



# YOUNG FEMALE ENTREPRENEURS STEPPING INTO THE DIGITAL AGE

PROJECT NUMBER: 2021-2-EL02-KA220-YOU-000051105

## PROJECT RESULT 2 ONLINE SEMINAR (E-COURSE) CURRICULUM

### "DIGITAL WELL- BEING"

[WWW.OMEGA-PROJECT.EU](http://WWW.OMEGA-PROJECT.EU)

# TABLE OF CONTENTS

<b>FRAMEWORK OF THE CURRICULUM</b>	<b>04</b>
• Identity of the project	04
• Project partners	05
• Publication	05
<b>ELEMENTS OF THE CURRICULUM</b>	<b>06</b>
• Introduction	06
• Understanding the Impact of Digital Skills Deficiency	07
• Addressing Challenges in Digital Skill Development	08
• Building the Entrepreneurial Mindset	11
• Enhancing Digital Skills and Competencies	12
• Business Skills Development for Young Female Entrepreneurs	14
• Group Dynamics	17
• Professional Development for Youth Workers and Trainers	17
• Equipping Youth Workers with Best Practices in Digital Education.	18
• Strategies for Transmitting Digital Skills to Young Women	20
• Promoting Social Integration through Digital Education	21
<b>EDUCATIONAL RESOURCES</b>	<b>22</b>
<b>RESOURCES OVERVIEW AND KEY COMPETENCIES</b>	<b>22</b>
<b>INTERNET SECURITY AND DIGITAL LITERACY RESOURCES</b>	<b>23</b>
<b>MODULE 1: THE CORE RULES OF INTERNET</b>	<b>24</b>
• Introduction	25
• Activity 1: Digital Literacy Discovery	25
• Activity 2: Creative Content Challenge	25
• Activity 3: Cybersecurity Escape Room	26
• Closing.	26
<b>MODULE 2: PHISHING TYPES AND HOW TO DEAL WITH PHISHING INCIDENTS.</b>	<b>27</b>

# TABLE OF CONTENTS

• Introduction	29
• Activity 1: Phishing Detective Challenge	31
• Activity 2: Phishing Incident Response Simulation	37
• Activity 3: Creating Personalized Phishing Prevention Plans	43
• Closing	49
<b>MODULE 3: HOW TO ENJOY THE BENEFITS OF DIGITAL TECHNOLOGY WHILST AVOIDING THE HAZARDS</b>	<b>50</b>
• Introduction	53
• Activity 1: Digital Wellness Check	53
• Activity 2: The Digital Guardians	53
• Activity 3: Balancing Act: Creating a Digital Wellness Plan	54
• Closing	
<b>MODULE 4: GAMING AND SOCIAL MEDIA ADDICTION</b>	<b>54</b>
• Introduction	56
• Activity 1: Identifying Addiction Warning Signs	57
• Activity 2: Digital Detox Challenge	58
• Activity 3: Creating a Healthy Digital Balance Plan	58
• Closing	58
<b>REFERENCES</b>	<b>58</b>
<b>WEBSITES</b>	<b>59</b>
	<b>60</b>

# FRAMEWORK OF THE CURRICULUM

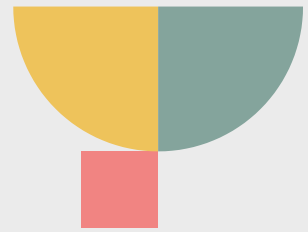
## IDENTITY OF THE PROJECT

The project OMEGA is a European project funded under the Erasmus+ programme. The aim of the project is to develop the digital skills and competencies of young women to increase their opportunities of integration into the labor market.

Having as target groups youth workers, trainers, ICT and digital technology experts involved in youth education belonging to partner groups, as well as low digital skilled women and young women belonging to disadvantaged groups (i.e. women living in remote areas, refugees, migrants), a project have the following objectives:

- Professional development of youth workers, who will learn various good practices regarding digital skill and competence development in order to transmit them to the young women (of different backgrounds) they will work with and increase their chances of employability and their chances of entering into the labor market, to raise awareness on the value of digital skills in finding a job nowadays, as well as their social integration in the modern society nowadays.
- Business skills development through becoming digitally literate and gaining knowledge on how to manage a virtual business which is invaluable in the sense that they develop digital skills and competences to young women that are considered important by employers nowadays or are considered important in starting their own businesses.
- New behaviors acquisition: they will become more open to dialogue with young people (in our case with young women) and with specialists on topics of interest in digital education.
- Communication and linguistic skills enhancement, fluency and courage to communicate on topics of interest of young people.
- Adjustment to the modern entrepreneurial digital mindset and advantage gain by using it in the labor market.
- Equipment with the necessary tools needed to enter the labor market faster.
- Empowerment of those women who are part of a population affected most by the effects of unemployment.
- Learn to use gaming experiences in an educational way that allows a more in-depth approach to the concept of Digital Entrepreneurship.

OMEGA is bringing together 6 European organizations with a common goal: contribute to the development of the entrepreneurial mindset and related digital skills in young female entrepreneurs who are motivated to become entrepreneurs but face a set of barriers related to access to training, business support services, language barriers, inadequate management and marketing skills.



The OMEGA project's objectives align with promoting gender equality, social inclusion, and economic empowerment. The project facilitates the integration of young women into the labour market by providing them with digital and entrepreneurial competencies. OMEGA is a 24-month EU project with an implementation period from 01.05.2022 - 30.04.2023.

## PROJECT PARTNERS

OMEGA project bringing together 6 organizations from 5 countries aiming to promote actions and exchange of good practices in the area of digital technology, in order to facilitate young women's professional integration into the labor market by developing their digital and entrepreneurial skills and ideas.

The partners of the Omega project are:

1. INSTITUTOYTO KOINONIKIS KAINOTOMIAS KAI SYNOPSIS (The Social Innovation and Cohesion Institute) – Greece.
2. ASOCIATIA A.S.E.L. RO (Association for Social Economy and Lifelong Learning) – Romania.
3. CENTER FOR EDUCATIONAL AND DEVELOPMENT INITIATIVES INNOVA LAB BITOLA - The Republic of North Macedonia.
4. Kadın ve Genç Girişim Merkezi Dernegi - Woman and Young Entrepreneurship Centre Association – Turkey.
5. YOUTH FOR EXCHANGE AND UNDERSTANDING INTERNATIONAL AISBL (Youth for Exchange and Understanding - YEU) – Belgium.
6. LYKEIO TON HELLENIDON - PARARTIMA VERIAS (Lyceum Club of Greek Women in Veria) – Greece.

## PUBLICATION

The joint work and synergy of the project partners within the OMEGA project will produce the following project results:

1. Methodological Handbook (e-Book) "Young Women Entrepreneurs and Digital Culture" development (PR1).
2. Online Seminar (e-Course) Curriculum "Digital Well-Being" (PR2).
3. Online Seminar (e-Course) Curriculum "Basic Principles of Strategic Marketing" (PR3).
4. Serious Video Game for Digital Entrepreneurship Education (PR4).

# ELEMENTS OF THE CURRICULUM

## Introduction

Increasing digital literacy and digital skills is essential for personal empowerment, education, employability, and active participation in the digital age. It equips individuals with the tools they need to thrive in an increasingly digital world. Also, developing digital business skills is crucial in today's technology-driven business landscape.

This curriculum allows the trainer/teacher who will implement the same, first to increase his/her set of knowledge with theoretical research and analysis, and then through the created modules to apply the same with practical exercises, assignments, studies, quizzes, presentations, videos, workshops, etc. in order to facilitate the transfer of knowledge to the target group defined in this document. Namely, there is a synergy in the creation of this curriculum, through field research in the various partner countries, theoretical research and insights, and on that basis the creation of appropriate modules.

This document incorporates several aspects, one part that makes a theoretical presentation of research and analysis, which is the main basis of the second segment of this curriculum, that is, the educational resources and modules.

The possible consequences in private and professional life of a lack of digital skills, as well as not using the benefits of digital opportunities, are elaborated. The challenges that arise in the development of digital skills have been identified, as well as the strategies that should be taken to solve them. The strategies that can be applied by trainers and youth workers in empowering young women and woman entrepreneurs in development of their digital skills are elaborated more specifically. Namely, the need for providing training and learning opportunities to teachers and trainers that will add significant value to the entire education ecosystem is evident.

The data analysis confirms the essential digital business skills that individuals, including young female entrepreneurs, need to possess in order to succeed in the digital world. Various digital tools and platforms that can be used by youth workers and trainers in the transmission of their digital knowledge to young women and/or women entrepreneurs are presented in an overview way. The importance of digital education for social integration in societies was also emphasised.

All these findings further emphasise the need for the development of this type of curriculum, which will not only develop certain digital skills, but will also teach the participants in the training more about safety and security in the digital world.

Existing educational resources are also presented, as well as the resources created with this module as an integral part of 4 created modules.

The modules and accompanying materials covered in this Curriculum can be used in training courses that would be held online, but also courses that are held with physical presence.

# UNDERSTANDING THE IMPACT OF DIGITAL SKILLS DEFICIENCY

According to UNESCO's definition, digital skills refer to the abilities needed to utilize digital devices, communication applications, and networks for information access and management. Digital skills, in this context, encompass the capacity to process and handle data, communicate and collaborate using digital tools, create digital content, ensure online safety and legal compliance, and tackle problems for personal growth, learning, work, and social engagement (Feijao, C., et al, 2021)

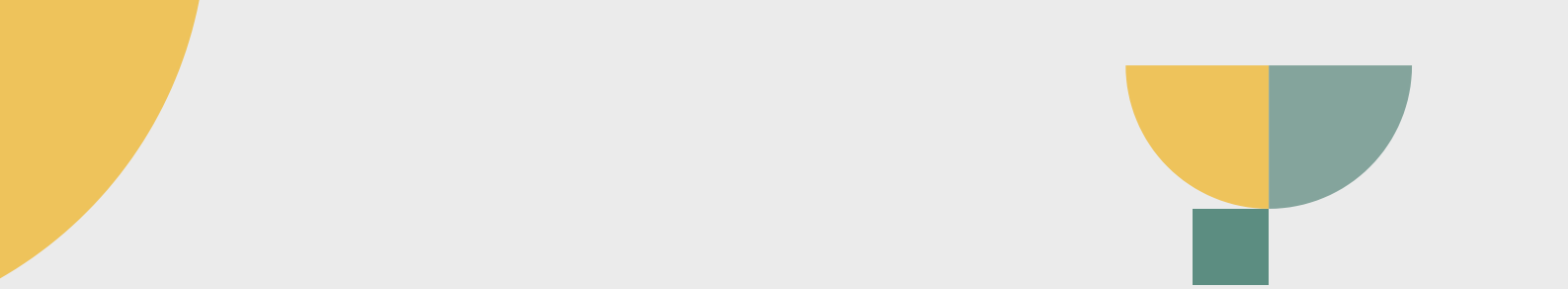
Understanding the impact of digital skills deficiency is crucial in today's increasingly digital and technology-driven world. Digital skills deficiency refers to the lack of essential digital skills and knowledge required to effectively navigate and utilize digital technologies.

The COVID-19 pandemic underscored the growing significance of the digital skills gap and accelerated the adoption of digital services. However, several persistent factors are further expanding this gap. Ongoing shifts in the economy and industries, largely driven by digitalization, are creating an increasing need for digital skills. Unfortunately, the supply of "tech talent" has not kept up with the rising demand for specialized digital skills. Moreover, potential digital talent often goes unnoticed due to obstacles related to education and qualifications, as well as unequal access to digital resources. Socioeconomic status and the digital divide also limit access to and development of digital skills, exacerbating the problem (Feijao, C., et al, 2021, p.10).

Digital skills deficiency can have far-reaching consequences across various aspects of individuals' lives, businesses, and society as a whole. In today's rapidly evolving job environment, individuals lacking essential digital skills might face challenging obstacles when trying to secure employment across a wide array of sectors. As more jobs need digital literacy, individuals without these skills may have fewer employment options and lower earning potential. A lack of digital skills can thereby widen the wage gap because individuals who have them benefit more from available employment opportunities. Also, employees who lack digital proficiency may find it difficult to complete duties effectively at work. This can lead to reduced productivity, errors, and increased workloads for others.

Furthermore, numerous essential services have changed their main ways of distribution to online platforms. These services cover a broad range of important fields, and digitalization is now accepted as standard practice. Governments use online portals for various services, educational institutions use digital learning platforms, healthcare providers increasingly offer telemedicine consultations, and financial institutions provide digital banking options. A rising digital gap, however, is a key concern brought on by this digital transition. When attempting to obtain these crucial services, people who lack the basic digital skills and access to technology may run into severe obstacles.

Students who lack essential digital skills frequently struggle to stay up with contemporary educational practices and resources. In addition to limiting their current academic achievement, this struggle might also have far-reaching effects on their employability and future economic prospects.



Furthermore, graduates who lack these crucial skills may find themselves at a considerable disadvantage while looking for job opportunities because the labor market continues to demand digital literacy across various industries. Beginning in school, the digital divide can last throughout a person's career, restricting access to high-paying jobs and limiting long-term earning potential.

Lack of digital literacy can make people and businesses more vulnerable to cyber threats and online scams. They might be unable to recognize phishing attempts, protect sensitive data, or properly handle security incidents, leaving them exposed to various risks. In essence, a person's or organization's capacity to proactively protect against these risks and effectively respond when they occur is undermined by a lack of digital skills, which also increases susceptibility to cyber-attacks and online scams. Cultivating digital literacy and cybersecurity awareness is essential for being resilient in the face of an ever-growing range of digital hazards as the digital landscape continues to change.

## ADDRESSING CHALLENGES IN DIGITAL SKILL DEVELOPMENT

In today's rapidly evolving digital landscape, acquiring and enhancing digital skills has become imperative for individuals, organizations, and nations alike. A wide range of skills are included in digital skills, from fundamental computer literacy to complex data analysis and programming. To ensure efficient skill development, there are a number of challenges that must be resolved despite the growing relevance of digital skills. The basic challenges in the development of digital skills and strategies to overcome them are presented in the text below:

### Challenges in Digital Skill Development

- The demand for digital skills among employees has grown significantly, driven by the rapid advancement of technology. However, there is a noticeable shortage of individuals with these skills, creating a digital skills gap in the workforce. Many employees lack the necessary skills to navigate digital transformation effectively, and businesses often face challenges in finding qualified talent for roles that require digital expertise. The COVID-19 pandemic has exacerbated this gap as digitalization accelerated, with many jobs moving online, thereby increasing the demand for digital skills even further. In this context, bridging the digital skills gap has become a pressing concern for both individuals and organizations as they adapt to the evolving digital landscape. (Fejjao, C., Flanagan, I., Van Stolk, C. and Gunashekar, S., 2021)
- Lack of standardized curricula and certifications for digital skills - European institutions at the university level, on average, are slow to adapt their curricula to meet the demands of specialized digital skills. When they do make changes, these adjustments tend to follow a traditional approach and may not align well with the rapidly evolving needs of the labor market. Moreover, there is a scarcity of new specialized Master's programs in Key Enabling Technologies (KETs) offered by European universities. Even among those that exist, only a few rank highly in terms of quality and relevance in the field of KETs. European universities, on average, also show limited responsiveness to the growing need for re-skilling and upskilling the adult population, which is crucial in a rapidly changing digital landscape. (EIT Digital, 2022)



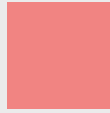
- There is a notable gap in the supply of digital skills training, particularly for adults in the middle of the digital skills spectrum. Many initiatives by non-governmental organizations (NGOs) primarily focus on providing basic digital skills to underprivileged groups through short crash courses. On the other end of the spectrum, more privileged individuals with existing skills can access advanced training. (EIT Digital, 2022)
- However, there is a significant segment of the population, often belonging to the lower-middle class, that falls between these two extremes and is in need of upskilling and reskilling. These individuals may not require highly specialized skills but do need to enhance their digital competencies for daily life and work. Many employees in various fields can benefit from improved digital skills. Unfortunately, this large group often doesn't find appropriate courses in primary and secondary education, lacks access to university-level programs, and is not typically the target audience for private sector specialized skill offerings. Private sector initiatives tend to focus on younger individuals (18-35 years old), leaving this middle-aged workforce underserved.

