Digital Hygiene: Handbook for VETs

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Project No: 2022-1-LV01-KA220-VET-000086725 | Project title: Good Digital Hygiene for Startups

Table of Contents

Module 1 - Digital Hygiene for VET Professionals 5

Unit 1 - The Significance of Digital Hygiene in VET Education 5

Digital Hygiene and Cybersecurity 5

Digital Hygiene in VET Organizations 5

Unit 2- Skills and Requirements for VET Trainers & Educators 8

Roles and Responsibilities for VET Organizations 8

Digital Skill Frameworks 10

Skills for VET Trainers and Educators 12

Unit 3 - Adapting Digital Hygiene into VET Curriculum and Training 15

Unit 4 – Good Practice Example – Digital Hygiene for VETs 18

Description of the situation 18

The solution 18

Sources 22

Module 2 - Digital Hygiene Customized Curriculum for VETs 23

Introduction 23

Unit 1 – Curriculum Overview 23

Program Aim & Objectives of the Module 24

Teaching Methodology 24

Assessment and Continuous Improvement 24

Conclusion 24

Unit 2 – Key Learning Areas 26

Overview of the Curriculum 26

Introduction to Digital Hygiene 26

Network & Cybersecurity 28

Data and File Management 29

Software Management 30

Data Backup and Recovery 32

Cryptography, Authentication, and Password Management 33
Mobile Device Management and Security 34
Unit 3 – Digital Hygiene Assessment and Feedback Mechanisms for VETs 36
Introduction 36
Assessment Strategies 36
Feedback Mechanisms 37
Implementing Feedback into Curriculum Development 37
Conclusion 38
Unit 4 – Good Practice from VETs 39
Introduction 39
Case Study 1: CyberVET Academy 39
Case Study 2: TechBridge VET 39
Case Study 3: SecurePath Institute 40
Implications for Best Practices 41
Case Study 4: DigitalDefenders College 41
Case Study 5: InnovateTech Institute 42
Summary of Good Practices 42
Conclusion 43
Key Takeaways and Best Practices 43
Sources: 45
Module 3: Implementing & Sustaining 48
Unit 1 - Building a Digital Hygiene Culture in Startups and VET Institutions 48
What is Digital Hygiene Culture? 48
Development of Digital Hygiene Culture in the Leadership Level 48
Development of Digital Hygiene Culture in Group Level 49
Development of Digital Hygiene Culture at the Individual Level 50
Unit 2 - Monitoring, Review, and Continuous Improvement of Digital Hygiene Practices 53

Institutional Level Practices 53
Individual Level Practices 55
Unit 3 - The Future of Digital Hygiene: Challenges and Opportunities 57
A-Emerging Technologies 57
B-Regulatory Challenges 58
C-Opportunities for Innovation 59
Unit 4 - Digital Hygiene Culture Good Practice Use Case: 61
Digital Hygiene Use Cases Around the World 61
Sources 64

Module 1 - Digital Hygiene for VET Professionals

Unit 1 - The Significance of Digital Hygiene in VET Education

Digital Hygiene and Cybersecurity

Digital hygiene refers to the practices and habits individuals employ to maintain their online privacy, security, and overall well-being. It encompasses a broad range of proactive behaviors and measures aimed at protecting personal information, preventing online threats, and minimizing risks associated with digital activities. Examples of digital hygiene practices include using strong passwords, enabling two-factor authentication, updating software regularly, being cautious about sharing personal information online and managing one's digital footprint. Digital hygiene is a concept that is closely associated with another concept, namely cybersecurity. Often digital hygiene is considered a proactive element of cybersecurity that is a responsibility of an individual.

Cybersecurity is a specialized field dedicated to protecting computer systems, networks, and data from unauthorized access, cyberattacks, and other security breaches. It involves the implementation of technical measures, security protocols, and defensive strategies to safeguard digital assets and mitigate potential risks posed by various cyber threats. People responsible for cybersecurity often work to identify vulnerabilities in systems, develop security solutions, monitor suspicious activities, and respond to security incidents to ensure the integrity, confidentiality, and availability of information and resources. As a consequence, cybersecurity activities are often performed by professionals as opposed to digital hygiene which may be the responsibility of everyone.

Digital Hygiene in VET Organizations

Various organizations tend to expect their employees to follow some general rules to make sure that the rules and best practices of digital hygiene are abided. Vocational education and training (VET) organizations have some general guidelines that are valid for all the organizations that work with people and their personal information and with proprietary services and products that are developed, stored, and shared via a digital environment. However, they have some specific challenges related to the type of service they are providing as well as the unique nature of their target customers. Educators often find themselves in a situation where

they need to provide additional guidance to their customers. This may mean that they have to be agents of digital hygiene while performing the training, e.g., providing the intended service.

There are several reasons why digital hygiene is considered very important specifically for VET organizations:

- **Protection of sensitive information**

When performing their work VET organizations often handle a wealth of sensitive information, including student records, academic data, and financial details. Some of this information may be crucial for the organization when performing learning analytics or evaluating the services provided to the customers. Practicing good digital hygiene helps safeguard this information from unauthorized access, data breaches, and cyber threats, ensuring the confidentiality and integrity of sensitive data.

- **Preservation of institutional reputation**

When handling the data that is entrusted to a VET organization without the appropriate level of care, the organization may inadvertently change how its customers and partners view it. A data breach or security incident can have significant reputational damage to a VET organization. By prioritizing digital hygiene practices, institutions demonstrate their commitment to security, trustworthiness, and professionalism, thereby enhancing their reputation among stakeholders, including students, parents, employers, and regulatory bodies.

- **Compliance with regulations**

Depending on their nature of work and how they connect to their customers, VET organizations are subject to various regulations and compliance requirements related to data protection, privacy, and cybersecurity. Adhering to digital hygiene best practices helps ensure compliance with relevant laws and regulations, mitigating the risk of regulatory fines, penalties, and legal liabilities associated with non-compliance.

- **Support for learning and teaching**

Digital technologies play a crucial role in modern education, facilitating online learning, collaborative projects, and digital assessments. These technologies are used to develop, manage, and share training materials, organize training environments, manage the involvement of participants in them, or analyze data gathered during the training process. By maintaining a secure and reliable digital infrastructure, VET organizations can provide a seamless learning experience for students and educators, fostering innovation, creativity, and engagement in teaching and learning activities.

- **Mitigation of cybersecurity risks**

The education sector may be targeted by cybercriminals seeking to exploit vulnerabilities in digital systems and networks or the lack of knowledge and skills of students and trainers who are not used to being involved in training in a digital environment. Implementing digital hygiene measures helps mitigate cybersecurity risks,

including malware infections, phishing attacks, ransomware threats, and unauthorized access to educational resources, thereby safeguarding the continuity of educational services and operations.

- **Promotion of responsible digital citizenship**

For some of the participants of the process it may be the first opportunity to be involved in the manner of training that is conducted in a digital environment or uses a digital environment to create, manage, and share training materials, conducts knowledge sharing, and communication with other participants via digital means, or uses digital tools to perform administrative tasks during the training. VET organizations have a responsibility to educate their students and staff that are involved in the training about safe and responsible digital practices. By integrating digital hygiene education into VET curriculum and training programs, institutions empower learners with the knowledge, skills, and attitudes needed to navigate the digital landscape effectively, protect their online identities, and contribute positively to digital society.

- **Preparation for future careers**

In today's digital age, digital literacy and cybersecurity awareness are essential skills for individuals entering the workforce. While learning some of the skills related to digital hygiene may not be the main goal of a student, participation in training can provide them with opportunities for improvement of those skills which might prove useful in the future. The trainers and organizers of training should also be aware that there might be a need to allocate time and resources for this specific purpose. By promoting digital hygiene practices, VET organizations equip students with the foundational knowledge and skills required to navigate digital challenges in their future careers, whether in traditional or digital industries. The same also applies to the trainers who by participating in the training using digital environments and tools safely and responsibly keep their teaching practice modern and may encounter new opportunities for their career.

In general, digital hygiene is important for VET organizations at the company level as well as an individual employee and their customer level to protect sensitive information, preserve institutional reputation, comply with regulations, support learning and teaching, mitigate cybersecurity risks, promote responsible digital citizenship, and prepare students and to some extent also their trainers and other employees for success in a digital world. By prioritizing digital hygiene, VET organizations can create a safe, secure, and conducive learning environment that empowers learners to thrive in the digital age.

Unit 2- Skills and Requirements for VET Trainers & Educators

Roles and Responsibilities for VET Organizations

First, let us start with who may be the roles involved in VET training that should be aware of digital hygiene issues and should possess respective skills. Depending on the situations when conducting and participating in the training that is performed in digital environments and using digital tools VET trainers and educators may face different divisions of individual tasks that are performed by participants of the process. Therefore, implementing and managing digital hygiene in a vocational education and training (VET) organization may require coordination and collaboration among various stakeholders with different roles and responsibilities. Trainers may have the luxury of being supported by a fully grown IT staff to care for technical aspects of the training or they may have to rely on their skill and knowledge. For that reason, skills and requirements for the VET trainers and educators may vary depending on the organization they are part of.

There are several typical roles and responsibilities for individuals who may be involved in the process or training in today's digital environment each with their own assignments and skill requirements:

- **Chief Information Officer (CIO) or Chief Technology Officer (CTO)**

The CIO or CTO is mainly concerned about developing and overseeing the organization's digital hygiene strategy, policies, and procedures. They participate in setting the goals for the organizations with digital hygiene and cybersecurity kept in mind. Their responsibilities include ensuring alignment of digital hygiene efforts with the organization's overall IT and security objectives, allocating resources and budget for digital hygiene initiatives and cybersecurity measures, and providing leadership and guidance to IT and security teams responsible for implementing digital hygiene practices.

- **IT Security Manager or Cybersecurity Officer**

Some organizations may have a dedicated position of IT Security manager or a cybersecurity officer or someone fulfilling the role as part of their job description. Such a role would design and implement cybersecurity controls, safeguards, and risk management measures to protect VET systems, networks, and data. They would also conduct regular security assessments, audits, and vulnerability scans to identify and mitigate potential threats and vulnerabilities, monitor security incidents, respond to cybersecurity incidents, and coordinate incident response activities. On occasion, this role develops and delivers cybersecurity training and awareness programs for staff which makes them assume the role of a VET trainer. Sometimes they may also be invited to train students to promote good digital hygiene practices outside of their organization as experts.

- **IT Administrator or Systems Administrator**

IT administrators are responsible for managing IT infrastructure for the organization and may complete some assignments for the VET trainers, sometimes in the background, without being noticed. Their responsibilities include maintaining and administering VET systems, servers, and network infrastructure following digital hygiene standards and best practices; managing user accounts, access controls, and permissions to ensure secure access to VET resources and data; installing, configuring, and updating security software, patches, and firmware to protect against known vulnerabilities and exploits that may be encountered when using digital tools and performing actions during the training such as sharing training materials or communicating between the participants. They are also responsible for monitoring system logs and alerts for suspicious activities, unauthorized access attempts, or security breaches.

- **Data Protection Officer (DPO) or Privacy Officer**

Data protection officers play an important role in VET since there are rules and regulations at the national and international levels that require careful attention to how VET organizations manage the sensitive data of the participants of the training. This role ensures compliance with data protection regulations and privacy laws governing the collection, use, and storage of personal data in VET environments; develops and maintains data protection policies, procedures, and documentation, including data protection impact assessments (DPIAs) and privacy notices; handles data subject access requests, privacy complaints, and inquiries related to data protection and privacy practices, collaborates with IT and legal teams to address data security incidents, breaches, and privacy breaches.

- **Educational Technologist or Instructional Designer**

While previous roles may be encountered in any organization, the education technologist or instructional designer is directly related to training and education performed by the organization. Their responsibilities include integrating digital hygiene principles and practices into the VET curriculum, instructional materials, and learning activities; providing training and support to educators and instructional staff on incorporating digital hygiene education into teaching practices, evaluating, and recommending educational technology tools and resources that prioritize security, privacy, and accessibility for VET learners.

- **End Users (Staff and Students)**

The last role is often divided into two groups but they both have similar responsibilities with regards to digital hygiene. End users are expected to follow digital hygiene policies, guidelines, and best practices when using VET systems, devices, and online resources. The organization's training staff may be required by the company to perform training or administrative activities in a specific way set by the organization's rules and policy. As such they may be required to participate in cybersecurity awareness training and education initiatives to enhance their understanding of digital risks and responsibilities and report security incidents, suspicious activities, and cybersecurity concerns to appropriate IT or security personnel for investigation and resolution.

However, VET trainers should be aware of their role as counselors to the students who may need guidance when using a digital environment that may not be familiar to them during the training.

An individual in a VET organization may fulfill several roles at once during the training or they may be able to concentrate only on a few responsibilities. Regardless, by defining clear roles and responsibilities for individuals involved in implementing and managing digital hygiene in a VET organization, institutions can effectively collaborate to establish a culture of cybersecurity awareness, promote good digital hygiene practices, and protect the confidentiality, integrity, and availability of VET resources and data. However, organizations will require those individuals to possess certain skills and knowledge to perform the abovementioned practices.

Digital Skill Frameworks

There are existing competence frameworks established to describe the set of skills that should be possessed by those involved in performing various activities in a digital environment. Some of them include general digital skills while some may be more specific for the issues of cybersecurity and digital hygiene. The following frameworks are helpful when identifying digital hygiene skills for VET trainers and educators as well as identifying the possible training needs for the students participating in education in the digital environment.

- **Digital Competence Framework for Citizens (DigComp) [1]**

The DigComp 2.2 framework, developed by the European Commission, is the newest version of the Digital Competence Framework for Citizens. It defines the key components of digital competence in five areas: Information and data literacy, Communication and collaboration, Digital content creation, Safety, and Problem-solving. Each area is further divided into specific competencies that describe the skills and knowledge needed to be proficient in digital environments.

This framework serves as a guide for individuals to assess and improve their digital skills and for educators and policymakers to design curricula and policies that support digital education and training. DigComp 2.2 also introduces proficiency levels and examples of use, making it practical for various educational and professional settings. The framework emphasizes the importance of being able to operate effectively and critically in a digital society.

