



© 2026 DMCA512.com – All Rights Reserved

Worldwide Copyright & Trademark Brand-Protection Services

Contact: dmca@dmca512.com

PREFACE

Cyberstalking and online harassment have become widespread digital threats that can escalate across platforms, jurisdictions, and even national borders. Victims often feel overwhelmed or unsure where to begin. This handbook provides a structured, authoritative guide to understanding cyberstalking, documenting evidence, strengthening digital defenses, and navigating reporting pathways in the United States and internationally.

DMCA512.com has spent more than two decades protecting creators, brands, and individuals from online abuse, impersonation, copyright theft, and digital exploitation. This handbook reflects that mission: empowering victims with clarity, structure, and actionable steps.

ABOUT DMCA512.COM

DMCA512.com is a global enforcement and brand-protection agency specializing in:

- Copyright enforcement
- Trademark protection
- Impersonation removal
- Deepfake takedowns
- Evidence preservation
- Cross-platform monitoring
- Creator and business protection

Our mission is to protect your work, your brand, and your identity across the global digital landscape.

For information on retaining our services: [✉ dmca@dmca512.com](mailto:dmca@dmca512.com)

SECTION 1 – UNDERSTANDING CYBERSTALKING

What Cyberstalking Is

Cyberstalking is a pattern of repeated, unwanted, intrusive behavior carried out through digital means. It may involve threats, impersonation, monitoring, extortion, doxxing, or attempts to cause emotional distress. It becomes a criminal offense when it causes fear, substantial emotional harm, or involves threats of injury or death.

Common Forms of Digital Harassment

- Persistent unwanted messages
- Threats of violence or extortion
- Identity theft or impersonation
- Posting private information (doxxing)
- Tracking, monitoring, or hacking devices
- Harassing communications across state or national borders
- Revenge-motivated harassment
- Deepfake misuse or synthetic impersonation

Key U.S. Federal Laws

- 18 U.S.C. § 2261A – Cyberstalking
- 18 U.S.C. § 875 – Interstate Threats & Extortion

- 47 U.S.C. § 223 – Harassing Telecommunications
- 18 U.S.C. § 1030 – Computer Fraud and Abuse Act (CFAA)
- 18 U.S.C. § 1028 – Identity Theft

SECTION 2 – IMMEDIATE SAFETY & REPORTING

Emergency Response

If you are in immediate danger, contact 911. If a child is involved, contact the National Center for Missing & Exploited Children (NCMEC).

Evidence Preservation

Document everything:

- Screenshots of messages, posts, emails
- URLs and profile links
- Timestamps and platform names
- IP logs (if available)
- Threats, extortion attempts, impersonation
- Copies of police reports or platform reports

Store evidence in multiple locations and avoid altering screenshots.

U.S. Federal Reporting

- FBI IC3: <https://www.ic3.gov>
- FBI Cyber Division: <https://www.fbi.gov/investigate/cyber> (fbi.gov in Bing)
- Cyber Tipline: <https://report.cybertip.org>
- USPS Inspector General: <https://www.uspis.gov>

International Reporting

- Canada: RCMP Cybercrime, Anti-Fraud Centre
- UK: Action Fraud, NCSC
- EU: Europol EC3, ENISA
- Australia: ACSC, eSafety Commissioner
- New Zealand: CERT NZ
- India: National Cyber Crime Portal

- Interpol: Cybercrime Directorate

SECTION 3 – PLATFORM REPORTING

Social Media

- Facebook: <https://www.facebook.com/help>
- Instagram: <https://help.instagram.com>
- X (Twitter): <https://help.twitter.com>
- TikTok: <https://support.tiktok.com>
- YouTube: <https://support.google.com/youtube>

Messaging Platforms

- WhatsApp: <https://www.whatsapp.com/safety>
- Telegram: <https://telegram.org/faq>
- Discord: <https://support.discord.com>

Online Marketplaces

- eBay: <https://www.ebay.com/help>
- Amazon: <https://www.amazon.com/gp/help>

SECTION 4 – DIGITAL SECURITY & MFA

Account Hardening

- Strong, unique passwords
- Multi-Factor Authentication (MFA)
- Updated recovery settings
- Removal of unused apps and permissions

Device Security

- Updated operating systems
- Antivirus and anti-malware tools
- Avoiding public Wi-Fi for sensitive tasks

Privacy Protection

- Limit public visibility
- Remove personal data from broker sites
- Use a VPN when appropriate

Multi-Factor Authentication (MFA)

MFA requires two or more forms of verification before granting access. It combines:

- Something you know (password)
- Something you have (phone, authentication app, hardware key)
- Something you are (biometrics)

Types of MFA

- SMS codes
- Authentication apps
- Push notifications
- Hardware security keys

Why MFA Matters

Cyberstalkers often attempt password guessing, credential stuffing, SIM-swapping, and account recovery abuse. MFA blocks most of these attacks even if the attacker has your password.

SIM-Swapping Defense

- Lock your mobile account with a PIN
- Avoid posting your phone number publicly
- Prefer app-based MFA over SMS

SECTION 5 – DMCA512.COM SERVICES & CONTACT

Copyright & Trademark Enforcement

DMCA512.com provides:

- DMCA takedowns
- Trademark enforcement
- Removal of impersonation accounts
- Deepfake and stolen-content removal
- Cross-platform monitoring
- Evidence preservation

Digital Abuse Response

Support for creators, brands, and individuals facing:

- Harassment
- Impersonation
- Identity misuse
- Unauthorized content distribution

Evidence Support

Structured logs, timestamped captures, and defensible documentation for escalation to platforms, attorneys, or law enforcement.

CONTACT & RETAINER INFORMATION

For clients, creators, brands, agencies, and individuals seeking professional enforcement or protection services:

 dmca@dmca512.com DMCA512.com – Worldwide Copyright & Trademark Brand-Protection Services

COPYRIGHT PAGE

DMCA512.com Cyberstalking & Harassment Handbook © 2026 DMCA512.com – All Rights Reserved Unauthorized reproduction, distribution, or modification is prohibited.