IMPACT AFRICA EDUCATION FOUNDATION
IMPACT AFRICA TECHNICAL UNIVERSITY U.S.A
Address: 2235 Serena Hills Dr. Ramona, California. USA. 92065 .
Address: 51 Isipingo Street. Bellevue East, Johannesburg. 2198. South Africa
E-mail: President@impactafricanetwork.org
www.impactafricatechnicaluniversity.com
www.impactafricanetwork.org
www.impactafricatelevisionnetwork.com
+27 78 846 2440; +1 678 856 3709; +1 760 708 1888

IMPACT AFRICA TECHNICAL UNIVERSITY USA
WWW.IMPACTAFRICATECHNICALUNIVERSITY.COM
EMAIL: REGISTRAR@IMPACTAFRICATECHNICALUNIVERSITY.COM
IMPACTAFRICANET@GMAIL.COM
TEL/WHATSAPP +27 78 846 2440

INFORMATION DEPARTMENT
CYBER SECURITY

COURSE OUTLINES/SYLLABUS

In this course, Students will learn the fundamentals of cyber security also known as information security**, security threats, modes of attack,** and **cryptographic models. Access control, identification, and authentication** are also addressed**. Network security and operating system (OS**) hardening are explained along with **intrusion detection and prevention**. The course concludes with **global privacy laws** and some shots on **Ethical Hacking.**

MODULE 1: Introduction to Cyber security

This course begins with an overview of information security and its evolution. This first section introduces the core goals of information security; the CIA triad. Some common information security terms and processes used in the information security industry are defined and outlined. Types of controls and their function are categorized so the learner can comprehend the design of a defense-in-depth system. The unit concludes with a justification of why humans are known as the weakest link in information security and describes how security awareness training can serve to mitigate this risk. The topics in this unit are in preparation for the more detailed security topics in the following units.

MODULE2: Threats and Attack Modes

This unit introduces common threats and attack modes on information systems. The unit begins by differentiating between threats, attacks, and attack agents, and continues with a description of access control, spoofing, social engineering, application, web application, malware, and denial of service attacks. Understanding the method of an attack is instrumental to understand mitigation efforts used in information systems, and is a segway into the next unit on cryptographic models used to protect information from these attacks.

MODULE 3: Cryptographic Models

One of the earliest ways to encrypt a message was with a substitution cipher developed by Julius Caesar, known as the Caesar cipher. Today, in the information age, cryptology involves the use of computers to create complex algorithms. In this unit, we examine various symmetric and asymmetric key algorithms, as well as hashing algorithms. Encryption is a tool that can be used to support all three tenets of the CIA triad, the goal of information security.

MODULE 4: Access Control

The main goal of information security is to protect data from unauthorized disclosure. Access control models are used in an organization to provide the appropriate access to users based on individual or group privileges.

Privileges can be granted based on clearance levels, discretion, roles, or rules. The types of access control models used to restrict access that will be reviewed in this unit are mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), and rule-based access control (RB-RBAC).

Address: 2235 Serena Hills Dr. Ramona, California. USA. 92065 .
Address: 51 Isipingo Street. Bellevue East, Johannesburg. 2198. South Africa
E-mail: President@impactafricanetwork.org
www.impactafricatechnicaluniversity.com
www.impactafricanetwork.org
www.impactafricatelevisionnetwork.com
+27 78 846 2440; +1 678 856 3709; +1 760 708 1888

MODULE 5: Identification and Authentication
As users or systems attempt to access secured data, their identities must be verified. The fundamentals of system access consist of both identification and authentication. A user identifies with a username and an authentication method to prove their identity. Authentication methods can be simple or more complex, depending on the desired level of security. Today, banks are requiring two-factor authentication, or two ways to authenticate a member's identity. With so many passwords to remember, users want the technology to log in with one password and to authenticate across all systems, or the capability of a single sign-on. This unit will discuss identification, types of authentication, human authentication factors, authentication forms, authentication protocols, methods for single sign-on (SSO), and public-key infrastructure (PKI).

MODULE 6: Network Security
This unit will discuss the security of networks, the mode for data in motion. As data is transferred across networks, it becomes another point of potential information insecurity. Networks can be designed to secure data in motion, and firewalls can improve security when placed appropriately in a network. Wireless networks are more insecure, but that insecurity can be mitigated via encryption and tunneling. In this unit, we will discuss several methods for protecting networks, including designing secure networks, using firewalls, protecting wireless networks, and other preventive methods like honeypots, network sniffers, and packet capturing.

MODULE 7: Operating System (OS) Security
Any operating system (OS) connected to a network is considered at risk of unauthorized disclosure. Networks have security systems in place, but an OS should still be hardened in case of unauthorized access. This unit addresses the methods used to harden an OS, protection methods such as antivirus and antimalware software, and OS firewalls and security tools that can provide OS security.

MODULE 8: Intrusion Detection and Prevention Systems
Even though networks and hosts have security methods in place, hackers continue to attempt to intrude upon systems and sometimes and are successful at gaining access. Intrusion detection systems (IDS) are used to track these attempts or intrusions and have the ability to stop an intruder from gaining access to information thereby keeping the information secure. This unit will discuss the different types of intrusion detection and intrusion prevention systems and will differentiate between network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). Tools for system information and event management (SIEM) such as scanners, network scanners, and web applications are also discussed.

MODULE 9: Privacy Laws, Penalties, and Privacy Issues
As information security evolves, laws designed to secure information are also evolving. Whether in the workplace or on social networking sites, individuals around the world want their privacy protected. Countries are enacting laws to protect the privacy of their citizens, and organizations with a successful data breach are finding a breach to be costly not only monetarily but to their reputation as well.

Address: 2235 Serena Hills Dr. Ramona, Califonia. USA. 92065 .
Address: 51 Isipingo Streert. Bellevue East, Johannesburg. 2198. South Africa
E-mail: President@impactafricanetwork.org
www.impactafricatechnicaluniversity.com
www.impactafricanetwork.org
www.impactafricatelevisionnetwork.com
+27 78 846 2440; +1 678 856 3709; +1 760 708 1888

This unit will discuss the importance of electronic data privacy protection, global privacy laws, some areas and issues of online privacy, and the penalties and adverse effects of a data breach on organizations.

MODULE 10: Ethical Hacking Course (Hacking Wireless Networks)

Wireless Network are the most common and popular technology today. Using wireless network increase not only mobility in a network but also the flexibility for the end users. In this ethical hacking module, Students will learn the concept of wireless networks, threat, attacks and vulnerabilities on wireless technologies and defending techniques.