Introduction to Cyber Security

By : The Training Company ™

Short course, assessment, exam and certification.

Date : 21 May 2022

Who is this course for?

- Anyone new to cyber security who needs an introduction to security fundamentals
- Non-IT security managers
- Professionals with basic computer and technical knowledge
- Career changers to cyber security
- Managers, information security officers, and system administrators
- Anyone who writes, implements, or must adhere to an enterprise security policy

To determine if this course course is right for you, ask yourself five simple questions:

- Are you new to cyber security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Do you need to be conversant in basic security concepts, principles, and terms, but do not need extreme details?
- Have you decided to make a career change to take advantage of the job opportunities in cyber security and need some kind of training and certification to show the potential employers.
- Are you a manager who lays awake at night worrying that your company may be the next major data breach headline story in the news?

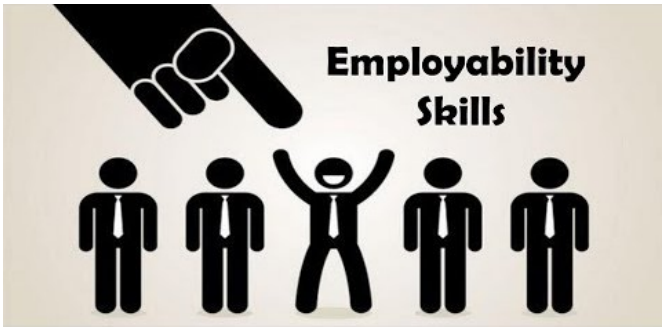
If you answer yes to any of these questions, the This course: Introduction to Cyber Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to cyber security.

This 2 month comprehensive course covers everything from core terminology to the how computers and networks function, security policies, risk management, a new way of looking at passwords, cryptographic principles, network attacks & malware, wireless security, firewalls and many other security technologies, web & browser security, backups, virtual machines & cloud computing. All topics are covered at an easy to understand introductory level.

This course is for those who have very little knowledge of computers & technology with no prior knowledge of cyber security. The hands-on, step-by-step teaching approach enables you to grasp all the information presented, even if some of the topics are new to you. You'll learn real-world cyber security fundamentals to serve as the foundation of your career skills and knowledge for years to come.

Written by a cyber security professional with over 30 years of industry experience in both the public and private sectors, This course provides uncompromising real-world insight from start to finish.

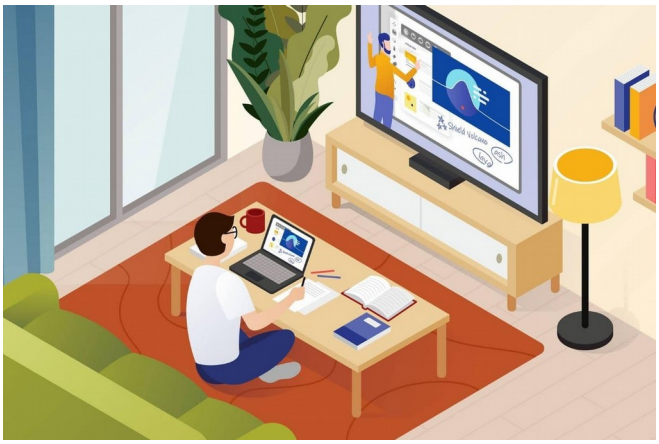
Enhance your employ-ability



Boosting your technical skills by understanding the world of cyber security and how it applies to your business and job role, or the career of your dreams, is one of the many reasons to up-skill in this field. All of the topics in our courses are based on the the skills that employers are actively seeking within the cyber security sector.

Learning these new skills that can be applied directly to real-world scenarios will enhance your employ-ability. Not only will you enhance your practical application of cyber security, but you'll have a credible qualification totally focused on cyber security, demonstrating that you see the value of cyber security for your sector. It also makes you an attractive candidate for developing, managing and planning cyber security solutions in your role, business or sector.

