenshot that looks fake?

1. **Do not rely on memory or argue about it.** Ask for the original file, not a photo or screenshot of it.
2. **Ask for the source.** For a chat, the message in the app itself or the app's own export. For an invoice, the PDF as sent. For a receipt, the shop's own record.
3. **Check it with the sender through a known channel.** Call the company on its official number and ask them to confirm.
4. **Look for inconsistencies:** fonts that change, rounding errors, wrong tax or business numbers, impossible dates, addresses that do not match, a profile picture or name format that does not match the real app.
5. **Check metadata**, but only as a clue. Details such as the app that created the file, or software that did not exist on the claimed date, can reveal a problem. Clean metadata proves nothing, because it can be stripped.

6. **Do not delete anything.** Preserve your own messages, emails and files from that time.
7. **For anything serious** (court, a regulator, a large sum), speak to a lawyer. Courts and experts decide what is authentic, not a website.

Red flags in a document or screenshot

- It arrives only as an image or screenshot, and the sender will not give the original.
- The sender pushes you to pay or agree immediately.
- Bank details changed from previous invoices.
- The date, time zone, phone number format or app layout looks slightly wrong.
- Parts of the text are sharper or blurrier than the rest.
- The file's metadata date does not fit the story, for example created after the date it claims.

How do I make my own screenshots and exports more reliable?

- **Capture the whole screen** including the date, time, contact name and web address, not a tight crop.
- **Keep the original export** from the app (chat export, email as .eml or .pdf), not only a screenshot.
- **Save it the same day** and do not edit, crop or re-save the original.
- **Make a dated, checkable record straight away.** A TimeBind can show that this exact file existed no later than a recorded time, and the free file comparison checker shows whether two files are identical.

5. What is backdating, and how do I protect myself in a dispute?

SHORT ANSWER

Backdating is making a document, message, photo or file look as if it was created earlier than it really was. File dates and metadata are easy to change, and AI makes convincing old-looking papers easier to produce. Protect yourself by **keeping original records made at the time**, putting agreements in writing the same day, and **dating your files when you create them**.

Most disputes come down to "what was agreed, and when?". The strongest position is simple: you have records made **at the time**, kept in their original form, with a date that does not rely only on you or on a setting someone can change. The table shows what to keep in common situations. It is general information, not legal advice.

What to keep, by situation

Situation	What to keep and date at the time	Backdating red flags
Landlord and tenant	Signed lease and every amendment. Move-in condition report and photos (with timestamps) on day one. Rent receipts. Repair requests sent by email or the portal.	A "condition report" or lease addendum nobody saw before. A repair notice that appears only after a dispute starts.

Situation	What to keep and date at the time	Backdating red flags
Contractors and builders	Written quote, signed scope and every variation, confirmed in writing the same day. Dated progress photos. Invoices as originally sent.	A "signed" variation that you never saw. An invoice whose metadata date is earlier than the job.
Workplace	Your contract and every version you were given. Dated notes of meetings (who, what, when). Performance reviews and warnings you received, as originals.	A warning or policy that is "dated" before the event but first appeared later. Documents that exist only as screenshots.
Insurance	Photos or video of valuables, serial numbers, receipts and valuations before any loss. Policy documents. All claim correspondence.	Receipts or photos created after the loss but dated before it. Edited images of damage.
Custody and family disputes	Message exports, handover and schedule logs, and records of agreed changes. Use any communication tool a court or agreement requires. Take legal advice early.	Edited chat screenshots. Recordings or messages that do not match the originals.
Creative work	Draft and project files, raw photos, stems, sketches. A dated record of the finished work before you share or send it.	A "first version" with a file date that cannot be matched to any earlier draft or backup.

How can I date a file so it cannot be quietly backdated?

