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

CyberPhish Extended 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	**02/05/2021**	**Original Draft**	**MECB Ltd (MT)**
2 Draft Version 2.0	**07/05/2021**	**Updated Draft**	**MECB Ltd (MT)**
3 Draft Version 3.0	**09/05/2021**	**Updated Draft**	**MECB Ltd (MT)**
4 Draft Version 4.0	**10/05/2021**	**Updated Draft following feedback from Partners**	**MECB Ltd (MT)**
5 Draft Version 5.0	**31/05/2021**	**Updated Draft following Feedback from Experts**	**MECB Ltd (MT)**
6 Final Version 1.0	**08/06/2021**	**Final Version for Distribution**	**MECB Ltd (MT)**

Contents

INTRODUCTION

The Cyberphish Extended Curriculum aims to deliver concise but far-reaching modules in cybersecurity with a particular emphasis on cyber phishing. The Curriculum is divided into three main sections namely:

- Train the Trainer Course – equipping trainers with the right mindset and skills to deliver the curriculum.
- Face-to-face / Online Training – setting up the modalities of how the curriculum training shall be delivered.
- The Curriculum (E-Learning Module) Structure – describing in detail the structure of the curriculum

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. TRAIN THE TRAINER COURSE

The following structure for the train the trainer course is designed in such a way to be either conducted face-to-face or online. The suggested duration may vary depending on the number of participants and the delivery requirements. Due to the nature of this Train the Trainer Course, it is being suggested to have groups of not more than twelve trainers per course.

The structure of the training programme is provided in the table below. The table offers **recommended topics** for the train the trainer meeting and recommended amount of time. It is at the descretion of the training organiation and the trainer to use, extend, decrease or increase the duration and content of the train the trainer programme as deemed fit and according to the preparedness of both the trainer and the learners.

It is pertinent to note the Train the Trainer course is intended for Trainers who are already knowledgeable about the subject of cybersecurity in general.

Organisers of the event could send a questionnaire to trainers before the training session to collect the level of trainers and understand what the trainers expect from this training event. Following feedback from the questionnaire, organisers could adjust the training event agenda accordingly.

Structure	Train the Trainer Course delivered in a short 4 day program aimed at equipping trainers with the adequate skills and competencies	
Aim	Empower trainers with basic facilitation and training design skills to deliver effective training sessions in Cybersecurity	
Program		
Day 1	A Day in the life of a student	
Item Nº	*Item*	*Suggested Time*
D1-01	Introduction and get-to-know session • Ice Breaker or Team Building Activity to get to know each other - *Low Tech Social Network (ice breaker)* - *Marshmallow Challenge (team building)*	0.5 hour

D1-02	Understanding and Dealing with Different Learning Styles • A brief introduction to different learning style models - *Introducing different learning styles (e.g. 7 learning styles, Kolb's learning cycle) as the basis for the subsequent sections.*	0.5 hour
D1-03	The Trainer as a student – Experiencing learning methodologies (Part 1) *The aim of this session is to engage the trainers in understanding and experiencing different pedagogical settings and teaching methods as students. A face-to-face or virtual (online classroom) shall be set with the trainers acting as students.* • Introduction to different pedagogical settings and teaching methods - *In the first part of the session, the main trainer shall introduce a number of different pedagogical settings and delivery methods. (e.g. Workshops, Practical Sessions, Discussions, Debates, Case Studies etc.)* • Experiencing different teaching methods - *In the second part of the session, the trainers/learners shall be exposed to these different teaching methodologies.*	3 hours
D1-04	Networking Break	0.5 hour
D1-05	The Trainer as a student – Experiencing learning methodologies (Part 2) • Discussion, feedback and sharing of best practices - *Sharing of feelings, attitudes, feedback on the experience of Part 1* - *Sharing of best practices on how to improve the learning experience of the students*	1 hours
D1-06	Day 1 – Summary and Conclusion	0.5 hours
Day 2	Refreshing Essential Soft Skills	
Item Nº	*Item*	*Suggested Time*
D2-01	Introduction to day 2 – The importance of Soft Skills • A brief introduction to the importance of soft skills in delivering a lesson - *Brief introduction focusing mainly on Presentation, Facilitation, Classroom Management and Giving constructive feedback*	0.5 hour
D2-02	Essential soft skills for delivering training sessions (Part 1) • Presentation Skills - *Presentation Structuring (e.g. number and format of slides, using online tools)* - *Aspects of Presenting (e.g. body language, voice tonality, body language)* - *Delivery of short presentations (face-to-face or online) with peer feedback and review* • Facilitation Skills - *Facilitating a group discussion (e.g. Probing, Redirecting and Rephrasing questions)* - *Facilitating collaboration (e.g. Brainstorming, Mind mapping, Six Thinking Hats),* • Using Digital Tools to aid Soft Skills - *Using digital tools to facilitate presentations and discussions* - *Introduction to digital/online tools including but not limited to MS Teams, Zoom, Skype, Google Meet, Mentimeter, Kazoom and so on.*	2 hours
D2-03	Networking Break	0.5 hour
D2-04	Essential soft skills for delivering training sessions (Part 2)	2 hours

