



Ed-Tech
A F R I C A

CYBER SECURITY

3 MONTHS





Ed-Tech

A F R I C A

Transforming education
through technology



Course Aims & Objectives

You will have an introduction to Cyber Security and its aspects as well as basic terms and nomenclature involved with it. Moving further, you will have all the basic requirements at your fingertips to have a vast understanding of Cyber Security as a whole.

This course will provide you with an overview of the cybersecurity landscape as well as national and international views. We'll go through the legislative landscape that affects cybersecurity, as well as the most common threat actors.

To assess the learning level and progress with continuous and rigorous ways to ensure highest level of knowledge and professional exposure ensuring a practical approach.

Learn about the evolution of cybersecurity as a field, as well as the standards, regulations, and frameworks that arose to respond to evolving cyber threats.

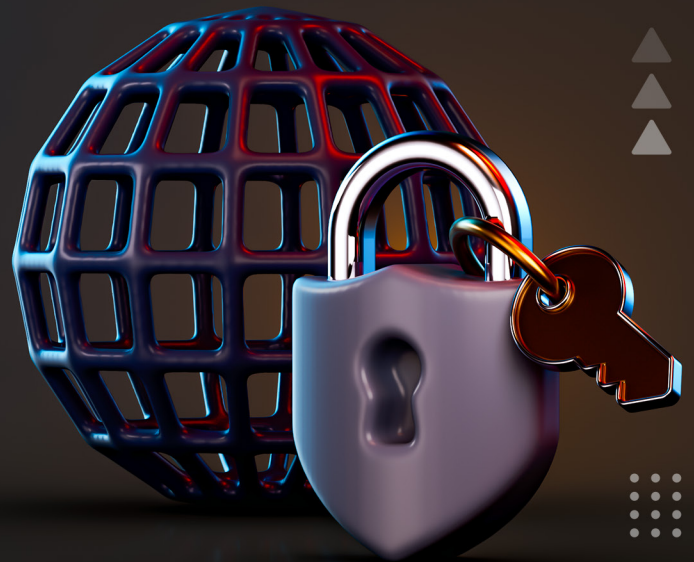
Define and apply essential concepts and words in the realm of cybersecurity.

Gain an advanced level of understanding for future prospects and professional level requirement.

Curriculum Index

- * **Introduction to Cybersecurity, CIA Triad, Elements of Cybersecurity**
- * **Malware types**
- * **NETWORK BASICS, TYPES, TOPOLOGIES**
- * **IMPORTANT PROTOCOLS AND PORTS**
- * **OSI AND TCP/IP MODEL**
- * **FIREWALLS, HONEYPOTS**
- * **MITM, DNS HIJACKING, ARP, POISONING, WIRELESS ATTACKS**
- * **CLOUD FUNDAMENTALS, SAAS, IAAS, PAAS**
- * **VIRTUALIZATION AND HYPERVISOR**
- * **API SECURITY**
- * **CRYPTOGRAPHY BASICS**
- * **DEFENSE IN DEPTH, CYBERWARFARE (CASE STUDY)**

What is Cyber Security?



Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- Network security
- Application security
- Information security
- Operational security
- Disaster recovery and business Continuity
- End-user education

It is used by most companies to;

- Protect against phishing schemes
- Ransomware attacks
- Identity theft
- Data breaches
- Financial losses

Examples of Cyber security:

- Antivirus and Antispyware programs
- Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.

JOB OPPORTUNITIES

- * Chief Information Security officer (CISO)
- * Security Architect
- * Cybersecurity Engineer
- * Malware Analyst
- * Penetration Tester
- * Computer Forensics Analyst
- * Application Security Engineer
- * Cloud Security Specialist

TYPES OF CYBER THREATS

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

MALWARE

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL INJECTION

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

PHISHING

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

MAN-IN-THE-MIDDLE ATTACK

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecured WiFi network, an attacker could intercept data being passed from the victim's device and the network.

DENIAL-OF-SERVICE ATTACK

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.



Ed-Tech
A F R I C A

☎ +267 3914472

🌐 ED Tech Africa

📷 Ed-Tech Africa

📞 +267 75 546 649

📧 @edtech.bw

▶ edtechafricabw

www.ed-techafrica.com

www.ed-techafrica.com