Understanding Cyberstalking

Cyberstalking is a serious form of online harassment that can cause significant emotional distress and fear.

- Sending threatening or obscene messages or emails
- Posting personal or sensitive information online
- Engaging in online harassment or bullying
- Monitoring an individual's online activity
- Spreading false information or rumors about an individual
- Attempting to intimidate or control an individual through technology.

by Walter Houser
Volunteer
Montgomery County
Police Department

Impact of Cyberstalking

1 Emotional Distress

Cyberstalking can cause significant emotional distress, fear, and anxiety, impacting the mental well-being of the victim.

2 Identity Theft

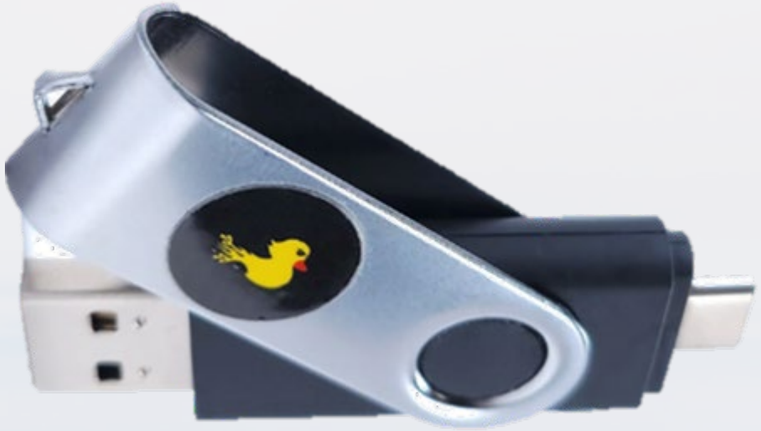
It can lead to identity theft, financial fraud, and physical danger, resulting in long-term consequences for the victim.

3 Financial Loss

Stalkers can compromise victim’s credit cards and financial accounts.

4 Effort and Time

Victims often spend significant time and effort resolving fraudulent activities, disputing charges, incurring legal expenses, and restoring their identities.



Tools Cyberstalkers Use

1 Social Media Platforms

Fake Accounts monitor and interact with their targets anonymously.

2 Email and Communication Monitoring

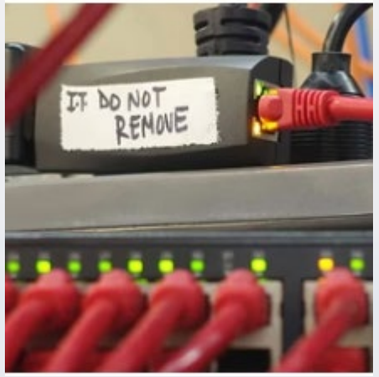
Email Spoofing: Cyberstalkers send emails that appear to be from a trusted source, aiming to deceive the victim.
Monitoring Software: Tools that intercept and monitor emails, messages, and other communication.

3 Online Databases and Public Records

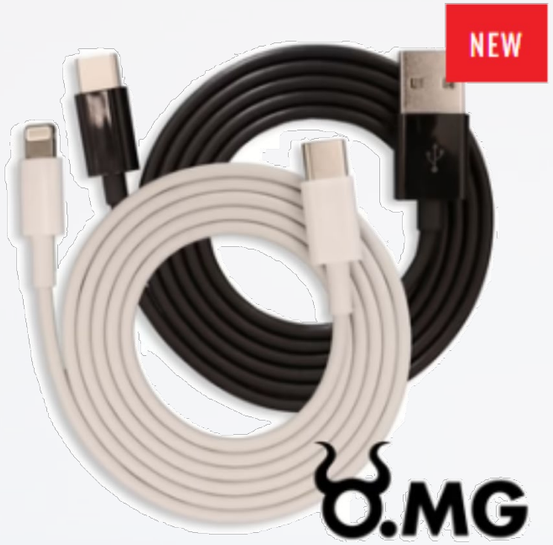
People Search Engines gather personal information about individuals from various sources.
Public Records Searches: Accessing public records to obtain information about a person's address, phone number, or other personal details.

4 Doxxing Software

Tools that facilitate the gathering and publishing of private or identifying information about an individual.



Tools Cyberstalkers Use



5 Spyware and Malware

Keyloggers: These record keystrokes on a victim's device, capturing passwords and sensitive information.
Remote Access Trojans (RATs): These allow unauthorized access to a victim's computer, enabling the stalker to control the device remotely.