### **The gender gap in digital skills.**

- It is important to distinguish between basic and advanced digital skills in the context of future job opportunities. While basic skills like using search engines and digital banking are necessary, advanced digital skills can provide access to high-paying jobs in the European digital economy. The labor market increasingly values a combination of both basic and advanced digital skills, as highlighted by the OECD. In the EU, there is a gender disparity, with men often having an advantage over women in essential digital skills, especially among older individuals (aged 55 or older). Among young individuals aged 16-24, both women and men are highly digitally skilled, with 59% of women and 60% of men possessing above basic digital skills. Finland, Malta, and Croatia have the highest percentages of young women with advanced digital skills, while Italy, Bulgaria, and Romania have the lowest percentages. However, as people get older, the gender gap in digital skills widens, and most older individuals tend to have low to basic digital skills. (European Institute for Gender Equality, 2020)
- According to the Global Gender Gap Report 2020 from the World Economic Forum, there is a global trend of decreasing women's active participation in the labor market. This decline is contributing to the widening financial disparities between genders. One of the key reasons for this trend is that women are often employed in sectors that are becoming increasingly automated. Additionally, women are less likely to pursue high-earning professions, many of which are technology-related. (Levorato, S, 2021)
- The gender gap in advanced and specialized digital skills becomes more pronounced when considering fields like artificial intelligence and blockchain. Few women choose to specialize in these emerging technologies during their tertiary studies. As a result, in 2018, only 20% of graduates in Information and Communication Technology (ICT) were women. This underrepresentation leads to an even smaller percentage of female ICT professionals, with only 17.7% of women pursuing careers as ICT specialists in Europe. (Levorato, S, 2021)

### **Strategies to Address Challenges Related to the Digital Skills Gap**

Huawei and All Digital (2022), with support from EY Advisory, conducted an analysis to explore the digital skills gap, its challenges, and potential solutions. Their study focuses on the EU-27, with a deeper examination of Finland, France, Germany, and Italy. The report highlights key policy discussions, including:



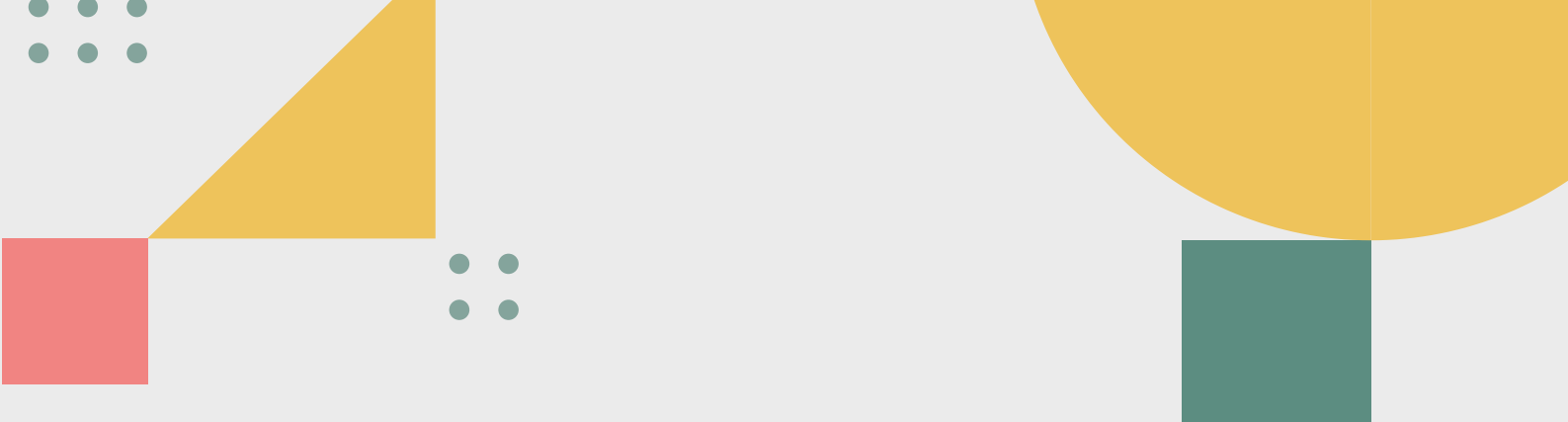
**Increasing and improving educational opportunities** – Companies can play a crucial role in expanding learning opportunities for students and workers. By doing so, they not only attract and train individuals in areas relevant to their business but also address potential gaps left by university curricula, such as practical application and specific competencies required in the workforce. The private companies can make a significant impact in mitigating skill mismatches by making training resources accessible to a broader segment of the active population, extending beyond their own employees. However, this approach may face challenges, especially when dealing with advanced courses designed for ICT specialists, as the general population may lack the necessary prerequisites for such training. In contrast, offering ICT training programs that focus on building foundational digital skills can benefit motivated individuals seeking to enhance their skill sets. This inclusive approach enables a wider audience to acquire essential digital competencies, aligning with the evolving demands of the job market.

In line with the previous point, companies can contribute to expanding training and learning certification opportunities. If certifications issued by companies, indicating successful completion of specific courses or learning paths, received official recognition from governments or other quality assurance entities, it would enhance trust in applicants holding these certificates. This recognition by governments can expedite the reduction of the digital skills gap, fostering stronger connections between private companies and suitably skilled individuals.

A critical focus for enhancing education systems is ensuring that educators themselves possess the necessary digital skills. Teachers serve as the foundation of any education system and play a central role in facilitating students' learning journeys. Therefore, it is essential for educators to have the relevant competencies to support students effectively. Providing training and learning opportunities to teachers and trainers can bring significant value to the entire education ecosystem. By equipping educators with the right digital competencies, they can better engage with modern teaching tools and techniques, adapt to evolving educational technologies, and ultimately enhance the quality of education provided to students. Google Growth and Huawei ICT Academy provide teachers with resources to enhance their digital skills and teaching abilities. Google offers digital skill courses and resources for both teachers and students, while Huawei offers teachers access to training courses, tools, masterclasses, and special initiatives like the trainer of the Year Award and trainer Forum. These programs aim to improve educators' overall classroom performance and digital proficiency.

**Overcoming the lack of standardized curricula and certifications for digital skills** is a significant challenge, but trainers and youth workers can take proactive steps to address this issue. Here are some strategies to consider:

- Trainers and youth workers can use their existing resources and adapt them to their needs. There are a number of existing resources available on digital skills, such as online courses, tutorials, and books. They can adapt these resources to their specific needs and audience.
- Developing their own curriculum and certifications. If trainers and youth workers have the expertise and resources, they can develop their own curriculum and certifications for digital skills.
- Partnering with other organizations, such as businesses, educational institutions, and non-profits, to develop and deliver digital skills training.
- Focusing on transferable skills. When developing curriculum and training materials, trainers and youth workers should focus on transferable skills that can be applied in a variety of settings. This will make the training more valuable to youth, even if they do not receive a standardized certification.



Overcoming the lack of standardized curricula and certifications for digital skills is a challenge, but it is one that can be addressed by trainers and youth workers who are proactive and creative. By following the strategies above, trainers and youth workers can provide youth with the digital skills they need to succeed in the digital world.

**Empowering young women entrepreneurs with digital skills** is a crucial step in bridging the digital skills gap and fostering economic growth. When young women entrepreneurs have the digital skills they need, they are better able to start and grow successful businesses, create jobs, and contribute to the economy. Trainers and youth workers can play a key role in empowering young women entrepreneurs with digital skills by implementing the following strategies and steps:

- Providing access to digital skills training and education through public libraries, community centers, online platforms, and other organizations. To achieve this goal, it's essential to provide a range of training options through various channels, making it accessible and affordable for all.
- Making digital skills training relevant to the needs of young women entrepreneurs. This means covering topics such as online marketing, social media marketing, e-commerce, digital security, digital wellbeing, different digital tools and technologies that are essential for success in the digital age.
- Providing mentorship and support to young women entrepreneurs through mentorship programs, online forums, and other resources. Mentorship can provide young women entrepreneurs with the guidance and support they need to develop and launch their businesses.
- Promoting role models and success stories. Highlighting the success of young women entrepreneurs who have used digital skills to build successful businesses can inspire other young women to pursue their entrepreneurial dreams.
- Creating a supportive ecosystem for young women entrepreneurs through creating networks and communities where young women entrepreneurs can connect with each other, learn from each other, and support each other.

By implementing these strategies and steps, trainers and youth workers can contribute to closing the digital skills gap among young women entrepreneurs, fostering their growth and success in the digital age, and promoting gender equality in entrepreneurship.

## BUILDING THE ENTREPRENEURIAL MINDSET

An entrepreneurial mindset is a mindset that embraces uncertainty and actively seeks opportunities. It involves innovative thinking, action-oriented problem-solving, and a focus on creating value and jobs. Developing this mindset is crucial for both economic organizations and the overall socioeconomic well-being of the population. It enables individuals to establish organizations based on valuable new ideas and fosters a culture that encourages and supports innovation. An entrepreneurial mindset is about seeing opportunities, being proactive, and making a positive difference, rather than being deterred by barriers or failures. It is particularly valuable for individuals and small and medium-sized enterprises (SMEs) navigating uncertain business environments to seize high-potential opportunities. (Assenge, E. et al., 2018)

An entrepreneurial mindset can be developed and continuously cultivated through a variety of strategies and techniques such as (MasterClass, 2021):

1. Setting clear goals and sharing them with others to stay motivated and focused.
2. Practicing decisiveness to make confident decisions, a crucial skill for entrepreneurs.
3. Reinterpreting failure as a positive learning experience and discussing it openly.
4. Confronting fears, such as public speaking, by exposing oneself to them through classes or experiences.
5. Embracing curiosity to continually learn, seek new experiences, and stay competitive in entrepreneurship.

Building an entrepreneurial mindset is an ongoing process that requires patience and continuous learning. Aspiring entrepreneurs can establish a basis for an effective, flexible, and innovative mindset by adopting the above principles into their daily lives.

## ENHANCING DIGITAL SKILLS AND COMPETENCIES

Enhancing digital skills and competencies has become an imperative in today's rapidly evolving technological environment. Digital competences are crucial for various aspects of our lives, including learning, work, and citizenship. Proficiency in using digital technology is essential for lifelong learning, employability, and inclusion. It empowers individuals to access information, acquire new learning and job prospects, foster creativity and entrepreneurship, discover opportunities, and assist others.

There is a significant digital skills gap, particularly in OECD countries, where a substantial portion of the workforce lacks proficiency in using digital technologies. This gap is even more pronounced among women. The disparity between the skills of young job seekers and employers' expectations is seen as a difficulty to economic growth. Additionally, the rise of young people entering the workforce in developing countries, emphasizes the urgency for policymakers and educators to adapt educational curricula to align with changing labor market demands.

The impact of ICTs extends beyond just employment; it also deeply influences social and civic engagement within societies. Possessing the essential digital competencies not only improves individuals' overall quality of life but also enhances their efficiency at work. Consequently, digital competencies and skills have become indispensable for active participation in the current and future global landscape as well as to benefit from existing and emerging technologies. (UN, 2018)

The developing technological landscape requires a variety of digital competencies to effectively adapt. Numerous organizations and initiatives have undertaken activities to define and classify the digital skills and competencies that will be crucial in the future. Table 1 provides examples of some of the categorizations of these skills and competencies:

**Table 1. Different categorizations of digital skills**

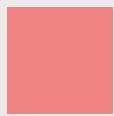
Job-ready digital skills for decent jobs (International Labour Organization and International Telecommunication Union (ITU))	<ul style="list-style-type: none"> <li>• Advanced digital skills (coding and other algorithmic knowledge)</li> <li>• Basic digital skills (related to the use of technologies)</li> <li>• Soft skills (such as communication and leadership)</li> <li>• Digital entrepreneurship (online market research and using financial platforms)</li> </ul>
Work-related skills (World Economic Forum)	<ul style="list-style-type: none"> <li>• Abilities (cognitive and physical)</li> <li>• Basic skills (content and processing skills)</li> <li>• Cross-functional skills (social systems, complex problem solving, resource management and technical skills)</li> </ul>
Future of work (OECD)	<ul style="list-style-type: none"> <li>• Technical and professional skills (specific and often industry-specific skills such as installation and operation of robots)</li> <li>• Generic ICT skills (skills needed to understand, use and adopt technologies; life-learning ability to adapt to technology changes)</li> <li>• Complementary ICT soft skills (creativity, communication skills, critical and logical thinking, teamwork, digital entrepreneurship)</li> </ul>

Source: UN (2018): “Building digital competencies to benefit from existing and emerging technologies, with a special focus on gender and youth dimensions”, Report of the Secretary General, p.4.

In the process of accepting, using, and integrating technologies into everyday life, there are four distinct levels of digital skills required. These levels encompass the skills necessary for initial technology adoption, basic usage, creative adaptation, and even the creation of entirely new technologies. These skill categories can be further divided into two broader groups: one consisting of skill sets that are essential for everyone, regardless of their profession or background, and the other comprising skill sets tailored for ICT professionals who work directly with information and communication technologies.

**Table 2. Categories and levels of digital skills**

Category	Levels	Skills
Digital skills for all	Adoption	Basic education and literacy. Familiarity with technology devices and services.
	Basic or generic use	Basic understanding of technologies, software and applications. Knowledge of digital rights, privacy, security and permanence of data. Ability to make use of information and data, ranging from basic issues of data storage, management, and organization to construct calculations and answer questions. Ability to use digital technologies to collaborate, communicate and create.
Digital skills for ICT professionals	Creative use and adaptations	Basic computing skills. Familiarity with basic algorithms.
	Creation of new technologies	Sophisticated programming skills; knowledge of complex algorithms



Source: UN (2018): “Building digital competencies to benefit from existing and emerging technologies, with a special focus on gender and youth dimensions”, Report of the Secretary General, p.5.

It is apparent that different approaches to digital skills are crucial as we deal with the constantly evolving environment of work and technology. The various categorizations and frameworks presented by organizations such as the International Labour Organization and International Telecommunication Union (ITU), the World Economic Forum, and the OECD underscore the complexity and diversity of skills required for today's job market. From job-ready digital skills to advanced coding and algorithmic knowledge, soft skills, and digital entrepreneurship, to a range of technical and professional competencies, these frameworks acknowledge the breadth and depth of the digital skill set. Moreover, they emphasize the importance of adaptability and lifelong learning in the face of constant technological advancements. The combination of these skill sets empowers individuals to not only succeed in prestigious jobs but also to succeed in the dynamic and transforming workplace.

## BUSINESS SKILLS DEVELOPMENT FOR YOUNG FEMALE ENTREPRENEURS

Empowerment of women and girls is one of the crucial elements of the Sustainable Development Goals 2030 and a key contributor to economic growth and development. Many women, both in the European Union and in its neighbouring countries still face economic, legislative and social barriers to entering the labour market, entrepreneurship and self-employment. (ETF, 2021)

Young female entrepreneurs face a number of unique challenges in the business world. They may not have the same access to resources and networks as their male counterparts, and they may also face gender stereotypes and discrimination.

However, there are a number of activities that young female entrepreneurs can do to develop their business skills and increase their chances of success. Some of these include:

- Participating in business training courses or workshops can be highly beneficial. These programs can equip individuals with fundamental business management knowledge, including marketing, finance, and accounting. It's worth noting that there are also numerous courses and workshops tailored specifically to address the needs and challenges faced by female entrepreneurs.
- Finding a mentor who can provide female entrepreneurs with guidance and support can be invaluable. A mentor can help develop a business plan, network with other entrepreneurs, and overcome challenges.
- Networking with other entrepreneurs is a great way to learn from others, find partners, and get support. There are a number of networking events and organizations for female entrepreneurs.
- Reading books and articles about business. There is a wealth of information available on business, including books, articles, and blogs.
- Getting involved in the entrepreneurial community. There are a number of organizations and communities that support entrepreneurs.



Here are some specific skills that are important for young female entrepreneurs:

- In today's digitized society, it is necessary for everyone, and especially for those who run a business, to develop digital skills, improve the ability to work with various digital tools and platforms and introduce them into business processes.
- Possessing the knowledge of how to develop a business plan serves as a roadmap for the enterprise, encompassing critical elements such as goals, mission, vision, strategies, and financial projections.
- Developing financial management skills involves mastering budgeting, financial forecasting, and effectively managing investments and funding.
- Acquiring skills in marketing and sales is essential for entrepreneurs. This includes expertise in market research and proficiency in digital marketing and sales techniques.
- Leadership skills are critical in entrepreneurship, encompassing decision-making, effective communication, team leadership and motivation, promoting collaboration and productivity, task delegation, and offering constructive feedback.

Research in the field of female entrepreneurship in the digital world, as well as the analysis of the research data from the previous research in the OMEGA project related to "Young Women Entrepreneurs and Digital Culture" confirm that the women entrepreneurs or potential entrepreneurs are most interested in developing the following knowledge and skills related to the digital world and culture:

- Cybersecurity and data privacy
- Digital well-being
- Balancing personal and professional digital lives
- Digital marketing
- Digital project management
- Basic design skills and web publishing

Based on the established findings of the necessary digital skills knowledge from the research conducted in the OMEGA project, the modules in this curriculum are designed.

All previously mentioned skills necessary for the business can be supported with the digital tools and platforms. They are knowledge needed to use digital technologies, tools, platforms to create, market, and sell products and services, as well as to manage and grow a business online. Young female entrepreneurs can benefit from a wide range of digital business skills to help them succeed in today's competitive business landscape. These skills can empower women to start, manage, and scale successful businesses. Here are some essential digital business skills that individuals, including young female entrepreneurs, can focus on developing:

- Cybersecurity Awareness - understanding the importance of securing customer data and transactions. Phishing and online scams - recognize common online threats and scams to protect your business.
- Regulatory Knowledge - understanding the legal aspects of running a digital business, including intellectual property rights and privacy regulations. Also, in this context is very important knowledge about data privacy laws and ethical considerations when collecting and using customer data.



- Social Media Marketing - learning how to effectively use platforms like Facebook, Instagram, Twitter, and LinkedIn for marketing strategies and customer engagement.
- Content Marketing - developing skills in creating and promoting valuable content such as blog posts, videos, and infographics.
- Email Marketing - understanding email marketing tools and strategies to build and nurture customer relationships.
- Pay-Per-Click (PPC) Advertising - understanding platforms like Google Ads and Facebook Ads for creating targeted ad campaigns.
- Project Management: obtaining expertise in project management software, including tools such as Trello or Asana, is essential for learning how to efficiently plan and track tasks and projects.