- **European e-Competence Framework (E-CF) [2]**

The European e-Competence Framework (e-CF) is a standardized framework to describe the competencies, skills, and proficiency levels of Information and Communication Technology (ICT) professionals developed to support the growth and mobility of ICT professionals. The framework consists of five competence areas related to ICT, such as Plan, Build, Run, Enable, and Manage. It contains 41 competencies in total and includes

proficiency levels that describe the knowledge, skills, and autonomy at each level, ranging from Foundation to Expert. It also includes samples of knowledge and skills related to the competencies.

The e-CF is aimed at helping organizations, HR managers, trainers, and educators to develop job roles and career paths for ICT professionals, enhance workforce management, and foster professional development in the ICT sector. It also serves as a tool for policy development, education, and training alignment within Europe's digital market.

- **European Cybersecurity Skills Framework (ECSF) [3]**

The European Cybersecurity Skills Framework (ECSF) is designed to harmonize and standardize cybersecurity skills, roles, and competencies across Europe. It serves as a foundational structure for developing and assessing cybersecurity skills, aimed at addressing the cybersecurity skill gaps and improving the cybersecurity posture of organizations and nations. The ECSF categorizes cybersecurity skills into several areas, detailing specific roles and competencies required in the field of cybersecurity. It outlines core cybersecurity roles that are typically needed by organizations, specific skills, and abilities required to perform effectively in these roles, and proficiency levels or levels of expertise, from beginner to expert, required for each competency.

This framework is useful for various stakeholders, including educational institutions, companies, and policymakers, to develop curricula, training programs, and career pathways in cybersecurity. It supports the creation of clear career structures in cybersecurity, making it easier to identify skill shortages and address them effectively.

- **Digital Competence Framework for Educators (DigCompEdu) [4]**

The DigCompEdu framework describes the requirements for the digital competence development of educators. It is specifically tailored for teachers at all levels of education, from early childhood to higher and adult education and it focuses on enhancing the digital skills necessary for effective teaching in increasingly digital learning environments. The framework is structured around six competence areas of professional engagement (Using digital technologies for communication, collaboration, and professional development.), digital resources (Creating and modifying digital resources and managing them effectively.), teaching and learning (Deploying digital technologies for preparing, implementing, and managing the teaching and learning process.), assessment (Leveraging digital technologies for assessment of, for, and as learning.), empowering learners (Using digital tools to enhance inclusion, personalization, and learners' active engagement.), facilitating learners' digital competence (Strategically promoting learners' digital skills and safe and responsible use of digital tools.). Additionally, the DigCompEdu framework identifies 22 individual

competencies and proficiency levels that range from "Newcomer" to "Pioneer," providing a path for educators' development in their digital practices.

This framework serves as a guide for educators to assess and improve their digital competencies and supports educational institutions in designing training programs and policies aligned with contemporary educational needs.

The frameworks mentioned above while general towards identifying the requirements of individuals and organizations participating in any practice in the digital environment provide a structured view of the scope of skills required from VET trainers and educators.

Skills for VET Trainers and Educators

To some extent, VET trainers and educators are no different from other participants in the digital environment. For that reason, the skills they require to adhere to good digital hygiene practice are skills that should be possessed by anyone. These skills encompass a range of technical, behavioral, and cognitive abilities. They also are a subset of skills that can be referred to as modern or future skills and based on the recent development of the digital environment these are the same skills that have been emphasized as skills that are crucial for organizations or the near future, like using cloud technologies, analyzing big data and using artificial intelligence tools to improve work productivity and efficiency [5,6].

However, the nature of their work requires VET trainers and educators to pay closer attention to how they handle data and interact with other participants in the training process. Here are some important skills needed for VET trainers and educators concerning good digital hygiene:

- **General cybersecurity awareness**

The skill includes understanding common online threats such as malware, phishing, and social engineering attacks, and knowing how to recognize and respond to them; knowing how to browse the internet safely, including avoiding suspicious websites, using secure connections (HTTPS), and being cautious when downloading files or clicking on links.

- **Data protection and privacy**

The skill includes being able to encrypt sensitive data, both in transit and at rest, and knowing how to securely delete or dispose of data when necessary; and understanding how to configure privacy settings on various online platforms and devices to control the sharing of personal information.

- **Device security and management**

This skill includes the practice of regularly updating software, operating systems, and applications to patch security vulnerabilities and protect against known exploits; the ability to create strong, unique passwords for

different accounts and use password management tools effectively to store and manage passwords securely; the practice of enabling and managing multi-factor authentication where available to add an extra layer of security to online accounts.

- **Safe digital communication**

This skill includes practicing secure communication practices such as using encrypted email services or selecting and using secure messaging apps when sharing confidential information or communicating with students, peers, colleagues, or partners outside of the VET organization; adhering to guidelines for identifying and avoiding phishing emails, scams, and other social engineering tactics that could compromise VET systems or lead to data breaches.

- **Digital footprint management**

This skill includes understanding the implications of one's digital footprint and taking steps to minimize exposure of personal information online; advising participants of the training to do the same.

- **Critical thinking**

This skill includes developing and applying critical thinking skills to evaluate the credibility of online sources, identify misinformation and scams, and make informed decisions about online activities when conducting or preparing for the training.

- **Continuous learning**

This skill includes participating in the general practice of improving one’s skill; learning new tools and approaches for training in a digital environment or using modern digital tools; and staying informed about evolving cybersecurity threats, privacy issues, and best practices through ongoing education and training.

- **Digital citizenship and ethics**

This skill includes practicing responsible digital citizenship when performing VET training by abiding by regulations and being respectful of the rights of other individuals and organizations; promoting responsible digital citizenship among students by teaching ethical behavior, respectful communication, and digital etiquette in online environments; fostering analytical thinking skills to help students evaluate the credibility of online information, recognize digital risks, and make informed decisions about their online activities; protecting the digital reputation of individuals and organizations participating in the process.

These skills may be referenced to the DigCompEdu framework described previously but they may not match individual competencies included in those frameworks directly. Rather there are elements in the competence area descriptions in the framework that correspond to the skills beneficial to VET trainers and educators.

Table 1. Link of suggested VET trainer skills to the DigCompEdu competence areas.

VET Trainer Skill	DigCompEDU Competence Area
General cybersecurity awareness	• Empowering Learners • Facilitating Learners' Digital Competence
Data protection and privacy	• Digital Resources • Facilitating Learners' Digital Competence
Device security and management	• Teaching and Learning • Facilitating Learners' Digital Competence
Safe digital communication	• Professional Engagement • Assessment
Digital footprint management	• Digital Resources • Facilitating Learners' Digital Competence
Critical thinking	• Teaching and Learning • Facilitating Learners' Digital Competence
Continuous learning	• Professional Engagement • Facilitating Learners' Digital Competence
Digital citizenship and ethics	• Empowering Learners • Facilitating Learners' Digital Competence

The skills provide the VET trainers and educators with the means to participate in educational activities while abiding by the best practices in digital hygiene. A down-to-earth reference of some of the best practices is available as a Digital Hygiene Cheat Sheet [7]. It describes 12 principles of secure digital life that all require some knowledge of the digital world, which include:

- keeping your working software, antivirus, firewall, etc. up to date,
- using safe passwords, managing them safely and using multi-factor authentication,
- being careful when downloading software,
- being aware of phishing and other suspicious attempts to compromise your assets,
- limiting your digital and social footprint,
- adopting a general "security first" mindset when dealing with information in the digital environment.

In VET training and education acquiring and practicing digital hygiene skills is important to provide a safe environment for information exchange.

Unit 3 - Adapting Digital Hygiene into VET Curriculum and Training

Digital Hygiene topics should be an everyday part of VET training. VET trainers and educators should follow the guidelines of sound digital hygiene when they are planning for and managing the training that implements the use of digital tools as part of providing the training environment; producing and distributing training materials; organizing peer-to-peer and trainer-to-student communications; analyzing the training results; and performing administrative procedures and planning for the improvement of the training process.

Additionally, VET trainers should be aware that even though the subject of the training may not be topics related to the digital world, some of this information may be needed to increase the effectiveness of the training conducted. Trainers should stay aware of the possible backgrounds of their students and adjust the schedule of the training by reserving time and spending effort on the explanation and demonstration of some training practices that will lead to improved digital hygiene for their students.

Of course, at times digital hygiene and other related topics may be the actual main topic of the training. In those cases, VET trainers and educators may proceed with guiding their students while they gain new knowledge and acquire new skills related to digital hygiene.

Digital hygiene from the VET trainers' perspective could be perceived as the practice of maintaining and ensuring safe and productive digital activities during the training that is provided regardless of the subject of the training. Several aspects of vocational and education training may require the use of a digital environment to enhance the training results and increase the satisfaction of the students participating in the training. Trainers should be aware of how the use of digital tools affects the training process and try and use the integrate of some the aspects related to digital hygiene into the training itself. Here are some of the options how to improve the training process:

- **Topics and course modules on digital safety**

When offering training content, proposing to start a specific training activity, or requiring the students to perform an administrative activity related to training, introduce some advice in the form of smaller training topics or more extensive modules that teach students about cybersecurity fundamentals, such as password management, recognizing phishing attempts, and securing personal and workplace data. When available tailor these topics to the specific industries, lines of work, work roles, or activities students related to the student's actual line of work or the expected line of work or future job position they are preparing to enter, making the information relevant and applicable.

- **Practical workshops, individual and group work**

When conducting practical assignments during the training like, for example, practical workshops or individual or group work assignments, implement workshops where students can practice setting up secure networks, using VPNs, installing and managing security software, and conducting regular security checks; or let them experience how some of the mistakes they may not be aware of are performing in a safe learning environment may potentially lead to problems. A hands-on approach and opportunities for trial and error help solidify theoretical knowledge through practical application.

- **Ethics and compliance**

During the training incorporate discussions and offer guidance on ethical behavior online and the legal implications of digital actions if the theoretical training topics or practical assignments have implications on some behaviors. This can cover topics like data privacy laws relevant to the subject of training or the roles and professional conduct of the students, ethical hacking, and the importance of maintaining a professional online presence.

- **Digital footprint management**

Educate students on managing their digital footprints, emphasizing the long-term impacts of online activities on personal and professional reputation. Training can include how to effectively use social media, manage digital content, and understand the consequences of online postings. Educate students on how digital tools that are used for work may also create some digital footprint and how the students should manage their work results and the results of others that are acquired during the collaboration.

- **Continual learning**

Be aware that modern digital landscapes are constantly changing. Based on their role and the line of work they come from or expect to join students may require new knowledge about topics related to the use of new digital tools. It is important to stay updated with the latest technologies and be aware of the newest threats that may affect the students learning the subject of the training. Raising awareness of new options in the digital environment and introducing new tools to the students may lead to higher perceived quality of the training and improve the knowledge and skills of the students. Seeking opportunities for continual learning and certification in digital security practices can become an integral part of the curriculum regardless of the main training topics.

- **Assessment and certification**

Assessments are part of training. Based on the subject and the goals of the training assessments may be more or less formal and may include the use of digital tools to perform the assessment and to gather and analyze the assessment results. Good practice is to make sure that the students are aware of the proper use of assessment tools. The contents of the assessments may include testing of the knowledge and skills gained specifically in digital hygiene as well as the knowledge of general subjects. Assessment and certifications may

be used to incentivize students and the form the results are presented in may require additional thought about the digital environment. The students may require help when acquiring and handling their new certification information or using their new qualifications to enhance their employability.

You may notice that some of the options for the improvement of the VET training concerning digital hygiene correspond to skills identified previously. All of these elements can be incorporated into VET programs and viewed from two different perspectives: what digital hygiene skills should be employed as part of the training and require additional attention during the training; and what are the additional opportunities for improving digital hygiene knowledge and skills during the training in addition to the main topics. Addressing these elements may improve the quality of the training and provide the students with additional benefits in their work environment that relies heavily on the options of the digital world.

From a practical standpoint, it means that VET trainers and educators should: introduce safe learning environments and tools specifically assigned to training, establish guidelines for handling training materials, use communication tools, and perform communications with the protection of personal information and proprietary information in mind, manage data about training process and results which often includes sensitive information, and follow and provide the general advice that facilitates the abiding to good digital hygiene practice.

Unit 4 – Good Practice Example – Digital Hygiene for VETs

Let's look at a good practice example of how digital hygiene can be introduced in VET organization for the safety of the organization and the use of VET trainers and the students participating in the training.

Description of the situation

A vocational education and training company wishes to provide online training for their students to avoid costly and time-consuming travel and to provide the students with the convenience of attending the training from their safe physical environments. The VET company has a staff of internal and external trainers who have different previous experiences with providing online training and may have different knowledge and skills related to conducting such training. The company also has internal employees who perform administrative activities related to training and handle information that is at times sensitive and should be addressed by the compliance rules and guidelines. Typically, the trainers will be expected to use Microsoft Teams environment for conducting the training, sharing the training materials, and communicating with the students, while internal support staff will be using Microsoft Teams and e-mail for managing students before, during, and after the training and some sort of document storage system for managing and sharing training materials.

The things that the VET company is concerned about are:

- mishandling of personal information by any of the participants of the training,
- careful use of proprietary information of the company and the external partners,
- limiting access to the training to only the intended audience,
- providing a rich experience for the students,
- keeping a certain level of reputation as a good training service provider in the market.

Let's see how digital hygiene issues can be addressed in this situation.

The solution

This kind of situation is complex and requires that attention be paid to several aspects related to digital hygiene:

- organizing setup of the Microsoft Teams environment and managing users during the training,
- training the trainers conducting the training,
- conducting the actual training sessions with the involvement of students and trainers,
- handling the training materials used during the training,

- organizing the communication between the trainer and the students and between the students themselves,
- conducting evaluations of the training and gathering feedback.

A more detailed description of good practice for each of these aspects follows.

Setup and Login Management

Teams For Education: A Teams environment separate from the Teams environment used for everyday communication and knowledge sharing by the employees of the VET organization was set up. Microsoft Teams for Education is available to those VET organizations that meet the requirements of official education organizations and provides additional features that are beneficial for conducting the training.

