Digital Hygiene Handbook for VETs and Start-Ups

Edited By
Prof. Dr. Tuğba Uçma Uysal
Assoc. Prof. Dr. Ceray Aldemir

GOOD START

Good Digital Hygiene for Startups

Gazi Kitabevi

Digital Hygiene Handbook for VETs and Start-Ups

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Digital Hygiene Handbook for VETs and Start-Ups

Edited By
Prof. Dr. Tuğba Uçma Uysal & Assoc. Prof. Dr. Ceray Aldemir

"En İyi Akademi, Bir Kitaplıktır."

Digital Hygiene Handbook for VETs and Start-Ups

Edited By
Prof. Dr. Tuğba Uçma Uysal: 0000-0002-3652-7221
Assoc. Prof. Dr. Ceray Aldemir: 0000-0002-7996-4886

ISBN • 978-625-365-692-8

Baskı • Ekim, Ankara 2024

Dizgi/Mizanpaj • Gazi Kitabevi
Kapak Tasarım • Gazi Kitabevi

Gazi Kitabevi Tic. Ltd. Şti.
Yayıncı Sertifika No: 44884

Merkez

Bahçelievler Mah. 53. Sok. No: 29 Çankaya/ANKARA
0.312 223 77 73 - 0.312 223 77 17
0.544 225 37 38
0.312 215 14 50
www.gazikitabevi.com.tr
info@gazikitabevi.com.tr

Sosyal Medya

gazikitabevi
gazikitabevi
gazikitabevi

Content Table

PREFACE

This e-book is the culmination of the "Good Digital Hygiene for Startups" project, supported by Erasmus+ under Project No: 2022-1-LV01-KA220-VET-000086725. In today's increasingly digital world, startups and Vocational Education and Training (VET) institutions face unique challenges in maintaining secure and efficient operations. Recognizing this, the project was developed to help small businesses and educators improve their digital hygiene practices—ensuring that both their data and systems are protected from cyber threats.

The e-book brings together practical insights, tools, and strategies crafted during the project, offering an accessible guide for anyone looking to boost their digital security. By exploring these concepts, readers can take proactive steps toward creating a safer and more secure digital environment for their organizations. In today's rapidly developing digital landscape, where our personal and professional lives are increasingly interconnected through technology, the importance of maintaining secure digital practices has never been more critical.

As digital tools continue to transform industries across the board, including education and business, the concept of "digital hygiene" has emerged as a foundational principle for safeguarding sensitive information and ensuring smooth operations. This book, Digital Hygiene Handbook for VETs and startups, provides a comprehensive guide for professionals in both Vocational Education and Training (VET) environments and startups. It focuses on practical strategies to integrate digital hygiene into daily operations, offering solutions to mitigate cybersecurity risks while fostering a culture of safety and innovation.

This handbook is unique in its dual focus on VET institutions and startups, recognizing that both sectors share common challenges yet operate within different contexts. VET institutions are tasked with preparing students for the workforce while navigating complex educational technologies, whereas startups must alter rapid growth with limited resources, often making them prime targets for cyber threats. The blend of theoretical insights and practical advice presented in this book ensures that it caters to both audiences, offering specific solutions tailored to their needs.

The journey of creating this book involved a collaboration of experts across the fields of education, technology, and business. Their collective wisdom shaped each chapter, bringing together best practices, lessons learned, and innovative approaches to digital hygiene. Every chapter is designed to provide readers with the tools they need to implement robust digital hygiene practices in their own

contexts, from foundational knowledge to advanced strategies for long-term sustainability.

The structure of the book reflects this dual focus. The early chapters lay the groundwork for understanding the significance of digital hygiene within VET and startup environments, including discussions on cybersecurity, data management, and ethical digital behavior. Subsequent chapters delve into the development of a customized curriculum for VETs, offering tailored educational approaches and strategies that can be directly implemented within training programs. The final sections of the book explore the application of digital hygiene practices, providing real-world examples and case studies that illustrate how organizations can build and sustain a culture of digital resilience.

Chapter 1: Digital Hygiene for VET Professionals expands on the unique challenges and responsibilities faced by VET educators and trainers in today's technology-driven world. The chapter delves into why digital hygiene is essential in the context of VET education, emphasizing its role in ensuring a secure learning environment for students. It also explores the critical skills VET professionals need to foster digital safety and provides practical advice on how to incorporate digital hygiene into the VET curriculum. Real-world examples demonstrate how these practices can be effectively applied in educational settings, ensuring that VET trainers can lead by example and equip their students with essential digital skills.

Chapter 2: Digital Hygiene Customized Curriculum for VETs takes the principles introduced in the first chapter and turns them into a structured learning pathway. This chapter presents a fully customizable digital hygiene curriculum designed specifically for VET institutions. It breaks down the core learning areas—such as network security, data management, and mobile device protection—offering educators a clear framework for teaching these critical concepts. Beyond the theoretical components, the chapter also emphasizes practical implementation, guiding educators on how to assess their students' understanding of digital hygiene through feedback mechanisms and performance assessments. The chapter closes with a compelling case study illustrating how these practices have been successfully integrated into a VET institution.

Chapter 3: Implementing and Sustaining Digital Hygiene shifts the focus to the long-term sustainability of digital hygiene practices in both VET and startup environments. Here, we explore strategies for building a strong culture of digital hygiene that extends beyond individual efforts and becomes embedded in the organizational ethos. The chapter discusses the importance of continuous monitoring and improvement, helping institutions and startups adapt their practices as new technologies and threats emerge. Additionally, it touches on the challenges and opportunities that lie ahead in the future of digital hygiene, including the role of artificial intelligence and other technological advancements. This chapter is brought to life with an example of how one organization has

successfully maintained a culture of digital safety over time, illustrating the real-world benefits of sustained efforts.

Chapter 4: Understanding Digital Hygiene for Startups takes a deep dive into the startup world, where digital hygiene can make or break the success of a fledgling company. Startups, which often operate with limited resources and without the robust security infrastructure of larger firms, are particularly vulnerable to cyber threats. This chapter introduces a conceptual framework for startups to understand the essentials of digital hygiene, outlining the necessary steps to protect sensitive data, safeguard intellectual property, and maintain operational efficiency. It also highlights the consequences of neglecting digital hygiene, providing stark examples of how startups have suffered due to preventable cyber incidents. Good practice examples from successful startups are shared to inspire and guide others on their digital hygiene journey.

Chapter 5: Digital Hygiene Tools & Integration in Daily Routines equips startup leaders and VET educators with a practical toolkit for maintaining digital hygiene. This chapter introduces the best digital hygiene tools available, including password managers, two-factor authentication, antivirus software, and data backup solutions. It also provides guidance on how to make digital hygiene a habit within daily operations, ensuring that these practices become second nature to all employees or students. With a focus on real-world applications, the chapter includes a detailed case study that demonstrates how a startup successfully integrated digital hygiene tools into its workflows, resulting in enhanced security and operational efficiency.