6 GPS Tracking Apps

Location Tracking Apps: These apps, when installed on a target's phone, can track the person's movements in real-time.

7 Webcam and Microphone Hacking

RATs and Webcam Hacking Tools: Cyberstalkers may attempt to gain unauthorized access to a victim's webcam and microphone for surveillance.

8 Denial of Service (DoS) Attacks

DoS Tools: In some cases, cyberstalkers might resort to disrupting a victim's online activities through DoS attacks, making online communication difficult.

How to Protect Yourself from Cyberstalking

Ask the harasser to stop

Maryland Law requires that the victim document having asked the harasser to stop the harassment.

Block the Stalker

Block the stalker's phone number and email address and set your social media accounts to private.

Document the Harassment

Record all communication and evidence of cyberstalking, including emails, text messages, and social media posts. Maryland Law requires the demonstration of a "course of conduct:" a series of harassing acts, not a single incident.

How to Protect Yourself from Cyberstalking

Report the harassment

Report the cyberstalking to the authorities, your internet service provider, or the social media platform used by the stalker.

Get Support

Reach out to friends, family, or a support group for emotional support. Contact a victim advocacy organization (see below).

Protect your personal information

Be cautious about the information you share online and take steps to secure your personal information, such as changing passwords regularly and avoiding oversharing on social media.

Secure Your Social Media Accounts

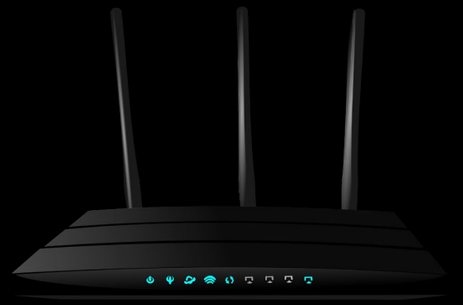
Adjust privacy settings on social media platforms to

- limit personal information exposure and
- reduce the likelihood of being targeted.

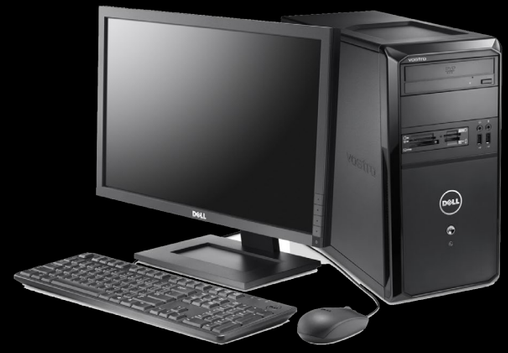
See National Cybersecurity Alliance (staysafeonline.org) Manage Your Privacy Settings. https://staysafeonline.org/resources/manage-your-privacy-settings/

Or the Office of the Privacy Commissioner of Canada Tips for using privacy settings. www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/?WT.ac=set-en-1

Use secure devices and networks



Secure all your devices and networks with regular updates and replacement of default passwords.