Single Sign-On (SSO): Implementation of SSO using a common authentication platform (like Active Directory) was performed to streamline access to Microsoft Teams, applications used within the Microsoft Teams environment, and other tools used centrally and with the approval of the VET organization during the training was performed.

Role-Based Access Control: Roles and permissions within Teams based on the user's position were assigned. Specifically, 4 roles were assigned each with their privileges in the Teams environment: systems administrator, training administrator (the person organizing training sessions before the training and analyzing the training results after that), trainer (the person conducting the training and practical assignments and handling the training materials during the training) and student, ensuring appropriate access to features and information.

Secure Authentication Practices: Where appropriate the users who were assigned greater privileges when accessing sensitive information, were trained to use multi-factor authentication (MFA) and strong passwords to enhance security.

Training the Trainers

Microsoft Teams Training Workshops: Dedicated workshops for trainers on how to use Microsoft Teams effectively were planned and conducted and internal and external trainers were invited to participate in receiving guidelines for safe conduct in Teams environment. The training included creating and managing teams and channels, scheduling meetings, and using collaboration features like shared files and chat.

Advanced Features Training: Additional training on advanced features such as breakout rooms, live events, and integrating third-party apps that can enhance the training experience was provided to trainers and the chance to practice these features as practical assignments during the training was offered.

Ongoing Support: For those trainers that needed the premises fully set physical training rooms were offered with secure connections to the internet. For those trainers that intended to use their premises, guidelines for safe conduct of training were provided. Contact information of dedicated IT support personnel was set up to help trainers in case of technical issues.

Conducting Training Sessions

Session Planning: Internal training administrators and trainers were trained in the use of a calendar to schedule sessions, set reminders, and provide an agenda upfront in the meeting invitation. Automated invites were set up for the students to minimize the risks of joining the wrong training sessions.

Interactive Features: All the trainers were advised to use additional Teams features like polls, quizzes, and whiteboards during sessions to engage students and enhance learning whenever possible. The use of additional tools and features was permitted but the trainers were advised to guide the students when using them for additional information or practical assignments.

Recording Sessions: Recording of training sessions was severely limited due to GDPR and only performed upon explicit agreement of all the students. When created the recordings were stored securely and accessible only to those who attended the training sessions, and only for a limited time. Although recordings in general are considered beneficial for students when reviewing the training content later, a VET organization should be aware of the risks related to them.

Breakout Rooms: Breakout rooms for group activities or discussions were set up by the training administrator, access rights were given, and appropriate training was conducted for the trainers, allowing trainers to hop between rooms to guide and monitor training progress.

Handling Training Materials

Files and Resource Sharing: All the training materials that were used during the training were stored on secure servers. The electronic keys to training materials or the actual copies of the training materials were handled by a dedicated training administrator. For less sensitive materials Teams' environment itself was used.

Collaborative Editing: When collaborating on documents or presentations in real-time during the practical assignments the trainers and students were advised to use official software like Office 365 integration and be mindful of oversharing the information.

Version Control: Version control of internal documents that were part of training materials was introduced within the VET organization. All the trainers were advised to take on the role of experts for external training

materials and were encouraged to consult the internal training administrators for versions of training materials, student guidebooks, and practice tests where applicable to reduce the damage to the reputation of the VET organization for not supplying up to date versions of training materials.

Communication Between Students and Trainers

Regular Updates: Teams chat was used to make announcements, share updates, and provide feedback on training sessions.

Dedicated Channels: Channels for specific training sessions and individual groups of students were created, facilitating focused discussions and resource sharing.

Private Chats: Additional private chats between the trainer and the students were limited to only situations where both sides agreed to extra communication organizing the exchange of the contact information centrally.

Evaluation and Feedback

Feedback Forms: The use of Microsoft Forms or dedicated software developed internally by the VET organization to collect feedback on training sessions was enforced. Links to the software used for feedback were distributed via Teams environment ensuring only the intended audience could participate in feedback. Access to the information provided in the feedback forms was limited to the internal training administrators of the VET organization.

Performance Tracking: Assignment features within Teams to give tasks, collect work, and provide graded feedback were utilized.

This setup of both technical environment as well as procedures and roles involved in the process ensures a comprehensive, secure, and interactive training environment using Microsoft Teams, catering to both trainers' and students' needs while maintaining a high standard of digital hygiene and efficiency.

Sources

1. Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. European e-Competence Framework, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accessed April 15, 2024].
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework Role Profiles, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [accessed April 15, 2024].
4. Punie, Y., editor(s), Redecker, C., European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print),978-92-79-73494-6 (pdf), doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466.
5. World Economic Forum, “Future of Jobs Report 2023”, https://www.weforum.org/publications/the-future-of-jobs-report-2023/
6. Chui, M., Issler, M., Roberts, R., Yee, L. “McKinsey Technology Trends Outlook 2023”, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable
7. Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [accessed April 15, 2024].

Module 2 - Digital Hygiene Customized Curriculum for VETs

Introduction

Digital hygiene has assumed a much larger and more significant role in our daily lives. With the rapid growth of digitization and its expansion into all spheres of human activity, there has risen an urgent need to ensure our digital environments are safe. One of the primary and fundamental safeguards in this regard is to ensure proper digital hygiene. This is especially true given the growing cyber threats organizations face. Digital hygiene primarily focuses on maintaining a healthy and secure digital presence, and this has become increasingly pertinent as more organizations move their activities online. This module is designed to provide a robust curriculum that can train students at the vocational level to develop, assess, and maintain good digital hygiene practices.

Taking this program will enable the student to acquire the requisite basic analytical and practical skills to effectively assess, maintain, and intervene where necessary to ensure digital hygiene within an organizational setting. This is a truly relevant program due to the high demand in the market for professionals with skills in this area. This development program has been benchmarked against best practices within this domain. The focus of this program being startups and SME professionals informed the choice of modules and structure. The essence is to build proficiency at that level, which means the program is designed and structured to be accessible to those willing to take it on a part-time or full-time basis. The program is also designed to be hands-on and practical-oriented with a short turnaround time. However, it is also designed to enable students to go at their own pace.

Unit 1 – Curriculum Overview

This handbook has been written to provide students currently enrolled or about to enroll in the Vocational Education and Training (VET) in Digital Hygiene program as well as instructors with relevant information with regards to the purpose, planning, structure, and assessment of the program. Recognizing that not all organizations are the same and require the same level of digital hygiene skills, this module and the different parts are modular in structure. This allows individuals who are proficient in certain areas to focus on or transition to other modules as their needs evolve. The ultimate goal of this program is to create a robust foundation in digital hygiene, empowering both students and instructors to manage and mitigate cyber risks

effectively. This curriculum is also designed to cover substantial parts of the base-level professional cybersecurity certifications, such as GIAC Security Essentials (GSEC) and the CompTIA Security+. It therefore provides added value and an increased incentive for students to participate in this program.

Program Aim & Objectives of the Module

The core objectives of the Digital Hygiene module are designed to enhance the cybersecurity posture of organizations by enabling participants to:

- Assess cyber-security threats organizations face.
- Assess and implement basic network security.
- To know how to deploy and maintain basic encryption protocols.
- Assess and implement Data management and security protocols.
- Assess and apply basic hardware and software security protocols.
- Manage security in the mobile environment.

Teaching Methodology

The program employs a blend of theoretical instruction and practical application. It leverages case studies, hands-on lab sessions, and interactive workshops to ensure that learners can apply the concepts they learn in real-world scenarios. This approach not only enhances understanding but also ensures that graduates are job-ready and capable of implementing comprehensive digital hygiene practices immediately upon completion of the program.

Assessment and Continuous Improvement

Assessment within the Digital Hygiene program is both rigorous and continuous, utilizing a variety of methods to evaluate participant knowledge and skills. These include quizzes, practical exams, project-based assessments, and a capstone project that encapsulates the entirety of the participants' learning. Feedback mechanisms are integral to the curriculum, providing participants with timely insights into their progress and areas for improvement. Additionally, the curriculum itself is regularly updated to align with the latest in cyber threat intelligence and technological advancements, ensuring relevancy and efficacy in addressing contemporary cybersecurity challenges.

Conclusion

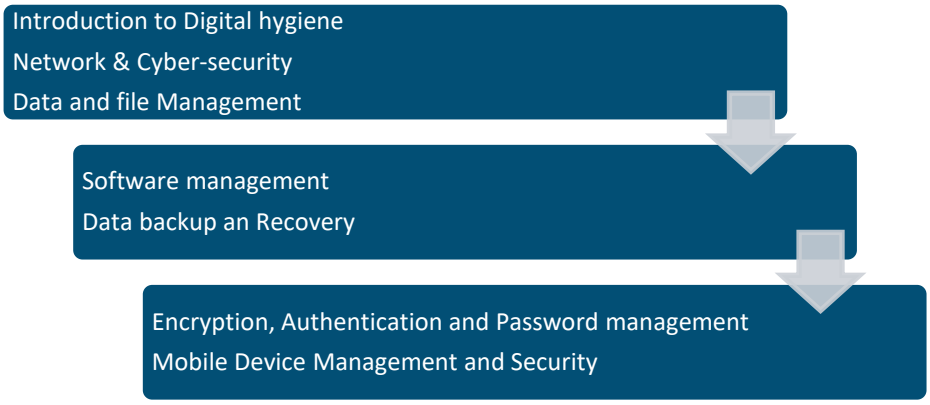
The Digital Hygiene program at the VET institution is designed not just to impart essential cybersecurity knowledge and skills, but also to instill a proactive and informed cybersecurity culture among participants. By the end of the program, participants are not merely graduates; they are empowered digital citizens, equipped to contribute significantly to the cybersecurity defenses of their organizations. This comprehensive

program is a cornerstone in preparing the next generation of cybersecurity professionals, ready to tackle the dynamic challenges of the digital age.

Unit 2 – Key Learning Areas

Overview of the Curriculum

Code	Learning Areas/Subjects
D21	Introduction to Digital Hygiene
D22	Network & Cyber-security
D23	Data and File Management
D24	Software Management
D25	Data Backup and Recovery
D26	Encryption, Authentication, and Password management
D27	Mobile Device Management and Security



Introduction to Digital Hygiene

This subject is designed to provide the students with a comprehensive overview of digital hygiene. This overview will provide both a conceptual overview of the content and some of the practical outworking when viewing the program from an integrative perspective. The primary focus will be on introducing the different areas of Digital hygiene and how the different subject areas are linked and related to each other. It will provide a preliminary overview of the basic principles and practices of Digital hygiene and how the different components fit together. This unit provides the foundational knowledge and understanding on which the other component areas can be built.

The Key Topics Covered in This Subject

- Understanding digital hygiene: An exploration of what constitutes digital hygiene and why it is critical in today's digital age.

- Digital hygiene essentials: Core practices and protocols that ensure the integrity and security of data and systems.
- The security implications of digital hygiene: A detailed look at how effective digital hygiene can mitigate various cyber threats.
- Digital hygiene implementation basics: Practical steps for instituting digital hygiene measures within personal and organizational contexts.
- Cybersecurity compliance: An overview of the basic national and EU policies, regulations, and compliance requirements on cybersecurity

Subject Learning Outcomes

By the end of this subject, students will be able to:

- Define digital hygiene and understand its critical components.
- Identify potential cyber threats and understand the role of digital hygiene in protecting against these threats.
- Implement basic digital hygiene practices across various platforms and devices.
- Communicate the importance of digital hygiene to peers and superiors, advocating for best practices within their organizations.
- Understand the basic cybersecurity compliance requirements

Teaching Methods

A blend of lectures, interactive workshops, and case studies will be employed to provide students with a robust learning experience. Each session aims to balance theoretical knowledge with practical application, ensuring that students can translate what they learn into actionable strategies in their workplaces.

Recommended Literature

- Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.
    - This book provides a thorough introduction to the domain of cybersecurity and is especially useful for entry-level cybersecurity certifications.
- Paula, D., Cruz, M., (2023), Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - This book is an essential read for understanding cybersecurity challenges and how to mitigate against them. It is especially relevant to new startup SME owners and students looking to seek to understand online safety.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
    - This reference provides an accessible overview of the key concepts and challenges in cybersecurity, making it an excellent resource for students starting their journey in understanding cyber threats and protection mechanisms.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
    - Bruce Schneier's book is crucial for understanding the landscape of data privacy and security, offering insights into how personal data is collected and used, and the importance of robust data management practices.

These resources are selected to provide theoretical knowledge and practical skills in network and cybersecurity, supporting the curriculum and enhancing the educational experience of VET students in digital hygiene.

Network & Cybersecurity

This subject is focused on providing the students with the necessary skills to identify, assess, and neutralize network threats. One of the key challenges faced by organizations in the current operating environments is ensuring network security. Since most networks are connected to the Internet, they are often exposed to malevolent actors who may try to exploit network vulnerabilities to access the network in an unauthorized fashion. To achieve this the student will be instructed in key network concepts, common protocols, ports, LAN, WAN, and cloud systems.

The Key Topics Covered in This Subject

- Introduction to cybersecurity
- Vulnerability analysis
- Threat and risk assessment
- Network security protocols – Firewalls, antivirus.
- Common cybersecurity attacks
- Common Cybersecurity tools
- Ethics in cybersecurity

Learning Outcomes

- Identify Key Network Concepts: Students will be able to describe the fundamental aspects of networks including LAN, WAN, and cloud systems, and understand their roles in organizational infrastructure.
- Assess Network Vulnerabilities: Learners will gain the skills to perform vulnerability analyses on various network systems to identify potential security weaknesses.
- Implement Security Measures: Students will be proficient in setting up and managing network security protocols such as firewalls and antivirus systems to protect against cyber threats.
- Conduct Threat and Risk Assessments: Equip students with the ability to assess and prioritize risks associated with cybersecurity threats to network systems.
- Understand Ethical Implications: Students will explore the ethical considerations in cybersecurity, understanding the responsibilities of protecting data and systems from unauthorized access.

Teaching Methods

- Interactive Lectures: Focused on introducing fundamental and advanced network concepts, security protocols, and ethical issues in cybersecurity.
- Hands-On Labs: Practical sessions in computer labs where students can use real and simulated network environments to apply security measures and tools.
- Case Study Analysis: Discussion and analysis of real-world cybersecurity incidents to understand threat mechanisms and effective countermeasures.