Chapter 6: Implications of Digital Hygiene in Startups concludes the book with a comprehensive look at the broader implications of digital hygiene for startups. This chapter explores how implementing good digital hygiene practices can lead to long-term benefits, such as enhanced customer trust, improved operational scalability, and reduced risk of costly cyber incidents. Conversely, it also examines the potential threats and consequences that arise when digital hygiene is neglected, offering a sobering reminder of the importance of this foundational element. A good practice example illustrates how one startup successfully navigated a cybersecurity challenge by implementing strong digital hygiene measures, offering a roadmap for others to follow.

This book was created with the aim that it will serve as a valuable resource for both VET professionals and startup leaders as they navigate the complexities of the digital world. I would like to extend my deepest gratitude to the experts and professionals who contributed their insights and experiences to this work. Their knowledge and dedication have been instrumental in shaping this handbook into a practical and insightful guide.

This handbook was made possible through the dedication and expertise of many individuals. We would also like to thank my colleagues, whose support and collaboration made this book possible. Their tireless efforts, from research to

editing, have ensured that this handbook is both comprehensive and accessible. Finally, we would like to express our gratitude to the Erasmus + European Union, whose support was instrumental in bringing this project to life.

Prof. Dr. Tuğba Uçma Uysal

Assoc. Prof. Dr. Ceray Aldemir

Chapter 1

Digital Hygiene for VET Professionals

Krista Brusova[1]

Uldis Zandbergs[2]

The term digital hygiene is one of the most important concepts in today's world, where educational and training tools and platforms have been integrated into virtually every part of life. Vocational Education and Training (VET) providers, who typically handle sensitive, digitalized data with the use of digital platforms for teaching and administrative functions, should ensure that the security of their data is protected, they concur with prevailing regulations, and that the whole learning environment is secure. Digital hygiene is a series of activities made to keep the safety, privacy, and moral conduct in the digital area and is in fact a major requirement for the VET trainers, teachers, and students.

This chapter discusses the relevance of digital hygiene for VET education, pointing out its contribution to data safety, promoting digital citizenship, faithful study and teaching. It also deals with the particular qualifications and characteristics of VET trainers and educators, synthesizing the frameworks serving as guiding principles for the attainment of these skills. At the very end, the chapter gets a bit more practical and argues the point how digital hygiene might be inflected to the VET curriculum; and it is enriched with accurate examples from best practice to show where it works well in the actual occupations.

1.1. 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

[1] Baltic Computer Academy (BDA), krista.brusova@bda.lv

[2] Baltic Computer Academy (BDA), uldis.zandbergs@bda.lv

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 for 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 that 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 practice 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 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 their customers and partners view them. 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 and manage the involvement of participants in them, or analyse data gathered during the training process. By maintaining 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 be 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 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 is 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 the 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 company level as well as 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.

1.2. 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 division 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 own 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),

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, 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 occasions this role develops and delivers cybersecurity training and awareness programs for staff which makes them assume the role of a VET trainer. And 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 in accordance with 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 national and international level that require careful attention to how VET organizations manage sensitive data of the participants of 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 VET curriculum, instructional materials, and learning activities; and 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 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 in order 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 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 competences 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 competences, 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 competences 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 competences.

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 competences 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 competences and supports educational institutions in designing training programs and policies aligned with contemporary educational needs.

The frameworks mentioned above while general in their nature towards identifying that 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.

1.3. 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 digital hygiene good 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 modern or future skills and based on the recent development of the digital environment these are the same skills that have been emphasized as skill 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 of the training process. Here are some important skills needed for a VET trainers and educators with regards to 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; 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; 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 and 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 digital environment or using modern digital tools; 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 to regulations and being respectful of the rights of the 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 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 competences 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 skill 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 practice in digital hygiene. A down-to-earth reference of some of the best practice is available as a Digital Hygiene Cheat Sheet [7]. It describes 12 principles of secure digital life that all require some knowledge of 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.

1.4. 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; analysing 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 time 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 in vocational and education training may require use of 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 integration 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 ro perform an administrative activity related to training, introduce some advice in 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 students' 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 own 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 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 subject. Assessment and certifications may be used to incentivize students and the form the results are presented in may require additional thought with regards to digital environment. The students may require help when acquiring and handling their new certification information or using their new qualification to enhance their employability.

You may notice that some of the options for the improvement of the VET training with regards to 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 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 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.

1.5. Good Practice Example – Digital Hygiene for VETs

In this section you will see some good practice examples of how digital hygiene can be introduced in VET organization for the safety of the organization and for 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 on-line training for their students to avoid costly and time-consuming travel and to provide the students with convenience of attending the training from their safe physical environments. The VET company has a staff of internal and external trainers that have different previous experience with providing on-line training and may have different knowledge and skills related to conducting such a training. The company also has internal employees that perform administrative activities related to training and handle information that is at times sensitive and should be addressed in accordance with 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 is:

- 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 rich experience for the students,
- keeping a certain level 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 students themselves,
- conducting evaluation 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 organization 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 withing Microsoft Teams environment and other tools used centrally and with an 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 own privileges in the Teams environment: systems administrator, training administrator (the person organizing training sessions before the training and analysing 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 a fully set physical training rooms were offered with secure connections to the internet. For those trainers that intended to use their own 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 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 on using additional Teams features like polls, quizzes, and whiteboard during sessions to engage students and enhance learning whenever possible. The use of additional tools and features were 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 regulations 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, and 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 on taking on the role of experts for external training materials and were encouraged to consult the internal training administrators of versions of training materials, student guidebooks and practice tests where applicable to reduce the damages 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: Use 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. The 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.

Conclusion

The term digital hygiene is one of the most important concepts in today's world, where educational and training tools and platforms have been integrated into virtually every part of life. Vocational Education and Training (VET) providers, who typically handle sensitive, digitalized data with the use of digital platforms for teaching and administrative functions, should ensure that the security of their data is protected, they concur with prevailing regulations, and that the whole learning environment is secure. Digital hygiene is a series of activities made to keep the safety, privacy, and moral conduct in the digital area and is in fact a major requirement for the VET trainers, teachers, and students.

This chapter discusses the relevance of digital hygiene for VET education, pointing out its contribution to data safety, promoting digital citizenship, faithful study and teaching. It also deals with the particular qualifications and characteristics of VET trainers and educators, synthesizing the frameworks serving as guiding principles for the attainment of these skills. At the very end, the chapter gets a bit more practical and argues the point how digital hygiene might be inflected to the VET curriculum; and it is enriched with accurate examples from best practice to show where it works well in the actual occupations.

Chapter 2

Digital Hygiene Customized Curriculum for VETs

Myra Qiu[3]

Adeyemi Banjo[4]

Digital hygiene has assumed a much larger and significant role in our daily lives. With 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 cyberthreats 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 which 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 were 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 program in development 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 orient with a short turnaround time. However, it is also designed to enable students to go at their own pace.

[3] Wittenborg University of Applied Sciences, myra.qiu@wittenborg.nl

[4] Wittenborg University of Applied Sciences, adeyemi.banjo@wittenborg.eu

2.1. 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 programme as well as instructors with relevant information with regards to the purpose, planning, structure, and assessment of the programme. Recognizing that not all organizations are the same and require the same level of digital hygiene skills, this module and the different components 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 programme.

