MODULE 4

TRAINING COURSE **Bridging the gap between Higher Education and the labour market**

Module 4	Online Security & Data Protection
Duration	180’
Program contents	4.1. Common threats 4.2. Cyber-hygiene 4.3. Personal protection 4.4. Password management
Expected outcomes	By the end of Module 4 participants are expected to: - understand the risk of the cyber-space - be able of identifying common threats - learn and apply the best practices of cyber-hygiene - understand the importance of creating strong passwords - understand the importance of using multi-factor authentication - understand the core features of certified-based authentication
Training methodology	MIGG Method (MIGG : Méthode d’ Intégration Guidée par le Groupe) + gamified (game-based) experience

SESSION PROGRAM

Activity	Time/duration
1. Topic introduction: Online security & Data protection (5’)	90’

2. Theoretical background (expositive) 2.1. Common threats: malware, phishing, social engineering, among others (15'). 2.2. Cyber-hygiene: best practices (15'). 3. Self-protecalso be presented, namelycused on password management) 3.1. Risks of weak password: understanding the impact of different attacks (15') 3.2. Recommendations to define strong passwords (10') 4. More robust authentication 4.1. Multi-factor authentication (15') 4.2. Certificate-based authentication (15')	
5. Group reconstruction (1st part) Ask teachers to write down the oral intervention individually, from memory, describing the main concepts (15')	15'
6. Group reconstruction (2nd part) Invite the teachers to compare and complete their notes with their neighbour in the row (groups 2 elements), and then to discuss in group, 3-4 elements, to complete the notes (15')	15'
7. Synthesis Conclude with a quick summary to the large group (key points only)	10'
8. Gamified experience: creating a strong password	20'
9. Recap	15'

STEP BY STEP

What to do	Details
1. Welcoming and module presentation Welcome all participants and present the key topics of the module.	**5''** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 1 to 2)

2. Topic about threats Introduce the key topics about the most common malware. Other threats will be also presented, namely related with phishing and social engineering.	**15'** • Keynote "Module 4" (slides 3 to 9)
3. Topic about cyber-hygiene Explaining what cyber-hygiene is, and how this affects the users' safety in the cyber-space. It will be demonstrated some of the best practices to be a cyber hygienic user.	**15'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 10-19)
4. Topic about risks of using weak passwords Define what is considered a weak password, followed by the risks of using these passwords, with practical examples.	**15'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 20-36)
5. Topic about recommendations to define passwords After presenting the impact of weak password, show the importance of using different types of characters (uppercase, lowercase, numbers, and special characters). This demonstration aims to show that the complexity of the password can make an attack infeasible during the password's lifetime.	**10'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 37-47)
6. Topic about multi-factor authentication Introduce the multi-factor authentication mechanisms, and how it works without too many technical details. Explain the use of this mechanism when the user is online or offline.	**15'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 48-54)
7. Topic about certified-based authentication The final topic of the expositive part of the section. Explaining a different paradigm for authentication, commonly used by machines to authenticate without credentials. Explain the importance of this type of authentication and some of its limitations.	**15'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 55-62)
8. Group reconstruction Organize the class in groups and ask teachers to write down the oral intervention individually, describing the main concepts from memory. After a quick break, the users should compare notes between them.	**30'** • "B2B_TrainingCourse_M4_Keynote_EN" (slides 63-66)

9. Synthesis Summarize the key topics, encouraging the importance of strong passwords and multi-factor authentication.	**10'**
10. Gamified experience Ask participants to play the game about creating a strong password available on https://tinyurl.com/2js5dv5c	**15'**
11. Recap After the participants play the proposed game, repeat the synthesis.	**15'**

SESSION RESOURCES

RESOURCES	• Presentation • Online game

REFERENCES	• Online:
	  ○ Back2Basics cybersecurity handbook
	  ○ https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits
	  ○ https://coretelligent.com/insights/7-cybersecurity-tips-for-practicing-good-cyber-hygiene/
	  ○ https://edu.gcfglobal.org/en/techsavvy/password-tips/1/
	• Books:
	  ○ Cyber Security Basics For Non-technical People, by Gerald Hinkle (2019)

ASSESSMENT /EVALUATION	Online quiz (suggestion)