- Group Projects: Teams of students will assess a hypothetical network setup for vulnerabilities and propose a comprehensive security strategy.
- Guest Speaker Sessions: Cybersecurity professionals are invited to share insights and experiences, emphasizing current challenges and emerging technologies.

Recommended literature

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7th ed.). Cengage Learning.
    - This guide covers a broad range of foundational topics in network security, suitable for students beginning their journey in cybersecurity.
- Marsh, N., (2023), Cybersecurity: A Fat-Free Guide to Network Security Best Practices (Fat-Free Technology Guides). This book provides a comprehensive insight into cyber threats and critical network security issues.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
    - A comprehensive resource that provides an in-depth look at the principles of information security, including detailed discussions on vulnerability analysis, threat, and risk assessment.
- Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson. Stallings' text provides comprehensive coverage of network security protocols and standards, ideal for students needing a detailed understanding of the technical aspects of securing networks.
- Computer & Internet Security: A Hands-on Approach 3rd ed. Edition by Wenliang Du

These academic resources will support the curriculum by providing both theoretical frameworks and practical insights into managing and securing network environments, aligning with the outlined learning outcomes and teaching strategies.

Data and File Management

Data as alluded to earlier is one of the most valuable assets organizations own. Consequently, the management of this asset has taken on an increasingly vital role within the organization. This is especially important because of the rise in security concerns in the cyber environment. Proper data management has become pivotal to effective cybersecurity, especially in capturing, organizing, and disseminating sensitive information. Data management refers to the principles and practices applied in the management and protection of data. Within the context of cybersecurity data management is also concerned with the protection of data from authorized access modification and transmission. In the current environment where huge volumes of data are collected, analyzed, and disseminated, the security management aspects have gained prominence. Therefore, there is a heightened requirement for professionals who are proficient in data management.

The Key Topics Covered in This Subject

- Data governance
- Data classification
- Encryption in data management
- Data Monitoring and Audit
- Data backup and recovery
- Data integrity and privacy

- Access controls and authentication

Learning Outcomes

- Understand Data Governance: Students will grasp the foundational concepts of data governance and its role in the organizational context.
- Classify Data: Learners will be able to classify data based on sensitivity and importance, applying appropriate security measures to different types of data.
- Implement Data Encryption: Students will understand and apply encryption techniques to protect data integrity and confidentiality during storage and transmission.
- Conduct Data Audits: Equip students with the skills to perform regular data monitoring and audits to ensure compliance with security policies and regulations.
- Manage Data Recovery: Students will learn strategies for data backup and recovery to ensure data availability and continuity in case of data loss or system failures.
- Ensure Data Integrity and Privacy: Learners will understand methods to maintain data integrity and manage privacy settings to protect user data from unauthorized access.
- Apply Access Controls: Students will be capable of implementing robust access controls and authentication methods to safeguard data access.

Recommended Literature

- Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition. This book provides a comprehensive view of data governance and security.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
    - This book provides practical tools and techniques for assessing information security risks, including those associated with data management.
- Bertino, E., & Sandhu, R. (2017). Data Privacy and Security. Springer.
    - A comprehensive overview of data privacy and security techniques, this text is crucial for understanding the complexities of protecting sensitive data in various environments.
- Swanson, M., & Guttman, B. (2016). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology.
    - This government publication offers guidelines and best practices for securing IT systems, including detailed sections on data management and security controls.

These academic resources will enhance the educational framework by providing theoretical knowledge and practical application examples, enabling students to become proficient in managing and securing organizational data effectively.

Software Management

Software management is a crucial element of cybersecurity. Software management includes the systematic process of planning, deploying systematic process of planning, deploying, monitoring, and maintaining software throughout its lifecycle. It encompasses tasks such as version control, patch management, licensing, and security updates. Effective software management ensures optimal performance, security, and compliance while minimizing risks and vulnerabilities. Modern organizations are faced with various

challenges regarding software security such as poor password policies, insecure API unpatched vulnerabilities, phishing, and data breaches to name a few. It is therefore imperative that they have trained personnel who are trained to effectively manage the organization's software and forestall software security breaches. This module will provide the student with basic hands-on knowledge on how to effectively manage the organization's software and minimize the risk of a security breach.

The Key Topics Covered in This Subject

- Application Security
- software testing and auditing
- Managing user access and privileges
- Implementing regular Update protocols
- Endpoint security measures

Learning Outcomes

- Master Application Security: Students will understand the fundamentals of securing applications from design to deployment, including common vulnerabilities and mitigation strategies.
- Conduct Software Testing and Auditing: Learners will gain proficiency in various methods of software testing and auditing to identify and resolve security issues.
- Manage User Access: Students will learn to manage user access and privileges effectively to ensure that only authorized users have access to critical software resources.
- Implement Update Protocols: Equip students with the knowledge to establish and maintain regular software update protocols to mitigate vulnerabilities.
- Enhance Endpoint Security: Students will understand endpoint security measures to protect organizational infrastructure from threats such as malware and ransomware.

Recommended Literature

- Du, W., (2022), Computer Security: A hands-on approach, 3rd edition. This book investigates software management, vulnerabilities, and mitigation activities.
- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional.
    - This book offers a comprehensive guide to integrating security practices into software development, making it essential for understanding application security and lifecycle management.
- Anton, A. I., & Earp, J. B. (2004). A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. Academy of Management Review.
    - Provides insights into managing user access and privileges by identifying key stakeholders and their needs, crucial for effective software management.
- Lindqvist, U., & Neumann, P. G. (2017). The Future of Cybersecurity: Challenges and Opportunities. IEEE Security & Privacy.
    - This article discusses future challenges and opportunities in cybersecurity, including the importance of continuous software updates and endpoint security measures.

These resources will support the curriculum by providing a solid theoretical foundation and practical insights into software management, ensuring students are well-equipped to handle software security challenges in modern organizational environments

Data Backup and Recovery

This module is designed to equip the students with a comprehensive understanding of the Backup and Recovery process and how it can be implemented. All modern organizations must have proper backup and recovery policies, protocols, and systems in place. Most current organizations are data-driven and consequently place a premium on the management of their data and informational resources. In principle, most organizations especially SMEs store their data in a centralized local or cloud database. Cloud-based systems have become more advanced and secure with very sophisticated management controls making them less susceptible to the traditional problems of destruction of the physical storage systems. However, they are still susceptible to human error, misconfiguration, and data breaches, therefore it is important for the IT personnel overseeing such systems to be conversant with the technologies, protocols, and processes involved. The module is designed to provide this knowledge to the student.

The Key Topics Covered in This Subject

- File Management
- Backup and Recovery Protocols
- Backup types
- Backup services and devices

Learning Outcomes

- Understand File Management: Students will learn the principles of effective file management, crucial for organizing data for backup purposes.
- Master Backup and Recovery Protocols: Learners will understand different backup and recovery protocols and how to apply them effectively in various scenarios.
- Identify Backup Types: Students will be able to distinguish between different types of backups (full, incremental, differential) and decide which is most appropriate for specific situations.
- Utilize Backup Services and Devices: Equip students with knowledge about various backup services and devices, including cloud-based and local backup solutions, and how to implement them securely.
- Mitigate Data Loss Risks: Students will understand how to plan and execute a data recovery strategy to minimize downtime and data loss in the event of data breaches or disasters.

Recommended Literature

- Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads. This book is into modern data protection and how this is integrated into the overall hardware and software security.
- Data Backup And Recovery A Complete Guide - 2023 Edition
- Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.
    - Offers comprehensive insights into disaster recovery planning, including detailed discussions on backup strategies as a critical component of disaster recovery.
- Duffy, D. (2014). Cloud Computing: Strategies for Cloud Computing Adoption. Faithful Pen Publishing.
    - Discusses the adoption of cloud computing, focusing on cloud-based backup services and the security considerations associated with them.

These academic resources will bolster the curriculum by providing students with both a foundational understanding and practical skills in managing and implementing data backup and recovery strategies, essential for minimizing potential data loss in modern organizational environments.

Cryptography, Authentication, and Password Management

Data and information have become one of the most crucial organizational assets and in many cases are the key determinant behind company valuation. The crucial nature of such assets makes it imperative for them to be treated with utmost care. One of the key tools for safeguarding data and information assets is cryptography. Cryptography is central to cybersecurity as it is essential to the protection of sensitive data and information and secure communications. It enables robust authentication protocols and password management. Cryptography enables proper implementation of authentication systems, which ensure the confidentiality, integrity, and availability of organizational data and information to the appropriate staff member.

The Key Topics Covered in This Subject

- Cryptography basics
- End-to-end encryption
- Encryption standards
- Multifactor authentication
- Key management
- Selecting the best standards for your business
- Best practices in implementing encryption technologies

Learning Outcomes

- Understand Cryptography Basics: Students will learn the fundamental principles of cryptography, including its history, purpose, and key mechanisms.
- Implement End-to-End Encryption: Learners will gain skills in setting up and managing end-to-end encryption to secure communications.
- Apply Encryption Standards: Students will be familiar with various encryption standards and learn how to apply them according to organizational needs.
- Utilize Multifactor Authentication: Equip students with the ability to implement and manage multifactor authentication systems to enhance security.
- Manage Cryptographic Keys: Students will understand key management processes and best practices to ensure the security and integrity of cryptographic keys.
- Select and Implement Encryption Technologies: Students will learn how to select appropriate encryption technologies for their business and best practices for implementation to protect data effectively.

Recommended Literature

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
    - This textbook provides a comprehensive introduction to the field of cryptography and network security, including detailed coverage of encryption technologies and authentication protocols.

- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.
    - Offers an in-depth exploration of modern cryptographic techniques, focusing on rigorous security proofs and practical applications.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
    - This book discusses the design and implementation of cryptographic systems, emphasizing the importance of proper implementation to prevent vulnerabilities.

These resources are selected to provide a theoretical background and practical skills in cryptography, authentication, and password management, supporting the curriculum's goal to equip students with the necessary knowledge to secure organizational data effectively.

Mobile Device Management and Security

Organizations are increasingly deploying mobile devices as a major work platform and means of communication. This is especially applicable to startups and SMEs where being agile and reachable at all times has become a major criterion for success. While mobile technology has advanced such that most advanced smartphones are as powerful and versatile as laptops and desktops, the wireless nature of such devices makes them susceptible to malevolent actors seeking to gain unauthorized access. This module is designed to provide insight into the vulnerabilities of these devices and their attendant platforms and how such risks can be minimized.

The Key Topics Covered in This Subject

- Understanding the threats to mobile devices
- Assessing the risks for mobile applications
- Inter-process communications firewalls
- Mobile security technologies
- Mobile data access controls and risk management

Learning Outcomes

- Identify Threats to Mobile Devices: Students will learn to recognize various threats that target mobile platforms and understand their potential impact.
- Assess Risks for Mobile Applications: Learners will gain skills in assessing risks associated with mobile applications, focusing on security vulnerabilities.
- Implement Mobile Security Technologies: Students will be able to implement and manage security technologies designed specifically for mobile devices.
- Manage Inter-Process Communications Firewalls: Equip students with the knowledge to configure and manage firewalls that control inter-process communications on mobile devices.
- Apply Mobile Data Access Controls: Students will learn how to establish and enforce data access controls to secure sensitive information on mobile devices.

Recommended Literature

- Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition. This book looks at the implications of the rapid integration of mobile devices into the organization's communication environment, the attendant security concerns, and how these can be mitigated.
- Russell, B., Van Duren, Drew., (2018), Practical Internet of Things Security - Second Edition: Design a security framework for Internet-connected Ecosystem
- Zdziarski, J. A. (2015). Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. O'Reilly Media, Inc.
    - This book offers a deep dive into the security architecture of iOS, discussing common vulnerabilities and providing strategies to secure iOS applications.
- Fried, S. (2011). Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. CyberAge Books.
    - This guide is essential for students and practitioners needing to understand the specific security challenges presented by mobile devices, which are increasingly used in both personal and professional contexts.

These resources will support the curriculum by providing both foundational knowledge and specific skills required to manage and secure mobile devices effectively, ensuring that students are well-prepared to address mobile security challenges in modern organizational contexts.

Unit 3 – Digital Hygiene Assessment and Feedback Mechanisms for VETs

Introduction

Assessment and feedback are crucial components of the educational process, providing both instructors and students with essential insights into the effectiveness of teaching and learning. In the context of a Digital Hygiene curriculum, robust assessment and feedback mechanisms are especially critical. They ensure that the knowledge and skills taught are not only understood and retained but are also applicable in real-world scenarios where digital security risks are prevalent.

This unit is designed to outline the strategies and methodologies for evaluating student performance and providing constructive feedback throughout the Digital Hygiene program. This involves a combination of theoretical knowledge assessments and practical, hands-on evaluations.

Assessment Strategies

Formative Assessments

- **Quizzes and Short Tests:** Frequent quizzes and short tests will be conducted throughout each module to assess understanding of key concepts and to provide immediate feedback. This helps in reinforcing learning and identifying areas where students may need additional support.
- **Practical Assignments:** Students will be given assignments that require them to apply theoretical knowledge to practical scenarios, such as configuring a firewall, designing a data recovery plan, or implementing encryption protocols.
- **Peer Assessments:** This involves students assessing each other's assignments or projects. Peer assessments can help develop critical thinking and analytical skills, as students learn to critique cybersecurity solutions based on best practices.

Summative Assessments

- **Final Exams:** Comprehensive examinations at the end of each module will test students on a wider range of topics covered throughout the course. These exams will include both multiple-choice questions and essay-type questions to assess students' theoretical and practical understanding.
- **Capstone Projects:** At the end of the program, students will undertake a capstone project that involves creating or managing comprehensive digital hygiene strategies for hypothetical organizations. This project will be evaluated on various criteria, including innovation, applicability, and adherence to cybersecurity principles.

Continuous Assessment

- **Portfolio Reviews:** Students will maintain a portfolio of their work and achievements throughout the program. These portfolios will be periodically reviewed by instructors to assess progress and provide personalized feedback.
- **Self-Assessments:** Encouraging students to engage in self-assessment can foster greater responsibility for their learning. Self-assessment tools and checklists will be provided to help students evaluate their understanding and skills.

