JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Cybersecurity Fundamentals for New IT and Business Staff Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Cybersecurity Fundamentals for New IT and Business Staff Training Course

Cybersecurity Fundamentals is a 1-week training course for new IT staff, business analysts and professionals moving into security roles, who leave with a Baseline Security Checklist for their own team. Every function now handles cloud accounts, remote endpoints and customer records, so a shared grasp of confidentiality, integrity and availability prevents the simple mistakes attackers exploit most. Jupiter Prime Training offers this course on cybersecurity fundamentals for new IT and business staff.

Why Cybersecurity Fundamentals Matters Now

Three forces raise the stakes for newcomers: phishing and credential theft that target ordinary users rather than servers, hybrid work that scatters laptops and phones beyond the office network, and customers and auditors who ask for evidence of basic controls before signing contracts. An organisation whose new joiners recognise attack paths and apply baseline hygiene closes most easy openings; one that leaves security to a small specialist group keeps reopening them. The course draws on the NIST Cybersecurity Framework 2.0 NIST CSF 2.0 functions and the control themes of ISO/IEC 27001:2022.

Who Gains Most from Cybersecurity Fundamentals

- Junior IT support staff who set up accounts, devices and access requests
- Business analysts who specify systems handling personal or financial records
- Professionals moving from networking or development into a first security post
- Project coordinators who track security requirements in technology rollouts
- Service desk agents who field suspicious emails and password reset calls

A newly formed IT or digital unit that sends several joiners at once gains most, because its members return with the same vocabulary and checklist.

Cybersecurity Fundamentals Capabilities

Participants move from recognising threats to applying the first line of controls on accounts, networks and devices.

- Apply the CIA triad to classify the records and systems a team handles — information owners
- Assess common attack paths such as phishing, malware and weak passwords — service desk escalation
- Specify least-privilege access and multi-factor authentication for user roles — system administrators
- Test basic network segmentation and firewall rules against simple scenarios — infrastructure leads
- Build endpoint hardening steps for laptops and mobile devices — device management owners

- Communicate suspected incidents clearly and promptly — the security function and line managers

Key Cybersecurity Fundamentals Terms

- CIA triad — confidentiality, integrity and availability, the three properties every security control aims to protect.
- Attack surface — all the points, such as accounts, devices and exposed services, where an intruder could try to enter.
- Least privilege — giving each user or system only the access needed to perform its task and nothing more.
- Multi-factor authentication — sign-in that requires two or more independent proofs, such as a password and a device prompt.
- Patch management — the routine of finding, testing and applying software updates that fix known weaknesses.
- Social engineering — manipulating people into revealing information or granting access, often through email, phone or messaging.

Cybersecurity Fundamentals Day by Day

Day 1: Security Principles and the Threat Picture

- CIA Triad Applied to Everyday Systems — Classifying What Needs Protection
- Threat Actor Types and Motives — Anticipating Who Targets the Organisation
- NIST CSF 2.0 Functions Overview — Locating Each Role in the Security Cycle
- Asset Inventory Basics — Knowing Which Devices and Accounts Exist
- Retail and Logistics Breach Stories — Tracing Simple Root Causes

Day 2: Attack Paths and Human Factors

- Phishing and Social Engineering Anatomy — Spotting Lures Before Clicking
- Malware and Ransomware Families — Recognising Infection Signs Early
- Password Attacks and Credential Stuffing — Strengthening Sign-In Practices
- Kill Chain Walk-Through — Seeing Where Defences Can Interrupt Attacks
- Reporting Suspicious Activity — Choosing the Right Escalation Channel

Day 3: Identity and Access Control

- Identity Life Cycle From Joiner to Leaver — Removing Orphaned Accounts
- Least Privilege and Role-Based Access — Approving Permissions With Discipline
- Multi-Factor Authentication Options — Selecting Methods for Each User Group
- Privileged Account Handling — Separating Admin Rights From Daily Use
- Access Review Routine — Confirming Permissions With Business Owners

Day 4: Network and Endpoint Protection Basics

- Network Segmentation and Firewall Concepts — Limiting Lateral Movement
- Secure Wi-Fi and Remote Access — Protecting Hybrid Workers
- Endpoint Hardening Settings — Reducing Laptop and Phone Exposure
- Patch Management Cycle — Prioritising Updates by Severity
- Backup and Restore Basics — Preserving Availability After Ransomware

Day 5: Practising the Baseline Security Checklist

- Asset and Data Classification Drill — Applying the CIA Triad to Team Systems
- Phishing Simulation Debrief — Applying Attack Path Knowledge to Real Lures
- Access Rights Spot Check — Applying Least Privilege to Sample Accounts
- ISO/IEC 27001:2022 Control Themes Mapping — Linking Checks to Recognised Controls
- Baseline Security Checklist — Completing Identity, Device, Network and Reporting Checks

Applying Cybersecurity Fundamentals After the Course

- Run the access spot check on one shared system and remove accounts belonging to leavers.
- Brief colleagues on the phishing reporting route using two recent lures the team received.

Cybersecurity Fundamentals Questions FAQ

What are cybersecurity fundamentals, and why do they matter now?

They are the core principles and baseline controls that protect accounts, devices, networks and records. They matter now because most intrusions still begin with phishing, reused passwords or unpatched devices that trained staff can catch.

Which roles gain most from cybersecurity fundamentals training?

New IT staff, business analysts and professionals moving into security gain most. Their daily decisions on access, devices and reporting shape the organisation's exposure from the start.

How does cybersecurity fundamentals training differ from a sector-specific AI security course?

It builds the general foundation that every later specialisation assumes. A sector-specific course applies machine learning defences to one industry's systems; this subject teaches the principles, attack paths and baseline controls that apply in any organisation.

What do you bring back from cybersecurity fundamentals training?

You bring back a Baseline Security Checklist. It covers data classification, access rights, multi-factor sign-in, device hardening, patching, backups and the route for reporting suspicious activity.

Cybersecurity Fundamentals: The Way Forward

The Baseline Security Checklist first informs which accounts, devices and shared systems a team should fix before anything else. Team leads, IT support and information owners use it to agree quick improvements and track them. After its first quarterly run, the threat assumptions behind it are worth revisiting, as attack paths shift and new services join the asset inventory.