IDENTITY DEFENSE 247

What to Do in the First 72 Hours of a Cyber Incident

A plain-English guide for small business owners who need to slow the damage, protect evidence, and recover with confidence.

The simple goal

You do not need to solve everything at once. Your first job is to slow the incident down, protect people and evidence, and get the right help.

Public customer guide | Version 1.0 | October 31, 2026

Start here

A cyber incident can be frightening, but a calm sequence matters more than technical expertise. This guide turns the first 72 hours into a practical plan you can follow with your team, your IT provider, your insurer, and your legal advisor.

The five-step path

Step	What you are trying to do
1. Stabilize	Stop the incident from spreading where you safely can.
2. Assign	Name one decision lead and one person to keep the record.
3. Preserve	Keep evidence, logs, messages, and a timeline.
4. Recover	Restore systems in a careful order and watch for reinfection.
5. Improve	Close the gaps that allowed the incident to happen.

What counts as an incident?

Signal	Why it matters
Suspicious email or password reset	It may be the first sign of account takeover.
Unexpected login or disabled account	A valid account may now be controlled by someone else.
Malware or ransomware message	The incident may already be active.
Missing data or changed payment instructions	The business may be exposed to fraud or data loss.
Supplier or customer reports a problem	A trusted account may be impersonating your business.

If ransomware is active now

Isolate affected systems, call your incident support contact, preserve the ransom note and logs, and do not rush to pay. Your insurer and legal advisor should be involved early.

First 15 minutes: stabilize the situation

Your goal is not to prove exactly what happened. Your goal is to slow the incident down and prevent avoidable damage.

Do these things first

- Confirm the concern is real enough to act on.
- Isolate affected computers from the network if you can do so safely.
- Do not power off a machine unless your response advisor tells you to.
- Reset passwords for affected accounts from a clean device.
- Sign out active sessions for affected email, banking, cloud, and remote access accounts.
- Open a written incident log with the current time and what you know.
- Use a separate communication channel if you suspect business email is compromised.

Keep evidence

Do not delete suspicious emails, files, logs, ransom notes, or browser history. These may be needed by your insurer, legal advisor, response provider, or law enforcement.

Do not do these things

- Do not discuss the incident publicly before you have a clear message.
- Do not wipe or reimage systems before evidence is preserved.
- Do not pay a ransom or transfer money without legal and insurer guidance.
- Do not rely only on the affected inbox for incident communication.

First hour: assign leadership and open support

Small businesses do not need a large response team. They need clear ownership and fast access to the right help.

Assign four roles, even if one person holds more than one

Role	Responsibility
Decision lead	Owns the response, approves downtime, and speaks with leadership.
Technical lead	Coordinates your IT provider, response support, account resets, and isolation steps.
Record keeper	Maintains timeline, actions, contacts, costs, and evidence locations.
Communication and risk lead	Handles legal, insurer, customer, and internal communication decisions.

Contact the right people early

- Internal decision maker and technical contact
- Cyber-insurance carrier or broker
- Legal counsel when personal, financial, health, or client data may be involved
- Incident-response support provider
- Relevant authorities, such as CISA and FBI IC3
- Key customers or partners if their data or payments may be affected

Estimate severity without overthinking it

Level	What it may look like	Immediate posture
Low	Suspicious message, isolated exposure, or one unusual account action	Investigate, reset affected credentials, and monitor closely.
Medium	Confirmed account takeover, malware on one device, or unusual payment activity	Isolate, preserve evidence, involve IT and insurer.
High	Ransomware, multiple systems affected, data theft, or business operations stopped	Activate full response support, legal counsel, insurer, and executive communication.

Use a clean communication channel

If business email may be compromised, move the response team to a separate phone thread, alternate chat workspace, or in-person channel.

Hours 4 to 24: contain the incident

Containment means limiting what the attacker can still reach. Move carefully so you do not destroy evidence or create new openings.

Contain accounts first

- Reset passwords for affected and high-risk accounts.
- Revoke active sessions, app permissions, and recovery methods where possible.
- Check for new mail-forwarding rules, delegates, or auto-forward addresses.
- Remove unknown admin users and unknown recovery contacts.
- Require a second verification step for sensitive accounts going forward.

Contain systems second

- Isolate affected computers or servers from the network.
- Disable remote access that is not required for response work.
- Apply emergency patches only when they will not interfere with evidence collection.
- Block known malicious senders, domains, or IP addresses at the network edge.
- Increase monitoring for unusual sign-ins, outbound email, and file changes.

Preserve what matters

Evidence	Why it helps
Emails and headers	Shows who sent the message and how it reached you.
Sign-in logs	Shows where and when access occurred.
Ransom note or extortion message	May help responders identify the threat.
Timeline of actions	Supports insurer, legal, and law-enforcement conversations.
Screenshots and exported logs	Preserves details that may disappear later.

