Title	Practical Cybersecurity
Long Title	Practical Cybersecurity
Credits	**10**
NFQ Level	Fundamental
Module Author	Prof. Donna O'Shea

Module Description:

In this module, learners will be provided practical skills necessary to secure their networks, data devices, cloud security, VPNs, website security, defending cell phones, securing accounts i.e. passwords, multi factor authentication, physical security and playing safe on social networking sites. This is a very practical hands on module with all learning reinforced on a state of art cyber range infrastructure. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Identify and apply key measures that will secure data, applications and hosts in a business.
LO2	Understand and apply key tools and configurations that will secure a network against a cybersecurity attack
LO3	Evaluate key risks and security measures that business owners should consider when moving their business to the cloud.
LO4	Assess key physical security risks and measures the mitigate against these risks.
LO5	Evaluate and apply security settings that will protect a business website and ensure that employees can safely browse online.
LO6	Assess and apply security measures for wireless and Internet of Things (IoT) devices.

Indicative Content

Security Fundamentals

Security goals. Security Management Process. The CIA Triad. Authentication. Authorization and Access Control. Accounting and Auditing. Common security practices. Privilege Management. Cryptography. Security Policies.

Identifying Security Threats and Vulnerabilities

Social engineering, malware, software-based threats, network-based threats, wireless threats and physical threats.

Securing data, applications and hosts

Defence in Depth and layered security. Securing a new computer. Data security and protection. Effectively erasing files. Secure Backups. Understanding digital signatures. Application security – what is it, patch management and software updates. Host security – Operating Systems config settings, hardening etc. VoIP – understanding VoIP and its security implications. Risks of file sharing technology.

Network Security

What are network devices. Intrusion Detection Systems (IDS) and Network IDS (NIDS). Firewalls. Virtual Private Network (VPN). VLans and Subnets. NAT. Wireless Network Security. LDAP. LDAPS. Multi Factor Authentication. Validate integrity of hardware and software.

Cloud Security

What is cloud computing. Cloud models. Cloud threats – interfaces, DoS, data theft, account hijacking. How to protect data and resources in the cloud. Privacy. Security as a service in the cloud.

Physical Security

Different types of physical security measures. Environment exposures, controls and monitoring. Forensic Requirements. Personal Identifiable Information (PII) – laws, regulations. Disposal of electronic devices. Protecting portable devices.

Web and Social Networking

Website security. Understanding website certificates. Evaluating Web browsers security settings. Browsing Safely – understanding active content and cookies. Playing safe on social networking sites.

Internet of Things (IoT)

Securing IoT devices. Advice for business about building security with the IoT. IoT Password requirements. IoT Software updates.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Practical Skills and Evaluation	Using the cyber range the learner will be expected to complete a series of labs and practical assignments applying security settings and configurations to data, applications, networks and hosts.	1,2,3,4,5,6	50.0	Every Second Week
Short Answer Questions	The learner will be assessed on the theoretical knowledge that was delivered as part of the module content.	1,2,3,	25.0	Week 7
Short Answer Questions	The learner will be assessed on the theoretical knowledge that was delivered as part of the module content.	1,2,3,4,5,6	25.0	End Semester

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.00
Lab	Lab to support the learning outcomes.	3.0	Every Week	3.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.00
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support the learning outcomes.	3.0	Every Week	3.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.00
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Recommended Book Resources

- **William Chuck Easttom 2019, Computer Security Fundamentals, 4th Ed., Pearson IT Certification [ISBN: 0135774772]**