Feedback Mechanisms

- **Instructor Feedback:** Feedback will be provided systematically for all assessments, focusing on the strengths and weaknesses of students' work. This feedback will be timely, specific, and constructive, aimed at encouraging students to reflect on their learning and identify areas for improvement.
- **Peer Feedback:** In group projects and peer assessments, students will be encouraged to provide feedback to each other. This will be structured to ensure it is constructive and focused on specific criteria.
- **Automated Feedback:** For certain types of assessments, especially quizzes and certain practical exercises, automated feedback systems will be utilized. These systems can provide immediate results and insights, allowing for quick remediation.
- **Feedback Loops:** Creating feedback loops within the curriculum where students can reflect on the feedback, revise their work, and resubmit it for further review fosters a growth mindset and continuous improvement.

Implementing Feedback into Curriculum Development

The feedback received from these various mechanisms isn't just for the students' benefit. It also plays a crucial role in curriculum development:

- **Curriculum Adjustments:** Regular reviews of student performance data and feedback will help in identifying areas of the curriculum that may need adjustments or enhancements.
- **Instructor Development:** Feedback from students can also guide professional development needs for instructors, indicating areas where they might need more support or training.

Conclusion

The assessment and feedback mechanisms designed for the Digital Hygiene curriculum in VET institutions are integral to ensuring that the educational objectives are met. By employing a variety of assessment strategies and multi-channel feedback systems, the program not only evaluates student learning effectively but also continuously improves teaching methods and curriculum design. This dynamic approach ensures that the curriculum remains relevant and effective in preparing students to tackle real-world digital hygiene challenges.

Unit 4 – Good Practice from VETs

Introduction

In the dynamic field of Digital Hygiene, theoretical knowledge paired with practical applications creates the most effective learning environment. This unit delves into good practices adopted by Vocational Education and Training (VET) institutions that have successfully integrated digital hygiene principles into their curricula. These case studies serve as benchmarks for developing and refining digital hygiene programs, providing insights into successful strategies and methodologies that can be replicated or adapted by other institutions.

Case Study 1: CyberVET Academy

Overview:

CyberVET Academy is known for its robust digital hygiene curriculum that combines rigorous academics with real-world application. This institution has become a model of how to seamlessly integrate emerging technologies and cybersecurity best practices into vocational training.

Key Strategies:

- Industry Partnerships: CyberVET has formed partnerships with leading tech companies to ensure that their curriculum is aligned with current industry standards and practices. These partnerships also facilitate guest lectures, internships, and access to cutting-edge technology.
- Simulated Learning Environments: The academy has invested in creating state-of-the-art simulated cybersecurity labs where students can safely explore and mitigate real-time cyber threats. This hands-on experience is invaluable.

Outcomes:

- A marked increase in student employability, with 90% of graduates securing jobs in cybersecurity within six months of graduation.
- Enhanced student engagement and satisfaction, attributed to the hands-on learning approach and direct industry involvement.

Case Study 2: TechBridge VET

Overview:

TechBridge VET stands out for its focus on mobile device management and security, areas of increasing concern in the digital hygiene domain.

Key Strategies:

- Modular Curriculum Design: The curriculum at TechBridge is highly modular, allowing students to tailor their learning paths according to their career goals and technological advancements.
- Community Projects: Students participate in community outreach programs where they apply their knowledge to help local small businesses improve their digital security measures.

Outcomes:

- Community projects have not only increased the practical skills of the students but also raised cybersecurity awareness among local small business owners.
- The modular approach has led to high flexibility in education, accommodating rapid changes in technology and student needs.

Case Study 3: SecurePath Institute

Overview:

SecurePath Institute has integrated digital hygiene across its vocational programs, demonstrating how cybersecurity is fundamental to various technical disciplines.

Key Strategies:

- Interdisciplinary Approach: By integrating digital hygiene lessons into programs like healthcare, automotive technology, and business management, SecurePath ensures that all students recognize the importance of cybersecurity in their respective fields.
- Continuous Curriculum Evaluation: The institute uses an AI-driven analytics system to continuously assess and update its curriculum based on the latest cyber threat intelligence and industry trends.

Outcomes:

- Students from non-tech programs graduate with a strong understanding of digital hygiene, making them more versatile and attractive to employers.
- The continuous curriculum evaluation has kept SecurePath at the forefront of digital hygiene education, adapting quickly to emerging threats.

Implications for Best Practices

The successes of these institutions illustrate several best practices that can be adopted or adapted by other VET providers:

- Industry Collaboration: Strong ties with industry not only keep the curriculum relevant but also enhance student job prospects post-graduation.
- Practical Application: Hands-on learning through labs, simulations, or community projects is crucial for understanding and applying digital hygiene principles effectively.
- Flexibility and Interdisciplinarity: A flexible and interdisciplinary approach ensures that digital hygiene education can quickly adapt to changes and cater to a broad range of vocational areas.
- Feedback and Continuous Improvement: Ongoing assessment and revision of the curriculum based on feedback from various stakeholders, including students, faculty, and industry partners, ensure the program's effectiveness and relevance.

Case Study 4: DigitalDefenders College

Overview:

DigitalDefenders College is renowned for its specialized approach to teaching cybersecurity, particularly emphasizing ethical hacking and digital forensic techniques. This VET institution is committed to producing skilled professionals ready to tackle the complexities of cyber threats in the modern digital landscape.

Key Strategies:

- Ethical Hacking Modules: Incorporating extensive modules on ethical hacking, the college provides students with the skills to identify and exploit system vulnerabilities, all in a controlled, ethical, and legal framework.
- Real-World Cyber Forensics: Students engage in practical cyber forensics exercises that mimic real-world data breach scenarios, helping them understand how to track, analyze, and mitigate breaches effectively.

Outcomes:

- Graduates are known for their proactive approach to cybersecurity, with many securing positions in high-stakes sectors such as finance and government.
- The hands-on experience in ethical hacking and cyber forensics has led to a high engagement level among students, fostering a deep understanding of the practical implications of cyber threats.

Case Study 5: InnovateTech Institute

Overview:

InnovateTech Institute has set itself apart by integrating advanced technology trends, such as Artificial Intelligence (AI) and Machine Learning (ML), into its digital hygiene curriculum. This approach prepares students for the increasingly AI-driven landscape of cybersecurity.

Key Strategies:

- AI-Driven Security Solutions: Teaching students to utilize AI and ML in developing sophisticated cybersecurity measures, thereby staying ahead of cybercriminals who are also using advanced technologies.
- Collaborative Projects with Tech Companies: Students work on projects in collaboration with tech companies, creating AI-based security solutions, that provide them real-time insights into industry challenges and demands.

Outcomes:

- Students have developed several AI-based security tools that have been adopted by partner companies, showcasing their direct impact on current cybersecurity solutions.
- The integration of AI and ML into digital hygiene education has not only made the curriculum more robust but also significantly increased student employability in tech-driven industries.

Summary of Good Practices

These additional case studies from DigitalDefenders College and InnovateTech Institute further reinforce the critical aspects of a successful digital hygiene curriculum in VET institutions:

- Specialization and Advanced Training: Programs that offer specialized training in high-demand areas of cybersecurity, such as ethical hacking and AI, can significantly enhance the relevance and attractiveness of the curriculum.
- Real-World Application: Practical, real-world application of learned skills, whether through cyber forensics or collaborative industry projects, ensures that students are not only familiar with theoretical concepts but are also proficient in applying them in real situations.
- Innovative and Future-Ready Curriculum: Keeping the curriculum aligned with the latest technological advancements prepares students for emerging threats and opportunities, making them valuable assets in any cybersecurity role they assume post-graduation.

- These examples showcase the diverse strategies that can be implemented to enhance digital hygiene education effectively, each contributing uniquely to the overarching goal of fostering skilled professionals equipped to protect digital assets in an increasingly complex cyber environment.

Conclusion

The five case studies explored by CyberVET Academy, TechBridge VET, SecurePath Institute, DigitalDefenders College, and InnovateTech Institute provide a rich tapestry of successful strategies and approaches in integrating digital hygiene into Vocational Education and Training (VET) curricula. Each institution, with its unique focus and methodology, underscores the pivotal role of practical, industry-aligned, and innovative education in preparing students to navigate the complexities of cybersecurity in the modern digital world.

Key Takeaways and Best Practices

- Industry Collaboration and Alignment: A common theme across all case studies is the importance of maintaining strong ties with industry leaders and companies. These partnerships not only keep the curriculum up-to-date with the latest technologies and practices but also enhance student employability through internships, real-world projects, and exposure to industry standards.
- Hands-On and Practical Experience: Each institution emphasizes the need for practical application of learned concepts. Whether through cyber labs, simulated environments, or real-world forensic investigations, hands-on experience is crucial. It not only cements theoretical knowledge but also prepares students for real-world challenges they will face in their careers.
- Specialized Modules and Advanced Training: Institutions like DigitalDefenders College highlight the benefits of offering specialized training in areas like ethical hacking and cyber forensics. Similarly, InnovateTech Institute's focus on AI-driven security solutions illustrates the advantage of integrating cutting-edge technologies into the curriculum, preparing students for future trends and innovations in cybersecurity.
- Interdisciplinary and Flexible Learning Approaches: SecurePath Institute’s integration of digital hygiene across various vocational programs exemplifies the value of an interdisciplinary approach, which broadens the applicability and relevance of cybersecurity education. Moreover, TechBridge VET’s modular curriculum design allows for greater flexibility, accommodating rapid technological changes and diverse student interests.
- Continuous Improvement and Adaptation: The use of AI-driven analytics by SecurePath Institute for continuous curriculum evaluation and the dynamic update protocols at InnovateTech Institute underscore the importance of ongoing assessment and adaptation. Keeping the curriculum

responsive to the evolving cyber threat landscape ensures that educational programs remain relevant and effective.

The synthesis of insights from these diverse VET institutions reveals that the effectiveness of a digital hygiene curriculum hinges on its ability to blend theoretical knowledge with practical skills, adapt to technological advancements, and foster strong industry connections. These elements are crucial in preparing students not just to meet the current demands of the cybersecurity field but to innovate and lead in the face of future challenges. This holistic approach not only enhances the learning experience but also significantly boosts the employability and readiness of graduates to protect digital assets in a globally connected world. As VET institutions continue to evolve and refine their programs, the lessons drawn from these case studies provide valuable blueprints for developing robust, comprehensive digital hygiene curricula that are equipped to meet the challenges of tomorrow's cybersecurity landscape.

Sources:

1. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
2. Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
3. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8th ed.). Sybex.
6. Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional.
7. Conklin, W. A., White, G., Cothren, C., Williams, D., & Davis, R. (2016). *Principles of Computer Security: CompTIA Security+ and Beyond* (5th ed.). McGraw-Hill Education.
8. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.
9. Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
10. Zdziarski, J. A. (2015). *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media.
11. Tipton, H. F., & Nozaki, M. K. (2013). *Official (ISC)2 Guide to the CISSP CBK* (4th ed.). CRC Press.
12. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.
13. Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.
14. Caloyannides, M. A. (2010). *Privacy Protection and Computer Forensics* (2nd ed.). Artech House.
15. Toigo, J. W. (2009). *Disaster Recovery Planning: Preparing for the Unthinkable* (3rd ed.). Prentice Hall.
16. Ross, R. S. (2013). *Managing Information Security Risks: The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Approach*. Addison-Wesley.
17. Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill Osborne Media.
18. Enck, W. (2011). *Understanding Android Security*. IEEE Security & Privacy Magazine.
19. Anton, A. I., & Earp, J. B. (2004). *A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts*. Academy of Management Review.
20. Liska, A., & Gallo, T. (2016). *Rethinking the Security of the Internet of Things*. Elsevier.
21. Clarke, N. L., & Furnell, S. M. (2016). *Cybersecurity Education: Strategies and Best Practices*. Springer.
22. Bishop, M. (2018). *Computer Security: Art and Science*. Addison-Wesley.

23. Eckert, J. W. (2017). *CompTIA Linux+ Guide to Linux Certification*. Cengage Learning.
24. Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.
25. Easttom, C. (2019). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education.
26. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
27. Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.
28. Goodrich, M. T., & Tamassia, R. (2019). *Introduction to Computer Security*. Pearson.
29. Dafoulas, G. A., & Maia, C. (2015). *Global Security, Safety, and Sustainability: Tomorrow's Challenges of Cyber Security*. Springer.

Online resources and websites:

- Cybersecurity & Infrastructure Security Agency (CISA)
    - Website: https://www.cisa.gov/
    - CISA provides a wealth of resources on cybersecurity best practices and threats, offering guidelines, tools, and alerts that are crucial for cybersecurity education and awareness.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - Website: https://www.nist.gov/cyberframework
    - NIST's framework is a widely used standard for managing cybersecurity risks, and it provides structured guidance that can be integrated into educational curriculums.
- Open Web Application Security Project (OWASP)
    - Website: https://owasp.org/
    - OWASP is an online community delivering free and open resources on web application security, including tools, standards, and best practices.
- SANS Institute
    - Website: https://www.sans.org/
    - A recognized leader in cybersecurity training, the SANS Institute offers a variety of research papers, training materials, and security guidelines.
- Krebs on Security
    - Website: https://krebsonsecurity.com/
    - Run by journalist Brian Krebs, this blog offers in-depth security news and investigation, focusing on the latest threats and breaches.
- Infosec Institute
    - Website: https://resources.infosecinstitute.com/

- Infosec Institute provides resources and training focused on information security, including insightful articles and industry updates.

- The Hacker News
  - Website: https://thehackernews.com/
  - An online cybersecurity news magazine, The Hacker News offers up-to-date information on current cybersecurity threats and innovations.

- Bruce Schneier's Blog
  - Website: https://www.schneier.com/
  - Bruce Schneier is a renowned security technologist whose blog provides insights into security and privacy issues in the digital world.

Module 3: Implementing & Sustaining

Unit 1 - Building a Digital Hygiene Culture in Startups and VET Institutions

What is Digital Hygiene Culture?