Networking is essential for entrepreneurs, and many women's business networks provide strong daily support to thousands of women entrepreneurs. Some examples include (Bekh, O., 2014, p.12-13):

- the FCEM (World Association of Women entrepreneurs promotes women's entrepreneurial initiatives and reinforces national associations of women business owners, paying particular attention to women's professional growth and skills issues;
  - the AFAEMME (Association of Organisations of Mediterranean Businesswomen), which represents 20 countries and includes 37 business women organisations;
  - the regional network of Resource Centres under FEM (Female Entrepreneurship Meetings) in the Baltic Sea Region;
  - the Enterprising Women networking community in the United Kingdom;
  - the Italy-based YWEA (Young Women Entrepreneurs Association), which supports growth and the internationalisation of women-owned companies.
  - SheEO: A global community of female entrepreneurs and investors who are working together to create a more equitable world.
  - The Female Founder School: A global online school for female entrepreneurs who want to start and grow their own businesses.
  - Women Who Code: A non-profit organization that is dedicated to helping women learn to code and build their careers in technology.
  - The Girls' Lounge: An online community and resource hub for young women who are interested in entrepreneurship and leadership.
- 
- Digital networking is so important in today's digital world, with a wealth of online forums, groups, and communities available for connecting with mentors and fellow entrepreneurs. LinkedIn, being a well-regarded digital professional platform, provides valuable opportunities for networking, establishing professional connections, and highlighting businesses.
  - Website Development and Management, including web design, entails acquiring knowledge of fundamental web design principles and using website builders or Content Management Systems (CMS) like WordPress to create and maintain a professional online presence.
  - Search Engine Optimization (SEO) involves acquiring knowledge on optimizing a website for search engines to enhance online visibility.
  - In today's digital world it is very important for young female entrepreneurs to gain knowledge and to increase skills related to e-Commerce. If they plan to sell products online, it is important to learn about e-commerce platforms like Shopify, WooCommerce, or Magento. Also, it is very crucial to understand how to set up secure online payment methods for the customers.





## GROUP DYNAMICS

Target groups for the implementation of the Curriculum are youth workers, trainers, involved in youth education, as well as low digitally skilled women and young women belonging to disadvantaged groups. Therefore, youth workers and trainers will develop the digital skills and competence needed for safe and secure operation in the digital world.

The curriculum will be a useful tool of quality for institutions, enterprises or individuals that wish to help newly educated, unemployed or disadvantaged young women entrepreneurs in their society gain advantage.

The examination of the current specialized consulting and training offerings for digitising businesses in all partner countries strongly backs the following suggestions for implementation of the Curriculum:

- Each partner organization will choose six participants who will acquire competencies through training events. This will enable them to develop digital skills and competences, while also promoting the significance of these skills in enhancing young women's employability and increasing their prospects in the labor market.
- The pace at which the training is put into action will rely on the resources at hand. However, it is recommended to conduct training sessions based on this Curriculum multiple times annually.
- To improve the ability of youth workers and trainers to effectively transmit their knowledge and skills to young women different methods and tools can be used for implementing the online training curriculum such as: online teaching platforms, pre-recorded video lessons, online education PPT presentation, digital solutions for implementation of virtual learning activities, face-to-face trainings, online games and simulations, problem-based learning, case studies and good practices analysis, quizzes and assessment for evaluation of the participants' understanding.

## PROFESSIONAL DEVELOPMENT FOR YOUTH WORKERS AND TRAINERS

The implementation of this curriculum, which incorporates 4 modules, will enable the professional development of youth workers and trainers in the field of digital education, digital literacy, acquisition and development of skills for using various digital tools and platforms, handling different types of phishing, preventing various digital threats, as well as studying numerous strategies for the same.

Furthermore, various good practices for digital education are elaborated upon, and a review of strategies for transferring digital knowledge to young women and the benefits of it for easier social integration has been conducted.



# EQUIPPING YOUTH WORKERS WITH BEST PRACTICES IN DIGITAL EDUCATION

Digital education is the innovative use of digital tools and technologies during teaching and learning, and is often referred to as Technology Enhanced Learning (TEL) or e-Learning. (Institute for Academic Development, 2018)

The European Commission launched the Digital Education Action Plan in 2017 in order to improve key competences and digital skills of European citizens. The Digital Education Action Plan (2021-2027) is a renewed EU policy initiative that sets out a common vision of high-quality, inclusive and accessible digital education in Europe, and aims to support the adaptation of the education and training systems of Member States to the digital age. (European Commission n.d.).

An innovative practice in both delivering digital youth work and also upskilling youth workers' digital competences include: information sharing on social media, online youth counselling, supporting digital literacy, enabling participation with digital tools, supporting cultural youth work online, supporting the development of technological skills, using digital games in youth work. (European Commission, 2018, p.6)

The field of digital education is dynamic and continuously evolving. As technology continues to evolve, new and innovative tools and resources will emerge to support youth workers in their efforts to deliver engaging and effective learning experiences to young people. Some of the future trends that are likely to shape the digital education of youth workers are: increased use of Artificial Intelligence (AI), Virtual Reality, Hybrid and Blended Learning Models, Gamification and Game-Based Learning, Video-based learning etc.

There are a variety of tools and resources that can be used for the digital education of youth workers for project management, education, communication, collaboration, promotion, research etc. Youth workers can be equipped or trained to transfer digital knowledge through different methods, as follows: online courses and workshops, software applications, webinars, podcasts, social media platforms, collaboration and communication tools, different types of digital platform and application etc.

Below, we elaborate some of the digital tools that can be applied in the work of youth workers, individuals, organizations and businesses.

## **Project management and communication tools:**

- Trello - a visual project management tool that uses boards, lists, and cards to help teams organize tasks and projects.
- Slack - is a widely used messaging and collaboration platform designed for teams and organizations to communicate and work together more effectively.
- Google Drive - is a cloud-based file storage and synchronization service developed by Google. It offers users a secure and convenient way to store, access, share, and collaborate on files and documents from virtually anywhere with an internet connection.

- Asana - is a popular project management tool that is known for its simplicity and ease of use. It offers a variety of features, including task management, project planning, and time tracking. Asana is a good option for teams of all sizes and for projects of all types.
- Basecamp - a project management and team collaboration tool that provides to-do lists, file sharing, and message boards.
- ClickUp - is a project management tool that offers a wide range of features, including task management, project planning, time tracking, and team communication.
- Doodle - is the fastest and easiest way to schedule anything – from meetings to the next great collaboration.
- Jamboard - is a digital whiteboard created by Google that can be used in collaboration with Google Workspace.
- MindMeister - is a popular online mind mapping and brainstorming tool that allows users to visually organize their thoughts, ideas, and information in a structured and collaborative manner.

#### **Surveys and analysis tools:**

- SurveyMonkey - useful for creating and distributing surveys.
- Google Looker Studio - A free tool for creating and sharing interactive reports and dashboards.
- Google Forms - easily create and share online forms and surveys, and analyze responses in real-time.
- Typeform - is an online form builder that allows users to create beautiful and interactive forms. It is often used for surveys, quizzes, polls, and other types of data collection.

#### **Promotion and content collaboration tools:**

- Canva is a graphic design platform that allows users to create social media graphics, presentations, posters, flyers, and other visual content. It is a popular tool for both individuals and businesses.
- Piktochart is a cloud-based infographic maker that allows users to create professional-looking infographics without any prior design experience. It offers a wide variety of templates and design elements that can be customized to create unique and informative infographics.
- Unsplash is a free stock photo website, popular choice for businesses and individuals who need high-quality images for their websites, blogs, social media accounts, and other marketing materials.
- Figma is a collaborative design platform that allows teams to work on designs together in real time. Figma is a good option for businesses and organizations that need to create and share designs with multiple people:
- Google Docs - is a web-based application developed by Google for creating, editing, and storing documents online.
- Prezi - is a web-based tool for creating presentations.
- MindMeister - is an online mind mapping tool that allows users to visualize, share, and present their thoughts via the cloud.

### Sharing tools:

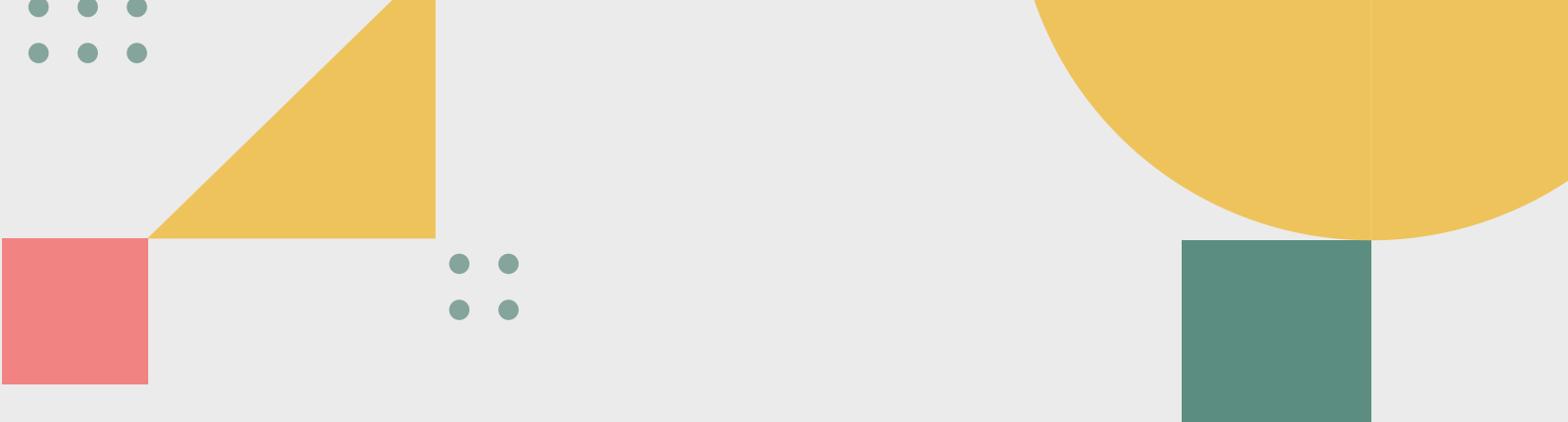
- Dropbox is a cloud storage service that allows users to store and share files online.
- Google Drive is a cloud-based storage service that enables users to store and access files online.
- Doodle is the fastest and easiest way to schedule anything – from meetings to the next great collaboration
- WeTransfer is a cloud-based content-sharing platform ideal for sharing large files.
- Google Calendar is the time management and scheduling tool created by Google.
- Bitly is a URL shortening service and a link management platform.

### Other digital tools and platforms:

- Learning management systems like Moodle, Blackboard can be used to create and deliver online courses and training programs
- Video conferencing platforms like Zoom, Microsoft Teams, Google Meet can be used to hold online meetings, workshops, and other activities.
- Gaming platforms like Roblox and Minecraft can be used to connect with young people and engage them in educational and social activities.
- As examples of best practices in digital education that can benefit youth workers in their work, we can highlight several successful programs and projects including:
- Collaborative Online Learning Database include range of interactive tools such as forums, social networking applications, and mini games.
- Digital Skills Pathways Programme for Youth Across Europe
- Verke - Centre of Expertise for Digital Youth Work in Finland, offer training and best practices in digital education.
- Digital, Responsible Citizenship in a Connected World (DRC) is an Erasmus+ project, offering guide, program, curriculum, app, platform related to digital citizenship and digital literacy.
- Dig-it Up! – A model for a training course aimed at creating pedagogical and digital bridges between youth workers and young people.

## STRATEGIES FOR TRANSMITTING DIGITAL SKILLS TO YOUNG WOMEN

Digitalization and use of ICT increase opportunities for young women to develop themselves and their businesses and to gain access to equal opportunities with men in business development. Gender inequality in the physical world is replicated in the digital world. Boys use far more digital platforms and services for a much wider range of activities than girls, and they are more likely to use the internet. In many countries, gender inequality means that women and girls have lower levels of education and less practice in using or creating digital content. As a result, women's and girls' digital adoption and use is frequently limited by lower levels of digital literacy, and a lack of confidence. The gender gap in digital literacy is growing as technologies become more sophisticated. (UNICEF East Asia & Pacific, 2021)



Europe's digital future includes big data, robotics, artificial intelligence, cybersecurity and the internet of things. There is currently a lack of around 1 million digital specialists. Recruiting more women will help meet Europe's increasing demand for digital experts. Also, women's online presence, free from fear and hatred, should equally be ensured. (European Commission, 2019)

This curriculum is intended for youth workers who need to equip themselves with digital education and transmit it on to young women (entrepreneurs or future entrepreneurs). There are different ways or strategies they can do:

- Workshops and training programs: Youth workers can offer workshops and training programs on digital skills to young women.
- Mentorship program: Youth workers can mentor young women on digital skills, providing them with guidance and support as they learn. This could involve meeting with young women regularly to discuss their goals, provide feedback on their work, and help them troubleshoot problems.
- Online resources: Youth workers can share online resources with young women on digital skills. These resources could include tutorials, articles, presentations and videos.
- Project-based learning: Youth workers can engage young women in project-based learning activities that involve using digital skills.
- Game learning program: Use games and other interactive activities to teach young women about digital skills.
- Invite female speakers from the tech industry to give talks and workshops to young women.

## PROMOTING SOCIAL INTEGRATION THROUGH DIGITAL EDUCATION

Social inclusion is a process that enables a young person to build up self esteem, self-realisation and resilience, to become an autonomous and productive member of society, able to reach self-fulfilment and contribute to the development of society as a whole. In order to support the social inclusion of young people, their participation in social, economic and political life should be promoted, based on the equality of rights, equity and dignity. (Şerban, A. et.al, n.d.)

Digital education can play a significant role in the social integration of young women by providing them with opportunities for personal growth, skill development, and meaningful connections.

Here are some specific examples of how digital education is being used to promote social integration of young women:

The Malala Fund is a non-profit organization that works to ensure that every girl has the opportunity to learn and lead. The Malala Fund uses digital education to provide girls in developing countries with access to education and training resources.

The Girls Who Code is a non-profit organization that works to close the gender gap in technology. The Girls Who Code offers free coding classes and workshops to girls ages 7-18.

The Global Girls Hub is a non-profit organization that uses digital education to empower girls and young women around the world. The Global Girls Hub offers online courses and training programs on a variety of topics, such as leadership, social entrepreneurship, and technology.



## EDUCATIONAL RESOURCES

Educational online resources for digital wellbeing for youth trainers encompass a wide array of digital tools, courses, and materials designed to equip trainers with the knowledge and skills necessary to promote a healthy and balanced use of technology among young people. These resources typically include informative articles, interactive courses, webinars, and workshops, all aimed at addressing the unique challenges and concerns related to digital wellness in today's interconnected world. They cover topics such as online safety, responsible social media use, managing screen time, and fostering digital literacy. By engaging with these resources, youth trainers can enhance their understanding of the digital landscape, stay updated on evolving digital trends, and develop strategies to empower young individuals to navigate the online world in a safe, informed, and responsible manner.

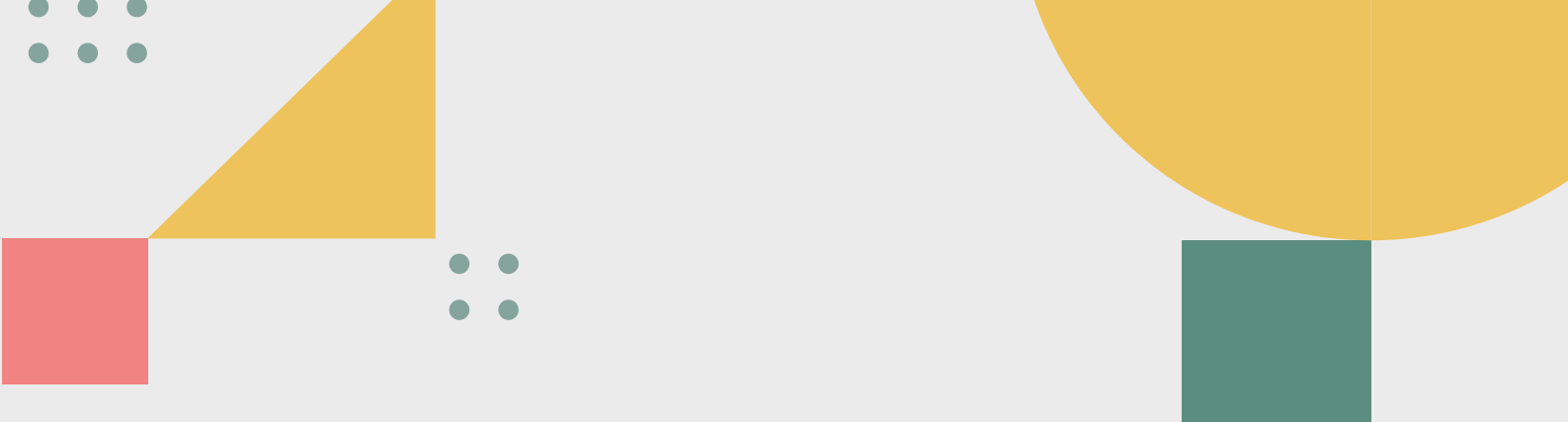
Here are some examples of educational online resources that are available for youth trainers on the topic of digital wellbeing:

- Google's Digital Wellbeing provides a variety of resources on digital wellbeing, including articles, videos, and tools. It also has a specific section for young people.
- Take Charge of Your Tech offers a range of resources on how to use technology in a healthy way, including tips on setting boundaries, managing distractions, and protecting your privacy.
- Digital Detox provides information on the benefits of taking breaks from technology, as well as tips on how to do it.
- The Center for Humane Technology is an organization that is dedicated to help people to use technology in a way that is good for them and society. They have a variety of resources on digital wellbeing, including articles, videos, and tools.
- The Digital Wellbeing Lab offer a variety of resources on digital wellbeing, including research findings, tools, and tips for youth trainers.
- NetSafe is a New Zealand based organization that provides resources for using technology safely and responsibly, with a specific section dedicated to young people and educators.
- Digital Wellbeing Education App is a short e-learning course for students on digital wellbeing. It is well placed to offer a range of resources to help teachers and their students understand the key capabilities and current debates around online education and digital wellbeing.