	• Classroom Management - *Sharing of best practices session on how to control, enthuse and involve learners both face-to-face and online* • Giving Effective and Constructive Feedback - *Short group debate (face-to-face or online workshop) analysing effective and constructive feedback techniques*	
D2-05	Day 2 – Summary and Conclusion	0.5 hours
Day 3	Delving into the Curriculum	
Item Nº	*Item*	*Suggested Time*
D3-01	Introduction to the Curriculum Structure and Teaching Modalities *A brief face-to-face or online session introducing the Curriculum Structure including the importance of learning outcomes together with the teaching modalities.*	1 hour
D3-02	Detailed Analysis of the Curriculum Topics (Part 1) *Explanatory Session on the first two introductive modules of the curriculum*	1 hour
D3-03	Networking Break	0.5 hour
D3-04	Detailed Analysis of the Curriculum Topics (Part 2) *Explanatory Session on the final two modules of the curriculum*	3 hours
D3-05	Day 3 – Summary and Conclusion	0.5 hours
Day 4	Final Workshop – Assessment of Essential Soft Skills utilising the Curriculum	
Item Nº	*Item*	*Suggested Time*
D4-01	Introduction to the Workshop *The final day shall consist of a workshop whereby all participants are expected to reflect on the experience gathered on Day 1, practice the skills acquired on Day 2 and utilising the curriculum explained on Day 3.* *Assessment shall be done in the form of feedback from fellow participating trainers.* *The duration of the workshop shall depend on the number of participants.*	0.5 hour
D4-02	Assessment of Presentation Skills *Trainers shall be asked to prepare and deliver a 10-minute presentation choosing any topic from the proposed curriculum. Peer assessment and feedback on the presentation including innovative techniques utilised shall follow each presentation.* Other Assessment modalities might be used at the discretion of the Trainer	0.25 hours per participant *(maximum 3 hours)*
D4-03	Networking Break	0.5 hour
D4-04	Assessment of Facilitation Skills *Trainers shall be asked to facilitate a 10-minute session choosing any topic from the proposed curriculum. Peer assessment and feedback on both facilitation skills and class management shall follow each session.* Other Assessment modalities might be used at the discretion of the Trainer	0.25 hours per participant *(maximum 3 hours)*
D4-05	Day 4 – Summary and Conclusion of the Train the Trainer Course	0.5 hours

2. FACE-TO-FACE / ONLINE TRAINING

A ***four-staged approach*** is adopted in integrating learners into the learning experience. At a glance:

Online Orientation Session	*Student Welcome Event*	*Module Delivery*	*Integration Workshop*	*Module Delivery*	*Course Completion*	*Concluding Networking Session*
Information on Training Institution - *Goals* - *Policies* - *Procedures* -	Introduction – Trainer Bio Training Institution Management Information System (MIS) - *Info on System* - *ID / Password* - *Resources* - *'Use' Policy* - *FAQ / Troubleshooting* Official Course Syllabus Assessment Methodologies Lines of Communication	Delivery of the module depending on the number of hours assigned per day. First Part (15 hours)	Online Feedback form concerning ongoing good practices and other practices which need addressing Discussion with Learners	Delivery of the module depending on the number of hours assigned per day. Second Part (15 hours)	Gathering of data - *From trainer: assessments* - *From students: digital training evaluation form*	Focus Session - *Discussion on Findings* - *Conclusions* - *Way Forward*
Continuous Tutor Support						
Continuous System Support						

i. Self-Guided Virtual Orientation Session

The first step in the orientation experience is to attend an **Online Orientation Session**. This session is a self-paced experience, allowing the learner the flexibility to learn about the institution providing the tuition (the training institution).

Prospective learners will have the opportunity to familiarise themselves with information related to (but not limited to) the training institution as a whole and the specific department concerned. Departmental goals, policies and procedures are highlighted, as well as the expectations of the training institution. To cater for visually and hearing impaired students, all orientation material and presentations shall be captioned and accessible for screen readers.

ii. Welcome Event

The new student cohort is welcomed at a **Student Welcome Event**. This event can be done either face-to-face or online. This meeting provides an excellent opportunity for students to meet the trainer and fellow students within the cohort, ask questions and become acquainted with the course logistics.