Ways to date a file, and what each really shows

Method	What it shows	Where it falls short
File date and metadata	A date your device or app recorded.	Can be changed in seconds, and copying or syncing can alter it.
Email to yourself or a cloud upload date	A message or file existed in an account at some time.	Depends on one company's records. You may not be able to prove it later.
Notary or witness	A person saw or certified something on a day.	Valuable for signing, but it does not fingerprint a digital file you can compare later.
Wayback Machine (web pages)	An archived copy of a public web page.	Only for public pages. Not for private files.
OpenTimestamps	A free, open standard that anchors a file's fingerprint to the Bitcoin blockchain.	Technical to use and to verify. You must keep the .ots proof file safe.
TimeBinder	A dated, checkable record that an exact file existed no later than a recorded time and still matches.	Does not show who made the file, who owns it, or that its contents are true.

If you need the full background, see how to prove a file existed before a date, hash timestamp vs notarisation and Wayback Machine as proof.

> **If the other side says your evidence is a deepfake**
>
> This is now a common tactic. Keep your originals, your backups and any dated record you made, and read what to do if the other side says your evidence is a deepfake. Get legal advice in any formal dispute.

6. How do I protect myself from fake IDs and identity theft?

SHORT ANSWER

Make it hard for criminals to use your identity: **freeze your credit where possible, use a password manager and two-step login, check whether your email appears in breaches, and stop sending unmarked ID photos**. If your identity is misused, report it quickly using the country table below.

AI can produce realistic fake IDs and doctored photos of real ones. The FBI lists fake driver's licences and credentials among the uses of AI-generated images in fraud (IC3 alert). The best protection is to make your real details useless to someone else.

What are the essential steps?

1. **Use a password manager** so every account has a unique password: Bitwarden, 1Password, Proton Pass or KeePassXC. The UK's NCSC explains password managers.
2. **Turn on two-step verification** on email, banking, phone account and social media. Prefer an authenticator app, a passkey (FIDO Alliance) or a security key over text-message codes. See CISA's More than a Password and the NCSC's 2-step verification guide.
3. **Check for breaches** at Have I Been Pwned. If your email appears, change that password everywhere you used it.
4. **Freeze your credit** where you can (see the table).
5. **Be careful sending ID.** Send an ID copy only when you must. Write "For [name], [purpose], [date] only" across the copy. Never send ID by an unverified link.
6. **Check credit reports** regularly, and set up alerts from your bank.

Credit freezes, ID help and where to report identity theft

Country	Protect and report
United States	Freeze your credit for free with Equifax, Experian and TransUnion; the FTC explains credit freezes and fraud alerts. Free reports at AnnualCreditReport.com. Report identity theft at IdentityTheft.gov.
United Kingdom	Report to Report Fraud (formerly Action Fraud). Cifas Protective Registration is a paid service that asks organisations to take extra checks; read its page for the current terms. See also Take Five to Stop Fraud.
Europe	Report to your national police. Ask your bank and national credit-reference agency about fraud alerts. Rules differ by country, so check your national consumer or data-protection authority.
Australia	Get free support from IDCARE (1800 595 160). Ask the credit reporting bodies, such as Equifax Australia and Experian Australia, about a credit ban. Report to ReportCyber.
Canada	Report to the Canadian Anti-Fraud Centre at reportcyberandfraud.canada.ca (1-888-495-8501). Ask Equifax Canada and TransUnion Canada about fraud alerts and security freezes.

What if my identity has already been misused?

1. Contact your bank and any affected company and ask them to close or freeze the accounts.
2. Place a freeze or fraud alert, then report it using the table.
3. Change passwords on email first, then banking and everything else, and turn on two-step login.
4. Keep a log: dates, names, reference numbers and copies of what you sent.
5. Replace stolen or copied ID documents as advised by the issuing agency.

7. How do I spot AI phishing emails, texts and fake websites?

> **SHORT ANSWER**
>
> Do not rely on spotting bad spelling, because AI writes flawless messages. Instead, **never use the link or number in the message**. Go to the website or app yourself, or call the organisation on a number you already trust. Then report the message.

AI lets scammers write fluent, personal messages in any language. The FBI notes criminals use AI text to reduce the spelling and grammar errors that once gave scams away (IC3 alert). So change the habit: judge by what the message asks you to do.