By using these resources, in addition to the materials provided in the curriculum modules, youth trainers can acquire the knowledge to educate young people on the significance of digital literacy, promoting digital well-being, and utilizing technology in a balanced and productive way.

## RESOURCES OVERVIEW AND KEY COMPETENCIES

The educational resources within this Curriculum are categorized into two parts. Part A comprises resources for Internet Security and Digital Literacy, while Part B includes educational materials focused on Digital Well-Being and addressing Social Media Addiction.



Each part includes two modules, making a total of four modules that are integral parts of this Curriculum. The first module is entitled “The Core Rules of the Internet”, which focuses on developing key competences of the participants, essential for navigating the digital world. The second module titled “Phishing Types and How to Deal with Phishing Incidents” aims to increase knowledge and awareness of the participants for cybersecurity. The third module entitled “How to Enjoy the Benefits of Digital Technology While Avoiding the Hazards” aims to raise awareness for Digital Wellness. And the fourth module is entitled “Gaming and Social Media Addiction”, that focuses on creating a healthy digital balance plan for the participants.

## INTERNET SECURITY AND DIGITAL LITERACY RESOURCES

### Overview

This module, titled "The Core Rules of Internet," is designed to provide participants with essential digital competences for effectively navigating the digital world.

Over the course of 150 minutes, participants will engage in a comprehensive learning experience covering a wide range of key competencies. These include Digital Literacy, which empowers participants to understand and navigate online platforms, evaluate online information, and practice responsible technology use.

The module also focuses on Online Communication and Collaboration, emphasizing netiquette, teamwork, and effective communication in digital spaces. Cybersecurity and Data Protection are addressed, making participants aware of common threats and how to protect themselves online. Additionally, participants will explore Digital Creativity and Content Creation through hands-on projects, fostering creativity while respecting copyright and ethical use of digital content. Critical Thinking and Media Literacy exercises enhance participants' ability to discern reliable information from misinformation.

The module also covers Digital Citizenship and Online Ethics, promoting responsible digital behavior, empathy, and inclusivity while addressing issues like cyberbullying. Practical methodology combines slide presentations with interactive components and hands-on exercises to ensure comprehensive learning and practical application of digital skills.

# MODULE 1: THE CORE RULES OF INTERNET

## Learning Outcomes - Key Competences

In this resource, participants will engage in activities that focus on developing key competences essential for navigating the digital world. The key competencies include:

### Digital Literacy: Understanding Online Platforms and Tools

Participants will explore various digital platforms, websites, and applications, equipping them with the ability to navigate the online landscape effectively. They will learn to evaluate the credibility of online information and practice responsible use of technology, including aspects of digital security and privacy.

### Online Communication and Collaboration

Through interactive exercises, participants will learn effective communication skills in digital environments, emphasizing the importance of netiquette. The module will delve into the etiquette of online forums, social media, and virtual meetings, while promoting teamwork and collaboration through digital tools.

### Cybersecurity and Data Protection

Participants will gain awareness of common cybersecurity threats and acquire knowledge to protect themselves and others online. Topics include the development of a robust password policy, employing encryption techniques, and understanding data protection and privacy laws.

### Digital Creativity and Content Creation

Engaging in hands-on projects, participants will explore various digital tools and software for content creation. They will nurture creativity in digital spaces by working on multimedia projects while understanding the importance of copyright laws and ethical use of digital content.

### Critical Thinking and Media Literacy

Through critical analysis exercises, participants will hone their ability to discern reliable information from misinformation encountered on the Internet. They will also explore methods to identify biases in online content and develop media literacy skills.

### Digital Citizenship and Online Ethics

Participants will explore the concept of responsible digital citizenship, understanding the impact of their actions on the online community. The module will promote online respect, empathy, and inclusivity while addressing cyberbullying and harmful online behavior.

## Materials/resources required

- Computers or Laptops with internet access
- Digital tools and software (word processors, presentation software, etc.)
- Handouts and worksheets
- Internet Access
- Stationery (pens, pencils, markers, etc.)





## Methodology

The methodology employs a two-part approach to ensure effective learning and practical application of the key competences. The first part involves slide presentations that illustrate fundamental best-practice methods for various aspects of digital literacy, online communication, cybersecurity, content creation, critical thinking, and digital citizenship. These presentations will be interactive and engaging, utilizing real-life examples and case studies to enhance comprehension. The second part of the methodology entails hands-on practical exercises where participants will actively apply their newly acquired skills. Through specific tasks and scenarios related to each competence, participants will utilize digital tools and platforms to complete the exercises. This combination of theoretical and practical components will enable participants to gain a comprehensive understanding of the core rules of the Internet, fostering confidence in their ability to apply these skills effectively in real-world situations.

## Introduction

### (Duration: 15 minutes)

In this activity, participants will take a virtual journey through various online platforms, websites, and digital tools. As a group, they will discuss their experiences, share their favourite online resources, and identify the challenges they face in the digital realm. This activity aims to create an interactive and engaging atmosphere, setting the stage for our exploration of essential competences for navigating the digital landscape.

## Activity 1: Digital Literacy Discovery

### (Duration: 30 minutes)

In this activity, participants will engage in a slide presentation that covers the fundamentals of digital literacy. They will learn about recognizing and navigating online platforms, understanding digital security, privacy, and responsible internet use. Interactive quizzes and discussions will reinforce the concepts and encourage active participation.

## Activity 2: Creative Content Challenge

### (Duration: 30 minutes)

In this hands-on activity, participants will put their content creation skills to the test. Working in groups, they will be given themes or topics to create multimedia content using various digital tools and software. They will apply their knowledge of copyright laws and ethical use of digital content while fostering creativity and teamwork.





### **Activity 3: Cybersecurity Escape Room**

**(Duration: 60 minutes)**

In this interactive and engaging activity, participants will be immersed in a cybersecurity escape room scenario. They will work collaboratively to solve puzzles and challenges related to cybersecurity and data protection. Through this activity, they will reinforce their understanding of common threats and the importance of safeguarding their digital information.

### **Closing**

**(Duration: 15 minutes)**

Each participant will have the opportunity to share their reflections on the key competences they have acquired during the module. They will then take part in a group discussion on the impact of responsible digital citizenship and how they plan to apply their newfound knowledge and skills to promote a positive online community. Finally, participants will collectively take a pledge to uphold the core rules of the Internet, committing to be responsible, respectful, and empathetic digital citizens.



## MODULE 2: PHISHING TYPES AND HOW TO DEAL WITH PHISHING INCIDENTS

### Learning Outcomes - Key Competences

Following completion of this module, learners need to be able to:

Upon completing this module, learners will be adept at recognizing diverse phishing attempts and understanding the tactics employed by fraudsters. Additionally, they will gain the skills to effectively address and prevent phishing situations, culminating in the creation of a customized prevention plan for heightened cybersecurity.

### Essential Skills include the following:

Critical for cybersecurity proficiency, essential skills encompass knowledge and awareness of cybersecurity, problem-solving, and critical thinking abilities. Additionally, a mastery of incident response and preventive techniques, coupled with strong collaboration and communication skills, constitutes a well-rounded skill set for navigating the dynamic landscape of digital security.


### Materials/resources required:

- Computers or devices for participants.
- Projector and screen for presentations.
- Phishing detection tools or simulations (for Activity 1 and 2).
- Handouts or worksheets for Activity 3.
- Whiteboard and markers.
- Internet access for research and examples.

### Methodology

The initial 15 minutes of the session are dedicated to establishing a positive and engaging atmosphere. This begins with a friendly greeting and a concise icebreaker exercise. The session then seamlessly transitions to Context Setting, where real-world examples of phishing incidents and their outcomes are shared to underscore the importance of the training module. The next focus is on The Significance of Phishing Awareness, highlighting why it is crucial to recognize phishing threats in both personal and professional contexts.

The potential hazards and implications associated with falling victim to phishing attacks are explored to emphasize the gravity of the matter. The Module Overview follows, presenting a clear outline of the training module's structure, goals, and the competencies participants are expected to acquire.



This overview acts as a roadmap, guiding participants through a purposeful learning experience and ensuring they are informed about the key aspects of the upcoming training. In Activity 1, participants engage in a Phishing Detection Challenge lasting 40 minutes, designed as an introductory exercise to enhance their ability to recognize common signs of phishing in emails or scenarios. The activity begins with a Presentation using a projector or screen to display exemplary phishing emails or scenarios.

Participants are encouraged to actively analyze these examples. Subsequently, a Group Discussion ensues, where the facilitator guides participants in collectively evaluating the examples. Individuals are prompted to share their observations, focusing on identifying phishing symptoms such as suspicious links, email senders, and content. The session concludes with a Debrief, offering a concise overview of the key discoveries and strategies employed during the discussion of the phishing instances. This activity aims to foster active engagement, critical thinking, and collaborative learning in the realm of phishing detection. In Activity 2, participants engage in a Simulation of Phishing Incident Response.

The activity begins with an Introduction, outlining the simulation's purpose: practicing incident response procedures in the context of a phishing incident. The Simulation Configuration involves establishing parameters for scenarios, ensuring participants have the necessary tools for reporting and responding. Participants are then actively engaged, following incident response protocols and reporting the simulated phishing incident. A crucial component is the Simulation Debrief, where the facilitator evaluates participants' responses, highlighting positive aspects and areas for improvement, and providing constructive criticism. Moving to Activity 3, participants develop Individualized Strategies for Mitigating Phishing Attacks. The Introduction emphasizes the goal of creating personalized prevention strategies for safeguarding individual and organizational interests. Participants receive explicit instructions and templates, with the option for solitary or small group work, encouraging brainstorming of technical and behavioral preventive measures.

The subsequent Presentation and Discussion phase allows individuals or groups to share their prevention plans, fostering active feedback, inquiries, and scholarly discourse. The Conclusion underlines the importance of consistently revising and implementing robust phishing prevention plans. As the session nears its end, the Conclusion summarily encapsulates key insights from the module, emphasizing the significance of heightened awareness and effective incident response. Future Actions underscore the need for an ongoing cybersecurity education culture and maintaining vigilance against phishing attempts. A Request for Feedback encourages participants to provide insights for content enhancement and identify areas of interest for in-depth exploration. Acknowledgements express gratitude for participants' engagement, concluding the session on a positive note. Supplementary materials or references are offered for further educational enrichment, if deemed relevant.

## Introduction (15 Minutes)

### Introduction to Phishing

Phishing is widely recognised as a highly pernicious and prevalent cyber hazard in contemporary digital technology. The phenomenon above refers to a nasty cyber activity organised by individuals with criminal intent who employ crafty and deceptive methods to exploit individuals' and organisations' trust and susceptibility. The perpetrators use meticulously devised strategies to manipulate individuals into disclosing sensitive and personal information, including passwords, credit card details, social security numbers, and other protected data.

This menace has a broad reach, impacting individuals from many backgrounds and organisations spanning multiple sectors. The rationale for its prominence is rooted in its inherent simplicity and efficacy. Phishing assaults necessitate minimal technical proficiency, yet they can generate substantial benefits for perpetrators by infiltrating personal or organisational data, resulting in financial ramifications, identity theft, data breaches, and compromised security.

In the contemporary era of extensive digital interconnectedness, phishing assaults manifest in diverse manifestations, leveraging distinct vulnerabilities to acquire confidential data illicitly. The attacks above encompass a spectrum of methodologies, varying from rudimentary and broadly employed methods to more intricate and focused strategies. The prevalence of many types of phishing attacks highlights the importance of thoroughly comprehending the range of threats and implementing efficient strategies to mitigate them.

During this training programme, participants will acquire vital knowledge, methods, and procedures to protect themselves and their organisations from hostile attacks. Upon completing this training module, participants will get an enhanced understanding of the diverse manifestations of phishing, the methodologies adopted by individuals engaging in cybercrime, and the indicators that should prompt vigilance. With this knowledge, individuals can safeguard their data, financial resources, and organisational reputation.

### Types of Phishing Attacks

- **Email phishing:** In email phishing assaults, fraudsters send misleading emails pretending to represent reliable businesses, institutions, or people. These emails frequently contain time-sensitive or attractive messages that manipulate recipients to engage in specific actions, such as clicking on potentially harmful hyperlinks, downloading files, or disclosing confidential information. Perpetrators depend on psychological stimuli to induce a perception of immediacy, intrigue, or apprehension, increasing the likelihood of recipients reacting without thoroughly examining the integrity of the message.
- **Spear Phishing:** Spear phishing represents a sort of assault characterised by its personalised and targeted nature. Adversaries acquire data from many channels, encompassing social media profiles and publically accessible information, to construct relevant emails to the intended receiver. Attackers employ a strategy wherein they use specific details, such as the recipient's name, role, or recent activities, to establish credibility and trust. This tactic is employed to enhance the probability of achieving their objectives. The successful execution of this form of attack necessitates meticulous reconnaissance and adept utilisation of social engineering techniques to accomplish its objectives.

- **Vishing (Voice Phishing):** In vishing attacks, fraudsters often employ voice communication over phone calls to trick people into disclosing critical information. Attackers use impersonating trustworthy entities or authorities to deceive victims by inducing a heightened sense of urgency or anxiety. The effective utilisation of social engineering strategies, in conjunction with the auditory modality, can increase individuals' vulnerability to disclosing personal information, passwords, or financial data.
- **Smishing, also known as SMS phishing,** is a cyber-attack method that employs text messages (SMS) to distribute harmful content, mirroring the tactics used in email phishing. Perpetrators use deceptive text messages that may encompass a distressing range, enticements to engage with hyperlinks or solicitations for sensitive personal data. Text messages' perceived legitimacy and immediacy may lead users to exercise less caution, rendering them vulnerable to such attacks.
- **Whaling:** High-profile people, such as CEOs, executives, or public personalities, are the target of whaling attacks. Adversaries exploit these persons' social standing and authority to persuade them into divulging confidential information or engaging in activities that undermine security measures. The implications of extracting data from such attacks can have significant and wide-ranging ramifications, considering the prominence of the individuals implicated.
- **Clone Phishing:** Clone phishing attacks exploit previously received authentic emails, enabling attackers to deceive unsuspecting individuals. Adversaries generate replicas of these electronic communications, modifying the hyperlinks or attachments to direct receivers towards malevolent websites or files contaminated with malware. Familiar email content and the sender's identity can reduce recipients' defences, increasing the likelihood of their engagement with the harmful components.
- **Pharming:** Pharming attacks involve the manipulation of the domain name system (DNS) to divert people from authentic websites to malicious ones covertly. The victims believe they are accessing genuine websites when redirected to counterfeit versions created to obtain their personal information illicitly. The attack above focuses explicitly on the foundational architecture of the internet and possesses the potential to impact individuals who exercise caution in their online activities.
- Each type of phishing attack capitalises on distinct communication routes and leverages various human vulnerabilities. By gaining a comprehensive awareness of the procedures and traits associated with misleading tactics, individuals and organisations can enhance their ability to safeguard themselves effectively. Throughout this session, we will explore several tactics to identify and protect against these attacks, improving our resilience against phishing threats.

### **The Significance of Phishing Awareness and Incident Response**

In the contemporary globalised society, characterised by extensive technological integration into our everyday routines, the menace of phishing assumes heightened significance. Phishing assaults present substantial threats to individuals, businesses, and society at large rather than being a mere inconvenience.

Phishing can be described as a sophisticated form of deceit, characterised by the deliberate and strategic manipulation of persons to elicit the disclosure of sensitive information, engagement with malicious hyperlinks, or downloading of damaging attachments.



The utilisation of deceptive strategies can result in data breaches, financial deficits, and significant harm to the reputation of individuals or organisations.

The issue of personal security encompasses a wide range of persons who may fall victim to phishing attacks, including individuals who are unaware of the risks and individuals in positions of great authority inside organisations. By increasing our level of consciousness, we can effectively protect our data, financial resources, and digital identities.

The repercussions of a successful phishing assault can have severe implications for businesses. The potential consequences include data security compromise, financial detriment, and legal obligations. Hence, individuals possessing expertise play a crucial role as the primary safeguard for an organisation.

Implementing a robust incident response strategy in the context of cyber resilience can play a crucial role in mitigating the adverse consequences of a phishing assault, hence minimising the extent of harm caused and facilitating the identification of perpetrators involved in cybercriminal activities. The enhancement of our collective preparedness serves to bolster our overall cyber resilience.

The main goal of a programme is to provide the participants with the necessary information and abilities to identify different types of phishing and successfully respond to phishing events. Upon completing this program, the participants will possess enhanced capabilities to safeguard themselves and the organisation against phishing risks.

## Activity 1: Phishing Detective Challenge

(Duration: 40 minutes)

### Recognising Phishing Attempts

- **1. Originating Address:**

It is imperative to scrutinise the sender's email address carefully. Perpetrators frequently employ addresses that strongly resemble authentic ones, albeit with minor deviations. The modifications might range from minor discrepancies, such as the absence of a character, adding an extra character, or a variation in the domain. It is advisable to consistently verify the sender addresses, mainly when the content of an email appears dubious.

