TOOLBOX TALK AWARENESS PACKAGES

HAZ-CYB · Cyber Security Awareness

Product Overview

Audience: All workers · Duration: 20–30 minutes

Version 1.0 · 8 November 2026

For everyone with a work email, phone or login: recognising scams and phishing, protecting accounts, and reporting quickly when something looks wrong.

Most cyber incidents in small and medium businesses start with a person: a convincing email, a fake invoice, a reused password or a lost phone. The consequences can include stolen money, lost data, systems that stop working and personal information exposed.

This talk teaches workers to recognise phishing and scams, use strong passphrases and multi-factor authentication, keep devices updated, handle information carefully, and report anything suspicious straight away without fear of blame.

Learning outcomes

By the end of the session participants will be able to:

- Recognise phishing emails, texts and calls, including fake invoices and changed bank details
- Use long, unique passphrases and a password manager if the business provides one
- Explain why multi-factor authentication matters, and never share a code
- Keep devices and software updated, and lock devices when unattended
- Handle personal and business information carefully, including on removable media and in the cloud
- Report a suspected scam, lost device or mistake quickly, through the right channel

What it covers

Module	Covers
Why it matters	How small businesses are targeted; Business email compromise and invoice fraud; Personal information and privacy
Spotting scams	Signs of phishing; Urgency, authority and pressure; Checking a request through another channel
Protecting accounts and devices	Passphrases and password managers; Multi-factor authentication; Updates, backups and locking devices
Your part	Reporting quickly; What to do if you clicked; Working away from the office

Activities

- Real or fake: workers sort six example emails and texts and point out the warning signs

© 2026 Orana Skills Centre. All rights reserved.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

- Changed bank details: a scenario of a supplier asking to change account details, and the checks before paying

What is in the package

Item	File
Editable PowerPoint presentation with speaker notes, plus PDF	02_TRAINING_PRESENTATION/Training Presentation.pptx and .pdf
Facilitator guide with a running sheet, discussion prompts and model answers	03_FACILITATOR_GUIDE/Facilitator Guide.docx and .pdf
Participant handout with the key points to take away	04_PARTICIPANT_HANDOUT/Participant Handout.docx and .pdf
Attendance record form, to capture who attended, when, and who facilitated	06_RECORDS/Attendance Record.docx and .pdf
Excel attendance register	06_RECORDS/Attendance Register.xlsx
Multiple-choice theory assessment, to record understanding if your business wants to	05_ASSESSMENT/Theory Assessment.docx and .pdf
Answer key for the assessment	05_ASSESSMENT/Assessment Answer Key.docx and .pdf
Certificate template	06_RECORDS/Certificate Template.docx
Start here: Read Me First, Product Overview, Permitted Use Terms, Version Information	01_START_HERE/ (four PDFs)

What you need to deliver it

- A facilitator such as a supervisor, leading hand or WHS adviser who has read the facilitator guide and knows your site's arrangements for the topic
- A screen or projector, or printed slides or handouts: it works in a crib room, site office or on a video call
- Your own site procedures for the topic, to point to during the session

Questions

Can we add our own site procedures and photos? Yes. The slides, handout and guide are editable, and the facilitator guide marks the places to add your own procedures, contacts and photos of your workplace.

Do we have to use the assessment? No. It is there if your business wants a record that each worker understood the key points. The attendance record on its own shows who attended and when.

Version 1.0 · 8 November 2026 · Orana Skills Centre. *© 2026 Orana Skills Centre. All rights reserved.*

© 2026 Orana Skills Centre. All rights reserved.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

TOOLBOX TALK

Cyber Security Awareness

Spot the scam, protect your accounts, and report it fast

20–30 minutes · All workers

[Company name] · [Date] · [Facilitator name]

CYB

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

What this talk is, and is not

This talk covers

- ✓ How businesses like ours are targeted
- ✓ Spotting phishing and invoice scams
- ✓ Protecting accounts, devices and information
- ✓ Your part: check, report, and what to do if you clicked

This talk is not

- ✕ IT administration or system set-up
- ✕ Incident response or recovery
- ✕ Legal or privacy advice
- ✕ Our policy: **[Your IT and acceptable use policy]**

Awareness only. Setting up and securing systems, and responding to an incident, is work for whoever manages your IT.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

Why it matters

Most cyber incidents in small and medium businesses start with a person, not a clever hack.