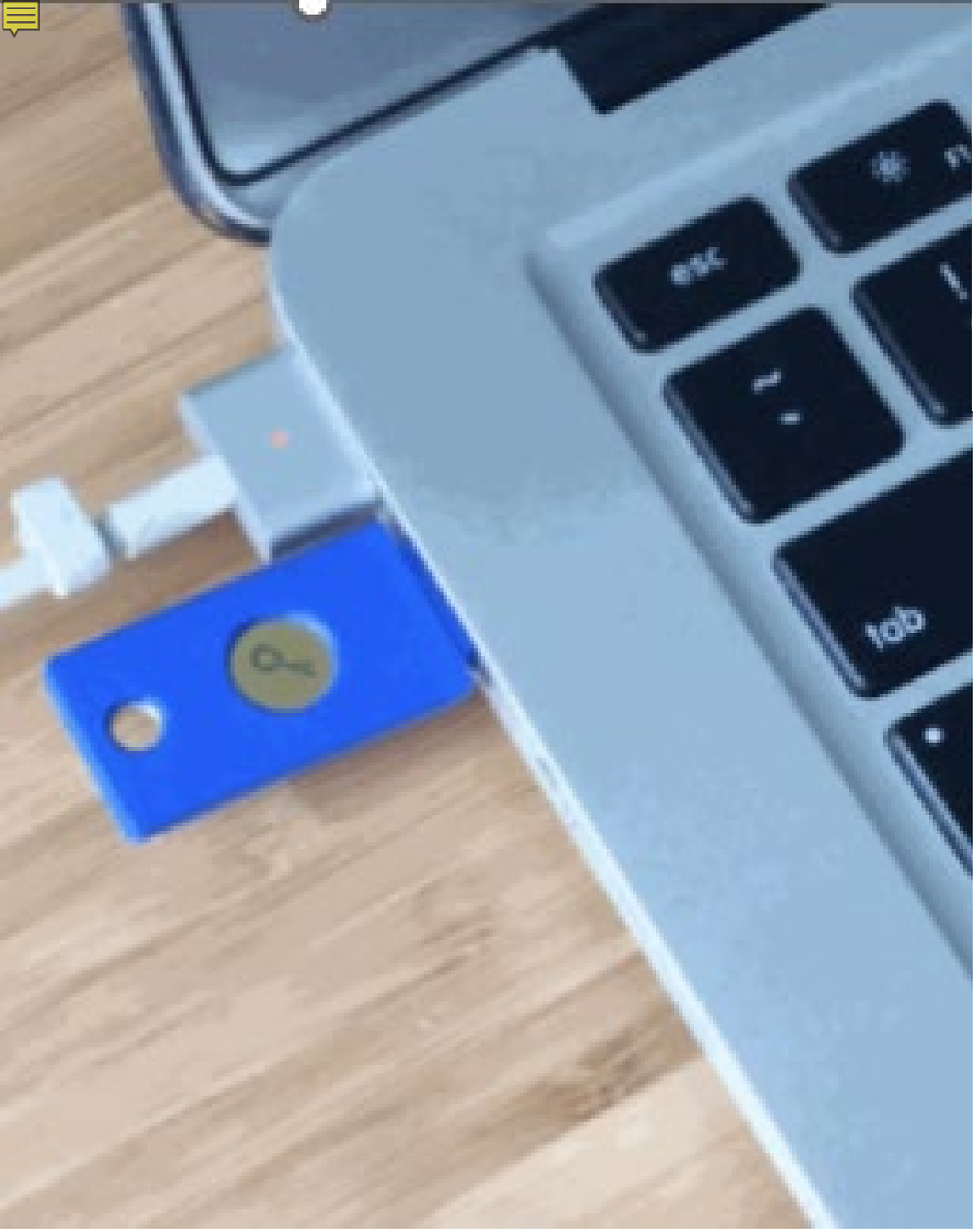


Use a VPN

A virtual private network (VPN) can protect your online activities from being monitored.

Get a password manager

- Get a password manager from a reputable source.
- Replace all your passwords with unique and strong passwords.
- If someone can access those accounts, they can easily see your location and text messages.