- **2. The Significance of Uniform Resource Locators (URLs) and Domain Names in Web Addressing**

It is advisable to position the mouse cursor over hyperlinks embedded within email messages to preview the underlying URL before initiating a click action. It is advisable to use caution when encountering hyperlinks that exhibit a URL distinct from the one explicitly mentioned in the accompanying text. Assailants might employ misleading anchor text to conceal the actual destination URL. It is essential to be vigilant for any misspellings, discrepancies in domain names (such as using .com instead of .org), or the existence of extra subdomains.

- **3. Instances of Grammatical Errors:**

Phishing emails frequently exhibit spelling errors, grammatical inaccuracies, or inelegant language usage. These flaws may indicate that the message needs to be comprehensively scrutinised and could be a phishing endeavour. Legitimate organisations commonly thoroughly evaluate their communications to ensure adherence to standards of professionalism and accuracy.

- **4. Immediate Inquiries:**

It is advisable to exercise caution when seeing emails that induce a sense of urgency or coerce individuals into promptly undertaking specific actions. Phishers employ temporally constrained language to influence recipients into making impulsive decisions. The individuals in question may assert that the account is at risk of suspension or that the individuals will encounter repercussions if prompt action is not taken. It is imperative to independently verify such assertions before responding.

- **5. Inquiries for Confidential Data:**

It is uncommon for reputable institutions to solicit sensitive data such as passwords, credit card details, or Social Security numbers through electronic mail or text-based communication. If one is presented with an unforeseen solicitation for such information, particularly from an unfamiliar entity, it is advisable to approach it with a sense of scepticism. Instead of providing an immediate response, it is recommended to establish contact with the organisation using proper means to authenticate the legality of the request.

- **6. Unusual Links or Attachments:**

It is advisable to avoid accessing attachments or clicking on hyperlinks originating from unfamiliar or unconfirmed sources. Perpetrators can incorporate malevolent software, commonly called malware, within attachments or employ hyperlinks to redirect them to websites threatening their digital security. It is advisable to take care, even in cases when the email looks to originate from a trusted source. It is imperative to authenticate the sender's identity before engaging with any documents or hyperlinks. By cultivating a sense of vigilance towards these prevalent attributes, individuals can acquire the capacity to differentiate genuine forms of communication from phishing endeavours. By regularly practising these skills, individuals and organisations can enhance their ability to safeguard themselves against these deceitful strategies. In the subsequent round of our programme, we will explore optimal strategies for mitigating phishing attempts and upholding digital security.

## **Outline of Activity 1**

The activity aims to increase participants' awareness of phishing attempts by including them in a practical exercise to analyse and recognise phishing indicators in real-world circumstances.

### **Materials Needed**

- Samples of phishing emails (digital slides or hard copy printouts).
- Use a flipchart or whiteboard and markers.
- The stopwatch or timer.



## **Guidelines for Activity**

### **Introduction (5 minutes)**

- Start by outlining the goal of the exercise, which is to improve participants' ability to spot phishing attempts.
- Stress the value of meticulousness and critical thinking when evaluating emails and internet content.

### **Possible Situation (10 minutes)**

- Present several phishing emails on a screen or as printed handouts.
- Include a brief explanation of each email's context, including the sender's name, the subject line, and related materials.

### **Personal Evaluation (10 minutes)**

If appropriate, hand out printed copies of sample phishing emails to attendees or display them on a screen.

Request that each person examine the emails on their own and point out any questionable content, such as:

- unusual email addresses from senders.
- unexpected inquiries about login credentials or personal information.
- language that is urgent or menacing.
- hyperlinks or URLs that seem suspect.

### **Discussion in Group (10 minutes)**

- Bring everyone together for a discussion in groups.
- Invite people to discuss their insights and discoveries.
- Encourage a conversation on typical signs of phishing attempts using the examples that have been examined.
- Inquire the participants what they would do if they received emails like these.

### **Conclusion (5 minutes)**

- Write a brief synopsis of the main ideas discussed.
- Emphasise the importance of recognising phishing efforts in personal and business settings.
- Stress that the abilities they will be honing through this exercise will help them be generally safer online.


## **Activity Content**

### **Introduction (5 minutes):**

#### **The objective of the Exercise:**

The main objective of the activity is to enhance the participants' proficiency in accurately recognising and detecting phishing endeavours. Phishing is a continuous threat in the contemporary digital environment, and the ability to discern and identify these deceptive practices is a crucial competency.

The importance of meticulousness and critical thinking cannot be overstated.



**The exercise will require utilising two essential abilities:** meticulousness and critical thinking. When examining practical instances of phishing emails and situations, it is crucial to emphasise the significance of carefulness. The process involves carefully examining each component, every term, and every connection with a critical perspective.

One may question the significance of this practice. Phishing attacks are progressively evolving in complexity and prevalence. Regardless of one's location, possessing the ability to recognise a phishing endeavour can serve as a safeguard for safeguarding personal information, financial resources, and digital identity.

The participants should prepare themselves to don their detective hats and practice these vital abilities. The trainer will provide participants with authentic instances of phishing emails in the real world. Participants can thoroughly examine these instances and identify the distinctive indicators of phishing endeavours.

It is important to remember that the knowledge acquired today can enhance one's ability to maintain online safety and protect personal and professional interests.

#### **Possible Situation (10 minutes)**

To explore tangible instances of phishing emails in real-world contexts. The cases below have been meticulously chosen to exemplify the wide range of strategic methods utilised by participants involved in cybercrime.

##### **Phishing Email 1 - "Urgent Account Verification"**

**Sender:** PayPal Customer Support support@paylpal.com (Note the misspelt domain.)

**Subject Line:** Urgent: Your Account Requires Immediate Verification

**Context:** The email claims to be from PayPal and requests immediate account verification by clicking a link. It threatens account suspension if not done within 24 hours.

##### **Phishing Email 2 - "Job Offer with a Catch"**

**Sender:** BestJobsNow Hiring Team jobs@bestjobsnow.com

**Subject Line:** Exclusive Job Offer - Apply Now!

**Context:** The email offers an enticing job opportunity but requires personal information and payment for a "background check" before proceeding.

##### **Phishing Email 3 - "Your Amazon Order Confirmation"**

**Sender:** Amazon Orders orders@amazOn.com (Note the zero instead of 'o' in "Amazon.")

**Subject Line:** Your Amazon Order Confirmation - Invoice Attached

**Context:** The email poses as an Amazon order confirmation but includes a suspicious attachment, supposedly an invoice, which may contain malware.

##### **Phishing Email 4 - "Social Media Account Compromise"**

**Sender:** Facebook Security security@facebooklogin.com (An imitation domain.)

**Subject Line:** Urgent: Your Facebook Account Security Alert



**Context:** The email alleges a security breach in your Facebook account and urges immediate login to secure your profile, leading to a fake login page.

**Phishing Email 5 - "Financial Statement Alert"**

**Sender:** YourBank Online info@yourbnkonline.net

**Subject Line:** Important: Your Financial Statement is Ready

**Context:** The email claims to be from your bank, notifying you of an available financial statement with a link that leads to a fraudulent website

These cases serve as illustrations of the extensive measures that cybercriminals are willing to take to mislead receivers. Frequently, those who engage in such activities imitate credible sources and utilise tactics of urgency or attractive incentives to influence others into undertaking actions that jeopardise their security.

As with the Phishing Detective Challenge, thoroughly examining these emails with great attention to detail is imperative. One should remain vigilant for the nuanced cues that may expose their propensity for deception. The next section of the exercise will develop the capacity to identify these indications. Maintaining a high level of attentiveness is necessary to unveil the concealed elements within phishing emails.

**Personal Evaluation (10 minutes)**

Thoroughly analyse these communications individually while maintaining a vigilant attitude towards identifying any elements that may raise doubts or concerns. Please search for the following:

**Unconventional Email Addresses:** Please verify the email address of the sender. Does the source exhibit the expected characteristics of legitimacy, or are there any anomalies or instances of misspelling?

**Queries Regarding Login Credentials or Personal Information:** It is advisable to diligently scrutinise any solicitations about providing login credentials, passwords, or personal information. Reputable organisations do not commonly use email to request this information.

**Importance of Language:** It is crucial to consider the linguistic choices employed in these electronic correspondences carefully. Do individuals use tactics that generate a perception of urgency or anxiety to persuade others to take action expeditiously?

**Suspect Links or URLs:** Look through any links or URLs that appear in the emails. Do these entities exhibit characteristics of authenticity, or do they show indications of suspicion or modification?

Participants are allotted 10 minutes to analyse these electronic mail correspondences individually. It is advisable to utilise this period judiciously and place confidence in one's intuitive faculties. If there appears to be any discrepancy or irregularity, it is advisable to note it.

### Discussion in Group (10 minutes)

**Group Formation:** The participants will be divided into smaller groups to engage in this conversation. Please locate a nearby group and assemble it nearby. In an online situation, utilising virtual breakout rooms is a viable option.

### Topics for Discussion

**Insights and discoveries:** Within the assigned groups, it is recommended that participants engage in a sequential exchange of ideas, focusing on the observations made during the analysis of the phishing emails. The trainer should ask questions such as “Did you see any sender email addresses that deviated from the norm, requests for personal information, employment of urgent language, or inclusion of suspicious hyperlinks that were particularly noteworthy to you?” The trainer should feel welcome to provide any further significant information.

**Common Indicators of Phishing Attacks:** Given the analysed instances, let participants discuss the customary indicators of phishing endeavours. What are the typical strategies employed by phishing emails to mislead recipients? The trainer should encourage participants to analyse any discernible patterns or indicators of concern that participants have observed.

**Actions Taken in Response:** Now, envision the scenario where participants have seen one of these fraudulent emails in their electronic mail inbox. What course of action would you undertake? The trainer should encourage participants to provide insights into the measures participants would take to protect their personal information and ensure their security.

**Group debate (7 Minutes):** The trainer should encourage participants to participate in a dynamic discussion within their respective groups, ensuring that participants incorporate the examples they have analysed.

**Group Discussion (3 Minutes):** The trainer reconvenes collectively and listens to each group's central insights and conclusions and kindly proposes a representative who would succinctly encapsulate the collective observations of the group about common indicators of phishing and the corresponding measures that the participants would undertake.

Provide each group with the chance to present their perspectives.

### Conclusion (5 Minutes)

As the trainer concludes Phishing Detective Challenge, it is imperative to briefly summarise the key concepts addressed and emphasise the importance of the knowledge acquired during this session.

### Summary of Key Concepts

In this activity, the participants actively analysed authentic phishing emails, enhancing their proficiency in detecting nuanced indications of phishing endeavours.

The discourse has encompassed conventional manifestations of phishing, including atypical email addresses, solicitations for personal data, employment of urgent or threatening rhetoric, and dubious URLs.

### Enhancing Online Safety

Furthermore, the skills that the participants are developing at present will contribute to enhancing y overall online safety. By further developing one's critical thinking abilities and improving attention to detail, individuals might enhance their ability to safeguard against many online hazards, extending beyond the scope of phishing attacks.

In the contemporary era characterised by the pervasive influence of technology, the cultivation of cybersecurity awareness emerges as a crucial asset. It is imperative to remember that the knowledge and skills acquired during today's activities hold significance beyond individual advancement, as they contribute to the overall welfare of one's community, workplace, and internet presence.

It is imperative to maintain a state of vigilance, remain well-informed, and consistently engage in the regular practice of these abilities.

## Activity 2: Phishing Incident Response Simulation (Duration: 40 minutes)

### Dealing with a Phishing Incident

- **Network Disconnection:** In the event of a suspected phishing attack, the initial course of action is to disconnect from the network. To impede the attacker from gaining additional access to the machine, it is advisable to disengage from Wi-Fi or sever the internet connection. This measure has the potential to mitigate the extent of harm and effectively cease any ongoing unauthorised actions.
- **Report:** It is essential to Promptly notify the IT department or security team of the occurrence. The timely reporting of the event allows for the implementation of appropriate actions to reduce the risk, ascertain the extent of the attack, and proactively safeguard other members of the organisation against similar incidents.
- **Altering Credentials:** Modify the passwords for accounts that may have been subject to unauthorised access. Commence the investigation by focusing on the history of the phishing effort and examining any affiliated statements. Ensuring the newly generated passwords possess robustness, distinctiveness, and resist easy guessing is imperative. Implementing multi-factor authentication (MFA) in all applicable instances is advisable to enhance security by incorporating an additional layer of protection.
- **Device Scan:** Conducting a comprehensive malware scan on devices that access the dubious email or hyperlink is essential. The presence of harmful attachments or hyperlinks may have facilitated the introduction of malware into your system. The process of scanning aids in the identification and subsequent elimination of possible risks, hence mitigating the risk of further compromise.
- **Disseminate Awareness:** It is essential to disseminate information regarding the incident among colleagues and employees to foster awareness and mitigate the risk of others being targets of comparable attacks. Education is a potent instrument in combating phishing attacks. By engaging in the act of sharing personal experiences, individuals contribute to the process of empowering others to identify and respond to instances of phishing successfully.

- **Extract Lessons from the Occurrence:** It is essential to conduct a thorough analysis of the occurrence to comprehend the factors that contributed to the successful attack and ascertain any existing vulnerabilities that were exploited. This observation can assist individuals and their organisations in enhancing security protocols to mitigate the occurrence of future incidents.
- **Enhance Security Measures:** Leveraging the incident as a strategic moment to bolster the organisation's security infrastructure is essential. Implementing supplementary security measures, revising existing policies, organising training sessions, and maintaining vigilance against emerging dangers are imperative to enhance security.
- **Engaging with Authorities:** In certain instances, particularly when a phishing incident results in monetary detriment or the exposure of confidential customer information, it may be imperative to enlist the assistance of legal authorities and regulatory bodies. Getting guidance from the legal team to ascertain the most suitable course of action to pursue is advisable.

It is important to note that timely and efficient responses to phishing incidents can reduce possible harm and thwart the attacker's objectives. By adhering to these procedures and engaging in cooperative efforts with the IT team and peers, the participants actively preserve a secure and robust digital ecosystem for themselves and the organisation.

### **Outline of Activity**

The exercise aims to replicate a real-world phishing attack and provide participants with experience with incident response protocols and making snap decisions. The aim is to enhance participants' ability to react appropriately during a phishing attempt.

### **Supplies Required:**

- Participants should have laptops or other devices with internet connection.
- An email that looks like a phishing scam (made with training software).
- The stopwatch or timer.
- Use a flipchart or whiteboard and markers.

### **Guidelines:**

#### **Introduction (5 minutes)**

- Introduce the exercise by outlining its go: practise incident response techniques and imitate a phishing incident.
- Stress how crucial it is to react quickly and precisely to lessen the effects of a phishing attack.

#### **Setup of the Scenario (10 minutes)**

- Distribute a mock phishing email to the recipients. This email ought to seem a lot like a legitimate phishing attempt.
- Give a succinct, persuasive description of the situation, including the sender's name, the subject line, and related content.

#### **Personal Response (10 minutes)**

- Give each participant a simulated phishing email to evaluate and choose the best action.
- Urge them to consider the precautions they would take to safeguard their accounts and information and confirm the email's authenticity.

### **Group discussion and decision-making (10 minutes)**

- Assemble individuals for a conversation in groups.
- Invite each person to present their unique answers and explain their choices.
- Assist the group in deciding what should be done in response to the phishing email that has been simulated.

### **Result of the simulation (5 minutes):**

- Outline the simulation's conclusion. Tell the group if they made the right choice or if any crucial steps were overlooked.
- Show the appropriate incident response steps on a whiteboard or flipchart, then contrast the participants' choices with them.

### **Debriefing (5 minutes)**

- Finish the exercise by holding a debriefing.
- Talk about the things learned from the simulation, the correct answers and the mistakes made.
- Stress the value of ongoing education and being ready for incidents.

## **Content of Activity**

### **Introduction**

The primary purpose of this simulation is two-fold: firstly, to provide participants with practical experience in effectively addressing a phishing issue, and secondly, to recreate a scenario where prompt action is crucial.

### **React Quickly and Precisely**

The importance of promptly and accurately responding to a phishing attack. In practical contexts, a prompt and precise reaction can effectively mitigate the consequences of such an assault. The distinction between a bit of inconvenience and a significant data breach or financial loss can be of utmost importance.

Phishing perpetrators frequently exploit a sense of urgency to deceive their targets into making impulsive decisions. Reaction strategies can enhance one's ability to remain composed, make well-informed decisions, and effectively safeguard oneself and one's organisation. Prepare participants to assess and apply their event response capabilities. The forthcoming scenario has been intentionally crafted to resemble an authentic phishing endeavour closely.

### **Setup of the Scenario (10 Minutes)**

To establish the context for Phishing Incident Response Simulation. Each participant will immediately get a simulated phishing email. The present electronic correspondence has been methodically composed to closely emulate a genuine phishing endeavour that one may experience in a real-life scenario. Each of the participants will receive a mock phishing email. The email has been meticulously crafted to closely resemble a legitimate phishing attempt that individuals might encounter in the real world.



## Scenario Details

**Sender's Name:** The sender of this mock phishing email is "Acme Bank Security Team," a name often used by cybercriminals to create a sense of trustworthiness.

**Subject Line:** The subject line reads, "Urgent: Security Breach - Immediate Action Required!" This is a classic tactic to induce a sense of urgency and panic.

**Content:** The email informs you of a security breach on your online banking account. It urges you to click a link within the email to "secure your account immediately" by providing your login credentials and personal information.