In particular, having been provided with the authorisation to use the training institution's information system, the trainer will deliver a concise introduction to the system as installed. Learners will be provided with user IDs and walked through setting passwords. Furthermore, guidance will be given regarding accessing the resources that learners are authorised to use. In this respect, a 'Use Policy' is read and signed. Recognising that this might come across as a lot of technical information, a 'FAQ and Troubleshooting' document will be made available for future reference.

The trainer can conclude the session by drawing a precise picture of the official course syllabus, the assessment methodologies, and the available lines of communication.

iii. Empowering the learners through ongoing support

In addition to developing learner mastery of knowledge, skills and attitudes relative to the Cybersecurity course of studies, the training institution recognises the importance of identifying and responding to the changing needs of the learners. As the first line of response, trainers will be available on a regular basis for positive interaction with students.

On a more official standing, an **Integration Workshop** will be organised after a predefined number of completed tuition sessions. Learner feedback will be gathered and discussed to determine how well the course progression matches the expectations of the students and the standards of the training institution.

Various training evaluation tools may be employed in advance of the integration workshop to aid in data collection. Indicators of success in this respect include, but are not limited to, the student acquisition of new skills and knowledge, a positive attitude towards the learning experience and efficiency impact.

In turn, this information is used to assure the improvement of the quality of the course program.

iv. Course Conclusions

Course completion is in itself a moment of recognition of significant accomplishment.

A **Concluding Networking Session** will be held of which the purpose is two-flow. Of upmost importance is that learners are given the opportunity to share a couple of hours of shared joy. However, the training institution will also concurrently take the opportunity to evaluate the success of the training program. *Kirkpatrick's Four-Level Training Evaluation Model*[1] will be employed in this respect.

Prior to the networking session, the training institution will gather information:

- *from the trainer re: assessments.*
  This will serve as a measure of how much the learners' knowledge and skills have changed since the inception of the program of studies.
- *from the learners.*
  A digital training evaluation form, enquiring feedback regarding the overall satisfaction with the learning experience, and the applicability (or otherwise) of their studies in the workplace.

With this data at hand, a **Focus Session** will be held during the networking event, wherein the training institution, through a structured panel discussion, can qualitatively measure results like productivity, quality and efficiency ratings.

3. THE CURRICULUM (E-LEARNING MODULE) STRUCTURE

3.1 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.

[1] Kirkpatrick, D. L. (1994). Evaluating training programs: the four levels. San Francisco: Berrett-Koehler.

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.

3.2 E-Learning Module Structure in Detail

3.2.1 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	

<table>
<tr><td rowspan="2"><b>1.1 Background – Challenges of the 4th Industrial Revolution</b></td><td colspan="3">• 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</td></tr>
<tr><td><i>Suggested Hours</i>
1.5</td><td><i>Minimum Slides</i>
23</td><td><i>Maximum Slides</i>
30</td></tr>
<tr><td rowspan="2"><b>1.2 History of Cybersecurity</b></td><td colspan="3">• 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</td></tr>
<tr><td><i>Suggested Hours</i>
1.0</td><td><i>Minimum Slides</i>
15</td><td><i>Maximum Slides</i>
20</td></tr>
<tr><td rowspan="2"><b>1.3 Definitions of Cybersecurity</b></td><td colspan="3">• Section about Cybersecurity jargon/terms & stats/sources</td></tr>
<tr><td><i>Suggested Hours</i>
0.5</td><td><i>Minimum Slides</i>
8</td><td><i>Maximum Slides</i>
10</td></tr>
</table>

3.2.2 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

<table>
<tr><td><b>Learning Outcomes</b></td><td colspan="3">• 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</td></tr>
<tr><td><b>Prerequisites</b></td><td colspan="3">Basic IT and Business Knowledge might be useful to better understand the module</td></tr>
<tr><td><b>Module Description</b></td><td colspan="3">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.</td></tr>
<tr><td colspan="4"><b>Module Sub Topics</b></td></tr>
<tr><td rowspan="2"><b>2.1 Fostering Cybersecurity within the European Union</b></td><td colspan="3">• Brief introduction on EU Policies and Initiatives aimed at promoting the concept of Cybersecurity</td></tr>
<tr><td><i>Suggested Hours</i>
1.0</td><td><i>Minimum Slides</i>
20</td><td><i>Maximum Slides</i>
30</td></tr>
<tr><td rowspan="2"><b>2.2 Legal Aspects of Cybersecurity</b></td><td colspan="3">• 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</td></tr>
<tr><td><i>Suggested Hours</i>
0.5</td><td><i>Minimum Slides</i>
5</td><td><i>Maximum Slides</i>
7</td></tr>
<tr><td rowspan="2"><b>2.3 Overview on the tendencies of Cybersecurity landscape</b></td><td colspan="3">• 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.
<i>Note: Discussion could be online of face-to-face with the trainer facilitating and providing guidelines to what is expected from the discussion.</i></td></tr>
<tr><td><i>Suggested Hours</i>
1.5</td><td><i>Minimum Slides</i>
23</td><td><i>Maximum Slides</i>
30</td></tr>
</table>