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

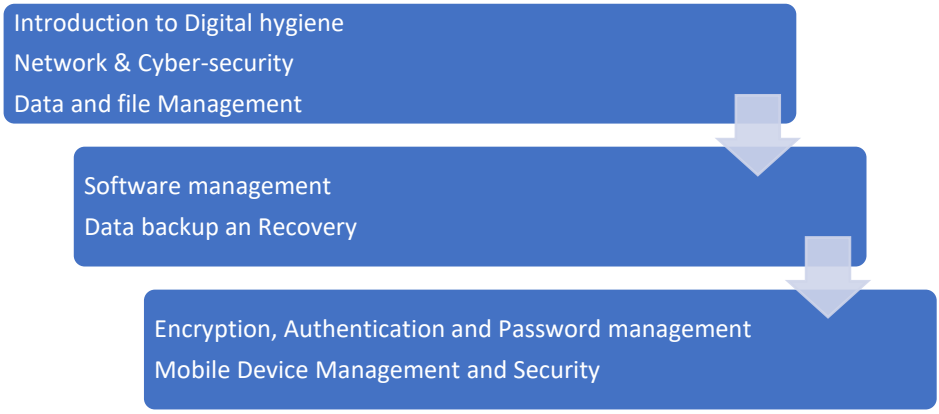
intelligence and technological advancements, ensuring relevancy and efficacy in addressing contemporary cybersecurity challenges.

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.

2.2. 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



2.2.1. Introduction to Digital Hygiene in VET Education

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 programme 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

Literature	Comments
Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.	This book provides a thorough introduction into 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 and SME owners and students looking to seeking 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.	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.

2.2.2. 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 invited to share insights and experiences, emphasizing current challenges and emerging technologies.

Recommended Literature

Literature	Comments
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.

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.

2.2.3. 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

Literature	Comments
Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition.	This book provides a comprehensive view on 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.

2.2.4. 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 with regards to software security such as poor password policies, insecure API's unpatched vulnerabilities, phishing, 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 the 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

Literature	Comments
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.

2.2.5. 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. It is crucial for all modern organizations to have proper backup and recovery policies, protocols, and systems in place. Most current organizations are data drive and consequently place a premium on the management of their data and informational resources. In principle most organizations and especially SME's 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

Literature	Comments
Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads.	This book 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	This gives you the questions to uncover the Data Backup And Recovery challenges you're facing and generate better solutions to solve those problems.
Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.	This book 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.	This book 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.

2.2.6. 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 it 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

Literature	Comments
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.
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.

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.

2.2.7. 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 Start-ups and SME's where being agile and reachable at all times has become a major criterion for success. While mobile technology has advanced such that most advanced smart phones are as powerful and versatile as laptops and desktops, the wireless nature of such devices makes them susceptible to malevolent actors seeking to gain unauthorize 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

Literature	Comments
Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition.	This book looks at the implication of the rapid integration of mobile devices into the organization's communication environment, the attendant security concerns and how these can be mitigated against.
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.

2.3. Digital Hygiene Assessment and Feedback Mechanisms for VETs

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 own 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.

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.

2.4 – Good Practice from VETs

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 in 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 their 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, which provides 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 from 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.

Chapter 3

Implementing and Sustaining Digital Hygiene

Vasileios Kratidis [5]

Sofia Nteliopoulou[6]

Today's institutions, whether startups or Vocational Education and Training (VET) units, are being technologically oriented. Still, with the continuous growth of modern technologies there arises a need for building and sustaining some level of a culture of hygiene on the digital space. Digital hygiene refers to those practices, actions and or behaviors and routines – regular or new – which are employed to discern, manage and use digital devices and resources in a secure, effective and efficient manner. Just as physical cleanliness is considered an important aspect of health, a form of hygiene applicable to the "wired" age is necessary for protecting information, improving mission processes, and protecting an organization or an individual's information assets from external breaches.

This chapter emphasises the significance of establishing and maintaining a culture of digital hygiene inside startups and vocational education and training institutions. It offers pragmatic solutions for integrating a framework of values and practices into the fundamental operations of these settings, fostering cybersecurity awareness, effective data management, and the ethical utilisation of digital tools. The objective is to enable organisations to implement continuous education, explicit policies, and optimal practices that guarantee enduring digital resilience. Startups and vocational education and training institutions can therefore reduce the risk exposure while enhancing productivity.

3.1. 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 first arose in early aughts to explain the principles for secure, organized and ethical digital practices, which aims 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

[5] Mathemagenesis, v.kratidis@mathemagenesis.com

[6] Mathemagenesis, s.nteliopoulou@mathemagenesis.com

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 which are based on collective responsibility and integrating safe digital practices.

This chapter explores 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 Leadership Level

In 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 actually 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. In order to guide their team through these changes, all leaders should first understand their own 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 in order 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, 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 foster 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 where 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 from a member of the 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 assessment 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 in 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 create 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 the daily web browsing activities consider 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 own digital security. Advise them on safe online practices.

STEP 4: Be aware of your smart-phone 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 to effectively bypass 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:**

  Weak passwords which are easily guessable might expose individuals and organizations to the risk of data breach. Thus, do not use your name or birthday as passwords. 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, 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 are 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.

3.2. 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 require 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 competences 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 policy makers were concerned about is AI. On December 9th, 2023, the European Union introduced a new law called "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 in 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, in order to ensure compliance with guidelines and avoid potential legal implications.

- **Security Check-Ups:**

Conducting a comprehensive review of your security settings are 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 through privacy measures, permissions and control over your latest activities. You can also use online sources that lets 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 Strength, 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 for the internal factors that shows 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 it in these categories: economic, social, political, technological and environmental.

b. Calculate the opportunities associated with each development. These could be financial resources, 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 new developments in the digital landscape.

- **Regular BackUps:**

  Backups are essential when there is a need to recover sensitive information, in the case of passwords 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 there are numerous steps that 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 behaviour 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 about 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 individual digital actions and 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 itself 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 it aligns with the current needs of your organization, and consider including skills related to emerging technologies.

3. 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.

3.3.1. 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 potentials to revolutionize the learning experience. Researchers suggest that AI can create realistic scenarios, simulations, or assessments that match the students' needs, interests, and abilities[27]. Realistic scenarios can offer hands-on, immersive experiences which can create crucial experiences for areas such as healthcare. In addition to that, healthcare education can benefit immensely from optimizing routine tasks, making diagnosis, or offering personalized medicine which necessitates discussions about making conversations around privacy and robust governance [28].

- **Improving Teaching and Assessment:**

  Adapting to Industry Trends, 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 students' 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's performance improvement [32]

3.3.2. 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), requires all establishments

inside and outside 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 themselves on their own biases about students. It is also increasingly important for policy makers to encourage the development of auditable and transparent algorithms [36].

- **Ethics of Emerging Technologies**

Similarly to the concerns about the algorithmic bias, 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' life [38].

3.3.3. 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 to tackle real-world challenges, and in the case of the 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, it is essential for VET providers, teachers and students 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 a 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, customer service scenarios powered by 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 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 allow 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]

3.4. 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 for 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 guide book 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) has 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 provides guidance for a variety of issues [55]. Available in 13 languages and constantly evolving with outside contributions, the Digital First Aid Kit is a valuable source in 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 over 20 countries with the goal of establishing 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 itself, 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 a 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. The complex issues like privacy, phishing, hacking and cyberbullying are translated to younger students in colorful animations which 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.

