Workplace cyber awareness practical pack

Use this pack with your team

This pack helps managers and business owners turn cyber awareness into everyday working practices. Use it to agree reporting routes, rehearse decisions and record improvements. It is designed for adult staff, not technical incident responders.

Appoint one owner to adapt the pack with your IT support, finance and data protection leads. Use your existing policies and response plan to settle who can authorise actions.

Start with	Use these pages	What you should have afterwards
Set up the pack	2 to 4	A tested contact card and a safe way to record an incident.
Practise with staff	5 to 9	A verification process, team discussion and three owned improvements.
Build it into routine work	10 onwards	An induction check, display reminder and review plan.

Prepare before sharing

1. Fill in the contact card with approved organisation details. Check the alternative route works when email is unavailable.
2. Replace the writing spaces in the Word copy with your local procedures, or print the relevant PDF pages and complete them by hand. The PDF is a print copy, not a fillable form.
3. Read the facilitator notes before the exercise. Use fictional information only. Do not send test phishing, change systems or make real payments.
4. Store completed internal records with appropriate access. Share the staff reminder widely, but restrict incident details and staff evidence.

The 15-minute briefing and 30-minute exercise are suggested agendas, not pass marks or guaranteed completion times. You can use individual pages without completing the whole pack.

Maintained by CompTech IT Solutions. Pack version 2026.10.2. Reviewed on 15 October 2026. This is a practical learning aid, not an external accreditation, NCSC endorsement or a substitute for your approved incident plan.

Your incident contact card

Complete and approve this page before an incident. Keep a current offline copy where staff, temporary colleagues and volunteers can find it. Do not add passwords, recovery codes or private contact details without approval.

Organisation name and site

_____

Card owner and approval date

_____

Role	Primary contact	Backup contact
IT or incident reporting	Name or team and safe contact route:	Alternative route if email is unavailable:
Incident coordinator	Name and work number:	Deputy and work number:
Data protection lead or DPO	Name and approved contact route:	Deputy or out-of-hours route:
Finance or payment approval	Name and approved contact route:	Deputy approver:
Out-of-hours response	When this route should be used:	Number and availability:

Approved device isolation instructions are kept at

_____

Offline response plan and safe communications route

_____

Test the card

- Ask a colleague to find and use the alternative reporting route without opening email. Agree a test with the recipient first.
- Check that the backup person knows their role and can access the plan. Update the card after staff, provider or telephone changes.

Tested by: _____ Date: _____
Next review: _____

If anyone is in immediate danger, follow your emergency arrangements. Cyber reporting must not delay urgent safeguarding or emergency action.

Respond in the first few minutes

Start with prompt reporting and a clear handover. These are staff actions; your authorised incident team decides containment, recovery and wider communications.

1. Pause the activity. Do not approve another prompt or share more information. Note the time and what you observed.
2. Use the contact card from a safe device. If email or the helpdesk is unavailable, use the alternative route.
3. Follow the approved instructions and tell the response team what has already happened. Keep the incident reference.

What happened	What to tell staff to do
Suspicious message only	Do not use its links, attachments or contact details. Report using the approved route.
Password entered or MFA approved	Tell IT immediately what happened. Use a safe device and approved service for account recovery; a password change alone may not end access.
File opened or device behaving unusually	Stop using it and follow approved isolation instructions. Ask IT if unsure. Do not wipe, investigate or attempt a private repair.
Information sent to the wrong person	Report promptly to the data lead and IT. Follow approved access-revocation steps; a recall or deletion request is not proof that exposure has ended.
Money sent or payment details changed	Contact your finance lead urgently. They should use the bank's independently verified fraud route and coordinate the response.

A short report you can use

"I am reporting a possible cyber incident. At [time] I [observed or did this]. The affected account or device is [approved identifier]. I entered a password / approved MFA / opened a file / shared information / did none of those. I have stopped and can be reached through [safe route]. What should I do next?"

Never include a password, one-time code, full payment card number or unnecessary personal information. Preserve relevant evidence through the approved route without forwarding it widely.

If a ransom demand appears, do not negotiate or pay on your own authority. Report it and let the incident coordinator direct the response.

Record an incident and hand it over

Use this worksheet in your approved incident system or restricted records. Record observations separately from assumptions. Do not copy passwords, sensitive attachments or unnecessary personal details into it.

Incident reference and recorder

_____

Date and time first noticed including time zone

_____

Affected service device or account identifier

_____

What was observed and what action was taken

_____

Known impact and what is still uncertain

_____

Reported to and time acknowledged

_____

Safe contact route and next update time

_____

Time	Action or decision and reason	Owner

Handover before you finish

- Confirm who owns the incident and when the next update is due. Record where evidence is stored, rather than copying it into multiple places.
- Ask the coordinator what you should stop doing and which approved workarounds are safe. Do not assume that a system working again means the incident is closed.

