Incident Response Plan Template

Template · Decisions Made Before The Crisis. Print This. Pin It Up.

When a compromise happens, you don't want to be making decisions under stress. Fill in this template now, store it where you'll find it under pressure, and revisit annually.

Contact Card (Fill In Now)

My primary contact (spouse, IT person, lawyer, etc.): _____

Bank fraud line (back of card): _____

Credit card fraud line: _____

Cyber insurance carrier (if any): _____ · Policy #: _____

FTC report URL: reportfraud.ftc.gov · IC3: ic3.gov

IRS Identity Theft: 800-908-4490

First Hour — Triage

1. **Disconnect** any obviously compromised device from Wi-Fi and Ethernet.
2. **Don't power off** immediately if forensics matter — preserves volatile evidence.
3. **Identify scope:** what was accessed, what was changed, what was taken.
4. **Document everything:** timestamps, screenshots, error messages, observed activity.
5. **Stop the bleeding:** change passwords from a CLEAN device. Email first, then bank.

First 24 Hours — Containment

- Email password rotated. MFA enabled (or moved to authenticator app).
- Bank / brokerage accounts: passwords rotated, login alerts enabled, transactions reviewed.
- Credit frozen at all 3 bureaus.
- Key services notified: bank, employer (if work device), email provider.
- Devices isolated and scanned with reputable AV.
- Logs preserved (don't 'clean up' yet — investigators may need them).

First Week — Recovery

- [ ] FTC identity theft report filed at reportfraud.ftc.gov.
- [ ] Police report filed (if loss > $1,000 or identity theft).
- [ ] All Tier-1 account passwords rotated and unique.
- [ ] MFA migrated to authenticator app or hardware keys on critical accounts.
- [ ] Credit reports pulled from all 3 bureaus and reviewed line by line.
- [ ] Recovery codes regenerated and stored offline.
- [ ] Old phone wiped if SIM swap was involved.
- [ ] Customers / employees notified (if SMB context).

Reporting Requirements (Fill In)

Industry-specific compliance (HIPAA / PCI / state laws): _____

Customer notification timeline (e.g., 72 hours under GDPR): _____

Insurance claim deadline: _____

Lessons Learned (After The Dust Settles)

Root cause: _____

What worked in our response: _____

What we'd change next time: _____

New defences added: _____

Sign-Off

Incident closed by: _____ · Date: _____