Buy Now

Cybercrimes Act 19 of 2020 and Business Email Compromise | Online law Course

This is a South African law that came into effect to combat growing cyber threats and provide a legal framework to prosecute cybercriminals.

Purpose of the Act:

- To criminalize certain cyber activities, such as hacking, phishing, identity theft, cyber fraud, and the distribution of harmful data.
- To protect individuals, businesses, and the state against cyber-related crimes.
- To allow for law enforcement to investigate, prosecute, and gather evidence for cybercrime cases.
- To ensure international cooperation in dealing with cyber threats that cross borders.

Key Offences Under the Act:

- Unauthorised access to data or computer systems.
- Cyber fraud and forgery.
- Malware creation and distribution.
- Cyber extortion.
- Identity theft and impersonation.

- Interception of communications without authority.
- Publication of harmful data, including revenge porn or racially offensive content.

Overview

Understand the implications of the Cybercrimes Act 19 of 2020 and learn how to protect your business from email compromise threats. This course covers legal frameworks, cybercrime prevention strategies, detection techniques, incident response, and compliance requirements, equipping you with the skills to safeguard your organization against cyber threats.

Description

The Cybercrimes Act 19 of 2020 is a pivotal law designed to address the growing threat of cybercrime in South Africa. This comprehensive course delves into the provisions of the Act and provides practical insights into combating business email compromise (BEC), a prevalent cyber threat that targets organisations globally. This course is ideal for IT professionals, cybersecurity specialists, compliance officers, and business leaders who want to enhance their understanding of the Cybercrimes Act and protect their organizations from cyber threats. By the end of the course, you will be equipped with the knowledge and skills to implement effective cybersecurity measures and respond to cyber incidents confidently.

Course Content

Unit 1: Introduction to the Cyber Security Act 19 of 2020

- Overview of the Cyber Security Act
- Key Definitions

Unit 2: Cybersecurity Fundamentals

- Principles of Cybersecurity
- Data Protection and Privacy
- Secure Data Handling
- Ransomware

Unit 3: Recognising and Preventing Business Email Compromise (BEC)

- Understanding BEC
- Preventative Measures

Unit 4: Compliance with the Cyber Security Act

- Duties Under the Act and Penalties for Non-Compliance
- Penalties for Non-Compliance

Unit 5: Practical Cybersecurity in the Workplace

- Daily Cybersecurity Practices
- Creating a Secure Work Environment

Accreditation

- Non-accredited: Short course only
- Duration: 1h 30m
- Delivery: Classroom/Online/Blended
- Access Period: 12 Months

Print this Course Overview in PDF

Search...