Safeguarding against Phishing in the age of 4 Industrial Revolution (CyberPhish)

CyberPhish Short Curriculum

Project Duration: November 2020 – November 2022

Project No.: 2020-1-LT01-KA203-078070

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Document Control			
Revision #	**Revision Date**	**Description**	**Name and Surname**
1 Draft Version 1.0	**02/04/2021**	**Original Draft**	**MECB Ltd (MT)**
2 Draft Version 2.0	**07/04/2021**	**Updated Draft**	**MECB Ltd (MT)**
4 Draft Version 3.0	**10/04/2021**	**Updated Draft following Feedback from Partners**	**MECB Ltd (MT)**
4 Draft Version 4.0	**31/05/2021**	**Final Version following Feedback from Partners and Experts**	**MECB Ltd (MT)**
5 Final Version 1.0	**08/06/2021**	**Final Version for Distribution**	**MECB Ltd (MT)**

Contents

INTRODUCTION

The Cyberphish Short Curriculum describes in detail the structure of the curriculum and aims to deliver concise but far-reaching modules in cybersecurity with a particular emphasis on cyber phishing. It shall be used for implementation into Higher Education Institutions (HEI) study modules and for dissemination purposes in order to attract participants to the course.

This short version consists of three levels topics: main topics, subtopics and subtopics' items with the main target being students, other course participants and teachers. These can use this curriculum in order to understand main goals and objectives of this course.

It is important to note that although the delivery of the curriculum is intended to have a blended learning approach, the way it is structured, allows flexibility in its delivery.

The Curriculum engages in introducing cybersecurity with a specific focus on cyberphishing. It is aimed at business and individuals at large and is designed to get both, geared up for Industry 4.0 and the potential security challenges the latter brings

Through the delivery of the Curriculum, learners shall acquire the skills to recognise and handle cyber-attacks, and how to protect devices and data against brute force attacks

1. THE CURRICULUM (E-LEARNING MODULE) STRUCTURE

1.1 Introduction

The Curriculum is aimed at both businesses and individuals who are experiencing the inevitable positive and negative effects brought by Industry 4.0 and who want to learn more and be more equipped in dealing with the security challenges brought about by this forth industrial revolution.

The Curriculum is structured in four distinct parts commencing with an introduction to the field of Cybersecurity and the related challenges brought by the advent of Industry 4.0. It delves into Cybersecurity and its legal aspects at European level together with how Cybersecurity is being fostered within the European Union.

Considering the importance and effects of social engineering and its relation to cyber-attacks, the curriculum expounds on the recognition of cyber-attacks and how to handle the latter to avoid disastrous and irreversible impacts.

Apart from providing a concise description of the various modules, the curriculum structure includes learning outcomes per module and the suggested hours and learning modalities. It is pertinent to note that although the curriculum includes a number of hours per module, these hours are to be regarded as contact hours. The full curriculum totals 30 hours which are equivalent to 1 ECTS. It is being suggested that the same number of hours per module are to be considered for self-study and assessment.

Curriculum Module	***Aim of Module***
1.0 Introduction to Cybersecurity	This module aims to introduce the Cybersecurity course and its topics to both trainers and students in Higher Education Institutions. It starts with a brief history of Cybercrime development and reasons for its fast growth as well as historical stages and current status. It also outlines the cyber-attack challenges individuals and businesses are witnessing with the advent of Industry 4.0, including but not limited to the decreased global

		boundaries, widespread use of mobile technologies, cloud computing, Internet of Things (IoT) and Big data. Other challenges include third party risks, and growing threats including nation-state threats. The trainers will be able to find the necessary material to introduce the learners to the concept of Cybersecurity together with the normal challenges faced by businesses, with real case scenarios where possible. The module delves also into the numerous definitions and jargon used and found in the Cybersecurity field.
2.0	Overview of Cybersecurity within the EU	This module introduces the learner to the existing EU policies and initiatives aimed at promoting the concept of Cybersecurity. It also discusses legal aspects of Cybersecurity both within the EU as well as worldwide, exposing learners to numerous real life scenarios and case studies in the field. The module includes an overview of tendencies in the Cybersecurity landscape, including but not limited to statistics, trends, relevant threats, legal, reputational and financial risks and case study analysis.
3.0	Cyber-attacks – Social Engineering and Phishing	This module introduces the learner to Cyber-attacks with a particular focus on Phishing. It also delves into detail on the concept of Social Engineering and Reverse Social Engineering together with the strong link of social engineering to cyber-attacks. The module also presents different types of phishing attacks and techniques together with a number of real case study examples from the Project Partner countries.
4.0	Understanding and Handling Cyber-attacks	This module introduces the learner to the concept of e-safety and the importance of adopting a proactive approach to cyber threats through the concept of cyber hygiene. The module also provides a detailed approach on how to recognise and handle cyber-attacks. The module introduces the development and implementation of incident response plans in order to minimise the effects of cyber-attacks.

