

Avoiding Helper Scams in Online Content Removal Services

Scammers often prey on individuals who have been stalked online or who have had their intimate images distributed without their consent or are otherwise vulnerable. These “helper scams” may promise remedies they cannot deliver, for fees they will not refund. Scams disguised as offers to “help” vulnerable individuals are becoming more sophisticated and harder to recognize. Large Language Models (LLMs) have made it easy for fraudulent operators to create multi-page websites that use professional and polished language to appear credible.

At the same time, there are legitimate content removal services that can be both helpful and affordable. While CCRI and NRCC do not vouch for any particular service, the red flags and tips below are meant to help you evaluate the trustworthiness of services that claim to remove information or images from the internet.

Red Flags for Potential Fraud

1. False Partnership Claim.

CCRI and NRCC do not endorse any paid service offering the removal of personal information or images from the internet. Any claim that CCRI or NRCC recommends a paid content removal service is a red flag. We recommend you not use any service that makes such a claim.

2. Impersonation of Legitimate Free Services.

We do recommend certain free and legitimate resources, with the caution that scammers often create copycat or impersonation websites of them.

- For example, StopNCII.org is a free online tool for adults that helps prevent the further spread of intimate images across participating tech platforms. It is essential that a user visit [StopNCII.org](https://stopncii.org) specifically, as slight misspellings or look-alike URLs may direct visitors to harmful or fraudulent sites.
- Similarly, the Internet Crime Complaint Center (IC3), which allows individuals to report cybercrimes to the FBI, has [publicly warned about](#) scammers impersonating them.
- The Federal Trade Commission (FTC), which accepts reports regarding misconduct by tech platforms, has also [warned about impersonation scams](#).
- Unfortunately, we should expect these impersonations of legitimate sites to continue and proliferate. In this type of landscape, it is helpful to remember that StopNCII.org, IC3, and the FTC are free resources that will never ask for payment or financial information.

3. Overpromising.

Fully scrubbing material from the internet is difficult, and in some instances it may not be possible. Reputable image removal services will provide realistic, limited, and clear expectations about what they can and cannot do. Many reputation management companies have some capacity to remove certain types of information online, such as address history, phone numbers, email addresses, and social media information. Services that promise to permanently and quickly remove all content, including intimate images, from all sites and apps, are almost certainly over-selling their capabilities.

4. Urgent Requests for Unnecessary Sensitive Information.

Be wary if a company asks for your personally identifiable information (e.g., Social Security Number, passport number, driver's license number, etc.); banking credentials; passwords; or copies of identity documents without explanation.

5. Requests for Unusual Payment Methods.

Be cautious if the company insists on receiving payment with gift cards, wire transfers, cryptocurrency, or peer-to-peer payment apps without buyer protections. These payment methods can make it difficult to trace as well as challenging to recover funds if fraud occurs.

6. No Clear Data-Handling Practices.

A company should be able to explain how your information is handled, stored, who has access to it, how long it is retained, and whether it is shared with subcontractors or third parties.

- Read the fine print: Does the company reserve the right to sell or resell user or customer information? Will the company share information with marketing partners and affiliates? Will they use submitted user or customer data for unrelated and vague unexplained business purposes?

7. Mass-generated Content.

Common signs of mass-generated content (as opposed to original content of a legitimate service) include excessively long FAQ pages, hundreds of blog posts that do not hyperlink to an established and reputable author and/or are posted within a short time frame, and repetition of advocacy cliches or vague claims without offering new or substantive information. Informally, this is often referred to as "AI slop."

Tips

1. **Verified Customer Success.**

When possible, speak directly with someone you trust who has used the service and can describe their experience. Websites created using LLMs may feature hundreds or thousands of polished, glowing reviews that are misleading or fabricated. These fraudulent websites/services may even have strong ratings from platforms like the Better Business Bureau because they are new or short-lived without many complaints. It's important to exercise caution because services may show high ratings simply because few complaints have been filed yet, and some victims may not realize they have been targeted or may never file a complaint. It can be helpful to cross-reference a website's reviews across different platforms (e.g., Better Business Bureau, Google, Trustpilot, etc.), but there is no single trustworthy review platform. It is also important to keep in mind that even services recommended by well-meaning journalists or influencers may not be trustworthy, as they are likely consulting the same reviews and rankings. Remember that these content removal services are skilled in managing and manipulating their own reputation and reviews.

2. **Expertise and Longevity.**

It can be a good sign if the company has an established, multi-year track record providing general reputation management services. By contrast, services that are seeking donations or state in small print that they are in beta testing may be innovative philanthropic or investment opportunities. Extra caution is warranted before entrusting sensitive personal information or intimate images with new, experimental services that are not yet fully established.

3. **User Experience and Accessibility.**

A company's online portal should be easy to understand and navigate, including a clear interface for tracking requested takedowns and verifying successful removals.

4. **Customer Service.**

A reputable service should provide a reliable and responsive way to contact customer support. This should include a consistent telephone number (rather than one that changes frequently), an email address that uses the company's own domain name (not a generic provider such as Gmail or an address composed of random or unintelligible characters), or a chat function that uses professional language (rather than highly charged, urgent messaging designed to pressure users to utilize the service).

5. Clear Privacy and Cancellation Policy.

These policies should seem clear and reasonable. Check if there are tiered and/or subscription-based plans and if cancelling is a straightforward process. If you do engage a paid service, it is always a good idea to check your credit card statements to confirm that all charges are accurate.

6. Pause.

Finally, before deciding whether to choose a service, try to proceed deliberately and slowly after reviewing the sites using the tips above. These scams can be extremely difficult to identify, and even tech platforms struggle to detect and remove them. Exercising caution will likely prove beneficial in the long run.

More Information

When someone types “image removal” or “reputation management” into a search engine, the results can be overwhelming. We hope that the tips above can help you identify whether a takedown service is both reputable and likely to be effective.

For further information on stalking, domestic violence, image-based sexual abuse, and cybercrimes against individuals, please visit the following reputable nonprofit organizations.

- [Cyber Civil Rights Initiative](#) (CCRI)
- [National Resource Center on Cybercrimes](#) (NRCC)
- [National Network to End Domestic Violence](#) (NNEDV)
- [Stalking Prevention, Awareness, & Resource Center](#) (SPARC)

For information on what to do should you experience image-based sexual abuse, please visit the following resources.

- [CCRI's Safety Center](#)
- [NRCC's Know Your Rights: The Take It Down Act](#)