Conclusion

The term digital hygiene is one of the most important concepts in today's world, where educational and training tools and platforms have been integrated into virtually every part of life. Vocational Education and Training (VET) providers, who typically handle sensitive, digitalized data with the use of digital platforms for teaching and administrative functions, should ensure that the security of their data is protected, they concur with prevailing regulations, and that the whole learning environment is secure. Digital hygiene is a series of activities made to keep the safety, privacy, and moral conduct in the digital area and is in fact a major requirement for the VET trainers, teachers, and students.

In this chapter 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.

In a nutshell, this chapter discusses the relevance of digital hygiene for VET education, pointing out its contribution to data safety, promoting digital citizenship, faithful study and teaching. It also deals with the particular qualifications and characteristics of VET trainers and educators, synthesizing the frameworks serving as guiding principles for the attainment of these skills. At the very end, the chapter gets a bit more practical and argues the point how digital hygiene might be inflected to the VET curriculum; and it is enriched with accurate examples from best practice to show where it works well in the actual occupations.

Chapter 4

Understanding Digital Hygiene for StartUps

Wojciech Duranowski[7]

Olga Pankiv [8]

4.1 - Conceptual Framework of Digital Hygiene

In the rapidly evolving landscape of digital entrepreneurship, startups face a myriad of challenges ranging from fierce competition to resource constraints. Amidst these challenges, ensuring robust digital hygiene practices is crucial for the startups' sustainable growth and success. The concept of digital hygiene draws upon several theoretical frameworks and principles from various fields, including cybersecurity, information management, and organizational behavior. There are some key theories upon which the concept of digital hygiene is based:

Cybersecurity theory

Cybersecurity theory encompasses various principles and models aimed at understanding and addressing cyber threats and vulnerabilities. The CIA Triad (Confidentiality, Integrity, Availability) is a fundamental concept in cybersecurity theory, emphasizing the importance of protecting data from unauthorized access (confidentiality), ensuring data accuracy and reliability (integrity), and maintaining data accessibility for authorized users (availability). Other cybersecurity theories, such as the Defense-in-depth model and the Zero Trust model, provide frameworks for designing and implementing robust cybersecurity strategies to mitigate risks and defend against cyber-attacks.

Information management theory

Information management theory focuses on the effective management of information assets within organizations. The Information lifecycle management model is a theoretical framework that describes the stages through which information passes from creation to disposal, emphasizing the importance of managing information throughout its lifecycle to ensure confidentiality, integrity, and availability. The principles of data governance, data stewardship, and data quality management are also central to information management theory, guiding how organizations can govern and protect their data assets effectively.

[7] Fundacja Eduvibes, wduranowski@gmail.com

[8] Fundacja Eduvibes,pankiv.ola@gmail.com

Human factors theory

Human factors theory explores the role of human behavior, cognition, and decision-making in the context of cybersecurity. The Human Error Theory suggests that human error significantly contributes to cybersecurity incidents and data breaches, highlighting the importance of training, awareness, and usability in mitigating human-related risks. The Theory of Planned Behavior and the Technology Acceptance Model (TAM) are other theoretical frameworks that explain how individuals' attitudes, beliefs, and perceptions influence their behavior toward adopting cybersecurity practices and technologies.

Organizational behavior theory

Organizational behavior theory examines how individuals, groups, and structures within organizations interact and influence behavior. The technology-organization-environment framework is a theoretical model that explains the factors influencing the adoption and implementation of information technologies within organizations, including technological factors, organizational factors, and environmental factors. The diffusion of innovations theory, developed by Everett Rogers, explores how new ideas, technologies, and practices spread within societies and organizations, providing insights into the adoption and diffusion of digital hygiene practices within startups and other organizational contexts.

Compliance theory

Compliance theory addresses the factors influencing individuals' and organizations' compliance with rules, regulations, and norms. The theory of planned behavior and the theory of reasoned action are theoretical models that explain individuals' intention to comply with rules and regulations based on their attitudes, subjective norms, and perceived behavioral control. These theories provide insights into how startups and organizations can promote compliance with cybersecurity regulations and standards through education, training, incentives, and enforcement mechanisms.

Thus, the concept of digital hygiene integrates multidisciplinary perspectives and approaches to address the complex challenges of cybersecurity, information management, human behavior, and organizational dynamics within startups and other organizations. Also, additional concepts provide a foundation for understanding and implementing digital hygiene practices within startups, ensuring the protection, integrity, and resilience of their digital infrastructure and operations:

A) Cybersecurity

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, cyber-attacks, and data breaches. It encompasses various technologies, processes, and practices aimed at safeguarding digital assets and ensuring the confidentiality, integrity, and availability of information.

B) Data Privacy

Data privacy refers to the protection of personal and sensitive information from unauthorized access, use, or disclosure. It involves compliance with regulations and standards governing the collection, storage, and processing of data, such as GDPR, HIPAA, or CCPA, to safeguard individuals' privacy rights.

C) Risk management

Risk management involves identifying, assessing, and mitigating risks associated with operating in a digital environment. It includes implementing controls and measures to prevent, detect, and respond to potential threats and vulnerabilities that could impact a startup's operations, reputation, or financial stability.

D) Compliance and regulatory frameworks

Compliance with regulations and industry standards is essential for startups to ensure legal and ethical operations. Regulatory frameworks, such as GDPR, HIPAA, PCI DSS, or SOX, provide guidelines and requirements for data protection, security, and privacy that startups must adhere to avoid legal and financial repercussions.

E) Information security management systems (ISMS)

ISMS frameworks, such as ISO/IEC 27001, provide a systematic approach to managing and protecting information assets within organizations. They include policies, procedures, and controls for managing risks, ensuring compliance, and continuously improving information security practices.

F) Data governance

Data governance refers to the management and oversight of data assets within an organization. It involves establishing policies, processes, and controls for data quality, integrity, and security to ensure that data is managed effectively, responsibly, and ethically.

G) Incident response and business continuity planning

Incident response and business continuity planning involve preparing for and responding to cybersecurity incidents and disruptions. Startups should develop comprehensive incident response plans and business continuity strategies to mitigate the impact of cyber-attacks, data breaches, or other disruptions on their operations and reputation.

So digital hygiene encompasses the set of practices and protocols aimed at maintaining the security, efficiency, and integrity of digital assets and operations. This conceptual framework delineates the key components of digital hygiene tailored to the unique needs and constraints of startups. The Scheme of the Conceptual Framework of Digital Hygiene for Startups is shown in Figure 1.