Red flags that matter more than spelling

- **Urgency or fear:** your account will be closed, a parcel is held, you owe tax or a fine.
- **A request to log in, pay, verify or download** from a link, attachment or QR code you did not ask for. The FTC has warned about QR codes placed in public places.
- **A sender address or web address that is almost right**, such as an extra letter or a different ending.
- **A message that asks for a code** (a one-time code is a key to your account, and no genuine company asks for it).
- **An unexpected voice, text or video follow-up** that pushes you to act on the email.

1. **Stop and do not click.** Hover to check the web address, or better, do not use the link at all.
2. **Go to the real site or app** by typing the address or using a bookmark.
3. **Check using another channel.** Ring the company on the number on your card or official website.
4. **Use a password manager.** It will not offer to fill your login on a look-alike site, which is a useful warning.
5. **Report and delete.** See the table below.

Where to forward phishing emails and texts

Country	Report phishing here
United States	ReportFraud.ftc.gov, and forward phishing emails to APWG at reportphishing@apwg.org. CISA explains how to recognise and report phishing.
United Kingdom	Forward emails to report@phishing.gov.uk and texts to 7726 (free), as explained on GOV.UK. See the NCSC's phishing guide.
Europe	Report to your bank, your national police or cybercrime unit and the impersonated organisation. Europol's report-a-crime page points to national reporting.
Australia	Scamwatch: report a scam and ReportCyber. Read Scamwatch's phishing scams page.
Canada	Report cybercrime and fraud or call the Canadian Anti-Fraud Centre on 1-888-495-8501. See Get Cyber Safe.

8. How do I protect my own work and records, and date my files when I create them?

SHORT ANSWER

Keep **originals untouched**, work on copies, keep **backups** in more than one place, and **date the original when you create it**. A dated, checkable record made at the time is far harder to dispute than a file date or a screenshot made later.

The aim is to be able to say, later: "This is the exact file I had, and here is a record made at the time that it existed." That helps in a dispute about photos, documents, designs, music, writing, receipts and agreements.

1. **Keep the original, and never edit it.** Copy the file and work on the copy. Set the original to read-only.
2. **Keep the metadata.** Camera photos hold the date, device and often location. Share a cleaned copy, but keep the original with its metadata. (Strip location before posting publicly.)
3. **Back up using the 3-2-1 idea:** three copies, on two kinds of storage, with one off-site. The NCSC explains backing up your data.
4. **Name and organise files clearly.** A dated folder for each matter, trip, job or project makes it easier to show a sequence of events.
5. **Make a dated, checkable record when you create or receive something important.** Options include OpenTimestamps (free, technical) and TimeBinder (below).
6. **Keep the proof with the file.** Store the certificate or proof file next to the original, and back both up.
7. **Check later.** If two copies are in dispute, compare them. Our free file comparison checker shows whether two files are exactly the same, using fingerprints made in your browser.

How does TimeBinder fit in?

TimeBinder is one tool for step 5. A **TimeBind** is a dated, checkable record that an exact file existed no later than a recorded time and still matches. Your browser makes a digital fingerprint (a SHA-256 hash) of the file, and the file stays on your device. TimeBinder records the fingerprint with the time and gives you a Proof of Time Certificate. Your **first Pooled TimeBind is free with no card**, then from US$5, and an ASAP TimeBind is US$15.

> **What a TimeBind shows, and what it does not**
>
> It shows that this exact file existed no later than the recorded time, and that a copy shown later still matches. It does **not** detect AI, show who made the file, who owns it, or that its contents are true. It does not replace legal advice. It is one useful record among others.

Start with the five short answers, for example how to timestamp a document for free and how to tell if a file has been changed, or read how to prove a photo is not AI for the honest limits of photos and video.

9. What should I do if I am hit by an AI scam, deepfake or forgery?

> **SHORT ANSWER**
>
> Stop, protect your money and accounts, keep evidence, then report it. The **first hour matters most** for money: call your bank. Then report to the police and your national fraud centre using the table below.