Kindly be advised that email is an integral component of the simulation, and there are no actual negative consequences associated with interacting with it. The objective is to respond in a manner that aligns with the principles and practises of incident response, drawing upon one's knowledge and expertise in the field. Give a brief moment to review email or electronic devices. It is advisable to locate the simulated phishing email in the mailbox. After obtaining the required information, it is advisable to exercise caution by abstaining from clicking on hyperlinks or divulging personal or sensitive data. In contrast, it is imperative to critically assess the content of the email and deliberate on an appropriate course of action for an answer.

The participants are allotted a specific duration of 10 minutes to thoroughly analyse the contents of the email and thereafter determine the appropriate line of action.

### Individual Response (10 minutes)

Conduct an individual evaluation of the simulated phishing email and determine the most suitable action in response. Consider the procedural measures one would take to authenticate the credibility of an email and safeguard one's accounts and personal data.

During this period, it is advisable to take into consideration the following factors:

**Assessing the Authenticity of Emails:** Evaluating the Sender's Name, Email Address, and Overall Visual Presentation of the Email. Are there any indications of legitimacy or any characteristics that raise suspicion?

**Content Evaluation:** An analysis of the email's content, encompassing the linguistic elements employed and the level of urgency indicated. Are there any indicators that raise concerns about the possibility of a phishing attempt?

**Links & Actions:** Look at any links or actions requested by the email. Would you be inclined to click on them? What are the reasons for or against it?

**Verification procedures:** Consider the measures that can be undertaken to authenticate the email's legitimacy and safeguard one's data.

The participants are allotted a specific duration of 10 minutes to do this activity successfully.





## Group Discussion and Decision (10 Minutes)

### Topics for Discussion:

**Individual Responses:** The initial step is requesting each participant to disclose their responses to the simulated phishing email. The trainers kindly asked the participants to elucidate the rationale for their decisions or refrain from creating.

**Collective Decision-Making:** After the individual shares perspectives, the participants will partake in a group discussion to reach a consensus on the most suitable course of action in response to the simulated phishing email.

The trainer should remember that the objective is to make well-informed judgements that precede safeguarding one's personal information and accounts are imperative.

The trainer should go to the second point and collaboratively develop a consensus on the action to pursue. The trainers encourage the participants to expand upon one another's perspectives as the participants collectively analyse the optimal course of action.

The active participation of all individuals in this debate is of utmost importance, as it reflects the collaborative effort necessary in real-world incident response situations.

The trainer should proceed with the collective decision-making process and expeditiously disclose the outcome of this simulated phishing incident.

### Simulation Outcome (5 Minutes)

#### The appropriate steps for incident response are as follows:

**Avoid Clicking on Links:** The first and most important thing to do is stop clicking on links or downloading any attachments from emails that seem dubious. By abstaining from such actions, the likelihood of exposing personal information to potential security vulnerabilities is reduced.

**Authenticating the Sender:** Ensuring the sender's credibility is of utmost importance. In the present scenario, it can be observed that the sender's name, namely "Acme Bank Security Team," was a counterfeit representation, a fact that the individuals accurately discerned.

**Trust Instincts:** It's critical to follow gut and recognise warning signs, such as the urgency of the email and its request for personal information. In the conducted simulation, the collective intuition exhibited by the participants proved to be advantageous.

**Contacting a Legitimate Source:** If an individual receives an email of a dubious nature from an organisation with which they have a relationship, it is advisable to establish contact with that organisation via their official website or telephone number to authenticate the email's legitimacy. To exhibit a commendable degree of attentiveness and prudence, which are crucial in ensuring personal data protection and overall security by following these prescribed incident response procedures.



The efficacy of the response to a simulated phishing attempt demonstrates individuals' proficiency in safeguarding themselves and their organisations against potential security risks.

It is important to remember that the abilities honed in this context can be applied to practical scenarios in the real world. It is imperative to maintain a state of vigilance, consistently engage in practice, and keep a sense of confidence in one's capacity to address phishing occurrences adequately.

### **Closing (15 minute)**

#### **Lessons Acquired**

The significance of refraining from clicking on dubious links or downloading attachments from unfamiliar sources has been emphasised.

Verifying the sender's legitimacy is an essential and critical component in the incident response process. In the conducted simulation, it was accurately determined that the sender had an intention to deceive.

Developing the ability to rely on one's intuition and being vigilant in detecting warning signs, such as a sense of urgency and solicitation of personal information, are essential in discerning phishing endeavours.

Verifying the legitimacy of suspicious emails can be achieved by establishing contact with the appropriate authoritative entity through formal communication channels.

The performance during the simulation was commendable, as participants made appropriate judgements to safeguard their personal information and ensure security.

### **Continuous Training and Preparedness**

The trainer must emphasise the significance of ongoing training and incident readiness. The landscape of cyber threats is constantly changing, necessitating a continuous state of preparedness. The following are a few significant points to consider:

It is imperative to remain well-informed by staying current on the most recent phishing strategies and adhering to cybersecurity best practices. The acquisition of knowledge serves as a formidable means of protection.

**Frequent Practise:** Incident reaction improves with practice, much like any other talent. Engage in periodic participation in simulated exercises, such as the one at hand, to maintain cognitive acuity.

**Disseminate Knowledge:** Disseminate the information acquired today to coworkers, acquaintances, and family members. A community with a high level of knowledge and awareness is better equipped to withstand and respond to cyber threats.

**Report unusual activity:** Notify the employer, IT department, or the relevant authorities if individuals encounter unique emails or believe they are the victim of a phishing effort.

## Activity 3: Creating Personalized Phishing Prevention Plans (Duration: 45 minutes)

### Best Practices for Prevention:

**1.Authentication of Sender:** It is imperative to consistently verify the sender's legitimacy before engaging with emails or accessing embedded links. It is advisable to exercise caution while examining the sender's email address. In cases of uncertainty, it is recommended to establish contact with the sender via a separate and reliable communication channel to verify the message's authenticity.

**2.MFA (Multi-Factor Authentication):** A Multi-Factor Authentication (MFA) system enhances the security of user accounts by necessitating an additional verification process in addition to the conventional password-based authentication. Various methods can be employed for user authentication, such as a text message, an authentication application, or a fingerprint scan. Implementing Multi-Factor Authentication (MFA) on user accounts substantially enhances unauthorised individuals' difficulty obtaining access.

**3.Recurrent Password Changes:** Regularly updating passwords mitigates the potential threat of unauthorised account entry. It is advisable to refrain from employing the same passwords for many accounts, as doing so might significantly amplify the consequences of a security breach. Using robust and distinctive passwords that incorporate a combination of uppercase and lowercase letters, numerical digits, and special characters is recommended.

**4.Protect Personal Data:** Exercising prudence when divulging personal or sensitive information online, particularly on social media sites, is advisable. Cybercriminals frequently exploit these platforms to extract information that can be utilised to construct more persuasive phishing assaults. It is advisable to use caution and restrict the extent of personal information disclosed in public domains.

**5.Education-Related Projects:** It is vital to enhance one's knowledge, as well as that of coworkers, about the potential hazards linked to phishing. Promoting a culture of heightened consciousness inside the organisation is essential by implementing regular training sessions, workshops, or educational initiatives. It is imperative to provide comprehensive training to staff to enhance their ability to identify indicators of phishing attempts and educate them on the appropriate protocols for reporting such incidents.

**6.Be Careful What Click On:** It is imperative to exercise caution and assess the authenticity of any hyperlink contained inside an email or text message before clicking on it. To accurately evaluate whether the intended destination aligns with the expected outcome, it is advisable to hover over the hyperlink and observe the displayed URL. In cases of uncertainty, it is advisable to access the website directly by manually entering the official URL instead of relying on hyperlink navigation.

**7.Safe Connection:** When transmitting confidential data over the internet, it is imperative to guarantee that the individuals are connected to a secure network. To ensure the security of a website, it is recommended to verify the presence of "https://" in the URL and a padlock icon in the address bar. This observation suggests that the established connection undergoes encryption, enhancing the security level for transmitting data.

**8.Continue to update software:** It is advisable to consistently maintain the currency of operating systems, apps, and antivirus software. Frequent software updates typically incorporate security patches to mitigate potential vulnerabilities that malicious actors could exploit.

**9. Employ email filters:** It uses spam and filtering mechanisms to detect and redirect potentially harmful emails to the designated spam directory. Although it is important to note that these filters may not be completely effective in detecting all phishing attempts, they offer additional protection.

**10. Keep Current:** To stay up-to-date, it is essential to remain informed on current phishing trends, strategies, and risks. Knowledge of developing strategies enables individuals to adjust their defensive measures and maintain a competitive advantage over hackers.

By taking these precautionary measures, individuals can effectively decrease their susceptibility to phishing assaults. Acquire the necessary information and tools to safeguard online presence, individually and within the organisation. In the subsequent part, we will examine the sequential actions to be undertaken in the occurrence of a phishing incident to guarantee adequate preparedness to respond efficiently and mitigate potential harm.

### Activity Outline

The exercise aims to give participants the tools to create customised phishing prevention strategies that meet their unique requirements, improving their capacity to defend their companies and themselves against phishing scams.

### Materials Needed

- Handouts or digital templates for participants to use when creating their plans.
- Whiteboard or flipchart with markers.
- Timer or stopwatch

### Instructions

- Start by outlining the goal of the exercise, which is to develop individualised approaches for preventing phishing scams.
- Stress that phishing is a persistent problem and that maintaining security requires a well-thought-out preventive strategy.

### Understanding Individual Needs (10 minutes)

- Start a conversation regarding each individual's obligations and roles in their personal and professional lives.
- Inspire people to consider their phishing dangers and vulnerabilities.

### Components of a Phishing Prevention Plan (10 minutes):

Talk about the essential elements of a successful phishing prevention strategy, such as:

- training and education.
- security software and email screening.
- robust password procedures.
- verification using multiple factors (MFA).
- protocols for reporting incidents.

### Individual Plan Development (15 minutes)

- Give attendees pamphlets or electronic templates to make phishing prevention plans unique.
- Request that participants complete the plan by adding specific tactics and activities they will use in light of their vulnerabilities and needs.

### **Group Sharing and Feedback (5 minutes)**

- Ask a select few to present their customised preventive strategies to the group. Encourage people to provide comments and ideas.

### **Review and Finalize (5 minutes)**

- Briefly describe the significance of having a customised plan to prevent phishing attacks.
- Participants should be urged to complete their plans and ensure they are workable and viable.

### **Closing Remarks (5 minutes)**

- Emphasise the significance of periodically evaluating and revising preventative plans to adjust them to new dangers.
- Express gratitude to participants for their enthusiastic involvement and dedication to enhancing their cybersecurity procedures.

## **Activity Content**

### **Introduction (5 Minutes)**

The goal is apparent: to provide each individual with a personalised defence plan against phishing attempts, one of the most persistent risks in the digital world.

### **The Goal of The Activity**

The exercise has a straightforward but essential goal: to develop individualised phishing protection strategies because phishing attempts are a constant threat rather than an isolated incident.

### **Phishing: An Ongoing Danger**

Attackers who use phishing constantly change and create new ways to trick and compromise people and businesses. The circumstances make keeping individuals' security up to date entirely dependent on having a well-thought-out preventive approach.

After completing the exercise, each participant will be equipped with a precise strategy to fend off any phishing efforts that may be made against them. The strategy will serve as a defence against shady communications and scams.

It is essential not to forget that security matters, whether preserving an individual's private data or protecting important information belonging to their company. Customising a plan to meet unique requirements can significantly increase resistance to phishing attacks.


### **Understanding Individual Needs (10 Minutes)**

#### **Personal and Professional Roles**

The trainer reminds the participants of their obligations and roles in their personal and professional spheres, such as a friend, family member, employee, or community member.

### **Discussion Points**

The trainer starts a conversation and invites the participant to weigh in on the following:



Personal Roles: In your own life, what roles do you play? Do you have siblings, parents, or friends? In these roles, how do you use digital technology?

Professional Positions: What function does your position have in your professional life? Do you deal with confidential data and correspond with clients and associates by email or online?

Contemplating Risks and Vulnerabilities: The trainer focuses on phishing-related dangers and vulnerabilities. Individuals are frequently the target of phishing attempts because of their roles and the information they handle. Below are many concepts that stimulate cognitive processes.

- **Which Kind of Data Do You Manage?** Consider the kinds of information you typically work with. Is it private financial information, private work-related information, or personal data?
- **Internet habits:** What are your usual email and internet service methods? Are there any particular internet habits that could increase your vulnerability to phishing scams?
- **Tools Employed:** Which gadgets do you utilise for work and personal use? Do they have enough security?

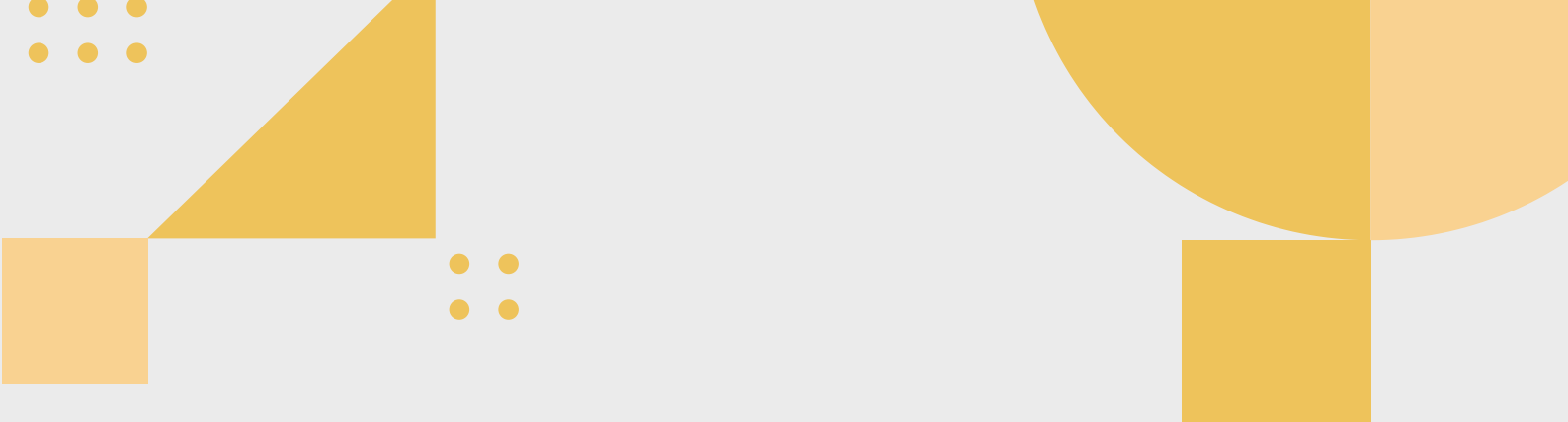
The trainer can identify unique vulnerabilities and hazards by thinking about these questions. The first step in customising phishing protection strategy to the individuals' particular requirements is developing this self-awareness.

The trainer invites the participants to consider these points for a moment. If the trainer likes doing so, share thoughts or observations about their roles and possible weak points. Their feedback will largely shape the trainer's unique preventive plan.

#### Components of a Phishing Prevention Plan (10 Minutes)

Investigating the essential elements of an all-encompassing phishing prevention strategy is appropriate. These elements serve as the cornerstones of defence against phishing scams. Each of the plans will be examined:

- **Training and Education:** Social engineering techniques are prevalent in phishing assaults as a means of tricking people. Education and training are essential to increase awareness and provide the knowledge necessary to identify phishing attempts.
- **Software for email filtering and security:** Security software and robust email filtering can provide an effective initial defence against phishing emails. These technologies aim to identify and hold suspicious emails before they get to the mailbox.
- **Robust Password Techniques:** One essential component of cybersecurity is passwords. Use complicated, one-of-a-kind passwords for every account. Using a reliable password manager is to help create and safely store these passwords.
- **MFA, or multi-factor authentication:** By requiring two different kinds of authentication, such as a password and a one-time code texted to a mobile device, MFA adds an extra layer of security. When it's feasible, turn on MFA to improve account security.
- **Procedures for Reporting Incidents:** Understanding when to report a suspected security issue or phishing effort is critical. Clearly define the processes for reporting incidents in both personal and work environments.



The above mentioned plan will strengthen defences against phishing attempts and should be included in a customised phishing prevention plan. Each of these components is essential for reducing the dangers of phishing and supporting the entire cybersecurity position.

### **Individual Plan Development (15 Minutes)**

#### **Assignment**

Review the handouts or digital templates that the participants have been provided with. The plan is intended to assist in creating a personalised strategy to thwart phishing attacks.

Complete Plan

#### **Here's how to move forward:**

- **Determine Requirements:** Based on the roles and responsibilities the individual previously addressed, determine their unique requirements and weaknesses.
- **Make definite goals:** What aims do individuals have for preventing phishing attacks? Are individuals trying to strengthen password security, raise awareness and educate others, or improve email security?
- **Actions and Strategies:** Individuals can find sections for each of the essential topics we covered, including MFA, email security, password practises, education and training, and incident reporting, in the given template. Considering their circumstances, list the tactics and activities individuals plan to use for each component.
- **Timeline and Accountability:** Consider establishing a deadline for each task and designating the person responsible for completing it.
- **Frequent Review:** Stress the significance of regularly updating and evaluating their plan to adjust to changing conditions and risks.
- **Share and Involve Others:** If appropriate, consider how individuals might include friends, family, and coworkers in their preventative initiatives. Promote a culture of cybersecurity consciousness within individuals' workplaces.

To develop strategies, the trainer reminds that individuals should be highly customised to their unique situations and priorities. Phishing prevention does not have a one-size-fits-all solution. Thus, their system should be flexible and change as the threat landscape does.

