GhostTrace LLC

Online Incident Evidence Checklist

If you've been scammed, impersonated, harassed, or targeted online, the first hour matters. This checklist walks you through the exact evidence to capture — in order — so you can report, recover, or hand off a clean record to authorities, a lawyer, or a professional investigator. GhostTrace LLC uses this same discipline in every case.

1) Freeze the scene — do not delete anything

- Do NOT delete messages, emails, or accounts — even embarrassing ones.
- Do NOT block the person yet (blocking hides evidence on some platforms).
- Do NOT reply, threaten, or negotiate. Silence preserves your case.

2) Capture full-context screenshots

- Include the sender's username/handle, the timestamp, and the URL bar in every screenshot.
- For DMs: capture the profile page first, then the conversation, then any attachments.
- Use your device's built-in screenshot — no editing apps, no crops that hide metadata.
- For a scrolling conversation, use the phone's 'full page' or 'scrolling capture' feature.

3) Record the technical fingerprints

- Copy every profile URL / permalink — not the shortened share link.
- Save the exact display name AND the underlying handle (they can differ).
- For emails: 'Show original' / 'View headers' and save the full raw source (.eml).
- For phishing links: right-click → copy link address; never click it.
- For crypto scams: copy the wallet address, transaction hash, and network.

4) Build a timeline

- One row per event: date, time (with time zone), what happened, where.
- Include first contact, escalation, payment/loss, and any warnings you received.
- A spreadsheet or a plain-text file both work — consistency beats formatting.

5) Preserve financial evidence

- Bank/credit card statements showing the transaction (PDF, not screenshots).
- Payment app receipts (Zelle, Cash App, Venmo, PayPal, wire confirmations).
- For crypto: wallet history export + block-explorer link for each tx hash.

6) Report — in the right order

- Report to the platform (Instagram/TikTok/Meta/X/etc.) using their impersonation or fraud form.
- Report to your bank / card issuer immediately for fraud reversal — most have a 60-day window.
- If you're in the US: file at reportfraud.ftc.gov and ic3.gov (FBI IC3).
- If minors are involved: report to CyberTipline (report.cybertip.org).
- Then file a local police report — bring the timeline and evidence bundle.

7) Lock down your accounts

- Change passwords on any account that could reach the compromised email/phone.
- Enable multi-factor authentication (authenticator app, not SMS) on email first.
- Sign out all active sessions and revoke third-party app access.
- Freeze your credit at Equifax, Experian, and TransUnion (US — free).

8) Package the evidence

- One folder per incident. Inside: /screenshots, /emails, /finance, timeline.txt.
- Name files with ISO date first — 2026-02-08_dm-thread-01.png — they sort correctly.
- Compute a SHA-256 hash of each file and save the hashes to hashes.txt — proves nothing was altered.
- Zip and store two copies: local drive + one cloud backup.

When to call in a professional

If the incident involves an active impersonation, a live harassment campaign, ongoing financial loss, or evidence you can't unpick alone — GhostTrace LLC can research the situation using lawful open-source techniques and produce a documented report you can act on. Open a case at ghosttrace.net or submit intelligence anonymously.
