

Personal Incident Response Checklists

Incident Response Checklist (First 30 Minutes)

Immediate Actions

- ☐ **STOP** - Don't continue using compromised accounts/devices
- ☐ **Document everything** - Screenshot with timestamps before anything changes
- ☐ **Assess safety** - Is there an immediate physical threat to you?
- ☐ **Preserve evidence** - Don't delete anything, even if embarrassing
- ☐ **Activate secure communications** - Switch to Signal/encrypted channels
- ☐ **Brief assessment** - What type of incident appears to be occurring?

Initial Notifications (within 1 hour)

- ☐ Technical support contacted (if needed)
- ☐ Legal counsel alerted (if sensitive data involved)

Personal Security Incident Checklist

If You're Being Targeted

- ☐ **Screenshot all threats/harassment** with full URLs and timestamps
- ☐ **Don't engage** with attackers on social media or email
- ☐ **Change passwords** on all important accounts immediately
- ☐ **Enable 2FA** on all accounts if not already active
- ☐ **Review recent account activity** for signs of unauthorized access

- ☐ **Alert personal contacts** about potential impersonation
- ☐ **Check data broker sites** for your personal information
- ☐ **Consider temporary social media break** if harassment is ongoing
- ☐ **Document impact** on work, sleep, mental health for potential legal action
- ☐ **Reach out for support** - to mental health resources and trusted colleagues

Evidence Collection for Personal Incidents

- ☐ Full screenshots (not crops) of all harassment
- ☐ Email headers saved, not just message content
- ☐ URLs and usernames of accounts involved
- ☐ Dates/times of all incidents with time zones
- ☐ Names of any witnesses
- ☐ Impact documentation (missed work, medical visits, etc.)

Incident Prioritization Matrix

Critical (Address Immediately):

- ☐ Social security numbers or personal ID info exposed
- ☐ Medical information exposed
- ☐ Any information about minors exposed

Low Priority (Address Within 48 Hours):

- ☐ Minor harassment targeting you
- ☐ Attempted attacks that failed
- ☐ Suspicious activity with no clear impact

Communication Protocol Checklists

External Communications Decision Tree

DO NOT contact external parties until you've answered:

- ☐ Do I understand what happened?
- ☐ Have I stopped the immediate problem?
- ☐ Do I have legal advice if needed?
- ☐ What is my key message?

Media Inquiries:

- ☐ Don't speculate about cause or scope
- ☐ Focus on what you're doing to address it

Groups and Allies You Work With:

- ☐ Alert them if they might be affected
- ☐ Share technical indicators (IPs, domains) if relevant
- ☐ Request additional resources if needed

Law Enforcement Contact:

- ☐ Consult legal counsel first
- ☐ Prepare incident timeline and evidence
- ☐ Understand what you're asking for (investigation vs. advice)

Evidence Preservation Checklist

Digital Evidence

- ☐ **Screenshots with timestamps** of all relevant activity
- ☐ **Full email headers** saved, not just message content
- ☐ **Browser history** exported before clearing
- ☐ **Account activity reports** downloaded
- ☐ **Social media posts** archived with metadata

Chain of Custody Documentation

For each piece of evidence:

- ☐ **What** - Specific description of evidence

- ☐ **When** - Date and time collected (with time zone)
- ☐ **Who** - Name of person collecting
- ☐ **Where** - Location/account/device evidence came from
- ☐ **Why** - Relevance to the incident
- ☐ **How** - Method used to collect/preserve
- ☐ **Chain** - Who has handled it since collection

Recovery and Lessons Learned Checklists

Device and Account Recovery

- ☐ **Malware removed** from all affected devices
- ☐ **Passwords changed** on all potentially affected accounts
- ☐ **Security software updated** on all devices

Post-Incident Review (Within 1 Week)

- ☐ **Timeline documented** - What happened when?
- ☐ **Root cause identified** - How did this happen?
- ☐ **Lessons learned captured** - What would I do differently?

Prevention Improvements

- ☐ **Insurance claims filed** if applicable

Quick Reference: When to Escalate

Get Help Immediately

- ☐ Any threat of physical violence
- ☐ Suspected criminal activity (hacking, stalking, threats)

- ☐ Social security numbers or payment card data compromised
- ☐ Media already reporting on the incident

Get Help Within 24 Hours

- ☐ Email account compromised
- ☐ Suspected state-sponsored or sophisticated attack

Monitor and Handle Yourself

- ☐ Minor social media account compromise
- ☐ Suspicious but unsuccessful login attempts

Emergency Contacts Template

Keep this information readily accessible and secure:

Support Contacts

- **Legal Counsel:** _____ (Phone: _____, Available: _____)
- **Technical Support:** _____ (Phone: _____, Signal: _____)
- **Mental Health Support:** _____ (Phone: _____, Crisis Line: _____)
- **Groups/Allies:** _____ (Phone: _____, Signal: _____)

Emergency Services

- **Local Law Enforcement:** _____ (Phone: _____)
- **FBI Field Office:** _____ (Phone: _____)
- **Crisis Counseling:** _____ (Phone: _____)

Key Account Recovery Information

- **Email Provider:** _____ (Account: _____, Phone: _____)
- **Social Media:** _____ (Account: _____, Recovery: _____)

Remember: Print and store this securely. Review and update every 6 months.