1. **Stop contact and do not pay more.** Do not argue with the scammer.
2. **Call your bank or card provider immediately** if money moved, and ask to stop or recall the payment.
3. **Secure your accounts.** Change passwords starting with email, turn on two-step login, and log out other devices.
4. **Keep evidence.** Save messages, numbers, usernames, links, receipts, emails (with headers if you can) and screenshots, and write a short dated timeline. Do not delete the conversation.
5. **Report it** using the table below. Reports help others and can help recover money.
6. **Freeze credit and report identity theft** if personal details were used.
7. **Tell the people affected** (family, your employer, your contacts) so they do not fall for the next step.
8. **Get support.** Scams are upsetting. Free victim support exists in most countries.

Where to report, by country

Country	Fraud and scams	Online abuse, deepfakes and images	Identity theft and support
United States	ReportFraud.ftc.gov (FTC), IC3.gov (FBI Internet Crime Complaint Center), your local police. FTC: what to do if you were scammed.	TakeItDown.ftc.gov, StopNCII.org, NCMEC Take It Down, CyberTipline, tips.fbi.gov.	IdentityTheft.gov; VictimConnect.
United Kingdom	Report Fraud (formerly Action Fraud), 0300 123 2040; Scotland: Police Scotland. Phishing: report@phishing.gov.uk and 7726.	Revenge Porn Helpline, StopNCII.org, Report Harmful Content.	Victim Support; Cifas identity advice.
Europe	Your national police and bank. Start at Europol's report-a-crime page to find where to report in your country.	StopNCII.org, Take It Down and your national police and online-safety helpline.	Your national data-protection or consumer authority and national victim support.
Australia	Scamwatch: report a scam, ReportCyber, your bank, your local police.	eSafety: report image-based abuse.	IDCARE, 1800 595 160.
Canada	Report cybercrime and fraud / Canadian Anti-Fraud Centre, 1-888-495-8501; your local police.	Cybertip.ca, NeedHelpNow.ca, StopNCII.org.	Equifax Canada and TransUnion Canada for fraud alerts; local victim services.

Numbers and rules change. In an emergency, call your local emergency number first (911 in the US and Canada, 999 in the UK, 112 in the EU, 000 in Australia).

10. Which tools can I trust, and which are free?

SHORT ANSWER

The tools below are real, working services checked on 11 November 2026. Use **reporting services and provenance data first**, then metadata and reverse image search, and treat AI detectors as a weak clue. Most online checkers **upload your file** to a company, so never use them for intimate, children's or confidential files.

Verified tools, what they do, and what to watch for

Tool	Use it for	Cost	Heads-up
REPORTING AND HELP			
ReportFraud.ftc.gov reportfraud.ftc.gov	Report scams and fraud to the US FTC	Free	US only.
StopNCII.org stopncii.org	Stop intimate images spreading (adults)	Free	Makes the fingerprint on your device. Adults only.
Take It Down (NCMEC) takeitdown.ncmec.org	Images taken when you were under 18	Free	Run by the US child-protection charity NCMEC.
CHECK WHERE MEDIA CAME FROM			
Content Credentials verify verify.contentauthenticity.org	Read signed origin and edit history in a file	Free	Most files have no credentials. Missing does not mean fake.
Google Lens lens.google.com	Reverse image search	Free	Uploads the image to Google.
TinEye tineye.com	Reverse image search for earlier copies	Free (limits)	Uploads the image. Sometimes shows a browser check first.
METADATA AND IMAGE FORENSICS			
ExifTool exiftool.org	Read all metadata in photos, PDFs and more	Free	Runs on your computer. Technical.
exif.tools exif.tools	View metadata in your browser	Free	Says it runs in your browser. Check its privacy notes.
Forensically 29a.ch/photo-forensics	Magnifier, error-level and clone detection	Free	Says images stay on your computer. Results need expertise.
FotoForensics fotoforensics.com	Error-level analysis for photos	Free	**Public site. Uploads are not private.** Do not use for sensitive images.
AI AND DEEPFAKE CHECKERS (A SCORE, NOT PROOF)			
Hive Detect (now Deploy) deploy.com/detect	Estimate if an image, video or audio is AI-made	Free tier	Uploads the file. Can miss fakes or flag real files.