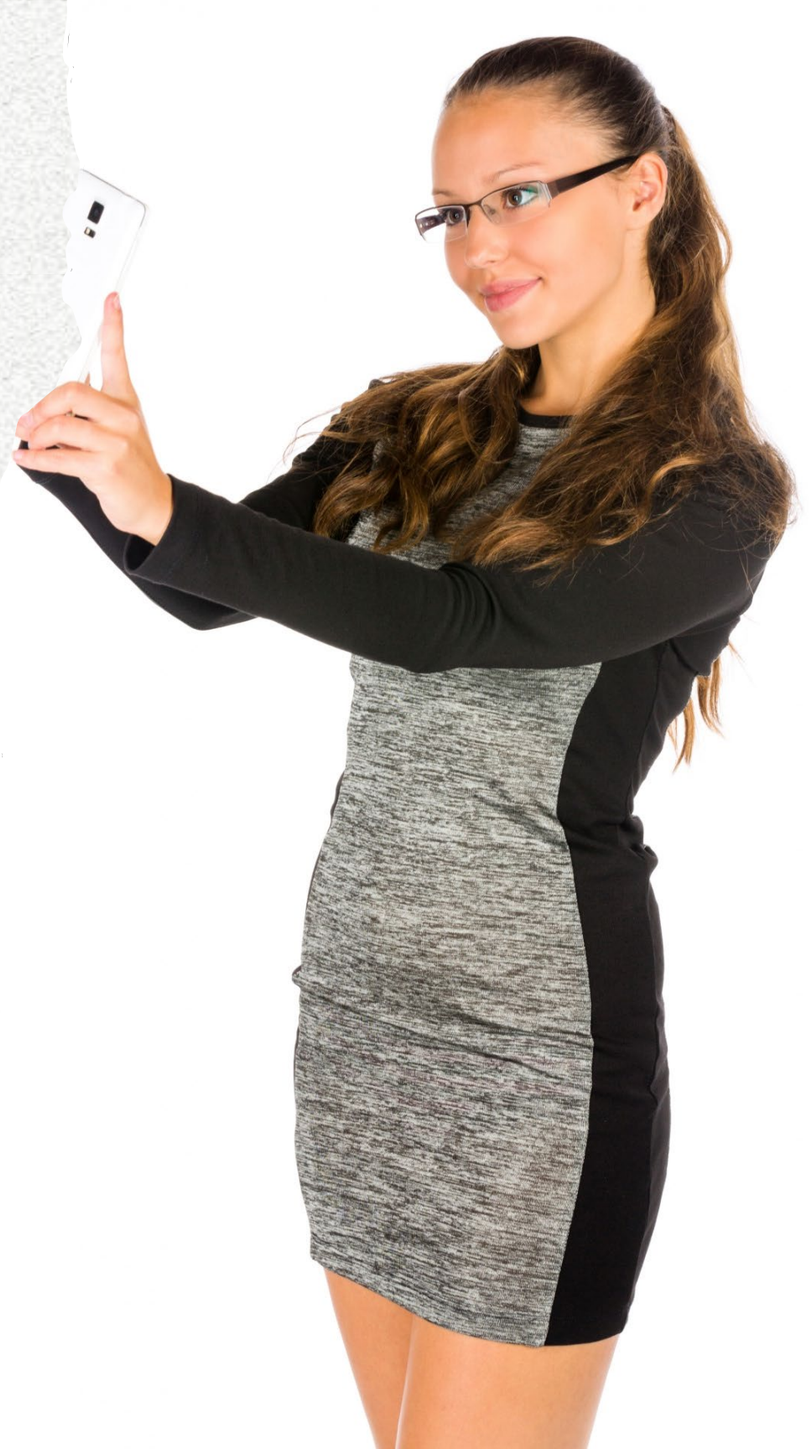


Enable multi-factor authentication (MFA)

Having more than MFA on all your online accounts makes it harder for the stalker to access your information.

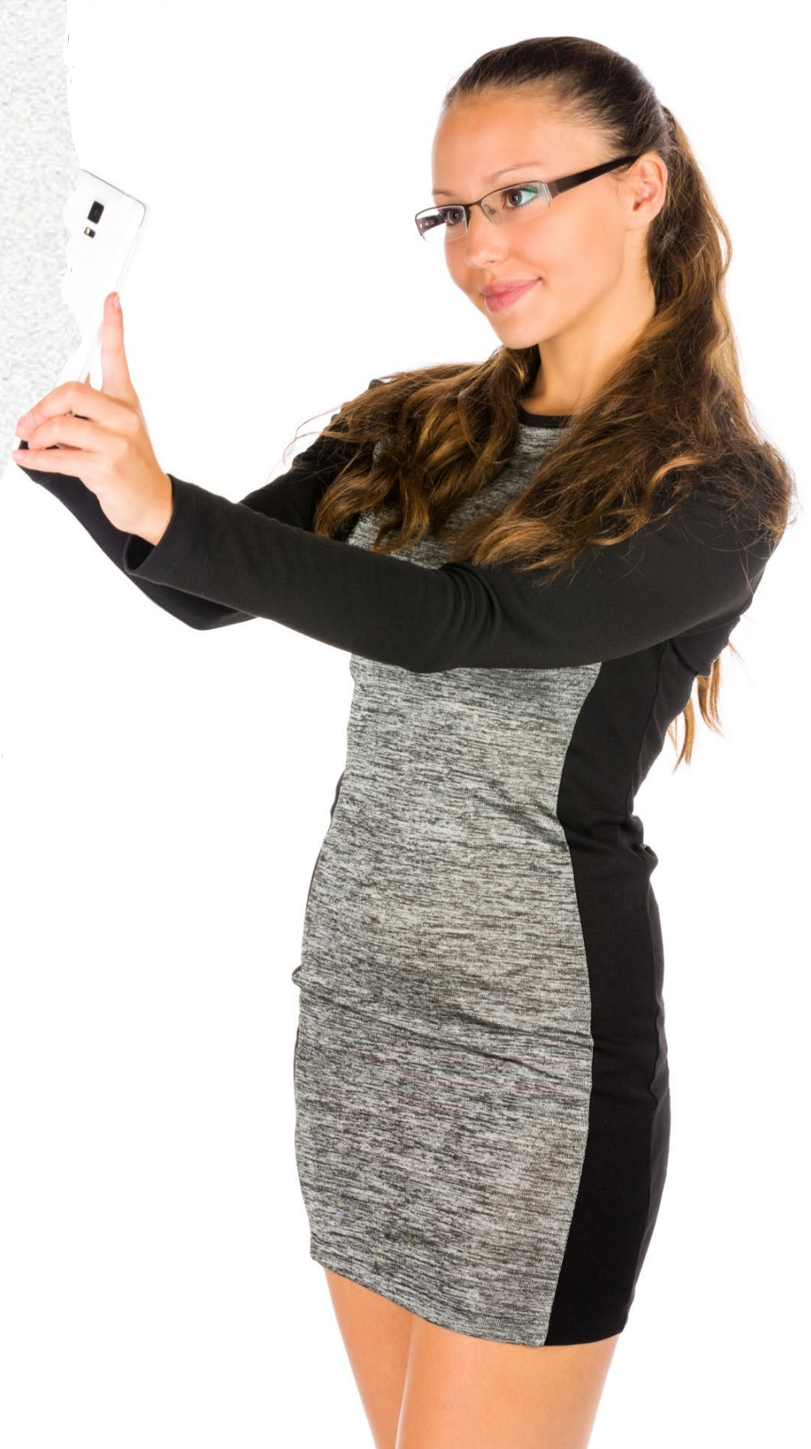
How can victims use copyright law to remove compromising selfie photos from internet sites?

