



AMTCE DIGITAL CYBER PROGRAMME

COURSE OUTLINES

Long Course Outlines

Description
AMTCE Digital Cyber Course Outlines
Chris Gilson
September 2022

Phase 1 - Cyber Skills Programmes.

- Cyber Awareness
- Getting Started in IT
- Cyber IQ & Bridging Programme
- Cyber Skills at Entry Level
- Core Digital Skills for Network, Cloud, Virtualisation & Cyber

Course Title		Category (Sector)	Duration
Cyber Awareness		Digital & Cyber	3 Hours Introductory Workshop + 10 hours On-line
Course Aim	Introductory Workshop and on-line, learning that covers core behaviours and phishing. The purpose of this course is to increase personal awareness & improve behaviours around the main cyber threats and existing regulation.		
Course Content	Modules	Description	
	Social engineering	The art of tricking people into taking actions they never normally would. Learn to recognise the signs.	
	Malware & breach recovery	Learn how to spot the signs of malware and know what to do if one of your devices becomes infected.	
	Device security	Your devices contain lots of personal information. Learn how to protect them, as well as save yourself some money.	
	Browsing securely	Some websites are safe to use. Others are not. Some are created deliberately to steal personal details or damage your devices.	
	Public Wi-Fi	Learn how to stream movies from anywhere in the world and stop search engines tracking you. Oh, and learn how to use Wi-Fi safely!	
	Preventing identity theft	This module will show you how to steal an identity. It'll also give you the tools to ensure you can prevent it happening to you!	
	Passphrases	Using a passphrase is the single most effective thing you can do to prevent cybercrime. Learn how to quickly create and remember them.	
	Am I really a target?	Does your role or the organisation you work for make you more of a target for cyber criminals?	
	CybEssentials	All first, second and third-tier security behaviours in a single module. The perfect one-stop shop refresher.	
	Threat focus: Browser-in-the-browser	Paige has seen the sign-in window a thousand times. How could she know it was a wolf in sheep's clothing?	
	Protecting your devices	When it came to device security, John had it all figured out. Unfortunately, so did Leah.	
	Are you really a target?	Joe is many things. A father, husband, amateur flautist, and the Head of Sales. He's also a target.	

	Supply chain: No weak links here	The surprising truth about your role in supply chain security, and how to reinforce your link.
	Working remotely	When a video call is the only form of human interaction, there's no wonder Sarah missed the red flags.
	Spotting fake emails	The true story of a prank so good, even the White House fell for it.
	Threat focus: Ransomware	Familiarise yourself with ransomware. Learn how it gets in, how to contain it and how to stay protected.
	Sophisticated attacks	Meet Sophie. Sophie breaks into buildings.
	Passphrases	I hack email accounts because I can. And because people make it easy for me.
	Security incidents: Your role	Peter just wanted to be loved. It was a big mistake.
	Preventing identity theft	Gemma was living a double life. The problem was, she didn't know it.
	Data privacy & your rights	Data privacy. It gives people powerful rights over how organisations use their data. It's everyone's responsibility to look after it.
	GDPR & your rights	GDPR. It gives people powerful rights over how organisations use their data. It's also everyone's responsibility to look after it.
Learning Outcomes	<ul style="list-style-type: none"> • Influence over seventy specific security behaviours to meet security awareness, compliance requirements and reduce human risk. • Assess security culture and measure behavioural change by visualizing risks, tracking progress with data and metrics you can't get anywhere else. • Nudge and support people across multiple platforms by giving people the push they need to act and provide real-time, frictionless help when they need it most. • Run phishing simulations that tell you what drives behaviours, find out why people click on, engage with, and report phishing attempts—or why they don't. 	
Learner Profile	All Staff who have not been exposed to cyber awareness training before.	
Certification/ Awarding Body	CybSafe Corporate Accreditation	

AMTCE DIGITAL CYBER PROGRAMME COURSE OUTLINES		
Course Title	Category (Sector)	Duration
Getting Started in IT	Digital & Cyber	2.5 Hours Workshop + 10 hours
Course Aim	This on-line, self-directed course will introduce key concepts in Information Technology. It steps through the building block ideas and concepts that will help in an Information Technology or Cyber career.	
Course Content	Modules	
	<ul style="list-style-type: none"> • Basic IT Concepts • Virtualisation Hands On • Operating Systems Hands On • Networking Hands On • HTML & World Wide Web • Intrinsic Security Hands On. 	
Learning Outcomes	<ul style="list-style-type: none"> • Explore all aspects of Information Technology that are present in today's organisations • Demonstrate how systems are interconnected from the individual user to the Network to the Cloud • Introduce the software development process and how applications have evolved • Explain other concepts such as Virtualisation, Containerisation and the importance of Cyber Security 	
Learner Profile	Individuals who are interested in IT and would like to know the basic computing concepts	
Certification/ Awarding Body	VMWare Academy	