Tool	Use it for	Cost	Heads-up
AI or Not aiornot.com/ai-image-detector	Estimate if an image is AI-made	Free and paid	Uploads the file. Can be wrong.
Deepfake-o-meter zinc.cse.buffalo.edu/ubmdfl/deep-o-meter	Run several research detectors on media	Free account	University research tool. Uploads the file.
Deepfake Total (Fraunhofer AISEC) deepfake-total.com	Analyse suspicious audio	Free	Uploads the audio. Research tool.
Gemini SynthID check support.google.com/gemini/answer/16722517	Check for Google AI watermarks	Free (Google account)	Only finds Google AI content. Uploads the file to Google.
ACCOUNT AND IDENTITY SAFETY			
Have I Been Pwned haveibeenpwned.com	See if your email appears in data breaches	Free	Never enter your password on the email search.
Bitwarden bitwarden.com	Password manager (open source)	Free and paid	Also stores two-step codes on paid plans.
1Password 1password.com	Password manager and passkeys	Paid	Free trial may be offered. Check current terms.
Proton Pass proton.me/pass	Password manager with email aliases	Free and paid	
KeePassXC keepassxc.org	Offline password manager	Free	Stores passwords in a file on your device.
Credit freezes consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts	Block new credit in your name (US)	Free	See the country table in section 6 for other countries.
DATING YOUR FILES			
OpenTimestamps opentimestamps.org	Free open standard for Bitcoin timestamps	Free	Technical. Keep the .ots proof file.
TimeBinder timebinder.io	A dated, checkable record that an exact file existed no later than a recorded time	First Pooled TimeBind free, no card; then from US$5	Fingerprint made in your browser; file stays on your device. Does not detect AI or show who made a file.
Free file comparison checker timebinder.io/free-tools/file-comparison-checker	See if two files are exactly the same	Free	Fingerprints made in your browser. Shows same or different, not which is older.

11. Frequently asked questions

Can I tell if a voice on the phone is an AI clone?

Not reliably. A cloned voice can sound exactly right, so do not trust the sound alone. Hang up and call the person back on a number you already have, and use a family safe word. No consumer tool can promise to catch a cloned voice on a live call.

What is a family safe word and how do I choose one?

It is a secret word or phrase that only your family knows, used to check that a caller is who they claim to be. Choose two or three unrelated words together in person. Avoid names, dates or anything on social media, and never text or post it. If the caller cannot say it, hang up and call back.

Should I pay if someone threatens to share fake nude images of me?

No. Stop contact, block the person, keep evidence and report it. Paying rarely ends the threats. Ask the platform to remove the image, use StopNCII.org (adults) or Take It Down (images of anyone under 18), and report to the police and your national fraud centre.

Can I get a fake nude of me removed from the internet?

Often, yes. Report it to each platform. In the US, covered platforms must remove reported intimate images, including AI-made ones, within 48 hours of a request, and you can report a platform that does not at TakeItDown.ftc.gov. StopNCII.org and Take It Down help stop copies spreading on participating platforms. No service can promise to remove every copy.

How can I check if a photo or video is real?

Check where it came from, run a reverse image search with Google Lens or TinEye, look for Content Credentials, and check the metadata. A detector can add a clue, but none gives proof. Confirm anything important with the person or source through a second channel.

Do AI deepfake detectors work?

Sometimes. They give a probability, and they can miss a fake or flag a real file, especially after a file has been compressed or re-saved. Treat them as one clue. Do not upload private or intimate images to them.

What is backdating, and why is AI making it worse?

Backdating is making something look older than it is. File dates and metadata are easy to change, and AI can produce convincing documents, receipts and chat screenshots. Records made at the time, kept in original form and dated by a method that does not rely on you, are harder to dispute.

How can I prove a file existed on a certain date?

Keep the original, and make a dated, checkable record when you create it. A TimeBind, or a free OpenTimestamps proof, can show that an exact file existed no later than a recorded time and still matches. Neither shows who made the file or that its contents are true.

What does a TimeBind prove?