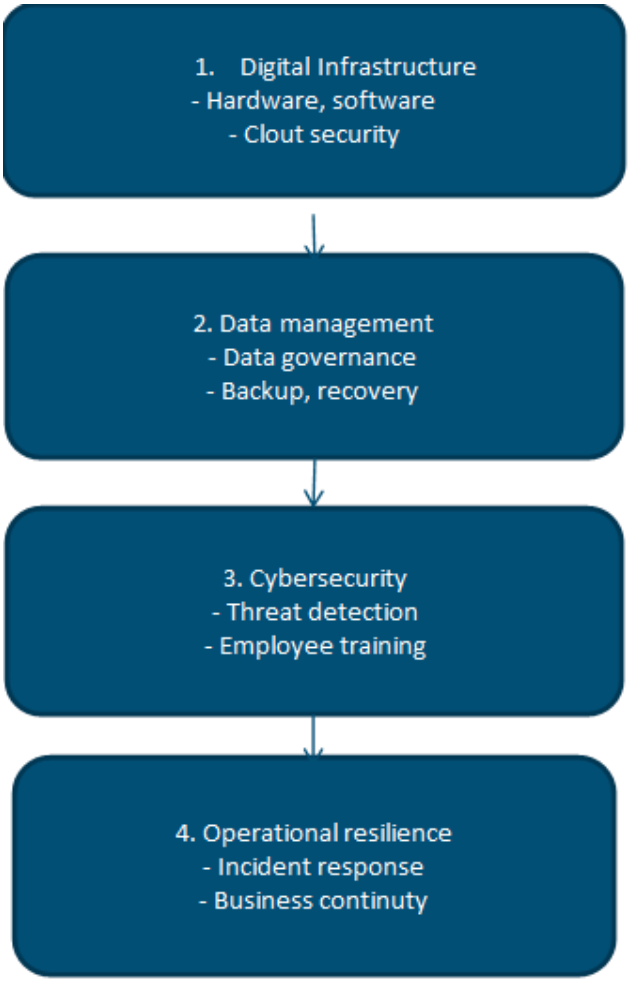


Figure 1. Scheme of Conceptual Framework of Digital Hygiene for Startups

This scheme outlines the four main components of Digital Hygiene for startups: Digital Infrastructure, Data Management, Cybersecurity, and Operational Resilience. Each component encompasses specific practices and protocols aimed at ensuring the security, efficiency, and integrity of digital assets and operations within a startup environment.

Digital infrastructure encompasses the hardware, software, and cloud services utilized by startups to support their operations and deliver products or services. It includes devices such as computers, servers, and networking equipment, as well as software applications and platforms.

Data management involves the governance, storage, and protection of data assets within a startup. It encompasses the collection, storage, usage, and sharing of data, as well as compliance with regulatory requirements and protection against data breaches.

Cybersecurity focuses on protecting digital assets and operations from cyber threats such as malware, phishing attacks, and unauthorized access attempts. It involves deploying proactive measures to detect, prevent, and respond to security incidents effectively.

Operational resilience involves ensuring the continuity and resilience of business operations in the face of disruptive events such as natural disasters, cyberattacks, or system failures. It encompasses planning, preparedness, and response measures to minimize downtime and maintain critical business functions.

Figure 2 demonstrates the digital hygiene process and its factors in startup activity.

This detailed figure illustrates the comprehensive digital hygiene process in a startup, highlighting key factors and components at each stage, from assessment and analysis to continuous monitoring and improvement.

The startup conducts a thorough assessment of its current digital practices and vulnerabilities, analyzing potential risks and threats to its digital infrastructure and data. Based on the assessment findings, the startup develops a comprehensive digital hygiene strategy tailored to its needs and goals, prioritizing areas of improvement.

The startup defines clear objectives and timelines for implementing digital hygiene measures, and allocating resources effectively, including budget, personnel, and technology. The startup provides training sessions and educational materials for employees on digital security best practices, fostering a culture of cybersecurity awareness and responsibility within the organization.

The startup continuously monitors and evaluates its digital hygiene efforts, conducting regular audits and assessments to identify areas for improvement and adaptation to evolving threats and challenges.

In conclusion, effective digital hygiene practices are indispensable for startups seeking to navigate the complex and dynamic landscape of digital entrepreneurship. By implementing the conceptual framework outlined herein, startups can fortify their digital infrastructure, protect their data assets, and enhance their cybersecurity posture.

