

FIRST 24 HOURS · FREE US GUIDE

Online harassment: what to do first

Save evidence safely, find the right reporting route, and keep track of your next steps.

Victoria, developer of Reputation Radar

In immediate danger? Call 911 in the US.

Your safety comes before collecting evidence or completing a report.

Start here

What is happening?

[Intimate photos have been shared, or someone is threatening to share them](#)

[I am being threatened, stalked, or having my details exposed](#)

[A fake account is pretending to be me](#)

[I want a harmful post or search result removed](#)

More than one route may apply. The guide is free to use, with no signup required.

Has someone taken over your account?

Use the service's official recovery process. From a device you trust, review your password, active sessions, recovery details, and two-step login. Follow the [FTC's account-recovery steps](#).

This guide focuses on US reporting routes. It is general information, not legal advice or an emergency service. Reporting does not guarantee removal.

If it is safe, save the relevant URLs and non-explicit messages, report the behavior through the platform's official process, and ask someone you trust for support. Choose a situation below for more specific steps.

[Evidence checklist](#) · [Reporting templates](#) · [Incident log](#) · [Questions](#) · [Sources](#)

01 / FIRST 24 HOURS

How to document online harassment safely

If it is safe to do so, save enough context to show what happened. You do not need a perfect evidence file before asking for help.

01. Record the location and time.

Keep the post or profile URL, account name, and date and time with a time zone. Note what happened and why it concerns you.

02. Keep context, not just a cropped sentence.

For non-explicit material, capture the message or page with surrounding context and identifying details. Keep original files and messages where possible. A screenshot can be useful without proving everything about a post.

03. Store the record privately.

Keep files somewhere only you or trusted helpers can access. Do not place intimate images or exposed personal details in a public web archive.

04. Save each reporting confirmation.

Record where you reported, when, any reference number, the response, and your next step. Use the [blank incident log](#).

Sexual images involving someone under 18

Do not download, forward, or ask someone to send an image to submit it to Take It Down. Record URLs and account details instead. Use NCMEC's guidance for material already on your device, or ask NCMEC for help. See [intimate-image support](#).

Ask for help with the record if you need it.

A trusted person can help organize URLs and non-explicit messages. Agree what they can access and share. You can take a break from checking the content.

Further guidance: [PEN America: documenting harassment](#) · [NCMEC: handling images safely](#)

What if someone threatens to share intimate photos?

If someone demands money or more images

Stop responding. Do not pay or send more images. Tell someone you trust, report and block the account, and keep existing messages without downloading or forwarding sexual images involving someone under 18. If you already paid, you can still get help. [Sextortion guidance](#).

Report images through the platform's removal process.

Use its process for intimate images shared without consent, including qualifying sexual deepfakes. Save the request and submission time. The [intimate-image request template](#) helps you prepare.

Under the TAKE IT DOWN Act, covered platforms must remove qualifying content within 48 hours of a valid request through their process. Within that period, they must also make reasonable efforts to find and remove known identical copies. This is not an internet-wide removal guarantee.

Under 18 in the image

[Take It Down](#)

Use this route even if you are an adult now. Do not download or share an image to submit it. If you do not have it on the original device, ask [NCMEC's CyberTipline](#) for help.

Adult in the image

[StopNCII.org](#)

If you are depicted and have the image, check the service's eligibility steps. It creates a digital fingerprint on your device for participating platforms. It does not cover the whole internet.

Both services use digital fingerprints rather than uploading your image for hashing. Coverage is limited to participating services and supported surfaces.

Support and follow-up

Free, 24/7 US support: [CCRI, 844-878-2274](#). Report threats to local police or the [FBI](#). If a covered platform lacks a working process or misses its removal obligation, [report it to the FTC](#).

[FTC: scope and deadlines](#) · [NCMEC FAQ](#) · [StopNCII limits](#)

03 / FIRST 24 HOURS

How to report threats, stalking, or doxxing

Posting someone's private details, such as their home address, to expose or target them is often called doxxing. Focus your report on what was posted and the surrounding threats or behavior.

You do not have to decide which law applies before asking for help. Describe what happened, including any offline contact or immediate safety concern.

Immediate danger: call 911 in the US.

A web report is not an emergency response.

Report the behavior and its context.

For non-emergency concerns, contact local law enforcement through its official channel. Bring URLs, messages, dates, and a short timeline. Explain any threats, repeated contact, or reason you think the person can reach you offline. Ask for a report number if a report is made.

You can also report to the platform.