- A convincing email, a fake invoice, a reused password or a lost phone
- Business email compromise: a criminal gets into, or imitates, a real email account, then asks for money
- The cost: stolen money, lost data, systems down, and personal information exposed
- Customers' and workers' personal information must be protected under privacy laws

Scams work on people, not computers.

A composite example

- An accounts officer gets an email from a regular supplier: 'Our bank has changed, please update our details before Friday's payment.'
- It comes from the supplier's real account, which has been hacked. Two invoices are paid to the criminal before anyone notices.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

Policy, privacy and reporting

The business should

- Set clear IT, privacy and acceptable use policies
- Provide secure systems: updates, backups, multi-factor
- Give everyone a simple, blame-free way to report
- Decide whether a data breach must be reported

You must

- Follow the IT and privacy policies you have been given
- Protect your logins, devices and information
- Check before you pay, change details or share information
- Report anything suspicious, lost or sent wrongly, fast

Some data breaches must be reported to the privacy regulator. The business decides, so it needs to know fast.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

The order of controls for cyber risk

1. **Elimination** Don't keep data you no longer need; never change bank details by email
2. **Substitution** A shared, secure system instead of files and passwords sent by email
3. **Isolation** Only the people who need access have it; separate admin accounts
4. **Engineering** Multi-factor authentication, automatic updates, backups, filters
5. **Administrative** Call-back checks, two-person payment approval, reporting
6. **People's vigilance** Spotting the scam: needed, but relies on everyone, every time

HIGHER ORDER

Work without anyone having to spot the scam.

LOWER ORDER

Rely on people doing the right thing, every time, tired or rushed.

Behaviours are not on the hierarchy, but behaviours and culture decide whether every control on it actually works.

Start at the top. Spotting scams is the last line, not the first.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.

TOOLBOX TALK · HAZ-CYB

Cyber Security Awareness

Participant handout · keep this

Most cyber incidents in small and medium businesses start with a person: a convincing email, a fake invoice, a reused password or a lost phone. Keep this page.

Signs of a scam

- Urgent: 'today', 'final notice', 'or your account closes'
- From someone with authority: the boss, the bank, a government agency
- Asks you to pay, change bank details, log in or share a code
- A sender address or link that is slightly wrong
- Unexpected: an attachment, a gift card request, a QR code

Check through another channel

1. Do not click, reply, scan or call the number given
2. Ring the person on a number you already have
3. Changed bank details: confirmed by phone, every time, before any payment

Protect accounts and devices

- Passphrases: four or more random words, different for every account
- Multi-factor authentication on; never share a code; deny prompts you did not start
- Install updates; lock your screen; keep devices with you

Handle information carefully

- Only collect, keep and share what the job needs
- Check the recipient before you send
- No work files in personal email or cloud; never plug in a found USB

If you clicked or lost something

- Report it straight away
- Say what you clicked, entered or sent, and when
- Do not try to fix it yourself
- Lost device: report it at once

Report to

- **[Who to report to here]**
- **[How to report a cyber incident here]**
- Report mistakes too: the business wants to know. The sooner, the better.

Urgent, unusual, asks for money or a code: stop, check, and report it fast.

This is awareness training. It is not a licence, a ticket, a permit or a competency. It does not cover setting up or securing IT systems, or responding to an incident.

© 2026 Orana Skills Centre. All rights reserved.

SAMPLE · HAZ-CYB Cyber Security Awareness v1.0 · The full package contains the complete materials.