Fictional example: “09:10, entered work password after an unexpected document message. No MFA prompt approved. Called IT at 09:12 from another device. Ticket EX-001. Awaiting instructions.” This describes facts without including the password.

Verify payments and sensitive requests

Use this before changing bank details, releasing customer, staff and supplier information or accepting an unusual access request. A genuine email thread, familiar name or urgent tone is not proof that the request is safe.

1. Pause the change or disclosure. Check whether it fits the expected work and your authority.
2. Contact the person through details you already hold independently. Do not use a telephone number supplied only in the message you are checking.
3. Confirm the purpose, recipient, amount or access needed. Follow your payment approval or information-sharing process.
4. Record who verified the request and who approved the action. If you cannot verify it, keep it on hold and escalate.

Practise three decisions

Situation	A useful response and why
A supplier changes bank details in a real invoice thread.	Call the established supplier contact from your approved records. Keep the change on hold until verified and approved; the mailbox may be compromised.
A senior colleague sends an urgent personal-message request for gift cards.	Use their established work contact route. Do not treat seniority or urgency as permission to bypass controls.
An expected document is in the approved platform with the expected access.	Review it there. Pause if it requests unexpected permissions or actions; do not reject all legitimate sharing simply because it arrived electronically.

Where we keep independently verified contact details

_____

Who can approve payments or sensitive disclosure

_____

How we record verification and an unresolved concern

_____

If a payment has already been made, use the incident contact card immediately. Do not continue the conversation with the suspected sender to investigate.

Run a 15 minute team briefing

Use this after the course or at a team meeting. Prepare the contact card and nominate a facilitator and note-taker. Tell everyone that the purpose is to improve the process, not to catch people out.

Time	Facilitator action	Evidence to look for
0 to 3 min	Ask each person to locate the normal and alternative reporting route.	Can staff find it without relying on email?
3 to 7 min	Read the supplier-bank-change example on page 5. Ask what the team would do next.	Independent contact and the proper approval route, not a reply in the same thread.
7 to 11 min	Ask what someone should do after entering a password on an unexpected page.	Immediate reporting, safe recovery instructions and no assumption that resetting a password ends the incident.
11 to 15 min	Agree one change, its owner and a date. Ask how a colleague would report a mistake.	A clear action and a reporting process that staff feel able to use.

Prompts for the facilitator

- If someone says “I would just delete it”, ask how IT would learn that an account or payment could be affected.
- If someone says “I would ask the sender”, ask how they would choose a separate trusted route.
- If nobody knows the alternative contact, record that as a process gap to fix. Do not score individual staff.

One gap we found

_____

Improvement owner and due date

_____

How we will check the improvement worked

_____

Include colleagues who work remotely or outside office hours. Their route to help should be as clear as the route available in the office.

Run a 30 minute incident exercise

This is a discussion exercise using a fictional situation. Do not send messages to real suppliers, alter systems or make payments. Stop the exercise if a real incident is discovered and use the approved reporting route.

Invite the manager or business owner, an IT contact, a finance representative and the data protection lead. Include someone who handles customer communications.

Facilitator preparation

Give participants the contact card and a blank action record. Nominate one incident coordinator and one note-taker. Read each update at the stated time, then let the group decide who acts, through which route and what they record.

Time	Read this update	Ask the group
0 to 5 min	At 09:15, a supplier asks why an invoice is unpaid. Finance finds a bank-detail change approved yesterday after an email in a genuine thread. The account owner also reports an unexpected MFA prompt.	What do we know, what is uncertain and who owns the response?
5 to 12 min	The supplier says the new bank account is not theirs. A colleague suggests replying in the email thread to ask what happened. A second payment is due today.	What must stop now? How do we verify and communicate through a safe route?
12 to 20 min	IT suspects the mailbox is compromised and needs time to investigate. A customer asks whether their information is affected. A manager wants to tell everyone the incident is resolved after a password reset.	Who decides what can continue, what can be said and when we update people?
20 to 30 min	Move to the debrief and action page.	Which three gaps would cause the most harm or delay? Who will fix and test them?

Record decisions and reasons rather than a transcript. Separate a capability you demonstrated from something the group assumes exists. If a contact or document cannot be found, record the gap.

Use these facilitator notes

There is no single script for every organisation. Look for sensible decisions consistent with local authority and policy. Use these notes to challenge assumptions and keep the exercise safe.

What a good response should include

- Finance stops the pending change or payment and contacts the bank through an independently verified route if money may have moved. Staff do not investigate by replying to the suspected mailbox.
- A named incident coordinator involves IT and the data protection lead. IT decides account containment and checks for continued access rather than relying only on a password reset.
- The team records known facts, affected services and uncertainty. The data lead assesses information risks and any notification duties using current guidance.
- One authorised person coordinates factual updates. Restoring access is not sufficient evidence that the incident is closed.