Use the category that fits: threats, harassment, or exposed private information. Do not wait for a case number to start a platform report. Add one if you have it. A case number does not guarantee that content will be removed.

If your personal details were posted

Record the URLs privately and report the exposure. You may also qualify for [Google Search removal](#). Removing a result does not remove the original page. Consider telling someone who can help with the immediate situation, such as a trusted person or workplace security.

Federal reporting options

Use tips.fbi.gov or 1-800-CALL-FBI for FBI tips. For internet crime, including online fraud or extortion, use [IC3.gov](https://ic3.gov). Neither replaces emergency help.

Save your IC3 confirmation when you submit.

IC3 does not email a copy of the complaint or provide investigation updates. Save or print the confirmation. An investigating agency may contact you for more information.

[PEN America: safety and support options](#) · [IC3: what happens after a report](#)

04 / FIRST 24 HOURS

What to do if someone is pretending to be you online

Keep the fake profile URL and examples of how it presents itself as you. If your real account was taken over, use account recovery instead.

Open the service's official help page or reporting process below. Follow its current requirements; it may ask you to sign in or provide identity evidence. Upload sensitive documents only through the official process.

Instagram	Impersonation reporting form . If it does not open, use Help inside Instagram and search for impersonation.
Facebook	Impersonation help . If the page asks you to sign in, use the app's Help Center for reporting options.
TikTok	Impersonation instructions . The help page distinguishes US and non-US forms and explains the ID step for the US route.
X	Authenticity policy and reporting link . Parody has specific requirements; its label alone does not settle every case.
YouTube	Impersonation policy and reporting instructions . Identify the channel and the specific content involved.
Reddit	Impersonation policy and reporting route . Explain the misleading identity claim.
LinkedIn	Fake-profile reporting instructions . Use the profile's report options and select impersonation when it fits.

Tell people who may be contacted.

Use a channel they already know belongs to you. Give a short factual warning; avoid reposting the fake account to a wider audience. Keep the platform's reply and any appeal instructions.

05 / FIRST 24 HOURS

How to request removal from a website or Google

A platform report, a request to a website owner, and a search-removal request do different things. One does not automatically complete the others.

Report a specific policy violation.

Explain what the post does: impersonation, threats, exposed private information, or another relevant violation. A statement being disputed or unflattering does not, by itself, guarantee removal.

Consider contacting the website owner.

If it is safe and appropriate, send a brief request with the exact URL and the change you seek. The [website-owner template](#) can help. Avoid direct contact if it may escalate threats or stalking.

Choose the Google route that fits.

- [Personal-information removal](#): check eligibility for exposed contact details and other sensitive information.
- [Intimate-image removal](#): a separate request about Google results.
- [Refresh outdated content](#): for removed pages or information that has changed at the source, not information still present there.
- [Legal removal requests](#): Google evaluates the request. A court order is not an automatic promise of removal.

Removal has limits.

A source can change before a search result updates. Removing a Google result leaves the original website and other search engines unaffected. Copies may remain elsewhere.

Before making legal threats

If your safety, work, or finances are at risk, seek advice from a qualified lawyer or an appropriate legal-aid service. Rules and deadlines depend on the circumstances and jurisdiction. Do not use a copyright claim unless it truthfully applies.

[Google: how removal requests are assessed](#) · [PEN America: legal resources](#)

If your address appears on people-search sites, use our [people-search removal guide](#). If a result belongs to someone else with your name, read [why searching your name can show someone else](#).

06 / FIRST 24 HOURS

Three reporting templates you can adapt

Replace the bracketed details. Include only statements you know are true and information needed for the request. These templates do not guarantee an outcome.

01 / A platform report

I am reporting [profile or post URL] for [impersonation / threats / exposed private information / other relevant category].

On [date and time, with time zone], [brief factual description]. The relevant context is [what the reviewer needs to understand].

Please review this under your [policy name, if known]. Supporting URLs: [links]. Please send the report reference and outcome to [contact method].

02 / A request to a website owner

Subject: Request about [page title or URL]

I am writing about [exact URL]. The page contains [identify the specific material]. I am requesting [a correction / removal of specified information] because [brief factual reason].

Please let me know whether you can make this change. You can reach me at [email]. Thank you, [name].

03 / A private heads-up

I want to flag [a fake account / online posts / unwanted messages] that may reach you. [One sentence explaining the situation, using only facts you can support.]

If you receive anything about this, please contact me through [known channel]. Please do not forward or repost it. [Optional: You can help by noting the sender and URL.]

For intimate images, use the [dedicated removal request](#). Do not attach intimate images to these general messages.