As we have discovered in the previous modules, Digital Hygiene is a term that first arose in the early aughts to explain the principles for secure, organized, and ethical digital practices, which aim to protect the data, privacy, and integrity of a system effectively [1]. In this module, we will explore the systemic application of these principles on a larger scale, customized for VET providers across Europe, and offer suggestions on building a better digital hygiene culture that will inspire innovation and enthusiasm in organizations.

So, what exactly is digital hygiene culture? Similar to many other network cultures that strive for a successful organization whether it is centered on structure or exploration [2], digital hygiene culture centers around a shared mindset. In this mindset, every member believes in the organization's mission and formulates strategies that are based on collective responsibility and integrating safe digital practices.

Let's explore how digital hygiene culture can be extended from the leadership level to working groups, and down to every individual.

Development of Digital Hygiene Culture in the Leadership Level

In a post-Covid era where remote work is the new normal, and the vulnerabilities in the digital world can be as emotional as well as technical [3] (e.g. social engineering attacks that might take the form of an emotional story that is a phishing attempt), the situation calls not only for a manager, but for a leader who can navigate the complexities of the digital world efficiently, while demonstrating digital hygiene practices as an integral part of the organizational values. Below are some of the important points where a leader can foster a secure and supportive digital hygiene culture:

- **Encourage Organizational Flexibility** [4]:

Leaders must ensure that their organizations are adaptable to digital advancements as well as challenges that might arise due to digital practices. To guide their team through these changes, all leaders should first understand their position, decisions, and emotions [5] in different circumstances before motivating others through a common objective.

- **Addressing Management Challenges** [5]**:**

Leaders in any organization must recognize potential management challenges that might arise from digitization, such as cybersecurity threats, privacy concerns, skill gaps, or issues raised by remote work. They should be ready to assess their teams' abilities in maintaining digital hygiene. This requires a certain level of technical expertise; therefore it is advised that the leaders can understand and articulate technical issues effectively with their teams.

- **Creating Relationships and Collaborative Processes 6:**

Leaders in any organization should create relationships with a wide range of stakeholders at both internal and external levels. This requires them to be highly coordinated and accountable, as well as taking charge to encourage a strong sense of collaboration between employees and other stakeholders.

- **Investing in Education and Training [5]:**

Leaders in any organization should invest in continuous education and training of themselves and their employees to stay updated on the latest digital hygiene practices and technologies. Some cybersecurity companies [7], as well as some governmental bodies in Europe such as the European Union Agency for Cybersecurity (ENISA), provide a variety of online and face-to-face courses on the topics of cybersecurity awareness and crisis management [8].

Development of Digital Hygiene Culture in Group Level

After a roadmap is laid for a digital hygiene strategy, the cybersecurity concerns of any organization should be also discussed at the group level. Working groups, including departments, programs, students, or project managers can contribute significantly to fostering a digital hygiene culture within their institutions, with the support and collaboration from relevant Computer Emergency Response Teams (CERTs) [Add this term to the Glossary].

Below are some important points that each working group can make use of to create a digital hygiene culture:

- **Establishing Effective Communication in Groups:**

One effective communication method for groups is to kickstart meetings or courses with discussions related to cybersecurity. Each group can spare five minutes in the beginning for members' questions. During these meetings, rules and guidelines about how devices must be used inside the departments or classrooms, can be further established to strengthen the digital hygiene culture [9].

Another helpful method for groups can be to require electronic signatures or QR codes for shared documents that can determine whether an email or a digital transaction is made by a member of group [10]. Another factor that requires attention is choosing safer storage options like cloud, rather than USB flash drives [10].

- **Establishing Effective Documentation Methods for Digital Attacks:**

Documenting digital attacks is a critical aspect of maintaining cybersecurity. All organizations should clearly explain the guidelines for documentation. Some of the procedures for developing documentation for digital attacks can be as follows [11]:

STEP 1: Keep an Organized Log: In the case of an incident, encourage every member of your team to include data points, such as date, time, email address, relevant links, account names, and metadata.

STEP 2: Implement Structured Templates: Use ready-made templates to document the data breach incidents. For example, you can use the incident log template from Access Now, an international NGO that aims to protect people's digital civil rights around the world.

STEP 3: Use Diverse Documentation Formats: Encourage your team members to use a diverse range of formats for documenting their issues. They can utilize Internet Archive's Wayback Machine to save a webpage or use video capture tools to record video as evidence of their issues.

STEP 4: Securely Store Information: Create backups on your own devices, in trusted storage options, and protect your files with encryption if possible.

- **Establishing Regular Digital Hygiene Assessments:**

Conducting regular audits and risk assessments can help identify vulnerabilities and ensure that digital hygiene practices are being followed [11]. Some of the ways of establishing regular digital hygiene assessments are as follows:

- Developing a routine of cyber hygiene habits, such as scanning for viruses, changing passwords, updating software, and cleaning hard drives [12].
- Using the right tools, such as a network firewall, antivirus software, encryption, or backup solutions [13].
- Seek out assistance from reliable services, which provide vulnerability scanning, web application scanning, and phishing assessments [14].

Development of Digital Hygiene Culture at the Individual Level

Human factors are one of the weakest components of cyber security. Some examples of human error in terms of digital practices can include Poor password management, accidental data deletion, or falling victim to phishing or other social engineering scams. However, it is always possible to reduce the risks by paying attention and following digital hygiene practices.

Here are some key points where each individual can contribute to creating a hygiene culture within an organization:

- **Be Mindful About Your Digital Footprint [15]:**

Navigating online spaces can be complex, and people should be vigilant about their digital footprint. Tracking mechanisms of web browsers, email providers, mobile apps, search engines, and social media platforms can compromise personal privacy. To enhance security in daily web browsing activities, sider these steps:

STEP 1: Be mindful of information shared on social platforms, and log out of your social media accounts, since social media sites can run analytics on your accounts even if you are not using them [16].

STEP 2: Use privacy-regarding browsers like duckduckgo.com and startpage.com that prioritize privacy and provide users with search results without personalized tracking.

STEP 3: Be aware of your social circles' online activities[16]: Recognize that the online presence of friends and family can impact your digital security. Advise them on safe online practices.

STEP 4: Be aware of your smartphone settings: Just like your laptops, your smartphones are also a crucial aspect of your online activities. Prioritize security by consistently logging out of apps that carry sensitive information. Logging off will also be beneficial for your work productivity. A study on monitoring smartphone usage found that by logging off and opting out from tracking cookies, the participants spent less time in each session [17].

- **Pay Attention to Software Updates:**

Frequent software updates are essential for good digital hygiene since failing to update your software or your web browsers can result in serious vulnerabilities.

A recent example demonstrating the importance of software updates arose in 2021, when Adobe revealed it is discontinuing Flash, with security vulnerabilities playing a large part in their decision [18]. The security vulnerabilities in question included the possibility of effectively bypassing web browser security measures. The computer emergency response teams (CERTs) had to address the issues. As this example shows, paying attention to updates is an important part of protecting your software and applications from vulnerabilities.

- **Use Strong Passwords[19]:**

Weak passwords that are easily guessable might expose individuals and organizations to the risk of data breaches. Thus, do not use your name or birthday as a password. The strongest passwords are the ones that will be easy to remember but hard to crack. Here are some tips on creating strong passwords, and how to remember them[19]:

STEP 1: Construct a sentence with different symbols, which will include uppercase and lowercase letters. For example, a sentence like "I Like Apples but I Hate Oranges" can be transformed into "IL@bIH0"

STEP 2: Use two-factor authentication: In addition to creating robust passwords, enhance your security with two-factor authentication (2FA). The authentication adds an extra layer of security by requiring a second verification step, such as a code sent to your mobile device, which will reduce the risk of authorized access.

STEP 3: Keep your passwords confidential, and store them securely if needed with a password manager, or authenticator app such as Dashlane or 1Password. (However, keep in mind that the security of these managers is only as strong as their weakest link!)

STEP 4: Ensure the safety of your passwords by regularly updating them.

- **Cautious Clicks: Be Aware of Phishing[14]:**

Phishing aims to trick people into giving their sensitive information by acting like a trustworthy source. Phishing is a serious crime. If scammers trick people into giving personal information, they could access their email, bank, or social media accounts. Therefore, if something looks a little out of the ordinary, or maybe an email asks you to verify personal information, especially with an attachment or a link they urge you to click, first of all, trust your instincts, and think before you click.

Unit 2 - Monitoring, Review, and Continuous Improvement of Digital Hygiene Practices

Think of your digital presence as a valuable asset like your house or your car. As you would be required to have regular maintenance sessions to keep your car or house safe and functional, in the same way, checking your digital hygiene practices is important to continuously keep your systems safe and functional. In this unit, we will look into the practices you can realize at the institutional and individual level to keep your competencies updated as the technology excels.

Institutional Level Practices

Here are some of the tools and methods that can be helpful to monitor, assess, and improve your digital hygiene at the institutional level.

- **Find the latest EU Regulations:**

Understanding and implementing the latest regulations help institutes identify the most pressing issues, and act accordingly to mitigate threats and harness benefits.

One of the most serious challenges that policymakers were concerned about is AI. On December 9th, 2023, the European Union introduced a new law called the "AI Act" which aims to "harness the potential benefits of the technology, while trying to protect against its possible risks, like automating jobs[20]." Staying informed of the latest European Union regulations on AI is crucial for responsible and authorized digital practices. You can review updated regulations such as the AI Act, online from the legislations page of the European Union, to ensure compliance with guidelines and avoid potential legal implications.

- **Security Check-Ups:**

Conducting a comprehensive review of your security settings is crucial in terms of monitoring the efficiency of your digital hygiene guidelines. You can use the routine security check-ups of Google and Facebook that guide you through privacy measures, permissions, and control over your latest activities. You can also use online sources that let you search across multiple data breaches, like haveibeenpwnd.com to be aware of the risks and the frequency of data breaches.

- **SWOT Analysis:**

SWOT is an acronym for Strengths, Weaknesses, Opportunities, and Threats, and it is a strategic analysis method that will create a roadmap for defining the position of any organization and strategies for future development.

Here are some tips to keep in mind while conducting a SWOT Analysis for your organization according to a study on the e-readiness of businesses[21]:

1. **Preparation for SWOT Analysis:**
    a. START WITH A PURPOSE: Consider the purpose and the long-term effects of applying a SWOT analysis.
    b. DEFINE AREAS to be ANALYZED: Identify specific areas related to Digital Hygiene Culture, e.g., employee awareness, following security protocols, infrastructure, etc.
    c. ASSIGN TEAMS to the DEFINED AREAS: Form teams who are experts in the areas you want to analyze, and ensure that all different teams are aligned on the methodology for conducting the analysis
2. **Strengths and Weaknesses Analysis:**
    a. IDENTIFY YOUR STRENGTHS and WEAKNESSES: An organization's strengths and weaknesses are signs of the internal factors that show the effectiveness and ineffectiveness of that organization. It is important to include justifications for the decisions on a particular factor to be considered as a weakness. (For example, outdated applications can be considered as a weakness due to the susceptibility of attack to the systems).
    b. DETERMINE THE RELEVANCE OF IDENTIFIED ISSUES: Determining what is a weakness and what is a strength can be confusing. Researchers suggest [21] using the '100 points Method' to evaluate and prioritize them. Each team member can have 100 points assigned to a strength or weakness, and the more points assigned, the more significant it is considered. After everyone assigns their points, the team averages them to determine their overall importance.
3. **Opportunities and Threats Analysis:**
    a. Evaluate the relevance and probability of threats by trying to organize them into these categories: economic, social, political, technological, and environmental.
    b. Calculate the opportunities associated with each development. These could be financial resources, an increase in the public interest, or international opportunities.
4. **Development of SWOT Matrix:** Select the strengths, weaknesses, opportunities, and threats, and group them according to the highest significance for your organization's Digital Hygiene Culture. Develop action plans based on identified strategies that might: (1) focus on correcting the weaknesses by taking advantage of your opportunities, (2) focus on taking advantage of a strength to benefit from an opportunity (3) focus on minimizing a weakness to avoid a threat, or (4) focus on taking advantage of a strength to prevent a threat.
5. **Review your results**: Regularly review the progress of implemented strategies and iterate the SWOT analysis periodically to adapt to new developments in the digital landscape.
    - **Regular BackUps:**

Backups are essential when there is a need to recover sensitive information, in the case of password loss, technical incidents, etc. Sometimes, monitoring the causes of a system crash is also possible by reviewing the security vulnerabilities or errors in the system. Using an open-source backup system, such as UrBackUp, which allows you to keep a copy of your documents, can be a valuable tool to monitor and review your digital hygiene practices in the case of an emergency.

Individual Level Practices

Each individual plays a significant role in developing a digital hygiene practice, and numerous steps can be taken to review, monitor, and develop your existing practices. Here are some ways to improve your digital hygiene on an individual level.

- **Awareness and Education:**

Embracing digital literacy is not just about knowing tools and methods, but also understanding the ever-evolving technological landscape as well. Educating ourselves about online threats, and staying up to date can be achieved through participation in continuous learning opportunities such as Microsoft Digital Literacy Courses, in which participants can learn about the basics of digital literacy, such as working with a computer. as well as advanced competencies such as creating content online. Similarly, researchers[22] point out the importance of teaching about media literacy, and safe and responsible internet use, which should reflect real-life experiences and interests of the individuals.

- **Responsible Online Behavior:**

Our online behavior has real-world consequences. As highlighted in academic studies[23] it is critical to engage ethically online, as well as being digitally literate. Responsible online behavior involves engaging in online discussions with respect and sensitivity. Furthermore, being aware of digital policies contributes to a safer and more respectful online community. If you are not sure about if your digital actions entail good practices. You can use the University of Michigan's Good Digital Citizen guide.

- **Review and Adaptation:**

Just like every aspect of the digital world, the technological landscape is dynamic and requires us to continuously adapt our practices. Therefore, reviewing our digital actions being adaptive to scams, recognizing phishing attempts, and being cautious with what you are downloading, are essential aspects of maintaining online safety.

A tool that can help you review practices, and get updated regularly is The Digital Competence Framework or DigComp. It is a reference tool for institutions, individuals, and educators which is developed by the EU

and keeps being updated with its last version 2.2 as of this handbook's publication date. DigComp is available on the EU Publications' website.

