CYBER360
TRUSTED SECURITY ADVISOR

SERVICE BROCHURE

CYBER360 / SPECIALIST SERVICES

Security Awareness

Recognise the risk. Know what to do. Speak up early.

Help your people make confident security decisions. Connect practical learning, relevant scenarios and clear reporting with the way your business actually works.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | UK & Middle East

01 / SCOPE & FOCUS

The right question. A useful assessment.

Help your people make confident security decisions. Connect practical learning, relevant scenarios and clear reporting with the way your business actually works.

Phishing & suspicious messages

Agreed email scenarios and practical learning around unexpected links, attachments and requests.

Help staff pause, check through a trusted route and report concerns. Simulations are optional and designed around a clear learning objective.

Social engineering & impersonation

Role-relevant scenarios involving impersonation, pressure or requests to bypass a normal process.

Practise verification and escalation. Any live phone, messaging or in-person simulation requires explicit scope and approval.

Payment & supplier-change requests

Finance, procurement and executive-support workflows, using fictional or approved test information.

Reinforce independent callback checks, approval boundaries and escalation. No real payment is required for an exercise.

Account & access habits

Practical guidance on passwords, password managers, MFA prompts and reporting unexpected account activity.

Connect expected behaviour to your own approved tools and processes, including what to do when a mistake happens.

Data handling & everyday work

Relevant examples around sharing files, handling sensitive information, remote working and approved collaboration tools.

Make policies usable through short examples and clear routes for asking questions. Topics and delivery formats are agreed.

Reporting & security culture

Your reporting channels, response ownership and feedback to staff after a concern is raised.

Help people speak up promptly, including after clicking or sharing something. Look for process friction as well as learning needs.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Understand the workforce

Discuss business risks, roles, working patterns, existing learning and the concerns your people encounter.

Agree the learning objectives

Choose the behaviours and processes to improve, with relevant audiences, formats and success measures.

Prepare & approve

Confirm content, communications, accessibility, reporting routes and any simulation permissions or exclusions.

Deliver & practise

Use agreed briefings, practical scenarios or simulation activity to connect learning with everyday decisions.

Review the evidence

Look at participation, understanding, reporting and response, while recording measurement limitations.

Reinforce & improve

Recommend targeted follow-up and process changes. Agree any ongoing programme or repeat activity separately.

WHAT YOU RECEIVE

Programme & learning outputs

- Agreed audiences, learning objectives and delivery plan.
- Relevant content or scenario materials in the agreed formats.
- Clear staff actions and links to your reporting and verification processes.
- Recommended reinforcement themes and follow-up activity.

Findings & practical priorities

- A summary of participation and available outcome evidence.
- Observed knowledge gaps and process or reporting barriers.
- Measurement limitations and agreed reporting levels.
- A debrief and prioritised recommendations for accountable owners.

03 / PREPARATION & NEXT STEPS

Start with the right context.

People & priorities

• Identify audiences, sensitive roles, business processes and the risks you want to address.
• Agree language, accessibility, working patterns and suitable learning formats.

Permissions & boundaries

• Approve any simulation with appropriate business, HR and privacy stakeholders.
• Confirm audiences, scenarios, exclusions, timing and named contacts before activity begins.

Reporting & support

• Give staff a clear route for reporting concerns or asking for help.
• Confirm who receives reports, how they respond and what feedback staff will receive.

Evidence & follow-up

• Agree useful measures, data access, retention and reporting levels.
• Plan the debrief, learning follow-up and owners for process improvements.

PRACTICAL QUESTIONS

Is this just an annual training course?

It can include training, but the aim is useful behaviour in everyday work. We shape the activity around your risks, audiences and existing programme; delivery formats, frequency and follow-up are agreed in the proposal.

Do we have to run phishing simulations?

No. Simulations are one possible activity, not a requirement. Briefings, discussion-based scenarios, process walkthroughs and clearer reporting guidance may be more suitable for the learning objective.

LET’S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

UK +44 20 3286 1927 | UAE +971 55 768 7199