It shows that an exact file existed no later than a recorded time and that a copy shown later still matches its fingerprint. The fingerprint is made in your browser and the file stays on your device. It does not show who made the file, who owns it, or whether AI was used, and it is not legal advice.

Is there a free way to date my files?

Yes. Your first Pooled TimeBind on TimeBinder is free with no card, then it is from US$5. OpenTimestamps is also free, but more technical. Cloud history, email to yourself and file metadata are free too, but they depend on records that can be changed or lost.

Where do I report an AI scam in my country?

US: ReportFraud.ftc.gov and IC3.gov. UK: Report Fraud (formerly Action Fraud). Australia: Scamwatch and ReportCyber. Canada: the Canadian Anti-Fraud Centre. Europe: your national police, starting at Europol's report-a-crime page. The table in section 9 has every link.

Should I freeze my credit to prevent identity theft?

In the US, a credit freeze is free and stops new credit being opened in your name, according to the FTC. Other countries have different tools such as fraud alerts, credit bans or protective registration. See the table in section 6.

Does this guide replace legal advice?

No. It is general information. If you face a formal dispute, a court case or a regulator, speak to a qualified lawyer where you live.

12. Quick link directory

Every external link in this guide. Keep this page for a printed copy.

United States

FBI IC3 alert, 3 Dec 2024	ic3.gov/PSA/2024/PSA241203
consumer.ftc.gov: scammers use ai enhance their family emergency schemes	consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
consumer.ftc.gov: image based abuse what know and do	consumer.ftc.gov/articles/image-based-abuse-what-know-and-do
TakeItDown.ftc.gov	takeitdown.ftc.gov/
NCMEC's Take It Down	takeitdown.ncmec.org/
FBI tips.fbi.gov	tips.fbi.gov/
NCMEC CyberTipline	report.cybertip.org/
FTC consumer alert	consumer.ftc.gov/consumer-alerts/2026/10/how-avoid-deceptive-sextortion-assistance-services-and-find-real-help
More than a Password	cisa.gov/MFA
Equifax	equifax.com/personal/credit-report-services/credit-freeze/
Experian	experian.com/help/credit-freeze/
TransUnion	transunion.com/credit-freeze
consumer.ftc.gov: credit freezes and fraud alerts	consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts
AnnualCreditReport.com	annualcreditreport.com/
IdentityTheft.gov	identitytheft.gov/
QR codes placed in public places	consumer.ftc.gov/consumer-alerts/2026/09/see-qr-code-parked-somewhere-dont-scan-ityet
ReportFraud.ftc.gov	reportfraud.ftc.gov/
cisa.gov: recognize and report phishing	cisa.gov/secure-our-world/recognize-and-report-phishing
IC3.gov	ic3.gov/
consumer.ftc.gov: what do if you were scammed	consumer.ftc.gov/articles/what-do-if-you-were-scammed
VictimConnect	victimconnect.org/

United Kingdom

Revenge Porn Helpline	revengepornhelpline.org.uk/
Report Harmful Content	reportharmfulcontent.com/
Report Fraud	reportfraud.police.uk/
ncsc.gov.uk: password managers	ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
ncsc.gov.uk: activate 2 step verification on your email	ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email
Cifas Protective Registration	cifas.org.uk/pr
Take Five to Stop Fraud	takefive-stopfraud.org.uk/
GOV.UK	gov.uk/report-suspicious-emails-websites-phishing
ncsc.gov.uk: phishing scams	ncsc.gov.uk/collection/phishing-scams

ncsc.gov.uk: always back up your most important data	ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data
Victim Support	victimsupport.org.uk/
Cifas	cifas.org.uk/individuals