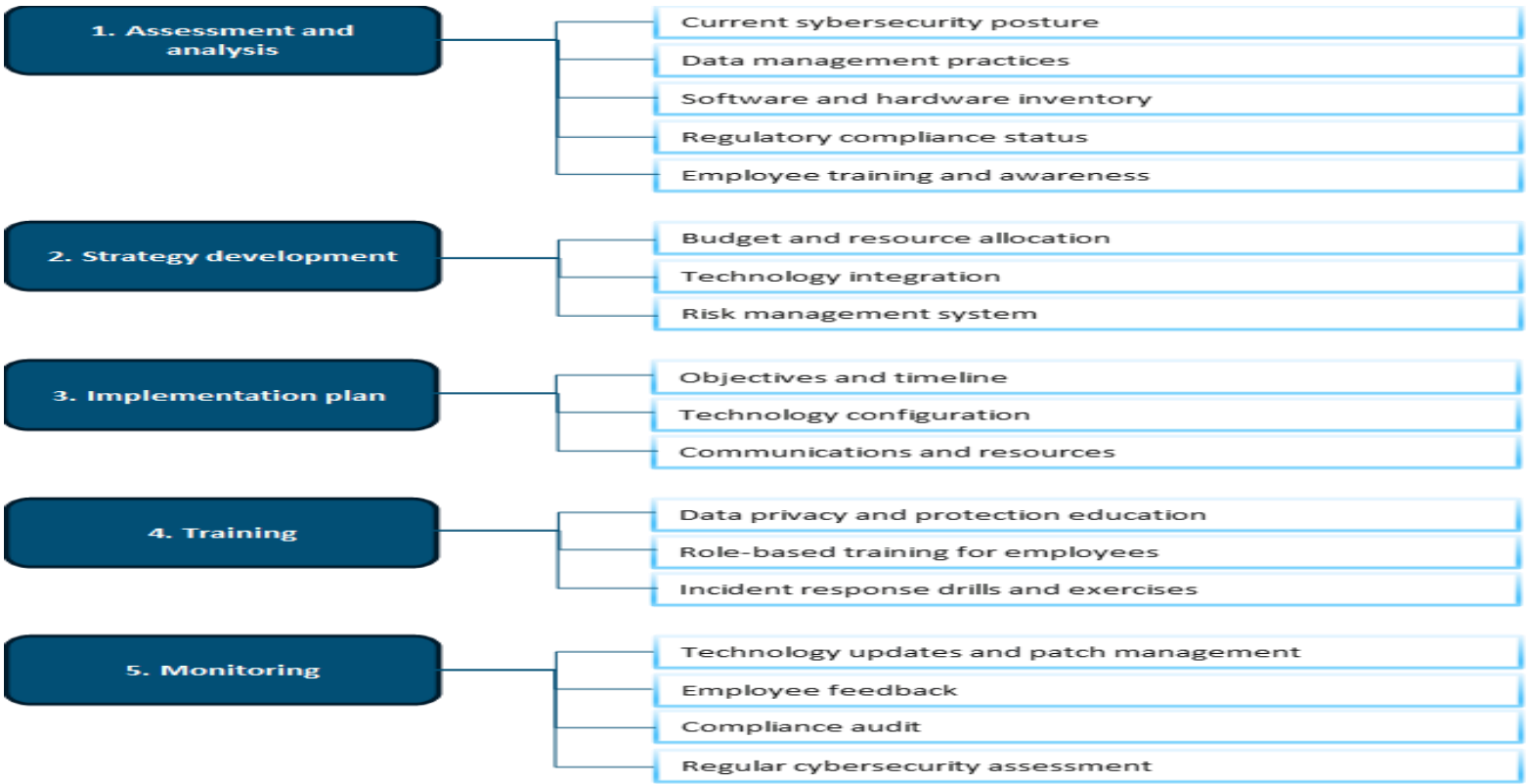


Figure 2. Digital hygiene process and its factors in startup

4.2. The Necessities and Essentials of Good Digital Hygiene for Startups

In today's digital age, startups rely heavily on technology to drive innovation, streamline operations, and reach customers. However, with the benefits of technology come risks, including cyber threats, data breaches, and operational disruptions. To navigate these challenges and ensure long-term success, startups must prioritize good digital hygiene practices. Good digital hygiene practices encompass a range of proactive measures and protocols aimed at safeguarding a startup's digital assets, infrastructure, and data from potential threats, vulnerabilities, and risks.

The necessities of good digital hygiene for startup:

1. Protecting against cyber threats and attacks

One of the primary reasons for maintaining good digital hygiene practices is to protect startups against cyber threats and attacks. In an era where cybercrime is on the rise, startups are prime targets for malicious actors seeking to exploit vulnerabilities in their digital infrastructure and systems. Cyber attacks, such as malware infections, phishing scams, ransomware attacks, and data breaches, can have devastating consequences for startups, including financial losses, reputational damage, legal liabilities, and operational disruptions. By implementing robust cybersecurity measures, startups can fortify their defenses and mitigate the risks posed by cyber threats, safeguarding their critical assets and ensuring business continuity.

2. Safeguarding sensitive data and intellectual property

Startups often deal with sensitive data, including customer information, proprietary technologies, trade secrets, and intellectual property. Maintaining good digital hygiene practices is essential for safeguarding this sensitive information from unauthorized access, theft, or compromise. Data breaches and unauthorized disclosures can not only result in financial losses and legal liabilities but also undermine customer trust and confidence, tarnishing the startup's reputation and brand image. By implementing data encryption, access controls, and data loss prevention measures, startups can protect their sensitive data assets and preserve the confidentiality, integrity, and availability of information, thereby maintaining the trust of customers, partners, and stakeholders.

3. Enhancing operational efficiency and productivity

Good digital hygiene practices also contribute to enhancing operational efficiency and productivity within startups. Outdated software, unpatched systems, and inefficient digital workflows can hinder productivity, hamper collaboration, and impede business growth. By regularly maintaining and updating their digital infrastructure, startups can

optimize performance, streamline processes, and eliminate bottlenecks, enabling employees to work more efficiently and effectively. Moreover, by leveraging automation, cloud technologies, and digital tools, startups can streamline workflows, automate routine tasks, and improve decision-making, driving innovation, and competitiveness in the marketplace.

4. Ensuring regulatory compliance and legal obligations

Compliance with regulatory requirements and legal obligations is another critical aspect of maintaining good digital hygiene practices. Startups operating in various industries are subject to a myriad of laws, regulations, and compliance standards governing data privacy, security, and protection. Failure to comply with these regulations can result in severe penalties, fines, and legal consequences, jeopardizing the startup's viability and reputation. By adhering to regulatory requirements, such as GDPR, HIPAA, PCI DSS, or SOX, startups can demonstrate their commitment to ethical business practices, earn the trust of customers and stakeholders, and mitigate legal and financial risks.

5. Fostering innovation

Lastly, maintaining good digital hygiene practices is essential for fostering innovation and adaptability within startups. In today's digital economy, where technological advancements and market disruptions are commonplace, startups must remain agile, resilient, and adaptable to thrive in a competitive landscape. By embracing emerging technologies, embracing digital transformation, and cultivating a culture of continuous improvement and learning, startups can position themselves for long-term success and sustainability, driving innovation, and creating value for their customers and stakeholders.

To sum up, maintaining good digital hygiene practices is indispensable for startups seeking long-term success, growth, and resilience.

4.3 - The Importance of Digital Hygiene

The importance of maintaining good digital hygiene cannot be overstated. From protecting sensitive data to mitigating cyber threats, digital hygiene practices are essential for individuals and organizations alike. In this case study, we explore the significance of digital hygiene through the lens of a real-life example, highlighting its impact on security, productivity, and overall well-being.

To understand the importance of digital hygiene, take a look at some digital hygiene practices.

1. Meet TechGenius, a dynamic startup based in Silicon Valley, specializing in developing cutting-edge software solutions for businesses. Founded in 2015, TechGenius quickly rose to prominence in the tech industry, attracting top talent and securing high-profile clients. However, as the company expanded its

operations and workforce, it faced new challenges in managing its digital infrastructure and safeguarding its digital assets.

TechGenius, like many startups, operated in a fast-paced environment where innovation and efficiency were paramount. However, amidst the hustle and bustle of daily operations, the company neglected to prioritize digital hygiene practices. Employees often used weak passwords, failed to update software regularly, and disregarded basic security protocols, leaving the company vulnerable to cyber threats such as phishing attacks and data breaches.

Realizing the critical importance of digital hygiene, TechGenius embarked on a journey to revamp its approach to cybersecurity and data management. The company launched an extensive digital hygiene initiative aimed at educating employees, implementing best practices, and strengthening its security posture.

TechGenius's digital hygiene initiative comprised several key components:

1. Employee training and awareness. The company conducted comprehensive training sessions to educate employees about the importance of digital hygiene. Topics covered included password management, email security, safe browsing practices, and data protection regulations. Through interactive workshops and online modules, employees gained a deeper understanding of cybersecurity risks and their role in mitigating them.

2. Policy development and enforcement. TechGenius developed robust digital hygiene policies and procedures to govern employee behavior and ensure compliance with industry standards. These policies addressed areas such as password complexity, software updates, access controls, and incident response protocols. To reinforce accountability, the company implemented regular audits and enforcement mechanisms to monitor adherence to these policies.

3. Technological solutions. In addition to education and policy measures, TechGenius invested in technological solutions to enhance its digital hygiene practices. This included implementing multi-factor authentication, encryption technologies, endpoint security software, and network monitoring tools. By leveraging these technologies, the company bolstered its defenses against cyber threats and safeguarded its digital infrastructure.

The implementation of TechGenius's digital hygiene initiative yielded significant results:

A. Improved security posture. By prioritizing digital hygiene, TechGenius strengthened its security posture and reduced the risk of cyber threats. Incidents such as phishing attacks and data breaches became less frequent, minimizing the potential impact on the company's operations and reputation.

B. Enhanced productivity. With fewer security incidents to contend with, employees were able to focus more on their core responsibilities, leading to increased productivity and efficiency across the organization. By streamlining

digital workflows and minimizing downtime, TechGenius achieved better outcomes and delivered superior results to its clients.

