CYBERCLAN™

What to Do If Your Business Is Hacked:

A 2026 Crisis Checklist

Under Attack? Guaranteed 15 minute response time.

US/CAD: 1 800 762 3290 **UK:** 0800 368 8731 **AUS:** 61 1800 413 128

It's 2 a.m., or worse, 2 p.m. on a Tuesday, and someone has just told you: "We've been hacked." Maybe it's ransomware locking every workstation. Maybe it's a customer emailing to ask why their card was charged twice by someone in another country. Whatever the trigger, you're now the decision-maker in an active cyber attack, and every hour matters.

If you've searched "company hacked now" or "what to do if hacked," you're not looking for theory. You need cyber attack response steps you can act on immediately, the kind that protect your business, your customers, and your legal standing in the first three days. That's what this checklist is for.

Why the First 72 Hours Decide the Outcome

Regulators, insurers, and courts don't judge you on whether you got hacked, they judge you on how you responded. Delayed containment lets attackers spread further. Delayed notification can turn a manageable incident into a regulatory penalty. Delayed communication turns a technical problem into a trust problem with customers and employees.

The first 72 hours aren't about fixing everything, rather it's about stopping the bleeding, preserving evidence, and making the right calls in the right order. To help you make the right choices, we put together a checklist you can use.

The First 72 Hours: Your Action Checklist

Hour 0-2: Stop the Damage, Don't Destroy the Evidence

1. Disconnect, don't power off. Pull affected machines off the network (unplug Ethernet, disable Wi-Fi) rather than shutting them down. Powering off can destroy volatile memory that forensic investigators need to trace the attacker's path.

2. Activate your incident response plan, or your phone tree if you don't have one. Identify who's in charge of the response right now. If you don't have a formal plan, designate one person (often the CTO, IT lead, or CEO in a small company) as incident commander so decisions don't stall waiting on consensus.

3. Call your cyber insurance carrier immediately. Most policies require notification within a specific window, and many insurers have a panel of pre-approved forensic firms and breach counsel; using an unapproved vendor can jeopardize coverage.

4. Do not engage the threat actor. Victims might log into the leak site portal, click the chat, and start talking. That destroys leverage, starts the actor's clock, and can prejudice the insurance position. Preserve the ransom note, do not delete it, do not respond without professional negotiation support.

5. Engage outside counsel who specializes in data breaches. Do this before you engage a forensics firm if possible. Communications routed through legal counsel can be protected under attorney-client privilege, which matters enormously if litigation follows.

6. Preserve logs now. Export firewall logs, VPN logs, authentication logs, and endpoint detection data before retention windows roll over or systems get rebuilt.

7. Isolate backups. Confirm your backups are offline, immutable, or otherwise unreachable from the compromised network. This is often the single factor that determines whether you pay a ransom or restore from backup.

8. Bring in a third-party digital forensics and incident response (DFIR) firm. Unless you have a mature internal security team, don't try to investigate this yourselves — you risk destroying evidence or missing the attacker's persistence mechanisms.

Hour 2-12: Contain and Assess

9. Change credentials for all privileged accounts — domain admins, cloud console access, VPN, email admin — starting with anything that shows suspicious login activity. Assume any password the attacker could have touched is compromised.

10. Force a password reset and revoke active sessions for all users, not just admins, if there's any sign of broad compromise (phishing campaign, credential-stuffing, or unclear scope).

11. Enable or verify multi-factor authentication on every account that supports it, especially email and remote access — attackers often try to re-enter through the same door.

12. Identify what type of incident you're dealing with. Ransomware, business email compromise, data exfiltration, and a defaced website all demand different next steps — your forensics team should confirm this early so you're not guessing.

13. Start an incident log now. Record every action taken, by whom, and at what time. This becomes critical for regulators, insurers, and your own after-action review.

Hour 12-24: Scope the Blast Radius

14. Determine what systems and data were accessed. Work with forensics to map which servers, applications, and databases were touched — this drives your legal notification obligations.