Regular updates to DigComp ensure that the framework remains relevant and reflective of the current digital environment. Just like DigComp, you can also review and update your digital hygiene practices to ensure that they align with the current needs of your organization, and consider including skills related to emerging technologies.

Unit 3 - The Future of Digital Hygiene: Challenges and Opportunities

As we head into the future, we are expected to see new challenges and opportunities in technological developments. The evolving landscape of digital technologies, especially Artificial Intelligence (AI), creates new complexities, as it gains more abilities and skills. Understanding these complexities and opportunities is essential to ensure a safe, secure, and innovative experience for all. In this unit, we will look at some of the most pressing issues for the future of digital hygiene, with a specific focus on emerging technologies, and what might they bring for innovation.

A-Emerging Technologies

Several emerging technologies such as Blockchain, Robotics, Internet of Things (IoT), Augmented Reality (AR), and Virtual Reality (VR) have been expected to shape the future. Among these, Generative AI chatbots like ChatGPT have made the most headlines, ever since its inception in 2022.

The rise of AI brings new dimensions to digital hygiene and cybersecurity. AI technologies can "already answer questions, write poetry, generate computer code, and carry on conversations."[24] Some experts believe that AI will put many workers at risk since the jobs will be automated[25], whereas many companies are already using generative AI for their practices[26]. So how can an educational institution such as VET institutions can benefit from the possibilities of AI?

- **Enhancing Learning Experience:**

In the area of Vocational Education and Training, generative AI can have big potential to revolutionize the learning experience. Researchers suggest that AI can create realistic scenarios, simulations, or assessments that match the student's needs, interests, and abilities[27]. Realistic scenarios can offer hands-on, immersive experiences that can create crucial experiences for areas such as healthcare. In addition to that, healthcare education can benefit immensely from optimizing routine tasks, making diagnoses, or offering personalized medicine which necessitates discussions about making conversations around privacy and robust governance [28].

- **Improving Teaching and Assessment:**

Adapting to Industry Trends and integrating AI into VET teaching and assessment in VET can help instructors optimize their workflow. NGOs and international organizations are already exploring the possibilities to improve the accuracy, completeness, and overall quality of the student's work, which can also provide immediate feedback[29]. Just as in healthcare education, giving AI the ability to rate student

work will undoubtedly raise questions about the ethics of AI, an important discussion point that teachers and parents should keep in mind.

- **Adaptive Learner Management Systems:**

Learning Management Systems (LMS) have already expanded the horizons of VET teachers as they offer teaching and learning materials in one location, as well as tracking learner progress and performance[30]. With AI, LMS has increased the possibility to revolutionize LMS [31]. AI-powered LMS can do advanced tasks beyond automation which can include predicting student performance, thus allowing teachers to create strategies for student performance improvement [32]

B-Regulatory Challenges

In the above units we have already explored how new technological advancements become more game-changing in various industries and educational systems. These advancements require all stakeholders to be responsible and encouraging for the safer usage of emerging technologies. Issues such as data privacy, algorithmic bias, ethical usage, and accountability require comprehensive regulatory frameworks.

- **Data Privacy in Education**

In the context of education, and especially online education handling large amounts of data, there are concerns about privacy and security [33]. Unauthorized access to a cloud or misuse of sensitive information poses a significant risk to educational institutions, and since 2018, The EU General Data Protection Regulation (GDPR), has required all establishments inside and outside the EU to comply with its objections for the protection and movement of personal data [34]. Therefore it is encouraged for every VET institution to monitor their compliance with GDPR and apply necessary measures as it evolves.

- **Algorithmic Bias**

An AI-powered LMS may inherit biases from the data used to train it. In terms of employment, AI-powered employment procedures can be especially harmful to some groups, as discovered in the case of an Amazon recruitment process where the predictive system was trained with a majority of male candidates' resumes. This created a bias where the male candidates became more preferable over women candidates [35]. Teachers themselves should be aware of this aspect of AI-powered systems, and cross-check on their own biases about students. It is also increasingly important for policymakers to encourage the development of auditable and transparent algorithms [36].

- **Ethics of Emerging Technologies**

Similar to the concerns about algorithmic bias, the integration of emerging technologies such as AI in education poses significant questions. What should be the role of emerging technologies in education in

terms of decision-making? Are there significant differences between diverse student groups on how emerging technologies impact their learning?

In the realm of AI, researchers consider privacy, bias, surveillance, and autonomy as key areas that point to ethical challenges for using these systems in education [37]. These areas as well as the sample questions above require more professional development opportunities for teachers to educate future generations on the ethical use and development of AI. In this context, initiatives like the EU's Digital Competence Framework (DigComp) can serve as a valuable guide.

Recognizing the importance of fostering ethical AI use, executive action makers such as the European Council are already in the process of defining ethical guidelines and promoting transparency that will keep the technology companies accountable. Apart from the AI Act regulation that is mentioned above, the European Union is also developing policies to support and foster the use of emerging technologies, such as VR, robotics, and biotechnology, which are expected to have greater effects on the citizens' lives [38].

C-Opportunities for Innovation

According to a 2021 OECD Report, Virtual Reality, Augmented Reality, Robotics, and Artificial Intelligence became increasingly widespread in VET for many industries, such as logistics, agriculture, hospitality, energy, and information technology, and it will become even more prevalent in the coming years [39]. In this section, we will look at how various industries are already utilizing these technologies and what potential lies ahead.

- **Information Technology (IT)**

Emerging Technologies such as virtual reality cloud labs can provide IT students with hands-on experience in diverse areas such as network configuration or cybersecurity [40]. Cybersecurity Labs [Insert Glossary Term here] simulates cyber threats and attacks, offering VET students a practical environment to understand the vulnerabilities in digital systems without having any real-world risks. Systems like High-Performance Computing [Insert Glossary Term Here], as well as Blockchain [Insert Glossary Term Here], offer new ways of training for cybersecurity [41].

- **Logistics and Transportation**

Commercial products like simulation games can help students tackle real-world challenges, and in the case of logistics, a commercially available game called Truck & Logistics Simulator does exactly that, where students can perform logistic tasks from beginning to end [39]. As technology plays a crucial role in the planning of complex tasks, VET providers, teachers, and students need to practice good digital hygiene and secure the integrity of information in the logistics networks while sharing information with commercialized products.

- **Agriculture**

From drones to AI, emerging technologies have the potential to increase the productivity of agriculture and farming practices, reduce environmental impact, and ensure increased incomes. Higher-resolution drone survey models can result in more efficient irrigation planning and more precise crop and livestock monitoring [42]. Similarly, AR can be used to advance smart farming [43] which aims to minimize risks, boost crop yields, and decrease stress in agribusiness [44]. The risks associated with using some of these technologies should not be neglected though [45]. By maintaining good cyber hygiene and incorporating responsible AI practices, the risks of using AI, AR, and other emerging technologies can be mitigated.

- **Hospitality**

Hospitality is one of the significant sectors in many countries in Europe, contributing to the economy while providing millions of jobs. Emerging Technologies can offer immersive learning experiences for hospitality and tourism students. Simulations of hotel management, and customer service scenarios powered by the Internet of Things [Insert Glossary Definition Here] that enable controlling room temperature, lighting, and other features can create better experiences for guests[46]. VR training models that are experienced with wearing a headset have already been utilized by prominent hospitality leaders of the industry [47]. The simulated world experience can help people learn faster, retain knowledge for a longer time, and be more engaged with training [48]. As much as these developments enhance the user experience, they can also be disruptive and disorienting to some users. That's why it is important to consider the user interface and user experience while implementing changes [49].

- **Renewable energy**

Emerging technologies such as AI-powered predictive maintenance systems, connected sensors, and augmented reality can accelerate the adoption of renewables [50] while simulating the operation and maintenance of solar panels, wind turbines, or hydroelectric systems allows students to gain practical skills in a controlled environment [51]. Just as in the agriculture sector, the use of emerging technologies comes with substantial risks which makes digital hygiene practices an important agent in safeguarding the systems[52]

The use of innovative technology such as robots, virtual reality (VR), augmented reality (AR), and simulators allows teachers to develop students' vocational skills while also fostering their digital and soft skills. These technologies are likely to become more common in VET in the years to come, as they have advantages in terms of flexibility, cost, and safety. [39] Teaching good digital hygiene is essential for integrating digital technology into our lives in safe, healthy, responsible, and respectful ways [9]

Unit 4 - Digital Hygiene Culture Good Practice Use Case:

In the previous units, we delved into the important aspects of cultivating a robust digital hygiene culture in both start-ups and VET institutions. We explored the significance of monitoring, reviewing, and continually improving digital hygiene practices to ensure a secure and efficient digital environment. These discussions highlighted the role of cultivating a good digital hygiene culture.

Now, as we step into the last part of Module 3, In Unit 4, we're about to dive into real-world applications with examples that showcase the practical use cases of digital hygiene principles.

Digital Hygiene Use Cases Around the World

- **A Specialized toolkit to promote digital hygiene practices (Serbia)**

A notable example of the application of good digital hygiene practices is a guide prepared by Share Cert, a foundation based in Belgrade emphasizing strategic cyber-security measures[53]. Through systematic categorization of the most common threats and security measures, this guidebook is supported through an open platform where individuals and organizations can be informed about the most pressing topics in the digital environment and have general tips about digital hygiene culture.

- **Public Awareness campaigns for the protection of Digital Rights (Greece)**

Another important initiative in terms of protection of digital rights is based in Greece and is called Homo Digitalis, a non-governmental organization (NGO) that focuses on the right to privacy, protection of personal data, prohibition of discrimination in digital spaces, and freedom of information. With its over 100 members, they actively participate in studies and conduct investigations on behalf of the public good which in return can help legislators understand better the issues related to digital rights [54].

- **A rapid response kit for an increasingly digital civic society (Global)**

The international networks of Computer Emergency Response Teams (CERTs) and Rapid Response Network (RaReNet) have collaborated to help rapid responders, digital security trainers, and tech-savvy activists to better protect themselves against the most common types of digital emergencies with what is called a Digital First Aid Kit, that guides a variety of issues [55]. Available in 13 languages and constantly evolving with outside contributions, the Digital First Aid Kit is a valuable source for promoting responsible and safe use of the Internet.

- **Building resilient tools to keep track of digital hygiene practices for the civic society (Global)**

The Center of Digital Resilience is a non-profit organization that operates in over 20 countries intending to establish resilient digital systems to ensure the safety of civic society [56]. Their projects include the provision of services and tools, such as a crowdsourcing tool designed for the identification and reporting of false

information, a digital platform for reporting security issues, a visualization tool for monitoring threats and attacks to the digital systems, and a community tool aimed to create a strong participation network within the CiviCERT.

- **Networks that facilitate exchange among response teams globally content to keep track of digital hygiene practices for the civic society (Global)**

CiviCERT is a network that brings CERTs, Independent Internet Content, and Service Providers, as well as NGOs and individuals [57]. The members of the network perform, coordinate, and support the response to digital security incidents reported to them in a collaborative mechanism where the viewpoint of other partners is needed. CiviCERT itself keeps up with good digital hygiene practices, where the members communicate over encrypted platforms, like an encrypted mailing list and a Malware Information Sharing Platform, to share information on emerging threats to civil society, and templates to ensure reliable and standardized procedures to handle emergencies.

- **Encouraging digital human rights in developing countries in (West Asia and North Africa)**

SMEX is an NGO that advocates for human rights in digital environments in West Asia and North Africa [58]. In terms of digital hygiene practices, they offer support to internet users, activists, and human rights organizations for their cybersecurity problems, and create programs to inform the general public about the regulations, and internet law. SMEX also actively collaborates with local and international partners to promote awareness and implementation of digital hygiene practices, fostering a safer online environment for individuals and organizations advocating for human rights in the digital space across West Asia and North Africa.

- **A Digital Skills Curriculum for K-12 Students (North America)**

The concept of digital hygiene is increasingly being held important in the educational systems worldwide. One of the organizations that specializes in preparing digital literacy material specific to K-12 students is Common Sense Media, an independent organization based in North America that aims to empower students, parents, and teachers with data-driven insights on the impact of media and digital environments on the kids' physical, emotional, social and mental needs [59]. Their research-backed Digital Citizenship Curriculum addresses important media and technology issues in schools such as: How to Protect Bullying? How to Protect Our Privacy? and How to Navigate Misinformation?

- **Educational Materials for Better Digital Literacy (North America)**

Center of Digital Literacy is an American non-profit that aims to promote the research and creation of open-source materials [60] as well as curriculum design tools, lessons, activities, and assessments that can be used and adapted to different educational contexts [61]. Media literacy is an important part of digital hygiene

practices and the emphasis on media literacy not only enhances digital hygiene but also cultivates a more informed and discerning society, better prepared to engage in the complexities of the digital world.

- **European Cyber Security Month (Europe)**

Each year October is celebrated as The European Cyber Security Month (ECSM), an important annual event organized by the European Union Agency for Cybersecurity (ENISA) and the European Commission [62]. Dedicated to strengthening cybersecurity awareness among EU citizens and organizations, ECSM is one of the many multi-dimensional approaches of the EU for fostering good digital hygiene practices. Throughout October, conferences, workshops, and webinars create an extensive campaign that not only raises awareness about cybersecurity but actively shares updated information and expert advice. Aiming to promote the safer use of the internet, ECSM provides digital hygiene tips and emerges as a comprehensive and collaborative effort, akin to global networks like CiviCERT and regional NGOs like SMEX, playing a vital role in promoting and sustaining good digital hygiene practices across the European Union.

- **Cybersecurity game for Preschool students (Global)**

Interland [63] is an interactive game by Google that is a part of "Be Internet Awesome" [64], an integrated program for promoting digital hygiene practices among young learners. As a dynamic and interactive game, Interland engages students through its gameplay, offering a hands-on approach to teaching some of the core aspects of good digital hygiene practices through gamification [65] SOURCE. Complex issues like privacy, phishing, hacking, and cyberbullying are translated to younger students in colorful animations that are suitable for their competency level [66] Overall, Interland stands as a noteworthy example of instilling good digital hygiene practices from a young age through using technology.

