QUICK REFERENCE

Incident Response Quick Reference

The first 60 minutes after a suspected breach — who to call, what to preserve, what not to touch.

Recognize an Incident

Treat any of these as a security incident until proven otherwise: suspicious email to many employees, computer behaving strangely, files you cannot access, lost laptop with customer data, unauthorized charges, locked out of accounts, fake emails appearing to come from leadership, website down or defaced, customers reporting strange messages. **When in doubt, treat it as an incident.**

Severity Levels

✓ **CRITICAL — Act now:** Ransomware actively encrypting, active intrusion in progress, customer card data confirmed stolen, major systems down. Call everyone, work after hours.

✓ **HIGH — Same day:** Confirmed malware, unauthorized access, lost device with sensitive data, large fraudulent transfer. Management notified, response team activated.

✓ **MEDIUM — Next business day:** Policy violation, possible data exposure, single-account compromise with limited damage. Investigate and document.

✓ **LOW — Log and monitor:** One suspicious email, failed attack attempt, general concern.

First 30 Minutes — Detect & Contain

Step 1: STOP and ASSESS (2 minutes)

- What happened? Is it still happening?
- How many computers or people affected?
- What data might be involved?

Step 2: CONTAIN (5 minutes)

- **Ransomware / malware:** Unplug infected computers from the network. Do NOT turn them off — that destroys evidence.
- **Account compromise:** Change the password, log out all sessions, review recent activity.
- **Lost device:** Remote-wipe if possible, rotate passwords for accounts on that device.
- **Fraudulent transfer:** Call the bank immediately. Every second matters.

Step 3: NOTIFY (5 minutes)

- Call your owner / incident commander
- Call IT support or your security consultant
- Do NOT post on social media. Do NOT discuss over email — email may be compromised.

Step 4: DOCUMENT (ongoing)

Start writing everything down: time detected, what you saw, what you did, who you told. Keep notes throughout the entire response — you will need them for insurance, legal, and post-incident review.

First 24 Hours — Assess & Investigate

- **Call in help:** IT / security consultant, cyber insurance, lawyer, FBI for major incidents
- **Investigate:** Exactly what happened, how, what data, who is affected, is the threat still live

- **Preserve evidence:** Do not delete anything. Screenshot everything. Save logs. Keep infected systems isolated, not cleaned.

Keep This Contact List Printed and Posted

- ✓ Owner / Incident Commander: [Name, mobile, email]
- ✓ IT / Security Support: [Name or firm, phone, email]
- ✓ Lawyer: [Name, firm, phone]
- ✓ Cyber Insurance: [Carrier, policy number, 24-hr claims phone]
- ✓ Bank (to stop fraudulent transfers): [Direct phone]
- ✓ FBI IC3 for cybercrime reporting: ic3.gov
- ✓ Web hosting provider: [Company, support phone]

What NOT to Do During an Incident

- ✗ Do not try to fix it yourself if you are not technical
- ✗ Do not turn off computers that may hold evidence
- ✗ Do not delete files or logs — even if they look suspicious
- ✗ Do not pay ransom without consulting FBI and insurance
- ✗ Do not notify customers before you know what actually happened
- ✗ Do not post on social media
- ✗ Do not ignore it and hope it goes away

The Best Preparation: Tabletop Exercise

Once a year, gather your team for a one-hour tabletop drill. Present a scenario — "Monday morning, Sarah's computer is showing a ransomware note." Walk through your plan step by step. You will find gaps: missing phone numbers, unclear roles, outdated contacts. Fix them now, not in the middle of a real incident.