

Incident Response Cheat Sheets: 5 Critical Steps for Digital Emergency Response

Follow these steps immediately when an incident occurs:

Step 1: STOP & DOCUMENT

- STOP using the affected account or device immediately
- Don't panic—take a breath and think clearly
- Take screenshots with full URLs and timestamps (not crops)
- Document what happened, when you noticed, what you clicked/saw
- Preserve evidence—don't delete anything, even if embarrassing
- Save email headers, not just message content

Why this matters: Your first action is to preserve evidence. Don't inadvertently delete information that can help you recover.

Step 2: ACTIVATE YOUR RESPONSE TEAM

Call contacts in this order (within 1 hour):

1. Incident Commander
2. Technical Lead
3. Communications Lead
4. Executive Contact

Template message: "We have a security incident involving [brief description]. I've documented what happened. Need immediate coordination—switching to Signal for secure comms."

- **Switch to Signal or encrypted channels immediately**

Step 3: SECURE THE SCENE

Immediate containment actions:

- Change passwords for affected accounts from a clean device
- Enable 2FA on all accounts if not already active

- Disconnect compromised devices from network (unplug ethernet/turn off WiFi)
- Review recent account activity for unauthorized access
- Alert personal contacts about potential impersonation

What NOT to do:

- Don't restart or shut down compromised systems
- Don't delete suspicious files or emails
- Don't communicate about the incident over potentially compromised channels

Step 4: ASSESS THE SCOPE

Key questions to answer:

- What data was accessed or compromised? (donor info, strategies, personal data)
- How many people's data may be affected?
- What types of data? (contact info, financial, sensitive personal data)
- Is the incident contained or ongoing?
- Can we fix it ourselves or do we need external help?
- Are other organizations or coalition partners affected?

Step 5: BEGIN RECOVERY

- Restore systems from clean backups
 - Apply security updates and patches
 - Review and strengthen access controls
 - Monitor for continued threats
 - Notify affected individuals if required by law
 - File required regulatory reports
 - Update Board and stakeholders as appropriate
-