Study online and continue your career



Our courses are available in distance learning, online, classroom and on premises formats. This allows you to learn whenever suits you best, wherever you are in the world. This allows you to fit your study flexibly around your work commitments and personal responsibilities, whether that is family and hobbies or activities that you complete in your free time. Incorporating online study into your daily routine allows you to study when you are most productive, whether that is first thing in the morning before you start work, during a lunch break, or after work.

Studying with us also means that you can continue in your current job role to simultaneously advance your practical and academic knowledge. This makes the learning material much more enjoyable and easier to comprehend as you can see first-hand the impact that you are making in the workplace and in your online course.

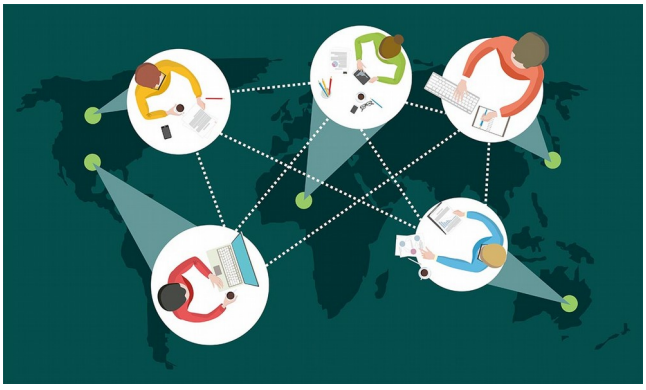
Push for best practice in your industry

The course curriculum as well as diverse and highly relevant, is taught by computer scientists specifically for professionals who recognize the importance of cyber security to their sector. This means that the course content is presented at a level that encourages you to critically engage in pushing the boundaries of best practice in your industry and potentially changing the way you impact business efficiencies in your sector.

Becoming an expert in cyber security will enable you to challenge current ways of working and change the way you perceive most things. Highlighting yourself as someone who strives for positive change, as well as an eagerness to learn the latest technologies could take you a long way in your career.

Network with experts across the world

Studying in a group allows you to grow your global network as you collaborate with professionals living and working across the world. This happens through live seminars, discussion forums, group projects and more.



Networking with people experiencing similar challenges across a variety of industries across the globe enriches your experience and gives you a deeper understanding of cyber security in your sector and others too.

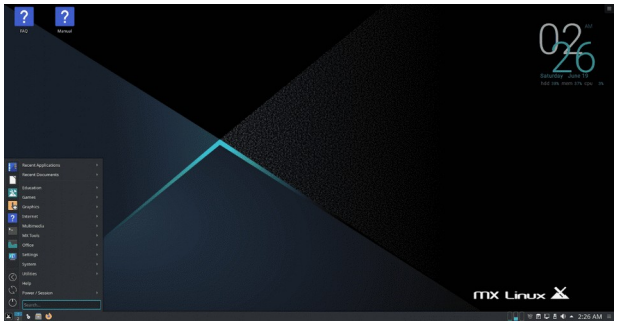
On an academic level, being able to discuss ideas with others can help you to understand and illustrate your work with examples. It also helps get experience in working with remote teams.

Certification

This course includes the MuftaSoft ™ Information Security Fundamentals certification. This certificate validates a practitioner's knowledge of security's foundation, computer functions and networking, introductory cryptography, and cybersecurity technologies. MuftaSoft certification holders will be able to demonstrate key concepts of information security including understanding the threats and risks to information and information resources and identifying best practices to protect them.

Prerequisites for the course

- Have a Linux Desktop loaded with MX Linux.
- Basic knowledge of computers.
- No previous security knowledge required.



Course outline.

Introduction to the following topics :

Cyber security terminology

Understanding Basic Security Frameworks

Fundamental frameworks, models, and approaches to cyber security including the CIA model.

Purpose of Cyber Security

Adversary Types

Vulnerability Types

Threat Types

Confidentiality Threat

Integrity Threat

Availability Threat

Fraud Threat

Testing for Vulnerabilities

Attacks

Brute Force vs. Heuristic Attacks

Cryptanalysis

Computer networks

Security policies

Incident response

Passwords

Cryptographic principles

Khawar Nehal’s 4 Layers of cybersecurity.

Physical security penetration testing

Khawar Nehal’s 6 Levels of security for LAN networks.

