SERVICE GUIDE

Security Awareness Training

How to build a program that helps people recognize threats, report them and stay alert.

01 · OVERVIEW

Why it matters

Most attacks still start with a person: a message that looks right, a call that sounds urgent, a file that seems harmless. Awareness training equips your people to spot these attempts and to report them, so a mistake becomes an alert instead of an incident.

A good program is not a yearly lecture. It is interactive, close to real work, adapted to your industry and followed up so that awareness stays alive.

Typical triggers

- Staff receive messages that look like customer or partner requests
- Teams handle sensitive data under time pressure
- New or seasonal staff join quickly
- Phishing or fraud attempts have already happened
- People use AI tools and are unsure what may be shared
- Standards or customers ask for regular training

Who benefits

Management
Fewer incidents and a culture where reporting is normal.

HR and team leads
Training that fits roles and shifts.

IT and security
Early warnings from employees.

All employees
Confidence to recognize and handle suspicious messages.

In this guide

01 Overview 2
02 What it is, and what it is not 3
03 How it works, step by step 4
04 What you receive 5
05 In practice 6
06 How to prepare 7
07 Questions, references and terms 8
08 How the services fit together 9

02 · SCOPE

What it is, and what it is not

What it is

- + Interactive, with real-world scenarios and practical exercises
- + Customized to your industry and threat landscape
- + Role-based: different groups meet different threats
- + Followed up, so awareness lasts

What it is not

- – Not a one-off compliance checkbox
- – Not blame: the aim is reporting, not punishment
- – Not a long generic course nobody remembers
- – Not a replacement for technical protection

Topics and formats

Phishing

Fake emails, messages and websites that steal logins or money. Includes links, attachments and QR codes.

Social engineering

Manipulation by phone, chat or in person: urgent requests, false authority, and impersonation, including voice or video that is faked with AI.

Malware

Harmful files and software arriving by email, downloads, fake updates or removable media.

Interactive formats

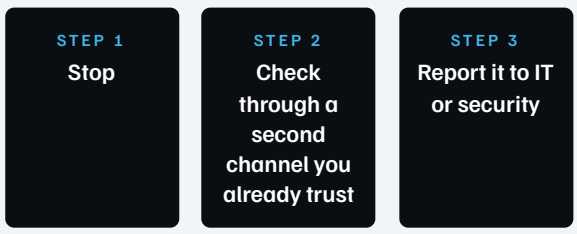
Live sessions, scenario discussions, practical exercises and simulated attempts, adapted to roles such as finance, HR, IT and management.

Six red flags in a message

1. Urgency or pressure: do it now, or else
2. An unexpected request for money, data or a login
3. A sender or web address that is slightly off
4. A link or attachment you did not expect
5. A change of bank details or a new payment route
6. Something that is too good, or too frightening, to be true

If in doubt

Do not click, reply or call back on the number in the message.



03 · PROCESS

How it works, step by step

A typical engagement, from the first conversation to clear next steps. Exact steps and timing are agreed with you when the work is scoped.

01 Discuss

Understand your people, industry and risks.

- Talk through who your teams are and how they work
- Learn which threats you already see and what happened before
- Identify roles that carry special risk: finance, HR, executives, support

YOU PROVIDE
Your people, your industry and your risks
Examples of real messages, if you have them

YOU GET
A shared starting point

02 Tailor

Build scenarios that fit your organization.

- Select topics and write scenarios from your industry and daily work
- Choose formats and length that fit shifts and schedules
- Decide how reporting works: whom to tell and how

YOU PROVIDE
Review of scenarios
A reporting route for suspicious messages

YOU GET
Scenarios and exercises that fit

03 Train

Practice recognizing and responding.

- Run interactive sessions on phishing, social engineering and malware
- Work through real-world scenarios in small groups
- Practice with exercises, so people try, not just listen
- Answer questions and discuss real examples

YOU PROVIDE
Time for participants
A suitable room or video call

YOU GET
People who practice

04 Reinforce

Keep awareness alive.

- Follow up after the sessions with reminders and short refreshers
- Review what people reported and what they found difficult
- Adjust topics as threats and your organization change

YOU PROVIDE
Feedback and reported incidents

YOU GET
Follow-up to keep awareness alive

04 · DELIVERABLES

What you receive

A program is more than sessions. It includes the scenarios, the materials people can come back to and the follow-up that makes habits stick.

01
Tailored scenarios
Examples and exercises from your industry and daily work.

02
Interactive sessions
Live training with practical exercises.

03
Role-based content
Different material for finance, HR, IT, executives and others.

04
Reporting guidance
A simple, known way to report suspicious messages.

05
Follow-up
Reminders and refreshers that keep awareness alive.

06
Feedback
What people found hard, and what to adjust next.

How to know it works

Reporting	**More reports**	Employees report suspicious messages, including false alarms.
Speed	**Faster reports**	The time from receipt to report gets shorter.
Practice	**Fewer mistakes**	Fewer people click or reply in exercises over time.
Culture	**No blame**	People say what happened without fear.

Success is not a perfect score. It is more reports, faster reports and fewer mistakes over time. Simple measures are enough.