C. Protected reputation. As a trusted provider of software solutions, TechGenius's reputation hinges on its ability to safeguard customer data and maintain high standards of security. By demonstrating a commitment to digital hygiene, the company earned the trust and confidence of its clients, positioning itself as a reliable partner in an increasingly competitive market.

D. Cost Savings. While investing in digital hygiene may incur initial costs, the long-term benefits far outweigh the expenses. TechGenius experienced cost savings in terms of reduced cybersecurity incidents, lower compliance penalties, and increased operational efficiency. By proactively addressing security vulnerabilities, the company avoided potentially costly repercussions associated with data breaches and regulatory non-compliance.

The case of TechGenius underscores the critical importance of digital hygiene in today's digital landscape. By prioritizing cybersecurity education, policy development, and technological solutions, TechGenius was able to mitigate cyber threats, enhance productivity, and protect its reputation and bottom line. This real-life example serves as a testament to the transformative power of digital hygiene in securing organizations against evolving cyber risks and driving sustainable growth and success.

Another example of the importance of digital hygiene practices is the case of SecureHealth.

SecureHealth is a healthcare technology startup revolutionizing the way medical records are managed and accessed. With a cloud-based platform designed to streamline patient care and improve healthcare outcomes, SecureHealth has quickly gained traction in the healthcare industry. However, amidst the rapid growth and adoption of its platform, the company faces significant challenges in ensuring the security and privacy of patient data.

Healthcare organizations are prime targets for cyber-attacks due to the sensitive nature of the data they handle. SecureHealth recognizes the critical importance of digital hygiene in safeguarding patient confidentiality and maintaining regulatory compliance. However, with the complexity of healthcare IT systems and the ever-evolving threat landscape, the company must stay vigilant and proactive in addressing cybersecurity risks.

SecureHealth takes a proactive approach to digital hygiene, implementing a comprehensive cybersecurity program tailored to the unique needs of the healthcare industry. The company prioritizes the following key components:

1. Data encryption and access controls. SecureHealth encrypts patient data both at rest and in transit, ensuring that sensitive information remains protected from unauthorized access. Access controls are implemented to restrict access to patient

records only to authorized healthcare professionals, minimizing the risk of data breaches.

2. Regular security audits and penetration testing. SecureHealth conducts regular security audits and penetration tests to identify vulnerabilities in its systems and infrastructure. By proactively identifying and remedying security weaknesses, the company strengthens its defenses against cyber threats and ensures compliance with healthcare regulations such as HIPAA.

3. Employee training and awareness. SecureHealth provides comprehensive cybersecurity training to all employees, emphasizing the importance of digital hygiene in safeguarding patient data. Employees learn how to recognize and respond to security threats, implement secure practices in their daily workflows, and adhere to company policies and procedures.

The implementation of SecureHealth's digital hygiene initiatives has yielded tangible results:

A. Protected patient data. By prioritizing digital hygiene, SecureHealth ensures the confidentiality, integrity, and availability of patient data, fostering trust and confidence among healthcare providers and patients alike.

B. Compliance with regulations. SecureHealth maintains compliance with healthcare regulations such as HIPAA, demonstrating its commitment to protecting patient privacy and meeting industry standards for data security and confidentiality.

C. Reduced risk of data breaches. With robust cybersecurity measures in place, SecureHealth minimizes the risk of data breaches and other security incidents, safeguarding its reputation and minimizing potential financial and legal consequences.

SecureHealth's experience highlights the critical importance of digital hygiene in the healthcare industry, where the stakes are high and the consequences of security breaches can be severe. By prioritizing cybersecurity measures such as data encryption, access controls, regular audits, and employee training, SecureHealth ensures the security and integrity of patient data, ultimately contributing to improved patient care and outcomes.

To grasp the significance of digital hygiene, consider examining additional digital hygiene practices.

FinTech Innovations is a startup disrupting the financial services industry with innovative digital banking solutions. Leveraging cutting-edge technology such as blockchain and artificial intelligence, FinTech Innovations offers secure, user-friendly banking services to consumers and businesses alike. However, as the company grows and expands its customer base, it faces increasing cybersecurity risks that threaten the security and stability of its platform.

Financial institutions are prime targets for cyber attacks due to the valuable financial data they possess. FinTech Innovations recognizes the importance of digital hygiene in maintaining the trust and confidence of its customers and partners. However, with the complexity of financial transactions and the evolving nature of cyber threats, the company must remain vigilant and proactive in protecting its digital assets and infrastructure.

FinTech Innovations implements a robust digital hygiene program to address cybersecurity risks and safeguard its platform. The company focuses on the following key initiatives:

1. Secure authentication and authorization. FinTech Innovations implements strong authentication mechanisms such as biometric authentication and multi-factor authentication to verify the identity of users and prevent unauthorized access to accounts and transactions.

2. Real-time fraud detection. FinTech Innovations leverages advanced analytics and machine learning algorithms to detect and prevent fraudulent activities in real time. By analyzing transaction patterns and user behavior, the company can identify suspicious activities and take proactive measures to mitigate fraud risks.

3. Continuous monitoring. FinTech Innovations maintains continuous monitoring of its systems and networks to detect and respond to security incidents promptly. The company employs a dedicated team of cybersecurity professionals who monitor suspicious activities, investigate security alerts, and implement timely remediation actions to address potential threats.

The implementation of FinTech Innovations' digital hygiene initiatives has led to significant outcomes:

A. Enhanced customer trust. By prioritizing digital hygiene, FinTech Innovations demonstrates its commitment to protecting customer data and financial assets, building trust and confidence among its users and stakeholders.

B. Reduced fraud and security incidents. With advanced fraud detection mechanisms and continuous monitoring, FinTech Innovations minimizes the risk of fraud and security incidents, ensuring the security and integrity of its platform and transactions.

C. Business continuity and resilience. By proactively addressing cybersecurity risks, FinTech Innovations enhances its resilience to cyber threats and disruptions, ensuring the uninterrupted delivery of financial services to its customers and partners.

FinTech Innovations' experience underscores the critical importance of digital hygiene in the financial services industry, where security and trust are paramount. By implementing robust cybersecurity measures such as secure authentication, fraud detection, and continuous monitoring, FinTech Innovations ensures the

security and stability of its platform, ultimately contributing to a safer and more secure digital banking experience for its customers

These examples illustrate the vital role of digital hygiene in safeguarding sensitive data, maintaining regulatory compliance, and protecting against cyber threats in diverse industries such as healthcare and finance. Prioritizing digital hygiene is essential for organizations seeking to mitigate risks, build trust, and drive sustainable growth and success in today's digital landscape.

4.4. Good Practice From Startups

To illustrate effective threat identification and preemptive measures, we will delve into an instance emphasizing cybersecurity training for staff members. This example serves to underscore the critical role of employee education in bolstering digital security measures.

CyberSec Europe

Context

CyberSec Europe is a cybersecurity startup based in Berlin, Germany, specializing in providing security solutions for small and medium-sized enterprises (SMEs). Founded in 2017, CyberSec Europe quickly established itself as a trusted provider of cybersecurity services in the European market. As the company grew and expanded its client base, it recognized the critical importance of cybersecurity education for its employees.