The Common Seven Layers Of Cybersecurity

Firewalls

Secure Configuration

User Access Control

Cybersecurity Administration

Malware Protection

System Safeguards

Network Defense

Patch Management

The need for cybersecurity

Attacks, concepts and techniques

Protecting your data and privacy

Protecting the organization

PCI-DSS, ISO-27001, NIST, SOC, SOX and HIPAA

Penetration Testing

Examining Cyber Threats More Closely

SQL/ Slammer Worm of 2003

Nachi Worm of 2003

Botnet Design

Botnet Arithmetic

Assets and Infrastructure

Calculating Risk

Making Security and Cost Decisions Based on Risk

Threat Trees and Completeness of Analysis

Threat Trees

Introducing Security Risk Analysis

Basic engineering and analysis methods for managing cyber security risk to valued assets.

Mapping Assets to Threats

Estimating Risk for Threat-Asset Pairs

Mapping Assets, Threats, Vulnerabilities, and Attacks

Course Objectives & Outcome Statements

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability for prioritization of critical security resources
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand how a computer works
- Understand computer network basics
- Have a fundamental grasp of any number of technical acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS, and more.
- Utilize built-in Linux tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, intrusion detection systems, sniffers, ethical hacking, active defense, and threat hunting.
- Understand wireless technologies including WiFi, Bluetooth, mobile phones and the Internet of Things (IoT)
- Explain a variety of frequent attacks such as social engineering, drive-by downloads, watering hole attacks, lateral movement, and other attacks
- Understand different types of malware
- Understand browser security and the privacy issues associated with web browsing
- Explain system hardening
- Discuss system patching
- Understand virtual machines and cloud computing
- Understand backups and create a backup plan for your personal life that virtually guarantees you never have to pay ransom to access your data

Computer Requirements

Important! You need a computer configured to these requirements.

A properly configured system is required to fully participate in this course. If you do not carefully read and follow these instructions, you will likely leave the class unsatisfied because you will not be able to participate in hands-on exercises that are essential to this course. Therefore, we strongly urge you to arrive with a system meeting all the requirements specified for the course.

This course includes both lecture and hands-on labs. There are specific computer configuration requirements to perform hands-on labs. If you take This course live in the classroom, you utilize a classroom network to connect to a lab server. If you take This course online via OnDemand, you connect to the lab environment via the Internet. To accomplish this, you need the following:

- A laptop running any distribution of Linux. MX Linux preferred.
- We do not recommend attempting to perform the labs with a small computer like a Raspberry PI. Less than 4GB of RAM can cause slow performance.
- Working internet connection to the computer.

Estimated times for this course.

Self Study : 40 hours.

Exams and assessments : 5 hours.

Assignments : 20 hours.

Online discussions : 10 hours.

The actual time required shall vary depending on the students methods of learning.

Time available to complete the course : 2 Months.

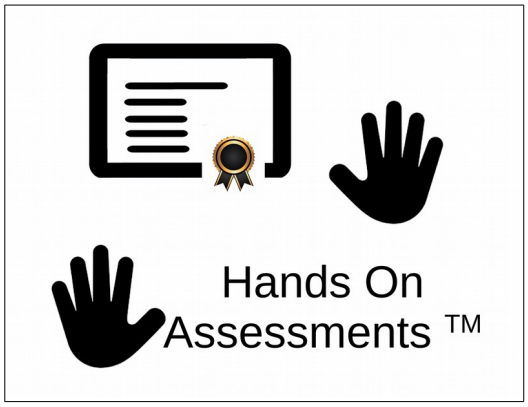
Course fees : LTC 3 (USD 209 / PKR 42167 / NANO 163)

Financial Aid available.

Group discounts available.

Includes :

- Access to course material
- Assessments
- Exams
- Shareable certificate
- Printed certificate
- Resources for each topic of training that includes videos, and reading material.
- Access to trainers to answer your questions via email, VoIP and video.
- Graded assignments, Labs, Quizzes, Assessments, Vivas and Exams.



Contact :

cybersecurity-course@atrc.net.pk

+92 343 270 2932

http://atrc.net.pk