

Doxxing Response Guide

Doxxing Response: Stages & Action Guide

(IMMEDIATE → NEXT → MEDIUM → LATER)

Being doxxed is frightening. Feeling scared, angry, or overwhelmed is normal. Pause, breathe, ask for help, and put safety first. Harassment campaigns can last—don't go through it alone.



Take a deep breath, try to stay Calm & assess

- Identify **what information was leaked** (address, phone, email, SSN, etc.) (check the table below)
- Think about **immediate risks** (physical safety, financial fraud, harassment).
- Monitor the intensity level and frequency of harassment (calls, txts, social media engagement, etc.)

If THIS happens...	Do THIS...
Only name/workplace posted	Lock accounts, 2FA, tighten privacy, notify employer, document
Home address published	Consider relocation, alert neighbors/security, call police, document
Phone/email exposed	Change passwords, block/report harassers, consider getting additional email/phone numbers, document
Financial info leaked	Call bank, freeze credit, fraud alerts, document
Direct threats	Call 911/police, preserve evidence (document)





IMMEDIATE — First 0–30 Minutes

Goal: Protect physical security, preserve evidence, reduce immediate exposure

Assess Immediate Risk & Safety



Why: Physical harm is the biggest risk.

→ **Action:**

- ☐  Assess physical safety. If you feel unsafe → **notify local police of the possibility of SWATTING** or call 911 and file a police report (get a report number).
- ☐  Alert employer/workplace security.

If Address Is Exposed

→ **Action:**

- ☐  Consider temporary relocation (trusted friend, hotel, safe housing)
- ☐ [Prepare go-bag](#).
- ☐  Home security: install home security cameras, preferably with a motion sensor, stickers/posters about the use of home security on doors and windows (for deterrence), and alert neighbors, friends, or building security to keep an eye out for suspicious people. *(NOTE: this can move to next)*
- ☐ Alert neighbors/building security.
- ☐ Notify police if threats mention location (mention SWATTING).
- ☐ Brief trusted contacts never to share your whereabouts or routines.

Tell a Trusted Person

Why: Doxxing and online harassment can be traumatizing; you do not have to do it alone.

→ **Action:**

- ☐ Notify a friend/family/colleague ASAP; assign roles if possible (e.g. monitoring accounts, documenting/saving evidence, emotional support, groceries, etc..).

- ☐ If work-related, inform HR/security or newsroom.
- ☐ Create a “doxxing buddy” system for collective care.

Reduce Public Physical Exposure (even after relocation)

Why: People can recognize us and know where we are (even after relocation) from our profile (think your car, your big dog, etc..)and daily habits. The goal is to decrease the likelihood of doxxing a second location.

Action:

- ☐ Keep a very low profile in your daily life (temporarily)
- ☐ Avoid wearing distinct clothing or accessories that you are known for (ex, bright backpack with pins, unique hat or scarf, etc...)
- ☐ Lean on your community to run your errands and walk your dog (if possible!)
- ☐ Vary your routines and routes

Document to Preserve Evidence

Why: Needed for takedowns, police, and possible legal action.

Action:

- ☐ Screenshots of all doxxing/harassment (include URLs, usernames, dates/times).
 - ☐ Track reshares/engagement → shows reach/risk.
 - ☐ [Keep a log: incident, platform, URL, evidence saved, actions taken.](#)
- ☐ Save voicemails, emails, and messages; [document offline incidents](#) (someone following you or in-person or physical confrontation)
- ☐ Use [templated log sheets](#) (spreadsheet or notebook) with columns for each key detail

Reduce Online Visibility

Why: Slows spread, reduces discoverability, and can help with lowering the level of harassment.

➔ **Action:**

- ☐ Make profiles temporarily private or deactivated
- ☐ Change usernames to something random (if possible, and can be done later).
- ☐ Do not engage with harassers if it brings more visibility to the doxxed content.
- ☐ Avoid posting in real-time; disable geotags.
- ☐ Report some of the abusive/doxxing posts on platforms.



NEXT — First 24 Hours

Lock Down Exposed Accounts

Why: To make it harder for someone to hack and get into your accounts.