Communicate clearly

Good communication reduces panic and prevents second-order mistakes. Keep it factual, short, and approved by the right people.

Internal employee message

Suggested wording

We are investigating a security concern. Do not click unexpected links, approve payment changes, or discuss this externally. If you notice unusual sign-in prompts, password resets, or missing messages, report them to the response lead immediately.

Customer or partner message

Suggested wording

We are investigating a security matter that may affect part of our operation. We are taking precautionary steps, reviewing the situation with qualified support, and will share updates when we have confirmed information. If you receive an unusual request from us, verify it through a known contact before acting.

What to track in your incident log

- Time the issue was discovered and who reported it
- Systems, accounts, and data possibly involved
- Actions taken and who approved them
- Contacts notified and when
- Costs, downtime, missing messages, or suspicious changes
- What remains unknown

Hours 24 to 72: recover safely

Recovery should be deliberate. Bringing everything back too quickly can give the attacker another opening.

Restore in this order

- Confirm the attacker no longer has valid access paths.
- Restore the most important business functions first.
- Use known-clean backups where restoration is needed.
- Re-image heavily affected devices instead of trying to clean every trace manually.
- Bring systems online one group at a time, not all at once.
- Monitor sign-ins, outbound messages, file changes, and payment activity for at least 48 hours after recovery.

Before you call the incident closed

Question	Pass condition
Are affected accounts secured?	Passwords reset, sessions revoked, forwarding rules removed, and recovery paths verified.
Are malicious access paths closed?	Unknown users, apps, tokens, and remote access removed or controlled.
Are systems clean enough to trust?	Known-malware removed, affected devices rebuilt where needed, and logs reviewed.
Are backups usable?	Restore test completed and evidence retained.
Can leadership explain what happened?	Timeline, decisions, costs, notifications, and open risks documented.

Do not rush the all-clear

If the same account, device, or behavior reappears, treat it as a continued incident rather than a separate nuisance.

After the first 72 hours: learn and strengthen

The incident is not truly over until the business understands how it happened and what will be different next time.

Hold a short after-action review

- What was the first warning sign?
- Which account, device, or process opened the door?
- What slowed the response?
- What worked better than expected?
- Which decisions need to be documented for insurance or legal reasons?
- What should be fixed in the next 30 days?

Common improvements after an incident

Area	Practical improvement
Identity	Require stronger sign-in protection for email, finance, cloud, and administrator accounts.
Recovery	Test backups and document the recovery order before you need it again.
Payments	Require a second verified channel for vendor, payroll, and banking changes.
Monitoring	Watch exposed emails, domain trust issues, and account-risk signals continuously.
People	Give staff a simple way to report suspicious messages without blame.
Vendor risk	Review who has access, what they can reach, and how they are monitored.

Printable first-response checklist

Use this page as a quick reference during an incident.

Time	Action
Now	Confirm the issue is real enough to act on.
Now	Isolate affected devices if safe.
Now	Reset affected passwords from a clean device.
Now	Open an incident log and assign a decision lead.
15 minutes	Preserve emails, logs, messages, and screenshots.
15 minutes	Move response communication to a clean channel.
1 hour	Call insurer, legal counsel, and response support as needed.
1 hour	Classify severity and identify critical systems.
4 hours	Revoke sessions, unknown admins, and unsafe access paths.
4 hours	Document all actions, approvals, and open questions.
24 hours	Contain systems, patch safely, and monitor activity.
24 hours	Prepare factual internal and external messages.
72 hours	Restore critical systems in stages from trusted sources.
72 hours	Verify clean access and monitor for reinfection.
After	Hold after-action review and assign 30-day improvements.

Helpful reporting and response resources

Use these channels when the situation calls for broader support. Save the links before an incident happens.

Resource	When to use	Link
CISA #StopRansomware	Ransomware guidance, reporting, and response resources.	https://www.cisa.gov/stopransomware
FBI IC3	Report internet-enabled crime, fraud, and ransomware.	https://www.ic3.gov/
CISA Report	Share cyber incidents and request assistance.	https://www.cisa.gov/report
Cyber-insurance carrier	Notify early when coverage, response support, or claims may be involved.	Use the number in your policy
Legal counsel	Involve when sensitive personal, financial, health, or client data may be affected.	Use your approved legal contact

How Identity Defense 247 helps

Identity Defense 247 helps small businesses see exposed email and domain risks, understand what matters, and take practical next steps before an incident becomes a business shutdown. If you are facing an active incident, use our incident-response resources and support pathway to move from uncertainty to action.

Need help now?

Use the Identity Defense 247 incident-response support pathway for practical next steps and escalation guidance.

Important note

This guide is educational and does not replace legal, insurance, forensic, or law-enforcement advice. Use qualified professionals when sensitive data, financial loss, ransomware, or business interruption is involved.