05 · IN PRACTICE

Seeing it at work

A program cycle that sticks

1 Kick-off
A first interactive session for everyone, on the threats that matter most to your organization.

2 Role-based
Sessions for groups with special risk, such as finance, HR, support, IT and management.

3 Practice
Exercises and simulated attempts, followed by a short, friendly debrief.

4 Refresh
Short reminders over time, adjusted to new threats and what people reported.

GOOD TO KNOW

Running exercises fairly

Practice

BE OPEN	Tell people that exercises take place as part of the program.
DEBRIEF	Explain afterwards what the signs were, so the exercise teaches.
RESPECT PRIVACY	Use work accounts only. Keep results confidential and avoid naming individuals.
REPEAT	Short, regular practice works better than one long course.

FOR AI PROJECTS

Awareness for teams that use AI

People now paste text, code and documents into AI tools. Teach which data must never go in, how to use approved tools and why AI-written messages and cloned voices make phishing and fraud harder to spot. Rules that are short and clear work better than long bans.

06 · PREPARATION

How to prepare

A little preparation makes the work faster, safer and more useful. Here is what helps most.

Before we start

- Describe your teams, roles and shift patterns
- Share real examples of suspicious messages, anonymized
- Decide how people should report suspicious messages
- Plan time for sessions and avoid peak periods
- Name a sponsor from management who takes part
- Decide which tools and data rules to teach

Typical ground rules

- + Training aims at learning, not at blaming
- + Examples are anonymized
- + Exercises use work accounts only
- + Results are used to improve the program, not to single out people

Common misconceptions

~~Our people are the weakest link.~~	**In practice:** People are also the best detectors. A culture of reporting turns them into a defense.
~~Once a year is enough.~~	**In practice:** Habits fade. Short, regular reminders keep awareness alive.
~~Technology will filter everything.~~	**In practice:** Filters miss some messages, and phone calls and chats bypass them completely.

07 · REFERENCE

Questions, references and terms

Frequently asked questions

How long are the sessions?
It depends on your teams and schedules. Length and format are agreed while tailoring the program.

Do you run phishing exercises?
Practical exercises are part of the approach, tailored to your organization and agreed with you.

Is it for all staff?
A common base for everyone, plus role-based content for groups with special risk.

Can it be done remotely?
Interactive sessions can be run in person or by video call.

What about new joiners?
Onboarding is a good moment for the basics, with follow-up later.

How do we measure success?
By reports, speed of reporting and fewer mistakes in exercises, without blaming individuals.

Reference frameworks and sources

NIST SP 800-50	Guidance on building a cybersecurity and privacy learning program.
NIST Phish Scale	A method to rate how hard a phishing message is to detect.
ISO/IEC 27001, Annex A	Includes a control on awareness, education and training.
National cybersecurity agencies	Many publish free guidance on phishing and social engineering.
MITRE ATT&CK	Shows how phishing and social engineering fit into attacks.

Terms in plain language

Phishing. Deceptive messages that try to steal logins, data or money.

Social engineering. Manipulating people to bypass security.

Pretexting. Using an invented story to gain trust.

Smishing and vishing. Phishing by text message or by voice call.

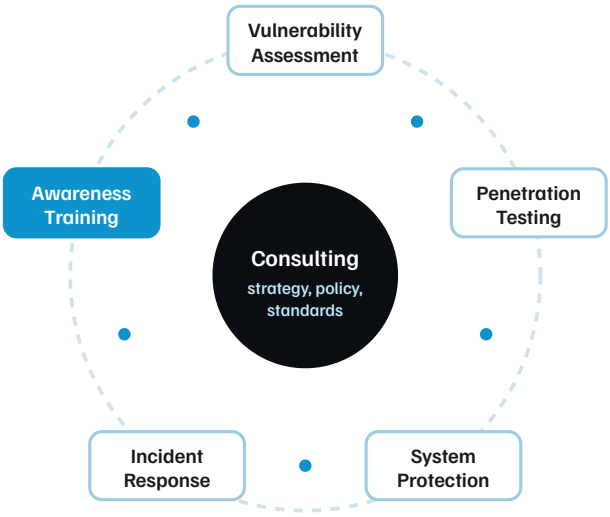
Malware. Harmful software.

Deepfake. Faked audio or video made with AI.

08 · NEXT STEPS

How the services fit together

Security works best as a cycle: find weaknesses, test them, protect, prepare to respond and keep people alert, all guided by a strategy. You can start with any one of them.



Vulnerability Assessment
Finds known weaknesses across your systems and ranks them.

Penetration Testing
Shows what an attacker can actually exploit.

System Protection
Closes gaps with layered, maintained defenses.

Incident Response and Forensics
Acts when something gets through, and learns from it.

Security Awareness Training (this guide)
Prepares the people who meet threats first.

Cyber Security Consulting
Sets strategy, policy and standards that tie it together.

Talk to a specialist about security awareness training.

Tell us what you are working on and what you need to protect.

EMAIL
info@cyberwhy.com

WEB
cyberwhy.com/services/security-awareness-training/

This guide describes how work of this kind typically runs. Scope, methods, timing and deliverables are agreed with you for your situation, and nothing in it is a guarantee. References to standards and frameworks are for orientation and do not mean certification. © CyberWhy. All rights reserved.