➔ **Action:**

- ☐ Change passwords (strong 16+ password, unique to this account)
 - ☐ Use a password manager.
- ☐ Enable 2FA (authenticator app/hardware key).
- ☐ Sign out of active sessions, check recovery settings.
- ☐ Watch for phishing, spear-phishing, or recovery scam attempts (fake emails or attempts to get your info). Verify all “security” emails by logging in directly.

Report & Request Takedowns

Why: to curb the spread of the information.

➔ **Action:**

- ☐ Report abuse to platforms.
- ☐ Contact admins/hosts/registrars.
- ☐ Request removal/delisting from data brokers and directories
- ☐ [Use template emails](#)—brief, factual, with direct links & screenshots

Initial Financial Protection

Why: Reduce fraud and identity theft.

→ Action:

- ☐ Notify bank/card issuers if data is exposed.
- ☐ Place fraud alert or freeze credit ([Equifax Freeze](#), [Experian Freeze](#), [TransUnion Freeze](#)).
- ☐ Monitor statements for unusual charges or transactions.
- ☐ Call the bank/credit card issuer if data is leaked.
- ☐ Replace compromised IDs (license, passport, SSN if needed).

Notify Organizations

Why: To get the support needed if they have escalation protocols and to protect others from possible escalations.

→ Action:

- ☐ Inform employer, newsroom, or professional association.
- ☐ Alert campus security/school admins if relevant.
- ☐ If you are an at-risk professional (journalist, advocate, educator), let your workplace/union know—they may have escalation contacts & protocols.

Legal & Law Enforcement

Why: For persistent harassment, threats, or escalations.

→ Action:

- ☐ File police report; request case number (check earlier in the document).
- ☐ Share evidence log.
- ☐ Consult lawyer/digital rights orgs.
 - ☐ Possible need for a cease and desist letter
 - ☐ Possible need for restraining orders
- ☐ Pre-warn the police about swatting risk.

Emotional Support

Why: doxxing can be traumatic and emotionally draining.

→ **Action:**

- ☐ Lean on trusted people/therapists.
- ☐ Use EAP programs.
- ☐ Crisis line if overwhelmed (U.S.: **988**).
- ☐ You do **not** owe public/social media statements.



MEDIUM — Days to Weeks

Goal: Stabilize safety, reduce exposure, prioritize recovery

Protect Communications

Why: To get the support needed if they have escalation protocols and to protect others from possible escalations.

→ **Action:**

- ☐ Call carrier → confirm SIM-swap protections.
- ☐ Use secondary number (Google Voice).
- ☐ Secure messaging apps (Signal, WhatsApp).
- ☐ Use encrypted messaging platforms and VPN for sensitive comms

Privacy Cleanup & Opt-Outs

Why: doxxing can be traumatic and emotionally draining.

→ **Action:**

- ☐ Continue to remove data from broker sites.
- ☐ Scrub alumni lists/directories.
- ☐ Schedule quarterly “self-doxxing” audits (Google search, broker checks, reverse image searches).

Home & Daily Security

Why: Enhance physical security and sense of safety.

→ **Action:**

- ☐ Update locks, consider cameras/signage if not implemented already.
- ☐ Vary routines, get help with errands.
- ☐ Consider LLC property ownership and mail forwarding.

Ongoing Monitoring

Why: Monitor events for next steps and to allow you to take some breaks.

→ **Action:**

- ☐ Set Google Alerts for your name.
- ☐ [Keep logging incidents.](#)
- ☐ Assign a trusted person to help monitor mentions.

Emotional Care

Why: Doxxing and online harassment come in waves.

→ **Action:**

- ☐ Continue therapy/peer support.
- ☐ Consider limiting social media as possible.
- ☐ Frame digital hygiene & collective defense as ongoing recovery and taking back control.

Refine Relocation Plans

Why: Monitor events for next steps and to allow you to take some breaks.

→ **Action:**

- ☐ Keep go-bag updated.
- ☐ Identify safe havens (if needed).

- ☐ Add encrypted USB backups, updated contacts, pet/dependent plans.