The trainer gives participants time to complete their phishing prevention strategy for the following fifteen minutes.

#### **Group Sharing and Feedback (5 Minutes)**

#### **Participants**

The trainer asks a few participants for a synopsis of their preventive strategies and summarises some of the most important tactics and actions, along with any special considerations arising from positions and duties. The trainer permits a couple of people to talk about their plans.

## Comments and ideas

Following the presentation of each participant's plan, the trainer invites all participants to provide comments and ideas. The cooperative idea-sharing process can improve preventative tactics and offer original solutions to phishing defence.

The trainer reminded that everyone may benefit from each other's experiences and insights and that no one correct method exists to develop a phishing prevention plan.

## Review and Finalize (5 Minutes)

### The Importance of a Personalized Plan

Developing a customised phishing prevention plan is a smart way to protect digital life and data. here are several reasons why this holds significant importance:

- Customised Defence: The strategy is made to fit unique roles, weak points, and internet usage patterns. It's made to deal with the particular difficulties encountered.
- Proactive Defence: Having a well-thought-out plan allows you to combat phishing attacks head-on. The individuals can take on the role of the first defence.
- Flexibility: The strategy should be dynamic. It changes in response to needs and the changing panorama of threats. It is essential to update and review it frequently to keep it functional.
- Self-assurance and empowerment: A plan helps feel confident to spot and stop phishing attacks.
- As the participants proceed, complete the following actions:

**Complete Planning:** Make sure plans are viable, actionable, and transparent. The goals should align with the described tactics and actions and be realistic.


**Schedule and Responsibility:** Decide who will be in charge of completing each task and establish reasonable deadlines. The secret to a successful deployment is accountability.

**Periodic Evaluation:** Agree to revisit and revise the plans frequently. Since the digital world is ever-changing, preventative strategies should also be flexible.

To explain, strengthen participants' cybersecurity defences by implementing concrete measures by incorporating these factors into the final planning process and dedication to phishing prevention. This will be a powerful disincentive to phishing attempts.

To conclude, customised preventive strategies are essential in the continuous fight against phishing attacks.





### **Closing Remarks (5 Minutes)**

#### **Adjusting to Changing Dangers**

The world of cybersecurity is always changing. Attackers that use phishing are constantly looking for new methods to trick and compromise. Nevertheless, substantial advancements have been achieved by implementing tailored strategies for mitigating phishing attacks. It is essential to have a dynamic defensive system; they are not static.

#### **Frequent Evaluation and Modification:**

The need to regularly evaluate and modify plans should not be underestimated. In response to evolving hazards, adapting and modifying the approaches employed is imperative. Engaging in this practice enables individuals to maintain an advantageous position over those who seek to exploit their vulnerabilities.

#### **Assured Cybersecurity Commitment:**

It is essential to remember that the actions undertaken directly influence one's digital existence in the future. By maintaining a high level of knowledge, exercising prudence, and actively seeking opportunities to familiarise oneself with the firm and its operations, individuals can effectively position themselves as formidable targets, posing a challenge to potential threats seeking to compromise their security.

### **Closing (Duration: 20 minutes)**

The Closing Reflection Circle aims to wrap up this cybersecurity training session. This exercise seeks to distill the essence of our talks and exercises, giving each person a chance to consider applying newly acquired knowledge and consider their own personal takeaways. Each participant is asked to share their learnings and "aha" moments from the session as the group forms a circle. Think about the most important lessons you've learned and how you can use them in both personal and professional settings. Think on the wider implications for improving cybersecurity in addition to the particular content. The following questions can help participants with their reflection: What caught your attention the most? How do you see applying incident response and phishing awareness knowledge to your day-to-day tasks or place of employment? Do you have any obstacles in mind, and if so, how do you intend to overcome them? Consider how cooperation can improve cybersecurity in your situation and whether the group exercises helped you grasp the material better. Participants are also invited to share one particular action or habit they plan to take in order to support a safer online environment. This group dedication strengthens the training's practical application and promotes a feeling of shared accountability. The Closing Reflection Circle fosters peer-to-peer learning and shared insights in addition to facilitating personal reflection. Let's acknowledge the accomplishments as the session comes to an end and accept our shared responsibilities for advancing cybersecurity. Your comments will reinforce the training's effects while also igniting a culture of ongoing development and alertness to online dangers. I appreciate your active participation and eagerly await your thoughts.





## MODULE 3: HOW TO ENJOY THE BENEFITS OF DIGITAL TECHNOLOGY WHILST AVOIDING THE HAZARDS

### Learning Outcomes- Key Competences

The learning outcomes of this module are both personal and practical. These outcomes reflect the knowledge, skills, and positive changes that individuals can gain by adopting responsible and mindful digital technology use. Here are some key competences as well as learning outcomes:

#### Digital Literacy:

Digital literacy encompasses an augmented capacity to critically evaluate online content, discern misinformation, and assess the reliability of digital sources. Moreover, it involves an improved understanding of navigating the digital landscape safely and effectively.

#### Digital Safety and Security:

Digital safety and security proficiency involve acquiring knowledge of best practices for safeguarding personal information and privacy online. This includes skills such as implementing strong passwords, enabling two-factor authentication, and adeptly recognizing and avoiding various cyber threats.

#### Time Management and Productivity:

In the realm of time management and productivity, individuals can enhance their proficiency by gaining increased awareness of effective screen time management and reducing digital distractions. This improvement extends to honing time management skills, resulting in heightened productivity and sustained focus.

#### Mental and Emotional Well-Being:

In the sphere of mental and emotional well-being, individuals can foster enhanced emotional intelligence and awareness of the impact of digital technology on mental health. This involves the development of effective strategies for managing stress, anxiety, and other negative emotions associated with digital use.

#### Balanced Digital Habits:

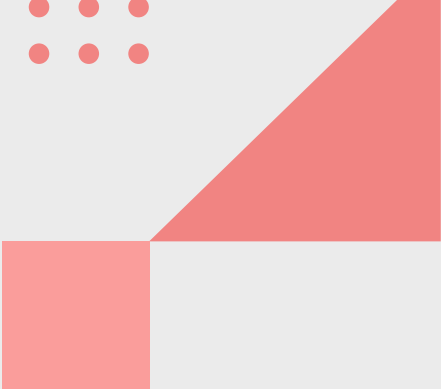
Achieving balanced digital habits involves developing the ability to set and maintain healthy boundaries with digital devices and technology. This includes acquiring knowledge on incorporating digital detox breaks and sustaining a harmonious balance between online and offline life.

#### Privacy and Data Control:

Proficiency in privacy and data control encompasses the skill of adjusting privacy settings on diverse online platforms and managing the sharing of personal data. This also involves heightened awareness of the potential consequences of oversharing and implementing measures to protect one's privacy effectively.

#### Media Literacy:

Media literacy involves an improved understanding of how media and advertising can influence online behavior and choices.



It also encompasses the ability to make informed and mindful decisions when encountering digital marketing and advertising, fostering a more discerning and critical approach to online content.

**Empathy and Digital Communication:**

Individuals develop empathetic and respectful communication skills for online interactions. This proficiency extends to the ability to recognize and mitigate the negative impact of online harassment and cyberbullying, fostering a more compassionate and considerate digital environment.

**Healthy Work-Life Balance:**

Attaining a healthy work-life balance involves establishing clear boundaries between work and personal life to prevent burnout and support overall well-being. This includes developing skills for effective remote work and maintaining a balance between professional and personal responsibilities, contributing to a more sustainable and fulfilling lifestyle.

**Teaching and Mentoring:**

Knowledge and skills to educate and mentor others in adopting responsible and mindful digital technology use, especially for parents, children, and community members.

**Community and Social Impact:**

Individuals gain the ability to promote digital wellness within their communities, encouraging the adoption of healthy digital habits. This contribution extends to fostering a safer and more responsible digital environment for all, emphasizing the collective responsibility for a positive online community.

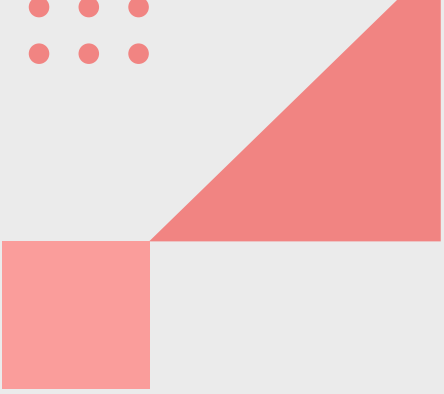
These learning outcomes contribute to personal growth, a healthier relationship with technology, and a positive impact on one's well-being and the well-being of the broader community. They empower individuals to harness the benefits of digital technology while minimizing its hazards and challenges.

**Materials / resources required**

- Laptops with internet access
- Digital tools and software (canva etc)
- Training Materials (pens, pencils, markers, etc.)
- A timer or a smartphone with a timer app, a notebook or digital note-taking app.
- Room for a big group, chairs (depending on the number of participants)

**Methodology**

Youth work involves engaging with young people to support their personal, social, and educational development. Non-formal education methodologies are flexible and practical approaches to teaching and learning that take place outside of traditional classroom settings. They can be highly effective in addressing digital technology use and safety within youth work.



When it comes to helping young people enjoy the benefits of digital technology while avoiding the hazards, it's essential to use effective methods that are engaging and educational. Here are the non-formal education methodologies that will be used to help young people for integrating digital wellness and responsible technology use into youth work:

**Digital Literacy Workshops, Media Literacy Programs, Group :**

- Organizing workshops and training sessions to enhance digital literacy. Training young people how to critically assess online information, recognize fake news, and use technology responsibly.
- Developing programs that focus on media literacy. Discussing how digital media can shape perceptions and behavior, and empower youth to make informed decisions about the media they consume.

**Interactive Discussions:**

- Facilitating open and nonjudgmental discussions about the challenges and benefits of digital technology. Encouraging young people to share their experiences and concerns related to online interactions.

**Peer-to-Peer Education:**

- Promoting peer-to-peer education where older, more digitally literate youth mentor and guide their peers in responsible technology use.

**Digital Detox Challenges and Monitoring:**

- Creating digital detox challenges as a group activity. Encourage young people to unplug from screens for a set period and discuss their experiences afterward.
- Offer guidance and support for youth in setting and managing screen time limits and ensuring they have a healthy balance between online and offline activities.

**Online Safety Workshops:**

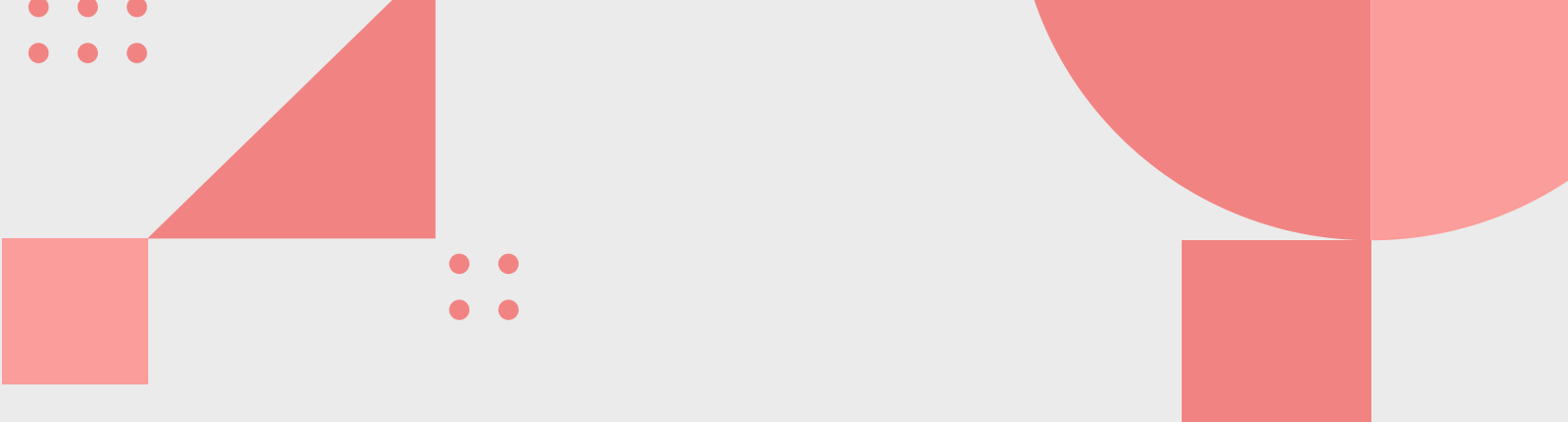
- Organize workshops on online safety, including topics like protecting personal information, recognizing and responding to cyberbullying, and staying safe while gaming.

**Role-Playing and Scenarios:**

- Using role-playing and real-life scenarios to help youth practice responsible digital decision-making. Exploring situations involving online conflicts, privacy, and peer pressure.
- Community Engagement:
- Encouraging young people to use digital technology for community engagement and social causes. Showcase how technology can be a tool for positive change.

**Regular Check-Ins:**

- Establish a culture of regular check-ins and open communication about digital technology. Encourage young people to share their concerns, questions, and successes.
- Digital Citizenship Curriculum:
- Implement a structured digital citizenship curriculum that covers various aspects of responsible technology use.



These non-formal education methodologies will be adapted to the specific needs and interests of the young people, especially young women we are working with. The goal is to empower them with the knowledge and skills to make informed, responsible, and mindful choices in their digital lives while enjoying the benefits of digital technology while minimizing hazards.

### **Introduction (Duration 20 minutes)**

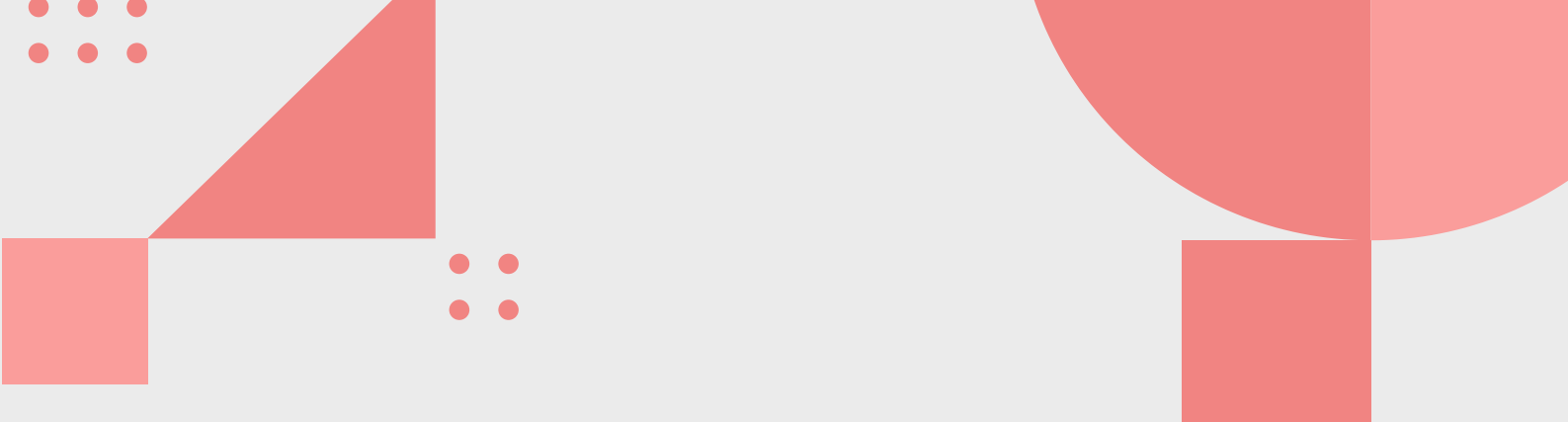
In this activity, participants are asked to consider significant turning points in their digital life, such as their first encounters with digital devices or memorable internet encounters. The highs and lows of their technological experiences are then visually represented on paper in the form of a timeline. After this time for reflection, participants gather in groups to share their digital timelines and discuss the similarities and differences between their experiences. An in-depth understanding of the ways that technology has influenced different journeys is provided by this interactive sharing session. This icebreaker concludes with a chance for each participant to consider how their relationship with technology has changed over time. Through the process of identifying particular obstacles, advantages, and areas they would like to delve deeper into, attendees establish the framework for our upcoming conversations about digital wellbeing. Our team's examination of digital wellbeing is based on these reflections. We will use these insights to develop a deeper understanding of our digital experiences and open the door to a healthier and more purposeful digital lifestyle as we move through the next activities.

### **Activity 1: Digital Wellness Check (Duration 30 minutes)**

This activity is designed to encourage individuals to take periodic breaks from digital devices and assess the impact on their well-being. The objective is to instill mindfulness about screen time and experience the positive effects of intentional breaks. Instructions for the game are straightforward: start by setting a 30-minute timer for the "digital detox" period. Participants are then challenged to completely disconnect from all digital devices, putting aside smartphones, tablets, and computers. During this time, engage in offline activities that promote well-being, such as reading a book, going for a walk, meditating, practicing a hobby, or having face-to-face conversations. To enhance the experience, participants are encouraged to take notes on their thoughts and feelings during the detox, reflecting on changes in mood, focus, or stress levels. After the detox period, spend a few minutes reflecting on the experience, identifying enjoyable aspects and any challenges or feelings of FOMO (Fear of Missing Out). Based on reflections, participants can set goals for incorporating regular digital detox breaks into their routine, specifying frequency and duration. The game concludes with a debriefing session, providing a structured opportunity to identify successes and areas for improvement. This process fosters better decision-making, skill development, and performance, making the "Digital Detox Challenge" a fun and interactive way to integrate digital wellness practices into daily life.