- If your own photos are being posted on internet sites, you may be able to use US copyright law to have them removed from internet sites in the United States.
- However, victims need to obtain the advice of legal counsel before proceeding.



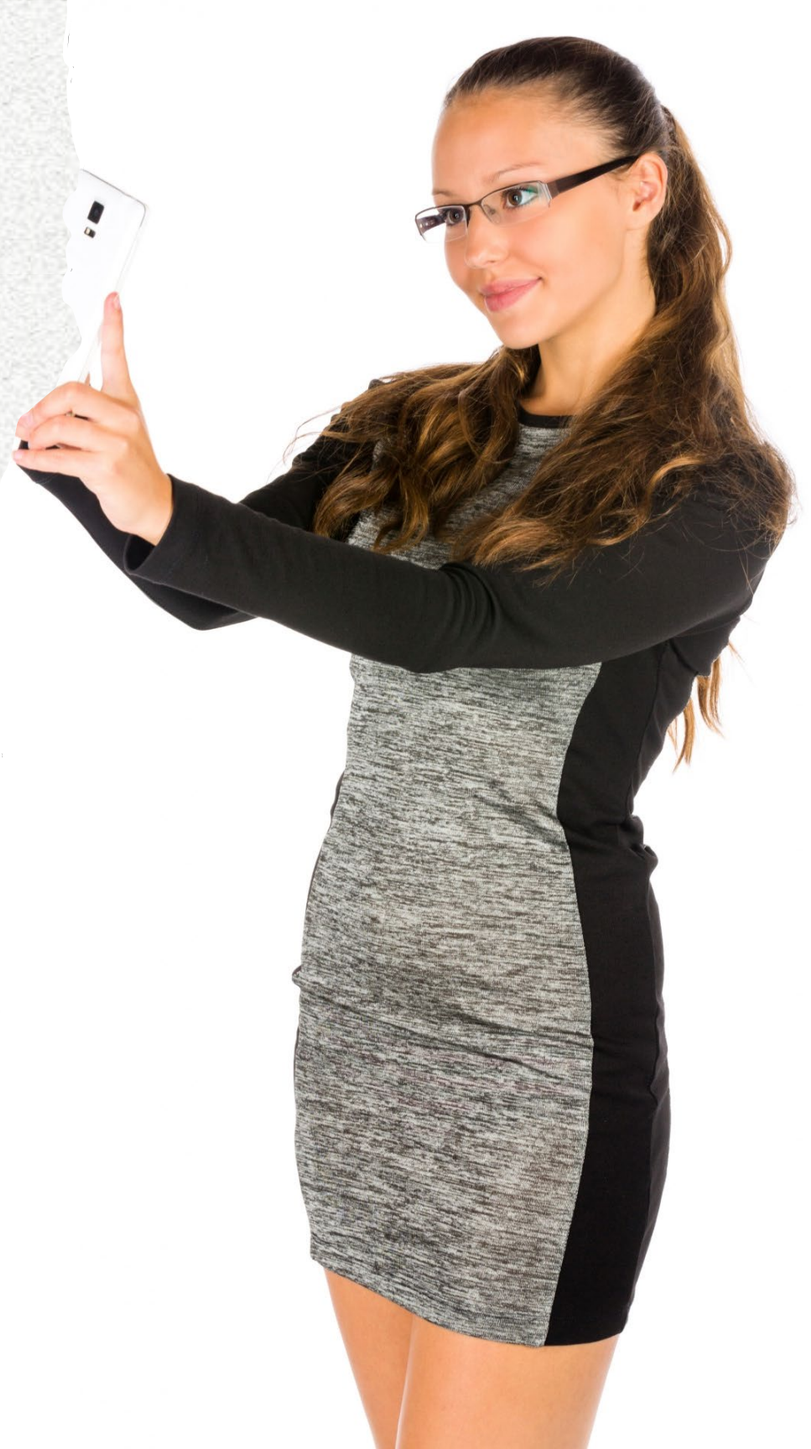
Using copyright law to remove compromising selfie photos from internet sites

