

LEARN / APPLY / REFLECT

Cybersecurity Essentials for Business Teams

A free course on practical cyber habits for business owners and staff. Learn to protect accounts, recognise phishing, maintain software and prepare for data recovery.

Your practical learning workbook

Follow the estimated study times shown for each lesson. Course totals include the external videos, notes, activities, a 10-minute understanding check and a 20-30-minute practical assignment. Reading the optional presenter scripts may take extra time.

Use fictional or non-confidential examples. Write on a printed copy or keep your answers in your own document. Online lesson pages also let you save activity notes on your current browser.

Your name: _____

Start date: _____

By the end, you can

- Recognise common account and phishing risks.
- Choose practical account protection and update habits.
- Explain why backup recovery must be tested.

Learning route

1. Everyday cyber responsibility
2. Strong, unique passwords
3. Multi-factor authentication
4. Phishing and payment changes
5. Updates and supported software
6. Backups and recovery

Complete the online understanding check and use the final assignment rubric to review practical application. This workbook is introductory learning, not a professional qualification.

LESSON 01 / PRACTICE

Everyday cyber responsibility

Identify everyday actions that reduce avoidable risk.

Make reporting easy and specific: staff should know a trusted contact and an alternative when email is unavailable. Describe what happened and when, without sharing passwords or secret codes. Managers should welcome early reports even when they prove harmless. Technical investigation and containment belong to the authorised response team; staff should follow its instructions.

Workplace example

A staff member reports an unexpected login alert immediately. The team checks the account and responds before assuming that the alert is harmless.

Your activity

Identify your security contact and one business system whose loss would interrupt work.

Self-check

What should staff do with an unexpected account-security alert?

- A. Ignore it until the next training session
- B. Report it through a trusted internal route
- C. Forward account passwords to colleagues

LESSON 02 / PRACTICE

Strong, unique passwords

Use safer account credentials without relying on memory alone.

Unique passwords reduce the damage from one compromised service. Use your organisation's approved password manager and recovery process. Protect the manager itself and avoid putting credentials in a shared spreadsheet or training worksheet. For shared business functions, ask IT for an approved access arrangement rather than circulating an individual's password.

Workplace example

A staff member reuses a password for a supplier portal and business email. A breach at one service can put the other account at risk.

Your activity

Review one important account. Check that its password is unique and stored in an approved manager.

Self-check

Why is password reuse risky?

- A. One compromised password can expose other accounts
- B. It makes screens load slowly
- C. It prevents software updates

LESSON 03 / PRACTICE

Multi-factor authentication

Explain how MFA adds protection to an account.

MFA adds protection beyond a password, but its methods differ. Where supported, ask IT about phishing-resistant options such as FIDO security keys or appropriate passkeys. Plan enrolment, lost-device recovery and alternative access before rollout. Never approve a request you did not initiate, and never read a one-time code to an unexpected caller.

Workplace example

A staff member receives an approval request while not signing in. They reject it and report the attempt rather than approve it to stop the notifications.

Your activity

Check whether your business email has MFA and locate the approved recovery process.

Self-check

What should you do with an MFA request you did not initiate?

- A. Approve it to clear the notification
- B. Share the code with the caller
- C. Reject it and report the unexpected request

LESSON 04 / PRACTICE

Phishing and payment changes

Recognise pressure tactics and verify requests independently.

Urgent language and a familiar logo are not reliable evidence of identity. Payment changes deserve an independent verification step and the usual approval controls. Use contact details already held in a trusted record, not details supplied in the change request. If someone has already interacted with a suspicious message, prompt reporting matters more than blame.

Workplace example

An email asks finance to replace a supplier bank account urgently. Finance calls its established supplier contact rather than the number in the email.

Your activity

Write a short verification procedure for requests to change bank details.

Self-check

How should a supplier bank-account change be verified?

- A. Reply to the same email and ask if it is genuine
- B. Call a trusted contact using an independently held number
- C. Accept it if the logo looks right

LESSON 05 / PRACTICE

Updates and supported software

Treat updates as part of routine business maintenance.

Use legitimate updates through your organisation's approved route. Business-critical systems may need compatibility checks, a maintenance window and a recovery plan. Delaying an update should be an owned risk decision with a deadline, not an indefinite habit. Keep an inventory so shared devices and unsupported applications are not overlooked.

Workplace example

A shared workstation misses updates because everyone assumes someone else owns it. Naming an owner makes routine maintenance visible.

Your activity

Identify one shared device and confirm who checks its update status.

Self-check

What is the best approach to shared-device updates?