Questions that expose a process gap

- “Show me where that number or instruction is kept.”
- “Who has authority to approve this action, and who is the deputy?”
- “What would you do if the usual system or person is unavailable?”
- “What evidence would support saying that this is resolved?”

A fictional first update

“We are investigating a possible cyber incident affecting [service]. Please use [approved alternative route] for urgent work and do not use unapproved workarounds. Report related concerns through [route]. We will provide the next update at [time].”

The coordinator must adapt and approve any real update. Do not claim that no data was affected while that is still unknown. Keep any external reporting decisions with the responsible authorised leads.

Turn the exercise into improvements

Finish with a small number of specific changes. Record the evidence you need to close each action, then return to it at the next meeting. The example below is fictional.

Gap	Action and proof it worked	Owner and due date
No one could find the backup reporting number.	Publish an approved offline card, then ask two colleagues on different shifts to find and use it in an agreed test.	Operations lead, within 7 days.

Your three priority actions

Gap and impact	Action and evidence required	Owner and due date

What worked and should be retained

_____

What we assumed but could not demonstrate

_____

Next review meeting and action owner

_____

Close actions with evidence

- Useful evidence includes a completed agreed contact test, an updated approved procedure, or staff demonstrating the reporting route. “Email sent” alone does not show people can use it.
- Escalate overdue actions to the person who can resolve the blocker. Check that the change is available to new starters, remote workers and people covering absence.
- Repeat the part of the exercise that exposed the gap. Keep a short record of what changed and whether the test succeeded.

Keep these records in your approved internal location. Do not put real incident details or completed staff records into the public training website.

Check understanding at induction

Use this with new starters, temporary staff and colleagues returning after a process change. Ask for a demonstration or explanation, then record any help needed. Course attendance alone does not establish understanding.

Colleague or approved staff identifier and role

_____

Manager and date

_____

Topic	Ask the colleague to demonstrate	Outcome or action
Access and accounts	Uses their own approved account and can explain how they protect it.	
Reporting	Finds normal and alternative reporting routes without relying on email.	
Messages and MFA	Explains what to do after a suspicious message or unexpected MFA prompt.	
Information handling	Checks the recipient and permissions in the approved sharing system.	
Payments and requests	Explains how to verify a change through an independently held contact.	
Role specific learning	Identifies any further training or local policy they need.	

Record “demonstrated”, “needs support” or “not applicable with reason”. Do not record passwords, MFA codes or sensitive test data.

Support or role specific learning agreed

_____

Owner and follow up date

_____

Next refresher under local policy

_____

Revisit these points after an incident, a role change or a change to your systems. Set the refresher date under your organisation’s policy.

Five everyday cyber habits

Display this page near shared work areas or include it in induction. Complete the two reporting routes before sharing.

Pause before acting

An unexpected request deserves a check. Urgency, a familiar name and an existing email thread do not prove it is genuine.

Verify through a route you trust

Use independently held contact details for payment changes and unusual information requests. Follow the normal approval process.

Protect your sign in

Use approved password tools and MFA. Deny and report an unexpected prompt. Never share passwords or one-time codes.

Share only what is needed

Check recipients and permissions in approved systems before sending. Report wrong-recipient mistakes promptly.

Report early

You do not need to be certain or investigate first. If you clicked, entered a password or approved a prompt, say so clearly so the response team can help.

Our normal reporting route

_____

Our alternative route when email is unavailable

_____

If there is immediate danger or an urgent safeguarding concern, follow the appropriate emergency or safeguarding route.

Keep the pack useful over time

Use the following as a suggested first-month rollout, then align reviews with your existing policies. Adapt the timescales to your risk and staffing rather than treating this as a certification checklist.

When	Practical task	Evidence of progress
Week 1	Approve and test the contact card. Choose a pack owner.	Staff can find both routes. Deputies know their role.
Week 2	Run the 15-minute briefing and update induction.	One owned action and recorded support needs.
Week 3	Run the discussion exercise with the relevant leads.	Three prioritised improvements with owners and dates.
Week 4	Check actions and repeat the weak part of the exercise.	Evidence that the process works, not just an updated document.

Review when something changes

Check contacts and instructions after a staff or provider change, a significant incident or an exercise finding. Revisit the pack when official guidance changes. Keep a master editable copy and retire outdated copies.

Official guidance for the pack owner

NCSC Small Business Guide Response and Recovery

NCSC Exercise in a Box

NCSC Top Tips for Staff

Links reviewed on 15 October 2026. These organisations have not endorsed this pack. Our scenarios and worksheets are practical examples for local adaptation.

Changes in pack version 2026.10.2: added incident records, worked verification examples, facilitator guidance, a discussion exercise, action tracking and professional PDF and Word editions. Course version 2026.10 is unchanged.