First-hour incident response card

For a suspected cyberattack. Fill in trusted contacts and keep this card accessible offline.

If you suspect a fraudulent transfer, call the originating bank immediately.
Use a number from bank records. Hold related payments and ask about a recall.

Emergency contacts

Incident lead

Backup incident lead

IT responder

Operational safety lead

Bank fraud line

Alternate communication channel

Response checklist

- ☐ **Record and call.** Call your incident lead and IT using trusted numbers. Note what happened, who reported it and when.
- ☐ **Use a clean channel.** Switch to a known-clean device and an agreed phone or messaging channel outside the affected systems.
- ☐ **Contain safely.** Isolate affected devices from the network where safe. Involve the safety lead before disconnecting critical equipment. If ransomware is spreading and isolation is impossible, power down affected devices only if safe. This can lose evidence held in memory.
- ☐ **Preserve evidence.** Keep original messages, logs, timestamps and payment records. Limit access and record each action as it happens.
- ☐ **Secure affected accounts.** Have IT restrict access from a clean device, revoke sessions where supported, rotate exposed credentials and review recovery methods, forwarding and app access.
- ☐ **Assess and notify.** Record affected services, data and locations. Involve legal, privacy and insurance leads as appropriate. Assign notification owners and deadlines.
- ☐ **Start continuity.** Use an approved manual workaround. Have responders and service owners verify systems and workflows before reconnecting.

Incident notes

First report (time and zone)

Became aware (time and zone)

Affected workflow or payment and who is affected

Actions taken (time, person and action)

Next update (time and zone, audience and trusted channel)

First-week cybersecurity checklist

Assign a person to each task. Check it off when the verification passes.

Business or team _____ **Week of** _____ **Accountable lead** _____

Task | **Owner role and name**

☐ **Assign leads and list critical workflows** — **Business owner** _____

Do. Name leads for IT, finance and incident response. List the workflows the business must keep running.

Verify. Check that each workflow has a named owner, a support contact and a list of its key systems.

☐ **Keep emergency contacts available offline** — **Incident lead** _____

Do. Save trusted numbers for the incident lead, backup, IT provider and bank fraud line. Agree on a backup channel.

Verify. In a drill, ask a staff member to find the list and reach the incident lead without company email.

☐ **Secure priority accounts** — **IT lead or provider** _____

Do. Require phishing-resistant sign-in, such as passkeys or security keys, for priority accounts where supported.

Verify. Check enforcement for admin, email, remote access, backup and finance. Test sign-in and recovery with a pilot account.

☐ **Triage urgent internet-facing risks** — **IT lead or provider** _____

Do. List public websites, VPNs and gateways. Check vendor advisories and apply urgent fixes or approved mitigations.

Verify. Check versions or controls after changes. Record each remaining high-risk item with an owner and due date.

☐ **Verify supplier payment changes** — **Finance lead** _____

Do. Hold payments with changed bank details until you call a supplier number already on file and a second person approves.

Verify. Rehearse a mock supplier change. Confirm both checks were recorded before any payment would be released.

☐ **Restore one critical record** — **Recovery owner** _____

Do. Restore a recent critical file or record into an approved test environment.

Verify. A business user opens it and checks its contents and date against a known record. Save the result and any gaps.

Gaps to close

Action, owner and due date

_____

_____

30-day cybersecurity checklist

Assign a person to each task. Check it off when the verification passes.

Business or team _____ **Milestone date** _____ **Accountable lead** _____

Task **Owner role and name**

☐ **Inventory devices and cloud services** **IT lead or provider** _____

Do. List work devices and cloud services, including supplier-managed systems. Record an owner and purpose for each.

Verify. Compare the list with device records, cloud admin reports and subscription bills. Log missing assets or owners.

☐ **Remove unnecessary access** **IT lead or provider** _____

Do. Review staff, contractor and vendor accounts, admin roles and app permissions. Remove access that is no longer needed.

Verify. Check a recent departure or run a test offboarding. Verify access is gone in email, cloud apps and remote access.

☐ **Review email and sharing controls** **IT lead or provider** _____

Do. Review external mail forwarding and public links. Restrict sharing of sensitive folders to approved people.

Verify. Confirm a standard test account cannot share a restricted test file publicly. Give each forwarding exception an owner.

☐ **Test priority alerts** **IT lead or provider** _____

Do. Pick a priority alert, such as an admin access change or backup failure. Name primary and backup responders.

Verify. Send an approved test alert after hours. Record who received it, who acknowledged it and how long it took.

☐ **Restore one critical service** **Recovery owner** _____

Do. Restore a critical service and its dependencies from trusted backups in an isolated test environment.

Verify. Compare restore time and data loss with agreed targets. Have a business user complete and sign off on a workflow.

☐ **Confirm supplier responsibilities** **Business owner** _____

Do. Record who patches, monitors and restores each critical supplier system, and how to escalate an incident.

Verify. Check written support terms. Confirm the incident lead can find the contact and response time without company email.

Gaps to close

Action, owner and due date

_____

_____

_____

90-day cybersecurity checklist

Assign a person to each task. Check it off when the verification passes.

Business or team _____ **Milestone date** _____ **Accountable lead** _____

Task **Owner role and name**

☐ **Expand phishing-resistant sign-in** **Identity owner** _____

Do. Extend passkey or security key requirements to more eligible accounts. Plan recovery before enforcing changes.

Verify. Check the policy against the account list and record any gaps. Test sign-in and approved recovery with a pilot account.

☐ **Verify network separation** **Network owner** _____

Do. Review guest, staff, admin and backup boundaries. Limit access between them to approved connections.

Verify. On a restricted test service, confirm guest access fails and an approved admin can connect.

☐ **Recover without a major dependency** **Recovery owner** _____

Do. In a test environment, rehearse losing a major dependency, such as your main sign-in provider or a critical supplier.

Verify. Have a business user complete a workflow with the fallback. Compare elapsed time and missing data against targets.

☐ **Resolve overdue security exceptions** **Business owner** _____

Do. Fix overdue exceptions or get an accountable leader to accept the remaining risk for a limited time.

Verify. Keep proof of the fix or a signed risk decision naming temporary safeguards, an owner and the expiry date.

☐ **Run an incident response exercise** **Incident lead** _____

Do. Walk through a ransomware or payment fraud scenario with IT, finance and a business owner.

Verify. Record who escalated and authorized containment. Note which decisions were timely and what the team missed.

☐ **Assign fixes and schedule retests** **Incident lead** _____

Do. Give each failed step an owner and due date. Schedule a retest of the failed steps.

Verify. Check the action log and retest date. Close each gap when the team demonstrates the fix works.

Gaps to close

Action, owner and due date

_____

_____