### **Activity 2: The Digital Guardians (Duration 45 minutes)**

This interactive and educational activity is designed to engage young people in fostering digital awareness, responsible technology use, and online safety. As participants embark on this quest, they take on the role of digital superheroes tasked with safeguarding their online world. The importance of responsible digital technology use and online safety is briefly highlighted, introducing "The Digital Guardians" as a group of young digital superheroes dedicated to protecting their digital realms. Participants are divided into small teams or pairs, each adopting the persona of a Digital Guardian.



Assigned specific challenges related to online safety or digital wellness, such as creating strong passwords or dealing with cyberbullying, teams research and discuss their topics using the internet as a resource. Creativity is encouraged in crafting engaging presentations or posters, allowing the use of visuals, artwork, or multimedia elements. During the presentations, each team has 5/7 minutes to share their findings and tips in a youth-friendly and engaging manner. The audience is encouraged to ask questions or provide feedback, fostering an interactive learning environment. The activity concludes with the "Digital Guardians Pledge," where all participants commit to being responsible digital citizens and sharing their newfound knowledge with peers. As a wrap-up, additional resources and tools for staying safe online are shared, expressing gratitude to the participants for becoming Digital Guardians. This activity not only educates them about responsible technology use but also empowers them to advocate for digital wellness and online safety within their peer groups. It serves as an engaging and interactive platform for young people to develop crucial digital citizenship skills.


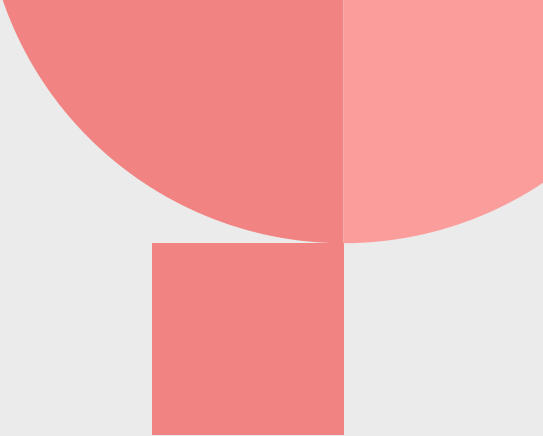
### **Activity 3: Balancing Act: Creating a Digital Wellness Plan** **(Duration 40 minutes)**

This activity is designed to help participants set clear goals and guidelines for balanced technology use, avoiding potential hazards. The objectives include improving overall well-being, enhancing productivity, protecting online security and privacy, fostering healthier online relationships, and encouraging a more balanced work-life integration. During this activity, trainers will guide participants through creating personalized digital wellness plans. Emphasizing that the plan is about finding the right balance rather than complete avoidance of technology, individuals will engage in self-assessment to evaluate current digital habits. Clear goals will be set using the SMART criteria, followed by the creation of digital guidelines aligned with those goals. Participants will incorporate digital detox plans, utilize technology tools, and practice mindful technology use. Regular evaluation and adjustments, seeking support, ongoing education, and practicing self-care are integral aspects of maintaining an effective digital wellness plan. The activity culminates in a presentation and discussion phase where individuals or small groups share their strategic plans, promoting further analysis and dialogue. Participants are reminded that their digital wellness plan should be tailored to individual needs, promoting a healthy balance that enhances life while minimizing negative impacts. Regular reviews and adjustments ensure the plan remains effective and aligned with well-being goals, providing a roadmap for intentional and conscious technology use.

### **Closing**

Closing remarks for a youth activity on digital wellbeing should inspire and motivate the participants while summarizing the key takeaways from the event.

- **Express Gratitude and Acknowledge Participants (Opening):** Start by thanking the participants for their active involvement in the activity. Acknowledge their time, enthusiasm, and contributions.
- **Reflect on the Activity (Summary):** Summarize the key points, activities, and discussions that took place during the event. Highlight the main topics or takeaways related to digital wellbeing.
- **Empower and Inspire (Motivation):** Empower the participants by emphasizing that they have the knowledge and tools to be responsible digital citizens. Encourage them to use their newfound insights to make a positive impact.

- 
- 
- **Share a Personal Anecdote or Inspiration (Optional):** Consider sharing a personal story, quote, or anecdote that illustrates the importance of digital wellbeing or responsible technology use. This can add a personal touch and connect with the audience.
  - **Reinforce Key Messages (Main Points):** Reiterate the central messages of the activity, such as the importance of online safety, privacy, digital literacy, and mindful technology use. Emphasize the significance of responsible digital citizenship.
  - **Empathy and Support (Community Building):** Encourage the participants to support one another and be empathetic towards friends and peers who may be struggling with digital challenges. Highlight the sense of community that has been created during the activity.
  - **Call to Action (What's Next):** Inspire the participants to take their learning and enthusiasm beyond the activity. Encourage them to share what they've learned with others, advocate for digital wellbeing, and be role models in their communities.
  - **Offer Resources (Additional Support):** Provide information about where participants can find further resources, tools, or organizations dedicated to digital wellbeing and online safety. Offer reading materials, apps, or websites that can help them on their digital wellness journey.
  - **Closing Remarks and Thank You (Closure):** Conclude your remarks by thanking the participants once again for their active participation and interest. Express your hope that they will continue to champion digital wellbeing.
  - **Closing Statement (Ending):** Remember to keep your closing remarks positive, engaging, and motivational.



# MODULE 4: GAMING AND SOCIAL MEDIA ADDICTION

## Learning Outcomes- Key Competences

In this resource, participants will gain a comprehensive understanding of the impact of gaming and social media addiction on young women's lives, learn strategies to maintain a healthy digital balance, and explore the educational potential of gamification for fostering entrepreneurial skills. In this module, participants will gain the following key competencies:

### Understanding Gaming and Social Media Addiction

Participants will explore the prevalence of gaming and social media addiction among young women, delving into its impact on mental health, productivity, and social interactions. Case studies and real-life scenarios will provide insights into the consequences of excessive digital engagement.

### Digital Balance and Time Management

Participants will learn techniques to manage screen time effectively and strike a balance between digital activities and other aspects of life. Setting personal boundaries and prioritizing offline activities will be emphasized to foster a healthy digital lifestyle.

### Responsible Digital Citizenship

This section focuses on responsible social media usage, online etiquette, and data privacy. Participants will understand how their digital reputation influences employability and entrepreneurial ventures. Also, they will be able to address cyberbullying and discuss prevention and coping strategies.

### Gamification for Digital Entrepreneurship

Exploring gamification principles, we'll discover how gaming experiences can enhance digital education and training. Participants will identify potential gaming opportunities that align with promoting entrepreneurial skills and mindset.

### Collaborative Gaming and Skill-building

Emphasizing teamwork and cooperation, this section will focus on developing problem-solving, communication, and critical thinking skills through collaborative gaming experiences. Discussion will be made on how these skills translate into entrepreneurial success.







### Digital Well-being and Self-Care

Participants will learn strategies to manage stress and prioritize mental well-being in a digitally-driven world. Mindfulness practices will be introduced to counteract the negative impact of excessive digital engagement. They will also emphasize the importance of self-care routines in nurturing an entrepreneurial mindset.

#### Materials / resources required

- Computers or Laptops with internet access
- Handouts and worksheets
- Internet Access
- Stationery (pens, pencils, markers, etc.)

#### Methodology

The methodology used for the Gaming and Social Media Addiction curriculum module will be interactive and participant-centered, emphasizing experiential learning and group engagement. The facilitators will use a combination of presentation slides to introduce key concepts, case studies, and real-life scenarios to highlight the impact of gaming and social media addiction on young women's lives.

Participants will actively participate in discussions, brainstorming sessions, and group activities to foster critical thinking and problem-solving skills. Worksheets and hands-on exercises will be provided to encourage self-reflection and the development of strategies for managing digital engagement responsibly.

Throughout the module, the facilitators will create a supportive and inclusive learning environment, encouraging open dialogue and the sharing of experiences. The ultimate goal is to empower participants with the knowledge and skills to navigate the digital landscape responsibly, enhance their employability prospects, and embrace the potential of gamification for promoting digital entrepreneurship.

### Introduction

#### (Duration: 15 minutes)

In the introduction, participants will be welcomed to the Gaming and Social Media Addiction module. The facilitator will provide an overview of the objectives, emphasizing the importance of understanding the impact of gaming and social media addiction on young women's lives. They will briefly outline the activities to be covered and set the tone for an interactive and participant-centered learning experience.





## Activity 1: Identifying Addiction Warning Signs

### (Duration: 45 minutes)

During this activity, participants will engage in group discussions and interactive exercises to identify the warning signs of gaming and social media addiction. The facilitator will present common behavioral patterns associated with addiction and provide real-life examples. Participants will work collaboratively to recognize these signs, exploring the potential consequences on mental health, productivity, and social interactions. Through this activity, participants will gain a deeper understanding of the challenges posed by addiction in a digital world.

## Activity 2: Digital Detox Challenge

### (Duration: 60 minutes)

The Digital Detox Challenge will encourage participants to take a break from digital devices and explore alternative activities. Divided into teams, participants will brainstorm and compile lists of engaging offline activities that promote social interactions, creativity, and personal well-being. Each team will then present their ideas, fostering a positive group dynamic and inspiring others to incorporate more non-digital activities into their daily lives. Through this challenge, participants will grasp the significance of finding a balance between online and offline experiences.

## Activity 3: Creating a Healthy Digital Balance Plan

### (Duration: 50 minutes)

In this activity, participants will work individually to develop their own Healthy Digital Balance Plan. They will reflect on their current digital habits, assessing the time spent on gaming and social media platforms. Guided by provided templates, each participant will set personalized goals for managing their digital engagement responsibly. The facilitator will support the participants in identifying strategies to achieve their goals, such as implementing screen time limits, setting specific digital-free hours, or participating in digital detox days. This activity empowers participants to take control of their digital behaviors and improve their overall well-being.

## Closing

### (Duration: 15 minutes)

During the closing session, participants will reflect on their learning journey throughout the module. The facilitator will encourage open sharing of insights, key takeaways, and action plans. Participants will have the opportunity to express how the module has influenced their perceptions of gaming, social media, and digital entrepreneurship. The facilitator will provide positive reinforcement, highlighting the importance of responsible digital engagement and the potential impact it can have on their future entrepreneurial endeavors. The closing will foster a sense of accomplishment and empowerment as participants leave the module equipped with valuable knowledge and strategies to navigate the digital world responsibly.



## REFERENCES:

1. Assenge, E. et al. (2018): "Entrepreneurial Mindset and Performance of Small and Medium Scale Enterprises in Macurdi Metropolis, Benue State – Nigeria", International Journal of Innovation. Available online at: <https://www.redalyc.org/journal/4991/499168322004/499168322004.pdf>.
2. Bekh, O. (2014): "Training and support for women's entrepreneurship" ETF working paper, p. 12-13. Available online at: [https://www.etf.europa.eu/sites/default/files/m/A6FAE24FIDE8FA27C12580DC005F733D\\_Women%20entrepreneurship.pdf](https://www.etf.europa.eu/sites/default/files/m/A6FAE24FIDE8FA27C12580DC005F733D_Women%20entrepreneurship.pdf).
3. EIT Digital (2022): "The Future of Education for Digital Skills". Available online at: [https://www.eitdigital.eu/fileadmin/2022/ecosystem/makers-shapers/reports/EIT-Digital\\_Report\\_The-Future-of-Education-for-Digital-Skills.pdf](https://www.eitdigital.eu/fileadmin/2022/ecosystem/makers-shapers/reports/EIT-Digital_Report_The-Future-of-Education-for-Digital-Skills.pdf).
4. ETF (2021): "Skills support for Women's Entrepreneurship to achieve more inclusive and prosperous societies". Available online at: <https://www.etf.europa.eu/en/news-and-events/news/skills-support-womens-entrepreneurship-achieve-more-inclusive-and-prosperous>.
5. European Commission (2018): "Council Recommendation on Key Competences for Lifelong Learning". Available at: <https://education.ec.europa.eu/focus-topics/improving-quality/key-competences>.
6. European Commission (2018): "Developing digital youth work: Policy recommendation, training needs and good practice examples". Available online at: <https://op.europa.eu/en/publication-detail/-/publication/fbc18822-07cb-11e8-b8f5-01aa75ed71a1>.
7. European Commission (2019): "Woman in Digital". Available online at: <https://digital-strategy.ec.europa.eu/en/library/women-digital#Why>.
8. European Commission (n.d): "Education and training glossary". Available at: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Category:Education\\_and\\_training\\_glossary](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Category:Education_and_training_glossary).
9. European Commission (n.d.): "What is Digital Education Action Plan?". Available online at: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>.
10. European Institute for Gender Equality (2020): "Gender Equality Index 2020: Digitalisation and the future of work". Available online at: <https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2020-report/digital-skills-and-training>.
11. Fejjao, C., Flanagan, I., Van Stolk, C. and Gunashekar, S. (2021): "The Global Digital Gap: Current Trends and Future Direction", RAND Europe. Available online at: [https://www.rand.org/pubs/research\\_reports/RRA1533-1.html](https://www.rand.org/pubs/research_reports/RRA1533-1.html).
12. Huawei and All Digital (2022): "Strategies to Address the Digital Skill Gap in the EU". Available online at: <https://www.europeandigitalskills.eu/sites/TDSG/uploads/files/white-paper-eu-digital-skills-gap.pdf>.
13. Institute for Academic Development (2018): "What is digital education?". Available online at: <https://www.ed.ac.uk/institute-academic-development/learning-teaching/staff/digital-ed/what-is-digital-education>.
14. International Telecommunication Union (2010): "World Telecommunication/ICT Development Report 2010: Monitoring the WSIS Targets". Available at: <https://www.itu.int/pub/D-IND-WTDR-2010>.
15. Levorato, S. (2021): "The gender gap in digital skills and jobs persists, but change is possible", European DIGITAL SME Alliance. Available online at: <https://www.digitalsme.eu/gender-gap-digital-skills/>.

## REFERENCES:

116. MasterClass (2021): "Business 101: How to Develop an Entrepreneurial Mindset". Available online at: <https://www.masterclass.com/articles/how-to-develop-an-entrepreneurial-mindset>.
17. Șerban, A. et.al (n.d): "Social Inclusion, Digitalisation and Young People", Council of Europe and European Commission. Available online at: <https://pjp-eu.coe.int/documents/42128013/47261953/053120+Study+on+SID+Web.pdf/0057379c-2180-dd3e-7537-71c468f3cf9d>.
18. UK, The Royal Society (2012): "Shut down or restart? The way forward for computing in UK schools". Available at: <https://royalsociety.org/~media/education/computing-in-schools/2012-01-12-computing-in-schools.pdf>.
19. UN (2018): "Building digital competencies to benefit from existing and emerging technologies, with a special focus on gender and youth dimensions", Report of the Secretary General". Available online at: [https://unctad.org/system/files/official-document/ecn162018d3\\_en.pdf](https://unctad.org/system/files/official-document/ecn162018d3_en.pdf).
20. UN (2018): "Building digital competencies to benefit from existing and emerging technologies, with a special focus on gender and youth dimensions", Report of the Secretary General". Available at: [https://unctad.org/system/files/official-document/ecn162018d3\\_en.pdf](https://unctad.org/system/files/official-document/ecn162018d3_en.pdf).
21. UNESCO Institute for Statistics (2018): "A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2". Available online at: <https://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf>.
22. UNICEF East Asia & Pacific (2021): "What we know about the gender digital divide for girls: A literature review". Available online at: <https://www.unicef.org/eap/media/8311/file/What%20we%20know%20about%20the%20gender%20digital%20divide%20for%20girls:%20A%20literature%20review.pdf>.

## WEBSITES

- <https://unevoc.unesco.org/home/TVETipedia+Glossary/show=term/term=Digital+literacy>
- <https://www.simplilearn.com/what-is-digital-security-article#:~:text=Digital%20security%20involves%20protecting%20your,stored%20within%20from%20unauthorized%20access>.
- <https://programs.online.utica.edu/resources/article/ten-ways-to-protect-your-identity>
- <https://terranovasecurity.com/top-examples-of-phishing-emails/>
- <https://www.eschoolnews.com/featured/2018/02/26/teach-media-literacy/>
- <https://www.unicef.org/tajikistan/cyberbullying-what-it-and-how-stop-it>
- <https://phishing.iu.edu/stories/index.html>
- <https://www.phishing.org/phishing-examples>
- <https://www.memphis.edu/its/security/phishing-examples.php>
- <https://www.lepide.com/blog/12-steps-to-take-to-recover-from-a-phishing-attack/>
- <https://terranovasecurity.com/top-examples-of-phishing-emails/>
- <https://expertinsights.com/insights/the-top-10-phishing-simulation-and-testing-solutions/>
- <https://www.forbes.com/advisor/business/best-phishing-simulators/>



# OMEGA

## YOUNG FEMALE ENTREPRENEURS STEPPING INTO THE DIGITAL AGE

PROJECT NUMBER: 2021-2-EL02-KA220-YOU-000051105

### PROJECT RESULT 2 ONLINE SEMINAR (E-COURSE) CURRICULUM

## "DIGITAL WELL- BEING"

[WWW.OMEGA-PROJECT.EU](http://WWW.OMEGA-PROJECT.EU)



Co-funded by  
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Youth and Lifelong Learning Foundation (INEDIVIM). Neither the European Union nor the granting authority can be held responsible for them.