1.2 E-Learning Module Structure in Detail

1.2.1 An Introduction to Cybersecurity

Title of Module	1.0 Introduction to Cybersecurity
Total Duration *(Hours / Slides)*	3 hours 46 – 60 Slides
Delivery Methods	Face-to-face Online Blended Delivery

Assessment	Face-to-face / Online Quiz
Learning Outcomes	• Have a general background to Cybersecurity in general • Understanding the challenges brought about by Cybersecurity • Understand how cyber-attacks have changed over time, leading to increased measures and hence the counter measures against cyber-attacks • Understand why it is important to follow the Cybersecurity landscape and why it is necessary to continuously update Cybersecurity knowledge. • Understand the different definitions related to Cybersecurity
Prerequisites	No initial knowledge required
Module Description	This module aims to introduce the Cybersecurity course and its topics to both trainers and students in Higher Education Institutions. It starts with a brief history of Cybercrime development and reasons for its fast growth as well as historical stages and current status. It also outlines the cyber-attack challenges individuals and businesses are witnessing with the advent of Industry 4.0, including but not limited to the decreased global boundaries, widespread use of mobile technologies, cloud computing, Internet of Things (IoT) and Big data. Other challenges include third party risks, and growing threats including nation-state threats. The trainers will be able to find the necessary material to introduce the learners to the concept of Cybersecurity together with the normal challenges faced by businesses, with real case scenarios where possible. The module delves also into the numerous definitions and jargon used and found in the Cybersecurity field.
MODULE SUB TOPICS	
1.1 Background – Challenges of the 4th Industrial Revolution	• Introduction to Cybersecurity • Brief history of Cybercrime development and reasons for its fast growth as well as historical stages and current status • Problem Background outlining the challenges businesses are witnessing against cyber-attacks • Challenges for business: - No boundaries; - Technologies: Wide usage of technologies (mobile technologies); - Cloud computing; - Big data challenges; - Risks from third-parties; - Internet of Things (IoT); • The challenge of growing threats; • Nation-State threats

Suggested Hours	*Minimum Slides*	*Maximum Slides*

	1.5	23	30
1.2 History of Cybersecurity	• Brief history of how approaches to cyber-attacks have changed over time, leading to increased measures and hence the counter measures against cyber-attacks. • This section might include local / European / International Case Studies		
	Suggested Hours 1.0	*Minimum Slides* 15	*Maximum Slides* 20
1.3 Definitions of Cybersecurity	• Section about Cybersecurity jargon/terms & stats/sources		
	Suggested Hours 0.5	*Minimum Slides* 8	*Maximum Slides* 10

1.2.2 Cybersecurity within the European Union (EU)

Title of Module	2.0 Cybersecurity within the EU
Total Duration *(Hours / Slides)*	3 hours 48 – 67 slides
Delivery Method	Face-to-face Online Blended Learning Discussions
Assessment	Face-to-face / Online Quiz
Learning Outcomes	• Understanding the legal aspects of Cybersecurity • Understanding the current EU policies related to Cybersecurity • Understanding EU laws related to Cybersecurity • Relating and comparing Cybersecurity Local Laws with EU Laws
Prerequisites	Basic IT and Business Knowledge might be useful to better understand the module
Module Description	This module introduces the learner to the existing EU policies and initiatives aimed at promoting the concept of Cybersecurity. It also discusses legal aspects of Cybersecurity both within the EU as well as worldwide, exposing learners to numerous real life scenarios and case studies in the field. The module includes an overview of tendencies in the Cybersecurity landscape, including but not limited to statistics, trends, relevant threats, legal, reputational and financial risks and case study analysis.
MODULE SUB TOPICS	

