CYBERCRAFT SECURITY

YOU’VE BEEN DOXXED

First 72 Hours Response Guide

Your personal information is now public.
Here’s exactly what to do in the next three days
to regain control.

Making people harder to find since 2023

00. IMMEDIATE RESPONSE

Stop. Breathe. Document.

If you're reading this, your personal information has been exposed online. The next 72 hours are critical. Your response must be methodical and calculated.

You Need This Playbook If:

- Your home address, phone number, or family details were posted online.
- Someone published your personal information to harass or threaten you.
- You're a public safety professional whose info became public after an incident.
- Your information appeared on a forum, social media, or doxxing site.

THE GOLDEN RULE

DO NOT ENGAGE. Do not reply to doxxers. Do not tweet at them. Do not email them. Any engagement confirms they've found the right person and that their tactics are working. Silence is your first defense.

HOUR 0-2: DOCUMENT EVERYTHING

Before you do anything else, create a permanent record. This evidence is critical for law enforcement and platform reports.

What to Capture:

- **Screenshot everything** - Posts, comments, profiles, URLs, timestamps.
- **Archive the pages** - Use archive.is or archive.org to create permanent snapshots.
- **Save metadata** - Note usernames, platform names, URLs, exact timestamps.
- **Don't engage** - No replies, no confrontations, no deletions yet (you need evidence).

> Create a dedicated folder: **"Doxxing Evidence [Date]"** - you'll need this for law enforcement and platform reports. Include everything: screenshots, archive links, timeline of events.

Assess the Damage:

Search for your information systematically:

Google yourself:

- Your full name + city
- Your full name + address
- Your phone number
- Your email addresses
- Your family members' names + your name

Check data broker sites:

- Whitepages.com, Spokeo.com, BeenVerified.com, PeopleFinder.com, FastPeopleSearch.com

HOUR 2-6: THREAT ASSESSMENT

Answer these questions honestly to determine your response strategy.

IMMEDIATE PHYSICAL SAFETY THREAT?

- Are there specific threats of violence?
- Has anyone shown up at your home or workplace?
- Are you in a domestic violence situation?
- Are you a public figure or controversial figure?

If YES to any: Contact local law enforcement immediately. Request extra patrol of your residence. Consider temporary relocation.

Is This Targeted or Opportunistic?

- One person or coordinated group?
- Specific vendetta or random attack?
- Ongoing campaign or single incident?

Organized campaigns require more aggressive countermeasures than opportunistic leaks.

HOUR 6-12: DIGITAL LOCKDOWN

Assume your accounts are the next target. Lock them down immediately.

Multi-Factor Authentication (MFA)

If you don't have MFA enabled, enable it now on all critical accounts.

> **AVOID SMS 2FA**
>
> If your phone number is exposed, you're vulnerable to SIM swapping. Use an authenticator app (Authy, Google Authenticator) or hardware key (YubiKey) instead of SMS.

Password Hygiene

- **Change primary passwords:** Email, banking, and social media.
- **Use a password manager:** Don't reuse passwords across sites.
- **Force logout everywhere:** Use the "Log out of all sessions" option available on most platforms.

Privacy Settings Audit

Switch all social media accounts to **Private** immediately:

- **Facebook:** Friends only; hide friend lists.
- **Instagram:** Private account; remove unknown followers.
- **Twitter/X:** Protect your tweets.
- **LinkedIn:** Restrict profile visibility to connections only.

HOUR 12-18: PHYSICAL SAFETY

If your home address has been leaked, digital security is secondary to physical safety.

Home Security Check

- **Inform household:** Let residents know about the situation calmly.
- **Lock doors/windows:** Ensure all entry points are secured.
- **Cameras:** Ensure Ring/Nest/CCTV are active and recording.
- **Mail:** Be cautious of unexpected packages.

Swatting Prevention

CONTACT LOCAL POLICE

Call your local police department's **non-emergency line**. Inform them you've been doxxed and there's a risk of "swatting." Ask to have a note placed on your address file.

Alternate Location

If credible threats of violence are made, leave. Stay with a friend or at a hotel. Pay with cash or a card not linked to your location history if possible.

HOUR 18-24: FINANCIAL LOCKDOWN

Contact Your Bank

- Inform the fraud department.
- Add a verbal password/PIN for phone support verification.
- Monitor for micro-transactions.

Freeze Your Credit

Freeze your credit at all three bureaus. This is free by federal law and prevents unauthorized accounts:

- **Equifax:** equifax.com/personal/credit-report-services
- **Experian:** experian.com/freeze
- **TransUnion:** transunion.com/credit-freeze

HOUR 24-48: PLATFORM REPORTING

Report Doxxing Posts

Report content specifically as ”Personal Information” or ”Doxxing.”

- **Reddit:** Report ”Sharing personal information.”
- **Twitter/X:** Use the dedicated private information form.
- **Google Search:** Submit a request at *support.google.com/websearch/answer/9673730* to remove PII from search results.

Data Broker Removal

Priority removals (refer to IntelTechniques.com for detailed steps):

1. Spokeo.com
2. Whitepages.com
3. Intelius.com
4. LexisNexis.com

HOUR 60-72: LONG-TERM STEPS

Employer and Family

Brief your employer and family. Use a script: *”I am the victim of a targeted harassment campaign. I wanted to alert you in case the harassers contact the company/you.”*

Law Enforcement

File a police report if there are threats or stalking. Bring your evidence folder.

72-HOUR CHECKLIST

□ Hour 0-2: Evidence folder created.

□ Hour 6-12: MFA enabled; passwords changed.

□ Hour 12-18: Social media private; police alerted for swatting.

□ Hour 18-24: Credit frozen at all bureaus.

□ Hour 24-48: Platform reports and Google removal requests.

□ Hour 60-72: Family briefed; long-term OpSec plan initiated.

NEED PROFESSIONAL HELP?

contact@cybercraftsecurity.com
cybercraftsecurity.com