TRAINER RESOURCES

CYBER SECURITY TRAINING

Lesson Plan — Trainer Guide

DURATION	GROUP SIZE	LEVEL
4 Hours	Up to 12 Learners	Awareness / Foundation

LEGISLATION	RESOURCES	ASSESSMENT
UK GDPR | Data Protection Act 20...	Handout, Quiz, Slides	Knowledge Check Quiz

LEARNING OBJECTIVES

- Understand the cyber threat landscape and common attack types
- Recognise phishing, social engineering and other human-targeted attacks
- Apply password security best practices and multi-factor authentication
- Understand data protection obligations under UK GDPR
- Know how to report a cyber security incident

SESSION PLAN

0:00–0:15	Welcome	**Welcome & Introductions**	Trainer intro, housekeeping, fire exits, learning outcomes for Cyber Security
0:15–0:30	Icebreaker	**Warm-Up Activity**	Icebreaker to engage learners and introduce the topic of Cyber Security
0:30–1:00	Theory	**Key Legislation & Background**	UK GDPR | Data Protection Act 2018 | Computer Misuse Act 1990 — why it matters, employer duties, employee responsibilities
1:00–1:30	Theory	**Core Knowledge — Part 1**	Key facts, statistics, risk factors, and underpinning knowledge for Cyber Security
1:30–1:45	Break	**Morning Break**	15-minute comfort break — trainer to prepare practical equipment
1:45–2:15	Theory	**Core Knowledge — Part 2**	Deeper dive into Cyber Security — common hazards, control measures, best practice
2:15–2:50	Practical	**Demonstration & Supervised Practice**	Trainer demonstrates key techniques; learners practise in pairs with trainer feedback
2:50–3:00	Break	**Short Break**	10-minute break — distribute quiz papers
3:00–3:20	Assessment	**Knowledge Check Quiz**	Learners complete the quiz individually; trainer collects and marks
3:20–3:40	Activity	**Group Scenario Exercise**	Teams work through a realistic scenario applying Cyber Security knowledge
3:40–3:55	Review	**Quiz Review & Q&A**	Go through quiz answers; address any misconceptions; open Q&A session
3:55–4:00	Close	**Summary & Close**	Recap key learning points, issue certificates, signpost further resources