AMTCE DIGITAL CYBER PROGRAMME COURSE OUTLINES		
Course Title	Category (Sector)	Duration
Cyber IQ & Bridging Programme.	Digital & Cyber	2.5 Hours Workshop + 15 hours
Course Aim	Cyber IQ training gives employees the knowledge and tools to recognize, avoid and report cyber-attacks and security incidents. This helps to keep organizations & people secure by preparing employees for cyber-attacks that make it past technical controls. IQ Training will help individuals to decide what type of cyber role, they would prefer and links to a role specific bridging programme.	
Course Content	Modules	
	<ul style="list-style-type: none"> • Introductory Workshop • Need to Know Series • Phishing, Vishing & Marine Lowlife series. • Password and Data Security • Social Engineering / GDPR • Malware & Ransomware / Removable Media • Physical Security & Working Remotely • Mobile Security / Safe Web Browsing • OWASP Series • Phishing Attacks 	
Learning Outcomes	<ul style="list-style-type: none"> • Introduce cyber definitions and language to help steer through the programme • Increase awareness about the major forms of attack and defence. • Identify the most appropriate, cyber role for the individual Trainees 	
Learner Profile	Individuals who are considering cyber as a career option and interested in entry roles.	
Certification/ Awarding Body	CompTIA	

AMTCE DIGITAL CYBER PROGRAMME COURSE OUTLINES

Course Title	Category (Sector)	Duration
Cyber Skills At Entry Level.	Digital & Cyber	2.5 Hours Workshop + 80 - 120 hours on-line (dependent on Role)
Course Aim	The aim of these programmes is to provide entrants to Cyber Security a learning pathway to achieve external accreditation and professional recognition for cyber- analysts, penetration tester, investigator, auditor & architect	
Course Content (Modules)	Module	Description
	Cyber Analyst Role	<ul style="list-style-type: none"> CompTIA A+ CompTIA Network+ Information Security Fundamentals CompTIA Security+ CompTIA CySA+ Fundamentals CompTIA CySA+ Linux Fundamentals
	Senior Cyber Analyst Role	<ul style="list-style-type: none"> CompTIA Advanced Security Practitioner (CASP+) CISA (Certified Information System Auditor) Certified Information Systems Security Professional (CISSP) Information Systems Security Engineering Professional (CISSP-ISSEP) SCADA Security Analyst Incident Response Certified Computer Security Incident Handler Vulnerability Assessment Network Traffic Analysis Cyber Range Cybersecurity Data Science

Course Content (Modules)	Cyber Investigator Role	<ul style="list-style-type: none"> • CompTIA Advanced Security Practitioner (CASP+) • Certified Information Systems Security Professional (CISSP) • Information Systems Security Engineering Professional (CISSP-ISSEP) • Information Systems Security Architecture Professional (CISSP-ISSAP) • Incident Response • Certified Computer Security Incident Handler • IACRB Certified Computer Forensics Examiner • Network Traffic Analysis Cyber Range
	Cyber Auditor Role	<ul style="list-style-type: none"> • CISA (Certified Information System Auditor) • Certified Information Systems Security Professional (CISSP) • Information System Security Management Professional (CISSP-ISSMP) • Certified Authorization Professional (CAP) • Cybersecurity Audit Fundamentals • Cybersecurity Administration • Intro to Vulnerability Management • Vulnerability Assessment
	Pen Tester	<ul style="list-style-type: none"> • Penetration Tester Role • Ethical Hacking • Certified Expert Penetration Tester (CEPT) • PenTest+ • Certified Ethical Hacker • Certified Mobile and Web App Penetration Tester (CMWAPT) • Penetration Testing Cyber Range
	Cyber Security Management	<ul style="list-style-type: none"> • CISA (Certified Information System Auditor) • Certified Information Systems Security Professional (CISSP) • Information Systems Security Architecture Professional (CISSP-ISSAP) • Security Architecture • Certified SCADA Security Architect (CSSA) • AWS Essentials & Solutions Architect Associate

Learning Outcomes	Provide and instruct Trainees in the learning pathway that gains accreditation for Entry Grade Roles <ul style="list-style-type: none"> • Cyber Analyst Role • Senior Cyber Analyst • Cyber Investigator • Cyber Auditor • Cyber Architect Role • Penetration Tester
Learner Profile	Individuals who have the right aptitude and attitude to cyber work and are considering it as a career option and interested in entry roles.
Certification/ Awarding Body	CompTIA and Professional Bodies

AMTCE DIGITAL CYBER PROGRAMME COURSE OUTLINES		
Course Title	Category (Sector)	Duration
Core Digital Skills for Network, Cloud Virtualisation & Cyber	Digital & Cyber	3 Hour Workshop & 28 Hours on-line.
Course Aim	Introduce Cloud and Virtualization concepts in everyday computing to include topics such as the benefits of virtual machines, the flexibility of cloud computing and the basics of vSphere components	
Course Content	Modules	
	<ul style="list-style-type: none"> • Data Centre Virtualisations • Network Virtualisation • Digital Workspace • Application Modernisation • Cloud Management & Automation • End Point Security. 	
Learning Outcomes	<ul style="list-style-type: none"> • Introduce Trainees to the major VMware NSX® components in the data, management and control planes. • Build and use a Virtual Machine to apply Network virtualization concepts. • Consider applications in multiple environments. • Assure that all systems are properly secured against threats. 	
Learner Profile	Individuals who wish to expand their skillset through access to the VMWare Academy to achieve recognised Technician or Professional status.	
Certification/ Awarding Body	VMWare Academy	