Europe

Europol's report-a-crime page	europol.europa.eu/report-a-crime

Australia

scamwatch.gov.au: how scammers use technology and ai	scamwatch.gov.au/stop-check-protect/help-to-spot-and-avoid-scams/how-scammers-use-technology-and-ai
scamwatch.gov.au: business email compromise scams	scamwatch.gov.au/types-of-scams/business-email-compromise-scams
esafety.gov.au: report image based abuse	esafety.gov.au/key-topics/image-based-abuse/report-image-based-abuse
esafety.gov.au: deal with sextortion	esafety.gov.au/key-topics/image-based-abuse/deal-with-sextortion
ReportCyber	cyber.gov.au/submit-a-report
IDCARE	idcare.org/get_help/help_main
Equifax Australia	equifax.com.au/personal/
Experian Australia	experian.com.au/
Scamwatch: report a scam	scamwatch.gov.au/report-a-scam
scamwatch.gov.au: phishing scams	scamwatch.gov.au/types-of-scams/phishing-scams

Canada

antifraudcentre-centreantifraude.ca: emergency urgence eng	antifraudcentre-centreantifraude.ca/scams-fraudes/emergency-urgence-eng.htm
Cybertip.ca	cybertip.ca/en/
NeedHelpNow.ca	needhelpnow.ca/en/
reportcyberandfraud.canada.ca	reportcyberandfraud.canada.ca/
Equifax Canada	equifax.ca/personal/
TransUnion Canada	transunion.ca/
Get Cyber Safe	getcybersafe.gc.ca/
Canadian Anti-Fraud Centre	antifraudcentre-centreantifraude.ca/report-signalez-eng.htm

International

StopNCII.org	stopncii.org/
APWG	apwg.org/reportphishing/

Tools and standards

Google Lens	lens.google.com/
TinEye	tineye.com/
Content Credentials verify tool	verify.contentauthenticity.org/
ExifTool	exiftool.org/
exif.tools	exif.tools/
Google's help page	support.google.com/gemini/answer/16722517
CCRI Safety Center	cybercivilrights.org/ccri-safety-center/

Bitwarden	bitwarden.com/
1password.com	1password.com/
Proton Pass	proton.me/pass
KeePassXC	keepassxc.org/
FIDO Alliance	fidoalliance.org/passkeys/
Have I Been Pwned	haveibeenpwned.com/
Forensically	29a.ch/photo-forensics/
FotoForensics	fotoforensics.com/
Hive Detect (now Deploy)	deploy.com/detect/
AI or Not	aiornot.com/ai-image-detector
Deepfake-o-meter	zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/
Deepfake Total (Fraunhofer AISEC)	deepfake-total.com/

Dating your files

timebinder.io: can screenshots be used as evidence	timebinder.io/blog/can-screenshots-be-used-as-evidence/
TimeBind	timebinder.io/screenshot-timestamping/
timebinder.io: file comparison checker	timebinder.io/free-tools/file-comparison-checker/
OpenTimestamps	opentimestamps.org/
TimeBinder	timebinder.io/
timebinder.io: how to prove a file existed before a date	timebinder.io/blog/how-to-prove-a-file-existed-before-a-date/
timebinder.io: hash timestamp vs notarisation	timebinder.io/answers/hash-timestamp-vs-notarisation/
Wayback Machine as proof	timebinder.io/compare/wayback-machine-as-proof/
timebinder.io: other side says your evidence is a deepfake	timebinder.io/blog/other-side-says-your-evidence-is-a-deepfake/
timebinder.io: answers	timebinder.io/answers/
timebinder.io: how to timestamp a document for free	timebinder.io/answers/how-to-timestamp-a-document-for-free/
timebinder.io: how to tell if a file has been changed	timebinder.io/answers/how-to-tell-if-a-file-has-been-changed/
timebinder.io: how to prove a photo is not ai	timebinder.io/blog/how-to-prove-a-photo-is-not-ai/

About TimeBinder

TimeBinder is one tool for dating your files. A **TimeBind** is a dated, checkable record that an exact file existed no later than a recorded time and still matches. Your browser makes the fingerprint and the file stays on your device. It does not detect AI, show who made a file, or replace legal advice.

Your first Pooled TimeBind is free with no card, then from US$5. timebinder.io · Free file comparison checker · Read this guide online

This is general information, not legal advice. Laws and reporting services differ by country and change over time. Links go to other organisations, and we do not control them. Updated 11 November 2026.