2.1	**Fostering Cybersecurity within the European Union**	• Brief introduction on EU Policies and Initiatives aimed at promoting the concept of Cybersecurity		
		Suggested Hours 1.0	*Minimum Slides* 20	*Maximum Slides* 30
2.2	**Legal Aspects of Cybersecurity**	• Legal Aspects of Cybersecurity worldwide (in general) and in the EU in particular including repurcussions of non compliance • The relationship, comparison and contrast of Cybersecurity Local Laws with EU Laws		
		Suggested Hours 0.5	*Minimum Slides* 5	*Maximum Slides* 7
2.3	**Overview on the tendencies of Cybersecurity landscape**	• The presentation of real Life scenarios and case studies including statistics, tendencies, relevant threats, risks (legal, reputation, financial) • A look into recent cyber-attacks and class discussion on the importance of upskilling in view of the possible risks brought about by cyber -attacks. *Note: Discussion could be online of face-to-face with the trainer facilitating and providing guidelines to what is expected from the discussion.*		
		Suggested Hours 1.5	*Minimum Slides* 23	*Maximum Slides* 30

1.2.3 Cyber-attacks: Social Engineering and Phishing

Title of Module	3.0 Cyber-Attacks: Social Engineering and Phishing
Total Duration *(Hours / Slides)*	10 hours 150 – 200 slides
Delivery Method	Face-to-face Online Blended Learning Usage of interactive tools (e.g. online scenarios tools) Discussions
Assessment	Face-to-face / Online Quiz
Learning Outcomes	• Understand the concept of cyber-attacks • Define Social Engineering and reverse social engineering • Understand the modalities of Social Engineering and its relationship with cyber-attacks • Understand the most common cybersecurity threats • Understand the main cyber-attack categories and techniques
Prerequisites	Basic IT and Business Knowledge might be useful to better understand the module

<table>
<tr><td>Module Description</td><td colspan="3">This module introduces the learner to Cyber-attacks with a particular focus on Phishing. It also delves into detail on the concept of Social Engineering and Reverse Social Engineering together with the strong link of social engineering to cyber-attacks.

The module also presents different types of phishing attacks and techniques together with a number of real case study examples from the Project Partner countries.</td></tr>
<tr><td colspan="4">MODULE SUB TOPICS</td></tr>
<tr><td rowspan="2">3.1 Introduction to Cyber-attacks</td><td colspan="3">• Brief introduction to Cyber-attacks in particular Phishing attacks</td></tr>
<tr><td>Suggested Hours
0.5</td><td>Minimum Slides
8</td><td>Maximum Slides
10</td></tr>
<tr><td rowspan="2">3.2 Social Engineering Modules and Manipulation</td><td colspan="3">• An overview of Social Engineering Models with particular emphasis on:
a) "Weapons of Influence" - R. Cialdini[1]
- Reciprocation
- Commitment and consistency
- Social proof
- Liking
- Authority
- Scarcity
b) Psychological aspects of Social Engineering
c) An overview of Reverse Social Engineering</td></tr>
<tr><td>Suggested Hours
4</td><td>Minimum Slides
60</td><td>Maximum Slides
80</td></tr>
<tr><td>3.3 Different Types of Phishing Attacks and Techniques</td><td colspan="3">• A section to define different types of Cyber-attacks (especially Phishing) and how to recognise them (following chapter), including but not limited to:
Categories
- GDPR related attacks
- Emails;
- Instant Messaging;
- Social networks;
- Websites;
- Lotteries scams;
- SMS;
- Phone calls;
- Face to face;
- Shoulder surfing;
Combination of techniques</td></tr>
</table>

[1] Cialdini, R. B. (2016). Pre-Suasion: A Revolutionary Way to Influence and Persuade. New York: Simon & Schuster. ISBN 978-1501109799.

<table>
<tr><td></td><td colspan="3">- Spray and Pray
- Spear Phishing
- Whaling
- Vishing
- Smishing
- Angler Phishing
- Clone Phishing
- Malvertising</td></tr>
<tr><td></td><td>Suggested Hours
4</td><td>Minimum Slides
60</td><td>Maximum Slides
80</td></tr>
<tr><td>3.4 Case Studies</td><td colspan="3">• Presentation of a number of different case studies from the Partner organisations
• Online or face-to-face discussion in Small Groups (5-6 students) Note: Discussion shall take the form of an exercise with each group finding and analysing a recent phishing attack to include details such as date of attack, information about victim, modalities of the attack, consequences, lessons learned and so on. Subsequently, a student from each group presents the results of the analysis to the whole class. Constructive feedback from trainer and peers shall also be provided.</td></tr>
<tr><td></td><td>Suggested Hours
1.5</td><td>Minimum Slides
22</td><td>Maximum Slides
30</td></tr>
</table>