3.2.3 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

<table>
<tr><td></td><td colspan="3">Online
Blended Learning
Usage of interactive tools (e.g. online scenarios tools)
Discussions</td></tr>
<tr><td><b>Assessment</b></td><td colspan="3">Face-to-face / Online Quiz</td></tr>
<tr><td><b>Learning Outcomes</b></td><td colspan="3">• 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</td></tr>
<tr><td><b>Prerequisites</b></td><td colspan="3">Basic IT and Business Knowledge might be useful to better understand the module</td></tr>
<tr><td><b>Module Description</b></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"><b>MODULE SUB TOPICS</b></td></tr>
<tr><td rowspan="2"><b>3.1 Introduction to Cyber-attacks</b></td><td colspan="3">• Brief introduction to Cyber-attacks in particular Phishing attacks</td></tr>
<tr><td><i>Suggested Hours</i>
0.5</td><td><i>Minimum Slides</i>
8</td><td><i>Maximum Slides</i>
10</td></tr>
<tr><td rowspan="2"><b>3.2 Social Engineering Modules and Manipulation</b></td><td colspan="3">• An overview of Social Engineering Models with particular emphasis on:
a) "Weapons of Influence" - R. Cialdini[2]
- 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><i>Suggested Hours</i></td><td><i>Minimum Slides</i></td><td><i>Maximum Slides</i></td></tr>
</table>

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

	4	60	80
3.3 Different Types of Phishing Attacks and Techniques	• 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** - Spray and Pray - Spear Phishing - Whaling - Vishing - Smishing - Angler Phishing - Clone Phishing - Malvertising		
	Suggested Hours 4	*Minimum Slides* 60	*Maximum Slides* 80
3.4 Case Studies	• 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.*		
	Suggested Hours 1.5	*Minimum Slides* 22	*Maximum Slides* 30

3.2.4 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

<table>
<tr><td><b>Delivery Method</b></td><td colspan="3">Face-to-face
Online
Blended Learning</td></tr>
<tr><td><b>Assessment</b></td><td colspan="3">Face-to-face / Online Quiz</td></tr>
<tr><td><b>Learning Outcomes</b></td><td colspan="3">• 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
• Design and implement and incident response plan to cyber-attacks</td></tr>
<tr><td><b>Prerequisites</b></td><td colspan="3">Previous modules</td></tr>
<tr><td><b>Module Description</b></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"><b>MODULE SUB TOPICS</b></td></tr>
<tr><td rowspan="3"><b>4.1 Basic Knowledge on e-security</b></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><i>Suggested Hours</i></td><td><i>Minimum Slides</i></td><td><i>Maximum Slides</i></td></tr>
<tr><td>0.5</td><td>8</td><td>10</td></tr>
</table>

<table>
<tr><td rowspan="2"><b>4.2</b></td><td rowspan="2"><b>Proactive actions</b></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><i>Suggested Hours</i>
2</td><td><i>Minimum Slides</i>
30</td><td><i>Maximum Slides</i>
35</td></tr>
<tr><td rowspan="2"><b>4.3</b></td><td rowspan="2"><b>Recognising Phishing Attacks</b></td><td colspan="3">• Case studies analysis by using techniques from section <i>3.3 – Different Types of Phishing Attacks and Techniques</i>
• 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>
<tr><td><i>Suggested Hours</i>
5</td><td><i>Minimum Slides</i>
75</td><td><i>Maximum Slides</i>
90</td></tr>
<tr><td rowspan="2"><b>4.4</b></td><td rowspan="2"><b>Handling Cyber-attacks</b></td><td colspan="3">• Guide on Cybersecurity, including a section on the damage caused by cyber-attacks to both the <b>individual</b> and <b>organisations</b> 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.</td></tr>
<tr><td><i>Suggested Hours</i>
5</td><td><i>Minimum Slides</i>
75</td><td><i>Maximum Slides</i>
90</td></tr>
</table>

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	*Minimum Slides*	*Maximum Slides*
		1.5	22	30