- This is a civil law procedure, not criminal law.
- So, law enforcement is not involved in this process.
- Also, civil proceedings are public, so victim’s identities are not shielded, as would be the case for a criminal case.
- It's crucial to be aware that laws and regulations surrounding revenge porn and privacy vary by jurisdiction.
- Victims pursuing this course of action should prioritize their safety and well-being and seek assistance from legal professionals specializing in intellectual property and cyber law.



Using copyright law to remove compromising selfie photos from internet sites

1. **Establish Copyright Ownership:** Victims may have copyright ownership of the images or videos if they were the creators.
2. **Register the Copyright:** While not necessary, registering the copyright can strengthen legal claims and provide additional remedies. If the photos were taken by a professional photographer, asking for a re-assignment of rights can strengthen the victim's argument in a take-down notice.
3. **Send a Cease and Desist Letter:** Have a legal representative send a cease and desist letter asserting copyright ownership and demanding the immediate cessation of distribution.
4. **DMCA Takedown Notice:** Use the Digital Millennium Copyright Act (DMCA) to submit takedown notices to have the content removed from online platforms.
5. **Legal Action:** If the situation persists, consider filing a lawsuit against the perpetrator for copyright infringement.



Urgent Support Contacts

1-800-799-SAFE

The National Domestic Violence Hotline

Confidential support, and referrals for victims of domestic violence, including cyberstalking.

https://www.thehotline.org/

855-4-VICTIM

Cybercrime Support Network

National non-profit organization organization providing support support and resources for victims victims of cyberstalking and cybercrime.

https://www.thehotline.org/

1-800-THE-LOST

National Center for Missing & Exploited Children

Resources and support for cyberstalking victims, including children and teens.

https://www.missingkids.org/

Urgent Support Contacts

(202) 544-5564

National Network to End Domestic Violence

A network of domestic violence violence programs that provides provides technical assistance, training, and resources for victims victims of cyberstalking.

https://nnedv.org/

(305) 974-1671

Cyber Civil Rights Initiative Initiative

A non-profit organization combating online abuse and harassment, including cyberstalking.

https://www.cybercivilrights.org/

(202) 467-8700

National Center for Victims of Crime

A national non-profit organization that provides resources and support for victims of crime, including cyberstalking.

https://victimsofcrime.org/

Urgent Support Contacts

(202) 470-4112

National Cybersecurity Alliance

A non-profit organization that that provides resources and information on cyberstalking and and online harassment.
https://staysafeonline.org/

301-279-8000

File a non-emergency police report to Montgomery County Department

Special Victims Investigations Division
Captain Jeffrey Bunge, Director
SVID Main Number: 240-773-5400
POL.SVIDDirector@montgomerycountymd.gov
ov

Questions

References

- Baker, R. (2020). "Using OSINT for Human Rights and Victim Support. Shmoocon. From https://youtu.be/tRzGiR4DS7w/
- Office of the Privacy Commissioner of Canada, Tips for using privacy settings.
- National Cybersecurity Alliance (staysafeonline.org) Manage Your Privacy Settings
- Schneider, A. (2023, August 26). Ignored by police, twin sisters took down their cyberstalker themselves. The Washington Post. From https://www.washingtonpost.com/technology/2023/08/26/revenge-porn-leaked-nudes-police/