Immediate Actions

✓ **Do Not Engage with the Attacker** – Responding can escalate threats.

✓ **Take Screenshots & Save Evidence** – Capture the URL, timestamps, and messages related to the content.

✓ **Use Archive Services** – Save the page using archive.org or take screen recordings.

✓ **Search for Duplicate Content** – Use Google Reverse Image Search, Yandex, or TinEye.

Reporting & Content Removal Requests

Social Media & Search Engine Takedown Requests

✓ **Google:** Remove Personal Content

✓ **Facebook & Instagram:** Report Violations

✓ **Twitter/X:** Privacy Violation Reporting

✓ **Reddit:** Report Policy Violations ✓ **YouTube:** Remove Harmful Content

✓ **TikTok:** Report Misuse

✓ **Porn Sites (e.g., Pornhub, XVideos):** DMCA & Abuse Reports

✓ **Google/Bing Search Results:** Request de-indexing from search results.

DMCA Copyright Takedown Requests

✓ **Submit a DMCA Request** via DMCA.com or Lumen Database

✓ **Contact the Website Host** – Use Whois Lookup to find domain ownership.

✓ **Send a Cease & Desist Letter** – Consult a lawyer or use online templates.

Contacting Legal Authorities & Organizations

✓ **File a Police Report** – Provide documented evidence and explain the severity of the situation.
✓ **Contact a Cybercrime Unit** – Local and federal authorities may investigate digital exploitation cases.

✓ **Seek a Lawyer Specializing in Digital Law** – Consider Minc Law or Carter-Ruck.

✓ **File a Case Under "Right to Be Forgotten" (Europe GDPR Cases)** – Request content removal under privacy laws.

✓ **Submit a Complaint to the FBI (USA Cases)** – FBI Internet Crime Complaint Center (IC3)
✓ **Contact a Victim Support Organization** – Cyber Civil Rights Initiative or RAINN

Local Crisis & Institutional Support

✓ **Notify School Faculty & Administration** – If the victim is a student, report to the school for guidance.

✓ **Report to HR (for Workplace Cases)** – If the abuse impacts employment, notify your employer.

✓ **Engage with Local Advocacy Groups** – Contact community organizations for immediate assistance.

✓ **Seek Counseling Services** – Online and local support networks are available for victims of digital abuse.

Protect Yourself Against Future Attacks

✓ **Enable Two-Factor Authentication (2FA)** – Secure your accounts with extra verification steps.

✓ **Tighten Privacy Settings on Social Media** – Reduce visibility of personal content.

✓ **Use Online Reputation Management Services** – Consider Reputation Defender or DeleteMe.

✓ **Monitor for Re-Uploads** – Set up Google Alerts with your name or use PimEyes for facial recognition tracking.

✓ **Consider a Private Investigator or Cybersecurity Expert** – Night Lion Security specializes in tracking digital offenders.

Final Steps: Advocate for Change

✓ **Raise Awareness** – Share your experience with trusted advocacy groups and legal bodies.

✓ **Support Stronger Digital Protection Laws** – Engage in petitions or policy discussions to combat AI-generated abuse.

✓ **Educate Others** – Spread information about online safety and reporting measures.

Share This Checklist

This document provides a structured response plan to help victims of AI-generated deepfake abuse, sextortion, and digital harassment.

Share it with others and encourage awareness to prevent online exploitation.