- A. Assume any user will eventually handle them
- B. Assign an owner and an approved update process
- C. Disable all updates permanently

LESSON 06 / PRACTICE

Backups and recovery

Understand why having a backup is different from proving recovery.

Recovery evidence should show what was restored, from which recovery point, how long it took and who checked usability. Protect backups from the same account compromise or incident that affects the originals. Test in a controlled environment and agree recovery priorities with the business owner. A green backup-job status alone cannot establish that business service will recover.

Workplace example

A company discovers that its backups do not include a critical shared folder. A restoration test finds the gap before a real outage.

Your activity

Ask when a critical file or system was last successfully restored and who verified the result.

Self-check

What best demonstrates that a backup supports recovery?

- A. A screenshot of a scheduled backup job
- B. A successful restore with usable data verified
- C. The age of the backup server

FINAL ASSIGNMENT / 20-30 MINUTES

Your cyber action plan

A supplier requests an urgent bank-account change. A shared PC has no maintenance owner, and nobody can show the last successful restoration test.

Prepare a one-page response addressing these five points.

1. Explain how the payment change will be verified.

2. Identify the trusted incident reporting and escalation route.

3. Assign account protection and device maintenance owners.

4. Describe a controlled restoration test and success evidence.

5. Prioritise actions with owners, dates and a review checkpoint.

Self-review rubric

For each point: 0 = missing; 1 = a relevant idea but vague or incomplete; 2 = a specific, feasible response linked to this scenario, with evidence or ownership where appropriate. Maximum 10. This is your self-rating, not an independent grade.

8-10: refine with your team. 5-7: strengthen weak areas. 0-4: revisit the relevant lessons. Any critical omission still needs attention regardless of the total.

WORKED RESPONSES / READ AFTER TRYING

Compare your reasoning

These are illustrative answers, not the only acceptable responses. Adapt them to your own context.

1. Everyday cyber responsibility

Record the time of the unexpected alert and the affected service. Contact IT through the established help route, without clicking the alert's link. The authorised team checks the account. If that route is unavailable, use the organisation's agreed alternative contact.

Knowledge check: B. Prompt reporting allows the organisation to investigate and respond.

2. Strong, unique passwords

For business email, confirm that the credential is unique and stored using the approved method. If it has been reused, change it through the genuine service and follow IT guidance for other affected accounts. Record only 'review completed' in this workbook, never the password.

Knowledge check: A. Attackers may try a stolen password on other services.

3. Multi-factor authentication

Check the business email security settings through the trusted service. Confirm the approved MFA method and recovery contact. If an unsolicited prompt appears, reject it and report it. Do not treat repeated prompts as a reason to approve access.

Knowledge check: C. Unexpected prompts may indicate an attempted account compromise.

4. Phishing and payment changes

Pause the payment-detail change. Call the known supplier representative using a previously verified number. Follow the finance approval process, record the verification, and only then update the authorised supplier record. If the request cannot be verified, escalate it without changing the details.

Knowledge check: B. Independent verification avoids relying on contact details controlled by an attacker.

5. Updates and supported software

The shared reception PC has a named owner. IT checks support status and applies approved updates in a scheduled window. After restarting, the owner checks essential functions. Any deferred update is logged with a reason, temporary controls and a review date.

Knowledge check: B. Named responsibility helps prevent devices from falling outside routine maintenance.

6. Backups and recovery

Restore a sample critical folder into an approved test location. Confirm that required files open and that dates and contents are correct. Record elapsed time, the recovery point and any missing data. Assign remediation and repeat the test after addressing gaps.

Knowledge check: B. A restore test checks that the data and process can support recovery.

FINAL ASSIGNMENT / WORKED EXAMPLE

Your cyber action plan

Pause the bank change and verify through an established independent contact. Use normal finance approvals and report suspicious indicators through the trusted route. IT reviews account protection and assigns the shared device owner. Schedule an approved restore test with the data owner, verify usability and record corrective actions. Do not put credentials in the plan.

Your next 30 days

Choose one action, its owner, its due date and the evidence you will review.

Continue your learning

<https://sarah-ching-academy.ferching.chatgpt.site/learn/cybersecurity.html>

Original Academy teaching notes, exercises and illustrative scenarios. External videos are credited on the online course pages. Presenter scripts are drafts; talking-presenter videos are not included in this workbook.

CISA: Secure Our World

<https://www.cisa.gov/secure-our-world>

CISA: Require Multifactor Authentication

<https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>

CISA: StopRansomware Guide

<https://www.cisa.gov/stopransomware/ransomware-guide>