LATER — Weeks to Months

Goal: Prevention, resilience, community readiness

Audit & Compartmentalize, Harden Accounts & Devices

Why: To reduce future risks.

Action:

- ☐ Separate emails for work/personal/public.
- ☐ Use aliases/pseudonyms.
- ☐ Rotate passwords, enforce 2FA.
- ☐ Keep systems and apps updated.
- ☐ Identity protection: Subscribe to ID-theft monitoring/legal services.

Community & Workplace Prep

Why: To reduce future risks.





Action:

- ☐ Update crisis response plans.
- ☐ Share protocols with peers.
- ☐ Encourage training on doxxing/swatting response.






Packing (go bag) for relocation

Emergency Go-Bag & Relocation Guide






Identification & Essentials

- ☐  ID, Passport, Driver's License
- ☐  Debit/credit card + some cash (small bills)
- ☐  Copies of important documents (digital + paper: lease, insurance, medical info)
- ☐  Keys (home, car, office if needed)



Digital Safety Kit

- ☐  Phone + charger + portable power bank
- ☐  Laptop or tablet (if needed for work/school)
- ☐  Passwords list in a secure app (or backup codes for 2FA)
- ☐  SIM card backup or alternate phone (if applicable)
- ☐  Headphones (for private calls/meetings and for comfort and music)





Clothing & Hygiene

- ☐  Change of clothes (neutral, non-identifiable)
- ☐  Extra underwear/socks
- ☐  Basic toiletries (toothbrush, toothpaste, soap, deodorant)
- ☐  Mask + sanitizer (if desired)
- ☐  Any daily medication

Safety & Privacy

- ☐  Hat, mask, sunglasses (to reduce recognition)
- ☐ If you have a dog, an unmarked collar/ leash
- ☐  Unmarked bag/backpack (avoid personal identifiers)

Comfort & Support

- ☐  Notebook + pen
- ☐  Small book / distraction item
- ☐  Comfort item (something grounding: scarf, token, small portable game etc.)
- ☐  Snacks + water bottle

Incident log sheet



Incident log sheet

[illegible]

Support Requests Templates



Doxxing Support Requests Templates

(Fill-in-the-blank style, ready to copy-paste or adapt)



Police Report / Law Enforcement

Script:

Hello, My name is And I am reporting an online harassment/doxxing incident.

- My personal information was posted: [address/phone/email/SSN/etc].
- I have received [direct threats / harassing messages / suspicious activity].
- I feel [unsafe at home / at risk of identity theft / targeted at work].
- Evidence: [screenshots, URLs, logs, voicemails].
- I request a case number and follow-up.

Name:

Date of Incident(s):

Preferred contact:



Platform / Host Takedown Request

Subject: Urgent — Doxxing/Harassment Content Removal

Hello, I am the subject of targeted doxxing/harassment.

The following content reveals my personal/private information:

- URL(s): [paste link(s)]
- Description: [posted address, phone, etc.]
- Date/time of posting: [insert]

This violates your harassment/doxxing policy.

Please remove it immediately and confirm action taken.

Thank you,

[Your Name]



Employer / Organization Notification

Email or message (preferably secure method)

Subject: Urgent — Safety Concern: Doxxing Incident

Dear [Relevant person/people],

I need to alert you to a current doxxing/harassment incident.

- My personal info (e.g., [address/phone]) has been posted online.
- I am experiencing [threats, harassment, account compromise].
- I have preserved evidence and reported it to [police/platforms].

Request:

- Please increase workplace security if possible.
- Provide safe escort/adjusted work arrangements if needed.
- Keep this confidential to minimize further exposure.

Thank you for your support,
[Your Name]

Credit Bureau Fraud Alert (U.S.)

Only through trusted portals: Place fraud alert or freeze credit ([Equifax Freeze](#), [Experian Freeze](#), [TransUnion Freeze](#)).

Hello, I am requesting a fraud alert / credit freeze due to identity exposure.

- Name:
- DOB:
- SSN (last 4 digits):
- Address:
- Phone/email:

Please confirm my credit file has been frozen / flagged.