07 / FIRST 24 HOURS

Intimate-image removal request template

Use the platform's designated process. Adapt this text to its form, keeping the required information together.

To: [platform's intimate-image removal process]

I request removal under the TAKE IT DOWN Act.

Who is making this request: [name of the person depicted]. [If applicable: I am their authorized representative, name and role.]

Material to remove: [exact URL or other location details for each image or video, plus a brief description sufficient to identify it].

Why I am requesting removal: I believe in good faith that the identified intimate depiction was published without my consent. [Add relevant facts. For a manipulated image, explain that it depicts you without your consent.]

Contact: [email or other contact information the platform can use].

Signature: [physical or electronic signature of the person depicted or authorized representative].

Date: [date].

If you are an authorized representative, adapt the consent statement to refer to the person depicted and explain your authority. Do not make statements you cannot support.

Before you submit

- Include enough location information for the platform to find the material.
- Use its official process. Do not repost the image to create a link.
- Keep your request, submission time, and any confirmation.

If the process fails: see [FTC reporting and specialist support](#). You do not need to wait for this request to seek help about threats or immediate danger.

Template based on the request elements in [Public Law 119-12, section 3\(a\)\(1\)\(B\)](#). Applicability depends on the content and platform; this is not a legal determination.

08 / FIRST 24 HOURS

A private incident log you can reuse

Print a copy for each incident or keep these headings in a private document. Record facts, not guesses about who is behind an account.

Fictional example

Incident 01: a profile uses my name and photo.
Recorded: September 21, 2026, 10:15 AM UTC-04:00.
Action: reported as impersonation; confirmation saved.
Next step: check for a response on September 23. This is a personal reminder, not a promised reply time.

01 / Record the incident

Incident number	Date	Time and time zone
Platform	Account name	
Exact URL		
What happened, including context or safety concerns		
Where I stored the record privately		

02 / Report and follow up

Reported to	Submitted: date, time, time zone
Report reference number	Date I will check again
Response received	My next action

Keep passwords, recovery codes, ID documents, and intimate images out of this log. A reference to a securely stored record is enough here.

Questions about online harassment

What should I do first if someone is harassing me online?

If you are in immediate danger in the US, call 911. Otherwise, save relevant URLs and non-explicit messages if it is safe, report the behavior through the platform's official process, and ask someone you trust for support. Use the [situation selector](#) for threats, intimate images, or impersonation.

Do I need a police report before reporting an account?

You can start a platform report without waiting for a police case number. Follow the platform's requirements and describe the behavior clearly. For threats, stalking, or safety concerns, you can also contact law enforcement. A case number does not guarantee removal.

What evidence should I keep?

Keep the exact URL, account name, date and time, relevant context, and reporting confirmations. For non-explicit material, screenshots can help preserve context. Do not download or forward sexual images involving someone under 18 to make a report. See the [evidence checklist](#).

Will removing a Google result delete the original post?

No. Google Search removal affects the search result. The original page and copies elsewhere can remain online. A platform report or website-owner request is a separate step. See the [removal routes](#).

Does every platform have to remove reported content within 48 hours?

No. The TAKE IT DOWN Act's deadline concerns qualifying intimate content on covered platforms after a valid request through their process. It is not a general deadline for harassment, disputed claims, or fake accounts. See the [scope and support options](#).

10 / FIRST 24 HOURS

Sources and support

Use the links beside each route for current instructions. Reporting processes can change. This guide focuses on US routes.

Immediate danger

Call 911 in the US. Online forms are not emergency services.

Intimate images and sextortion

[CCRI support: 844-878-2274](#) · [NCMEC Take It Down FAQ](#) · [CyberTipline](#) · [StopNCII FAQ](#) · [FBI guidance](#)

Platform removal obligations

[FTC: TAKE IT DOWN requirements](#) · [Public Law 119-12](#) · [Report a platform to the FTC](#)

Documentation and reporting

[PEN America's Online Harassment Field Manual](#) · [IC3 FAQ](#) · [FBI tips](#)

Account recovery and search results

[FTC: hacked accounts](#) · [Google: personal-information removal](#) · [Google: outdated content](#)

About this guide

I'm Victoria, the developer behind Reputation Radar. I created this guide to help you find a practical next step when something harmful appears online.

The guide is free. You do not need to buy a service to use it.

For a broken link or a question about the guide, email hello@reputationradar.me. This inbox is not an emergency service.

First 24 Hours · US edition 1.0 · September 21, 2026

General information, not legal advice. No promise of removal, investigation, or a particular outcome.

Reputation Radar is a service of VBInsights Solutions.