15. Identify whether personal data was involved. Customer names, Social Security numbers, health data, payment card data, or employee records trigger different (and often overlapping) breach notification laws depending on your jurisdiction and industry.

16. Check contractual notification obligations. Many B2B contracts and vendor agreements include breach notification clauses with tighter deadlines than the law requires — review these now, not after the legal deadline passes.

17. Loop in your cyber insurance-approved PR or crisis communications advisor if the incident is likely to become public or affect customers. How you communicate in the first days shapes the narrative for months.

18. Notify your board or ownership with a factual, non-speculative update: what happened, what's being done, what's still unknown.

Hour 24-48: Notify and Communicate

19. Determine your legal notification deadline. In the U.S., most state breach notification laws range from "without unreasonable delay" to a hard cap (commonly 30–60 days), but sector-specific rules (HIPAA, GLBA, PCI DSS) can require notification within 72 hours or less. Confirm your specific deadline with counsel immediately — don't rely on general knowledge, since these rules are updated frequently.

20. Notify law enforcement if appropriate. For ransomware or significant financial fraud, contact the FBI's Internet Crime Complaint Center (IC3) or your local field office. This is often required for insurance claims and can assist recovery in fraud cases.

21. Draft (but hold) your external notification. Work with counsel and comms to prepare customer, employee, and regulator notifications so they're ready to send the moment scoping is confirmed — but don't send prematurely with inaccurate details that you'll have to walk back.

22. Notify affected employees and vendors who may need to change their own credentials or watch for phishing attempts referencing your company.

Hour 48-72: Stabilize and Plan Recovery

23. Begin remediation of the root cause, not just the symptoms. If it was a phishing email, fix email filtering and run awareness training. If it was an unpatched server, patch every instance, not just the one that was hit.

24. Rebuild compromised systems from known-clean images or backups rather than simply removing malware — attackers frequently leave backdoors that a surface cleanup misses.

25. Set a controlled, verified restoration timeline. Don't rush systems back online without forensic sign-off that they're clean; reconnecting a compromised machine can restart the whole incident.

26. Finalize and send required notifications to regulators, affected individuals, and partners per the deadlines established with counsel.

27. Schedule a post-incident review for one to two weeks out, once the immediate crisis has passed, to document lessons learned and update your incident response plan.

Should You Pay a Ransom?

If this is a ransomware incident, resist the urge to decide alone or decide fast. Consult your insurer, legal counsel, and forensics team — paying a ransom carries legal risk (some sanctioned entities are illegal to pay), doesn't guarantee data recovery, and doesn't guarantee the attacker won't leak stolen data anyway. This decision should be made deliberately, with full information, not in a panic on hour one.

What Not to Do in the First 72 Hours

A few mistakes are common enough to call out directly:

- **Don't pay the ransom before consulting legal and insurance.** It may be illegal, futile, or unnecessary.
- **Don't post publicly before you know what happened.** A premature statement with wrong facts damages credibility more than a short delay.
- **Don't let IT "clean up" and reconnect systems before forensics has imaged them.** You'll lose the evidence needed to understand scope and satisfy regulators.
- **Don't assume it's over once systems are back online.** Attackers who established persistence can return weeks later if root causes weren't fully remediated.

After the First 72 Hours

Once the immediate crisis stabilizes, the real work of recovery begins: full forensic reporting, regulatory follow-up, customer trust rebuilding, and — critically — building or refining an incident response plan so the next event (and there's often a next event) doesn't start from zero. If you didn't have a written incident response plan before this happened, creating one is the single highest-value action you can take once the dust settles.

Being hacked is not a reflection of failure — it's increasingly a matter of when, not if, for any business with a digital footprint. What separates companies that recover cleanly from those that don't is not whether they got attacked, but whether they had a clear, rehearsed plan for exactly this moment. If this is your first time working through an active incident, keep this checklist bookmarked — and once you're through it, use the experience to build the incident response plan you wish you'd had going in.