Digital Emergency Response: 5 Critical Steps

Print this out and keep it handy for when things go wrong, and in case you're locked out of your accounts.

This checklist applies to incidents like:

- **Doxxing attacks** - Your home address, phone number, or family information published online
- **Account compromises** - Someone gains access to your email, social media, or organizational accounts
- **Phishing attacks** - Malicious emails targeting you or your organization's staff
- **Harassment campaigns** - Coordinated online abuse, threats, or intimidation
- **Data breaches** - Donor information, campaign strategies, or sensitive documents exposed
- **Website attacks** - Your organization's website hacked, defaced, or taken offline
- **Ransomware** – Your organization's digital assets frozen by an attacker
- **Surveillance detection** - Discovering you're being monitored at events or through digital means
- **Impersonation** - Someone creating fake accounts or profiles pretending to be you/your org
- **Legal threats** - Receiving SLAPP suits, subpoenas, or aggressive legal demands
- **Physical security concerns** - Threats that cross from digital to real-world safety

Step 1: KNOW WHO TO CALL

Make a list of important contacts. Set up a Signal group for your core team.

Incident Commander (Name/Phone/Signal)

- Overall response coordination
- External communications authorization
- Resource allocation decisions

Technical Lead (Name/Phone/Signal)

- System analysis and containment
- Evidence collection
- Recovery planning

Communications Lead (Name/Phone/Signal)

- Media relations and holding statements
- Staff notifications
- Stakeholder updates

Legal Contact (Name/Phone/Available hours)

- Law enforcement coordination
- Legal compliance (breach notification requirements)
- Evidence handling guidance

Executive Contact (Name/Phone/Signal)

Support Coordinator (Name/Phone/Signal)

- Staff wellbeing and mental health support
- Community impact assessment
- Coalition partner notifications

External Support Contacts:

- Technical Support: (Company/Phone/Signal)
- Mental Health Support: (Provider/Phone/Crisis line)
- Coalition Partners: (Key allies/Phone/Signal)

Step 2: STOP AND DOCUMENT

What to do immediately:

- **STOP using** the affected account/device
- **Don't panic**! Take a breath and think clearly
- **Document everything** you remember:
  - What happened? When did you first notice?
  - What did you click/download/see?
  - Take screenshots with full URLs and timestamps (not crops)
  - Email headers saved, not just message content
  - Names of any witnesses

For doxxing/harassment incidents:

- Screenshot all threats/harassment with full URLs and timestamps
- Don't engage with attackers on social media or email
- Document impact on work, sleep, mental health for potential legal action

Why this matters: Your first action is to preserve evidence. You do not want to inadvertently delete information that can help you recover from this attack.

Step 3: ACTIVATE YOUR PHONE TREE

Call in this order (within 1 hour):

1. **Incident Lead**
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."

Step 4: 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 signs of unauthorized access
- **Check data broker sites** for your personal information
- **Alert personal contacts** about potential impersonation

For organizational incidents:

- **Identify affected systems** - What accounts/systems are compromised?
- **Review admin access** - Check all administrative accounts
- **Audit recent changes** - What was modified in the last 30 days?
- **Check backup integrity** - Are backups clean and recent?

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 5: ENGAGE SYSTEMS AND PRACTICES

Assessment Questions:

- Data impact: What data might be compromised? Donor info, strategies, personal data?
- Scope: Are other organizations affected?
- Legal obligations: Do we need to notify supporters/donors?
- Notification requirements: What legal reporting requirements apply?

External Communications:

Do NOT contact external parties until you've answered:

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

Media Inquiries:

- Refer to designated spokesperson only
- Use pre-approved holding statements
- Don't speculate about cause or scope
- Focus on what you're doing to address it
- Emphasize commitment to security and transparency

Escalation Matrix:

Immediate Escalation Required:

- Any threat of physical violence
- Suspected criminal activity (hacking, stalking, threats)
- Social security numbers or payment card data compromised
- Systems completely down/inaccessible
- Coordinated attack affecting multiple organizations
- Media already reporting on the incident

Escalate Within 24 Hours:

- Email systems compromised
- Donor information potentially accessed

- Website defaced or hijacked
- Staff personal information exposed
- Suspected state-sponsored or sophisticated attack

Revision #12
Created 7 November 2025 18:06:21 by Josh
Updated 7 November 2025 18:22:44 by Josh