1.2.4 Overview of Understanding and Handling Cyber-attacks

Title of Module	4.0 Understanding and Handling Cyber-attacks
Total Duration *(Hours / Slides)*	14 hours 210 – 255 slides
Delivery Method	Face-to-face Online Blended Learning
Assessment	Face-to-face / Online Quiz
Learning Outcomes	• Acquire basic knowledge on e-safety and security • Understand different information content • Understand identity and distinguish between different attacks related to identity • Understanding the consequences of cyber-attacks to both individuals and/or organisations • Define and understand the importance of cyber hygiene as a proactive action to cyber-attacks • Understand and apply different methods of protection against cyber-attacks

<table>
<tr><td></td><td colspan="3">• Design and implement and incident response plan to cyber-attacks</td></tr>
<tr><td>Prerequisites</td><td colspan="3">Previous modules</td></tr>
<tr><td>Module Description</td><td colspan="3">This module introduces the learner to the concept of e-safety and the importance of adopting a proactive approach to cyber threats through the concept of cyber hygiene.

The module also provides a detailed approach on how to recognise and handle cyber-attacks.

The module introduces the development and implementation of incident response plans in order to minimise the effects of cyber-attacks.</td></tr>
<tr><td colspan="4">MODULE SUB TOPICS</td></tr>
<tr><td rowspan="2">4.1 Basic Knowledge on e-security</td><td colspan="3">• Differences of information contents (open, private, business, etc.); Intellectual property; Copyrights;
• Understand term Identity; be aware about identity theft and theft methods. Be aware about spyware, keyboard spy, fraud advertisement, Trojans. Know various ways how malicious software could get into device.
• Know about reasons and consequences of identity and personal data thefts in the workplace and on the internet (fraudulent information usage, threat of information loss, sabotage).
• Know about threats associated with personal data disclosure.
• A brief introduction to the effects of cyber-attacks to both the individual and the organisation. Further detail to be explored in section 4.4.</td></tr>
<tr><td>Suggested Hours
0.5</td><td>Minimum Slides
8</td><td>Maximum Slides
10</td></tr>
<tr><td rowspan="2">4.2 Proactive actions</td><td colspan="3">• Cyber hygiene on the Internet (minimise information about persons, including personal accounts on social media, which could be used by attackers)
• Cyber hygiene on the workplace
• Technological tools and measures (filters and block phishing emails)</td></tr>
<tr><td>Suggested Hours
2</td><td>Minimum Slides
30</td><td>Maximum Slides
35</td></tr>
<tr><td>4.3 Recognising Phishing Attacks</td><td colspan="3">• Case studies analysis by using techniques from section 3.3 – Different Types of Phishing Attacks and Techniques
• A section to recognise Cyber-attacks (with reference to the items in the previous chapter) including but not limited to:
- Critical Thinking
- Learn to hover links
- Understand URL
- Analysing messages
- Recognising red flags</td></tr>
</table>

	Suggested Hours 5	*Minimum Slides* 75	*Maximum Slides* 90
4.4 Handling Cyber-attacks	• Guide on Cybersecurity, including a section on the damage caused by cyber-attacks to both the **individual** and **organisations** and how to deal with Cyber-attacks based on the previous chapter. This should include but not limited to: - Safe Navigation - Creating Strong Passwords - Avoiding Attacks - Safe Online Shopping - Anti-Cyber-attacks Software installation - Dealing with Cookies - Taking appropriate Backups - Encrypting Files - Two factors authentication - Malware - Safe browsing • This section shall also include local / European / International Case Studies as examples referred to in previous modules • This section shall include easy Step -by-Step Instructions and images as appropriate • This section shall also include the reactive action of a cyber-attack including recovery procedures where an organisation and/or a user fall victims of a cyber-attack.		
	Suggested Hours 5	*Minimum Slides* 75	*Maximum Slides* 90
4.5 Minimising Damage through Incident Response	• Design, development and implementation of incident response plans indicating the suggested and best practise techniques to be actioned in the occurrence of a data breach incident. *Note: Part of section could be adapted according to countries specific*		
	Suggested Hours 1.5	*Minimum Slides* 22	*Maximum Slides* 30