In this module, we have discussed the implementation of and the importance of good digital hygiene practices. We looked at topics such as developing a digital hygiene culture in your organization at various management levels, exploring methods for continuous improvement of these practices, being informed about future opportunities to harvest and challenges to overcome, and then exploring case studies from around the world.

Check out the other modules of this guidebook for further advice and strategies on good digital hygiene practices, and visit the website of Good Digital Hygiene for Startups.

Sources

Unit 1 - Building a Digital Hygiene Culture in Startups and VET Institutions

[1] Boulet, C. (2006). Digital Hygiene: Clean Living on a Dirty Network. *Interface: The Journal of Education, Community, and Values 6(3).* Retrieved from: Digital Hygiene: Clean Living on a Dirty Network (core.ac.uk) [Access Date 05.12.2023]

[2] Groysberg, B., Lee, J., Price, J., & Cheng, J. Y.-J. (2018, January-February). The leader's guide to corporate culture. *Harvard Business Review.* Retrieved from: The Leader's Guide to Corporate Culture (hbr.org) [Access Date 05.12.2023]

[3] Trevors, M. (2017). Cyber hygiene: 11 essential practices. Software Engineering Institute Blog. Retrieved from https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/ [Access Date 05.12.2023]

[4] Ly, B. The Interplay of Digital Transformational Leadership, Organizational Agility, and Digital Transformation. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01377-8

[5] Harvard Business School Online. (n.d.). *How to Become a More Effective Leader.* Harvard Business School Publishing. Retrieved from https://info.email.online.hbs.edu/leadership-ebook

[6] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology,* 10, 1938. https://doi.org/10.3389/fpsyg.2019.01938

[7] Cisco. (n.d.) Cisco Learning Network Store. Retrieved from https://learningnetworkstore.cisco.com/

[Access Date 06.12.2023]

[8] European Union Agency for Cybersecurity (ENISA). (n.d.). Online training material for cybersecurity specialists: Technical and operational. ENISA. Retrieved from https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#identification_handling [Access Date 06.12.2023]

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

[10] Glazer, K. (2017, March 22). A quick guide to good digital hygiene. *Literacy Now*. Retrieved from https://www.literacyworldwide.org/blog/literacy-now/2017/03/22/a-quick-guide-to-good-digital-hygiene

[Access Date 06.12.2023]

[11] Documenting Digital Attacks (n.d). Digital First Aid. Retrieved from https://digitalfirstaid.org/documentation/

[12] Saraf, A. (2021, May 14). Three steps to healthy digital hygiene. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/05/14/three-steps-to-healthy-digital-hygiene/

[Access Date 11.12.2023]

[13] Kaspersky. (n.d.). Cyber hygiene habits: 11 ways to improve your security. Retrieved from https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[14] Cybersecurity and Infrastructure Security Agency (CISA). (2022). 4 things you can do to keep yourself cyber safe. Retrieved from https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe [Access Date 11.12.2023]

[15] CHAYN. (2018). *Do it Yourself Online Safety.* Retrieved from https://chayn.gitbook.io/diy-online-safety/english [Access Date 07.12.2023]

[16] Torbet, G. (2019, February 3). Social media sites can predict your behavior even if you don't use them. *Digital Trends.* Retrieved from https://www.digitaltrends.com/social-media/social-media-privacy-friends-prediction/

[17] Toth.R., & Trifonova, T. (2021). Somebody's Watching Me: Smartphone Use Tracking and Reactivity. *Computers in Human Behavior Reports, 4*, *100142*, https://doi.org/10.1016/j.chbr.2021.100142

[Access Date 07.12.2023]

[18] Brooks, T. (2021, July 29). Why You Should Update Your Web Browser. *How-To Geek.* Retrieved from https://www.howtogeek.com/725165/why-you-should-update-your-web-browser/ [Access Date 08.12.2023]

[19] Barrons, M. (2016, September 12). How to Create Secure Passwords You Won't Forget. *InfoWare Group Blog.* Retrieved from https://infowaregroup.com/blog/how-to-create-secure-passwords-you-won't-forget [Access Date 08.12.2023]

Unit 2 - Monitoring, Review, and Continuous Improvement of Digital Hygiene Practices

[20] Scott, M. (2023, December 8). Europe's plan to tame Big Tech: A new legal framework. *The New York Times*. Retrieved from E.U. Agrees on AI Act, Landmark Regulation for Artificial Intelligence - The New York Times (nytimes.com)

[21] Rehak, D., & Grasseova, M., (2011). The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis. In M. Alshawi & M. Arif (Eds.), *Cases on E-Readiness and Information*

Systems Management in Organizations: Tools for Maximizing Strategic Alignment (1st ed., pp. 162-184). IGI Global. https://doi.org/10.4018/978-1-61350-311-9

[22] Gleason, Benjamin & von Gillern, Sam. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. Educational Technology and Society. 21. 200-212. https://www.researchgate.net/publication/322733013_Digital_citizenship_with_social_media_Participatory_practices_of_teaching_and_learning_in_secondary_education [Access Date 20.12.2023]

[23] Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and Responsible Internet Use in a Connected World: Promoting Cyber-Wellness. *Canadian Journal of Learning and Technology, 47*(4), Special Issue.

Unit 3 - The Future of Digital Hygiene: Challenges and Opportunities

[24] Metz, C. (2023). What's the Future of AI? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/31/technology/ai-chatbots-benefits-dangers.html?searchResultPosition=1

[25] Gleason, Benjamin & von Gillern, Sam. (2023). Tinkering With ChatGPT, Workers Wonder: Will This Take My Job? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html

[26] Banholzer, M., Fletcher, B., LaBerge, L., & McClain, J. (2023, August 31). Companies with Innovative Cultures Have a Big Edge with Generative AI. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/companies-with-innovative-cultures-have-a-big-edge-with-generative-ai [Access Date 21.12.2023]

[27] Chng, E., Tan, A.L. & Tan, S.C. Examining the Use of Emerging Technologies in Schools: a Review of Artificial Intelligence and Immersive Technologies in STEM Education. Journal for STEM Educ Res 6, 385–407 (2023). https://doi.org/10.1007/s41979-023-00092-y [Access Date 21.12.2023]

[28] Spatharou, A., Hieronimus, S., & Jenkins, J. (2020, March 10). Transforming healthcare with AI: The impact on the workforce and organizations. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/industries/healthcare/our-insights/transforming-healthcare-with-ai

[29] Kopp, W., & Thomsen, B. S. (2023, May 1). How AI can accelerate students' holistic development and make teaching more fulfilling. *World Economic Forum.* Retrieved from

https://www.weforum.org/agenda/2023/05/ai-accelerate-students-holistic-development-teaching-fulfilling/

[30] Pappas, C., (2016, January 7). The Top 8 Benefits Of Using Learning Management Systems. *Elearning Industry.* Retrieved from https://elearningindustry.com/top-8-benefits-of-using-learning-management-systems

[31] Seo, K., Tang, J., Roll, I. *et al.* The impact of artificial intelligence on learner–instructor interaction in online learning. *International Journal of Educational Technology in Higher Education* 18, 54 (2021). https://doi.org/10.1186/s41239-021-00292-9

[32] Yadav, N. R., & Deshmukh, S. S. (2023). Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics. In *Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022)* Retrieved from https://www.atlantis-press.com/article/125986295.pdf

[33] Duball, J. (2020). Shift to Online Learning Ignites Student Privacy Concerns. *International Association of Privacy Professionals (IAPP).* Retrieved from https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/

[34] United States International Trade Administration. (n.d.). European Union - Data Privacy and Protection. Retrieved from https://www.trade.gov/european-union-data-privacy-and-protection

[35] Gonzalez, G. (2018, October 10). Amazon Abandons AI Recruiting Tool That Showed Bias Against Women. *Inc.* Retrieved from https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html

[36] Gatzemeier, S. (2021, June 18). AI Bias: Where Does It Come From and What Can We Do About It? *UC Berkeley School of Information Blog.* Retrieved from https://blogs.ischool.berkeley.edu/w231/2021/06/18/ai-bias-where-does-it-come-from-and-what-can-we-do-about-it/

[37] Akgun, S., Greenhow, C. Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI Ethics* 2, 431–440 (2022). Retrieved from https://doi.org/10.1007/s43681-021-00096-7

[38] Polluveer, K. (2023). Innovation Policy. *European Parliament Fact Sheet.* Retrieved from https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.6.pdf

[39] OECD (2021), Teachers and Leaders in Vocational Education and Training, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/59d4fbb1-en

4. Promoting innovative pedagogical approaches in vocational education and training | Teachers and Leaders in Vocational Education and Training | OECD iLibrary (OECD-ilibrary.org)

[40] eduLAB Pty Ltd. (2020, August 12). eduLAB Introduction Video. *Vimeo.* Retrieved from https://vimeo.com/447337687

[41] N.d. (2022, March 27). 7 Technology Innovations That Will Impact Cybersecurity in 2022 and Beyond. *Cloud Security Alliance Blog.* Retrieved from 7 Technology Innovations That Will Impact Cybersecurity in 2022 | CSA (cloudsecurityalliance.org)

[42] World Economic Forum. (2021, March). Artificial Intelligence for Agricultural Innovation. *Community Paper.* Retrieved from WEF_Artificial_Intelligence_for_Agriculture_Innovation_2021.pdf (weforum.org)

[43] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://blog.marketresearch.com/the-increasing-adoption-of-augmented-reality-ar-in-agriculture

[44] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://eos.com/blog/smart-farming/

[45] Tzachor, A., Devare, M., King, B., et al. (2022). Responsible artificial intelligence in agriculture requires a systemic understanding of risks and externalities. *Nature Machine Intelligence, 4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4

[46] Bettencourt, J. (2023, November 16). How the hospitality industry is using AR, and VR for the guest experience. *Hotel Management.* Retrieved from https://www.hotelmanagement.net/tech/how-hospitality-industry-using-ar-vr-guest-experience

[47] Kover, A. (2020, March 10). A new perspective on hospitality: How Hilton uses VR to teach empathy. *Facebook Reality Labs Tech Blog.* Retrieved from https://tech.facebook.com/reality-labs/2020/3/a-new-perspective-on-hospitality-how-hilton-uses-vr-to-teach-empathy/

[48] Guenther, D. (2021, September 9). Virtual Reality training prepares hospitality workers for the next era of travel. *Medium.* Retrieved from https://medium.com/@DanielGuenther/virtual-reality-training-prepares-hospitality-workers-for-the-next-era-of-travel-7a8d5d3b8be5

[49] Pencarelli, T. The digital revolution in the travel and tourism industry. *Inf Technol Tourism* 22, 455–476 (2020). Retrieved from https://doi.org/10.1007/s40558-019-00160-3

[50] Amon, C., Slaughter, A., & Motyka, M. (2018, September). Global renewable energy trends. *Deloitte.* Retrieved from https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/global-renewable-energy-trends.html

[51] Travelers. (n.d.). Predictive Maintenance at Solar and Wind Installations. Retrieved from https://www.travelers.com/resources/business-industries/energy/predictive-maintenance-at-solar-and-wind-installations

[52] Victor, D. G. (2019, January 10). How artificial intelligence will affect the future of energy and climate. *Brookings Institution.* Retrieved from https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

UNIT 4 - Digital Hygiene Culture Good Practice Use Case:

[53] ShareCert Toolkit. (n.d.). Retrieved from Cybersecurity Toolkit

[54] Homo Digitalis. (2022, July 13). A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million. Retrieved from https://homodigitalis.gr/en/posts/12155/

[55] Digital First Aid. (n.d.). Retrieved from Digital First Aid Kit

[56] Digiresilience. (n.d.). Retrieved from Center for Digital Resilience

[57] CivicERT. (n.d.). Retrieved from CiviCERT

[58] SMEX. (n.d.). Retrieved from SMEX

[59] Common Sense Media. (n.d.). Digital Literacy and Citizenship. Retrieved from https://www.commonsensemedia.org/what-we-stand-for/digital-literacy-and-citizenship

[60] Center for Media Literacy. (2005). Five Key Questions of Media Literacy. Retrieved from https://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf

[61] Center for Media Literacy. (n.d.). Retrieved from https://www.medialit.org/https://www.medialit.org/

[62] European Cyber Security Month. (n.d.). Retrieved from https://cybersecuritymonth.eu/

[63] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us/interland/

[64] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us

[65] Bogardus Cortez, M. (2018, April 17). The Digital Citizenship Curriculum: Digital Literacy, Cyber Hygiene and More. *EdTech Magazine.* Retrieved from How to Design Your Digital Citizenship Curriculum - EdTech (edtechmagazine.com)

[66] Bogardus Cortez, M. (2014, July 24). Digital Citizenship Game by Google & ITSE Aims to Educate. *EdTech Magazine.* Retrieved from Digital Citizenship Game by Google & ITSE Aims to Educate | EdTech Magazine

---

[12*] Durbin, S. (2019). The top 3 global cybersecurity threats of 2020. *Dark Reading.* Retrieved from **https://www.darkreading.com/vulnerabilities-threats/crystal-ball-the-top-3-global-cybersecurity-threats-for-2020** [Access Date 06.12.2023]

[13*] Ponemon, L., & Beri, S. (2014). *Data Breach: The Cloud Multiplier Effect.* Retrieved from **https://www.slideshare.net/Netskope/data-breach-the-cloud-multiplier-effect** [Access Date 06.12.2023]

[14*] Hadlington, L. (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*. **https://doi.org/10.1016/j.heliyon.2017.e00346**

[15*] Telefonica Tech. (2022, November 10). Human Factors in Cybersecurity: Protect Yourself. *Telefonica Tech Blog.* Retrieved from **https://telefonicatech.com/en/blog/human-factors-in-cybersecurity** [Access Date 11.12.2023]

[XXXXX] Irwin, L. (2020, June). *5 ways to detect a phishing email – with examples*. ITGovernance. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email [Access Date 08.12.2023]

[XXXXXXX] Federal Trade Commission Consumer Information (2019, May). *How To Recognize and Avoid Phishing Scams.* https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [Access Date 08.12.2023]

[XX] DCAF (Geneva Centre for Security Sector Governance), Babić, V., & Bratić, A. (2022, October). *Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs.* Retrieved from **https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf** [Access Date 06.12.2023]