Despite having a team of skilled cybersecurity professionals, CyberSec Europe identified a need to enhance its employees' awareness of cybersecurity best practices. With the increasing sophistication of cyber threats and the adoption of remote work arrangements, the risk of security incidents such as phishing attacks and data breaches was on the rise. CyberSec Europe understood that educating its employees about cybersecurity risks and protocols was essential to maintaining its reputation as a trusted cybersecurity provider.

Solution

CyberSec Europe implemented a comprehensive security training program for all employees, focusing on key areas such as threat detection, incident response, and compliance with data protection regulations such as the General Data Protection Regulation (GDPR). The training program was designed to be interactive, engaging, and tailored to the specific needs of CyberSec Europe's workforce.

The security training program was rolled out company-wide over three months. It consisted of a series of workshops, webinars, and hands-on exercises led by internal cybersecurity experts and external consultants. Topics covered in the training program included:

- Identifying and responding to phishing emails
- Creating and managing strong passwords
- Recognizing common signs of cyber attacks
- Safeguarding sensitive data and ensuring GDPR compliance
- Reporting security incidents and following incident response procedures.

To encourage participation and engagement, CyberSec Europe incentivized employees to complete the training modules and offered rewards for exemplary performance in security awareness exercises. The company also provided ongoing support and resources to employees, such as access to cybersecurity tools and online resources.

The implementation of regular security training yielded positive results for CyberSec Europe:

1. Increased security awareness. Employees became more vigilant and knowledgeable about cybersecurity risks, leading to a reduction in security incidents and data breaches.

2. Improved security practices. Employees adopted best practices in cybersecurity, such as using strong passwords, encrypting sensitive data, and reporting suspicious activities promptly.

3. Enhanced customer trust. CyberSec Europe's commitment to cybersecurity education demonstrated its dedication to protecting client data and privacy, enhancing trust and credibility among its customers.

4. Compliance readiness. By educating employees about GDPR requirements and other regulatory standards, CyberSec Europe improved its compliance posture and minimized the risk of regulatory penalties.

CyberSec Europe's proactive approach to cybersecurity education underscores the importance of regular security training for startups in Europe. By investing in employee awareness and empowerment, CyberSec Europe was able to strengthen its cybersecurity defenses, mitigate risks, and build trust with its clients. This real-life example highlights the effectiveness of security training in enhancing digital hygiene and safeguarding startups against cyber threats in the European market.

Ensuring good digital hygiene practices is crucial for startups in Europe to thrive in today's digital landscape. The increasing prevalence of cyber threats, data breaches, and regulatory requirements underscores the importance of prioritizing cybersecurity, data protection, and compliance efforts. By implementing robust digital hygiene measures, startups can safeguard their digital assets, protect sensitive data, and build trust with customers, partners, and stakeholders. However, achieving and maintaining good digital hygiene requires a concerted effort, ongoing vigilance, and a commitment to continuous improvement.

Recommendations for Improving Digital Hygiene of Startups in Europe

It is recommended that startups conduct regular assessments of their digital hygiene practices, including cybersecurity posture, data management protocols, and regulatory compliance status. This will help identify vulnerabilities, gaps, and areas for improvement.

Based on assessment findings, it is advisable for startups to develop comprehensive digital hygiene strategies tailored to their specific needs, goals, and risk profiles. Strategies should address key areas such as cybersecurity, data protection, compliance, and incident response.

It is recommended that startups invest in cybersecurity technologies and solutions to protect their digital infrastructure from cyber threats, malware, and data breaches. This may include firewalls, antivirus software, encryption technologies, and intrusion detection systems.

Startups should prioritize data protection and privacy by implementing robust data management protocols, including encryption, access controls, and data backup and recovery mechanisms. Compliance with regulations such as GDPR is essential for startups handling personal data.

It is advisable for startups to promote cybersecurity awareness and education among employees to ensure they understand potential risks, best practices, and procedures for maintaining good digital hygiene. Regular training sessions, awareness campaigns, and phishing simulations can help reinforce cybersecurity awareness.

Startups should develop and implement incident response plans to effectively respond to cybersecurity incidents, data breaches, or other emergencies. Plans should outline roles, responsibilities, and procedures for detecting, containing, and mitigating incidents.

Continuous monitoring and evaluation are essential for maintaining good digital hygiene. It is recommended that startups regularly assess the effectiveness of their digital hygiene measures, conduct audits, and reviews, and make necessary adjustments to address emerging threats and challenges.

Startups should stay informed about the latest cybersecurity threats, trends, and regulations affecting their industry. Regularly monitoring cybersecurity news, participating in industry forums, and collaborating with cybersecurity professionals can help startups stay ahead of evolving threats and risks.

To sum up, improving digital hygiene practices is essential for startups in Europe to protect their digital assets, mitigate risks, and maintain trust with stakeholders. By implementing comprehensive strategies, investing in cybersecurity technologies, promoting awareness, and continuously monitoring and adapting to changing threats, startups can strengthen their digital resilience and thrive in a competitive landscape.

Conclusion

It is recommended that startups prioritize cybersecurity education for their employees to build awareness and empower them to recognize and respond to cyber threats effectively. Training programs should cover topics such as phishing awareness, password management, and incident response protocols.

Establishing robust digital hygiene policies and procedures is essential for promoting a culture of cybersecurity within startups. It is advisable to develop policies that address areas such as password complexity, software updates, access controls, and data protection regulations.

Regular audits and enforcement mechanisms help ensure compliance and accountability within startups. It is recommended to conduct regular audits and implement enforcement mechanisms to monitor adherence to digital hygiene policies and procedures.

Startups should invest in technological solutions to enhance their digital hygiene practices. This includes deploying cybersecurity tools such as multi-factor authentication, encryption technologies, endpoint security software, and network monitoring tools to strengthen defenses against cyber threats.

Compliance with regulatory requirements and industry standards is critical for startups to demonstrate their commitment to ethical business practices and protect against legal and financial repercussions. Startups should adhere to regulations such as GDPR, HIPAA, PCI DSS, or SOX to safeguard data privacy, security, and integrity.

The concept of digital hygiene integrates insights from various disciplines, including cybersecurity, information management, human factors, organizational behavior, and compliance theory. By drawing upon these perspectives, startups can develop approaches to address the complex challenges of cybersecurity and data protection effectively.

Chapter 5

Digital Hygiene Tools & Integration in Daily Routines

Egemen KAHRAMAN[9]

Prof. Dr. Tuğba UÇMA UYSAL[10]

Assoc. Prof. Dr. Ceray ALDEMİR[11]

The vital essence of cybersecurity is the big thing that is creating strong cybersecurity practices that have been especially gaining attention since the last time humanity became connected through the world-wide web, especially now for the start-ups and small businesses that are mainly the victims of cyber-attacks. These firms, as a rule, do not have the luxury of much money, hence they have to concentrate on securing their digitalized assets and client data. One startup may initially shift focus to product development and marketing while another one may proceed to the market expansion, but in any case, a venture becomes long live and prosperous if it inherits strong digital hygiene as a habit. So, we come to the question: "What exactly is digital hygiene?" The answer is simple, it's nothing for certain, it's just the general idea that people are taking care of their digital lives. This includes practices that secure digital information and systems such as data breaches, malware, and unauthorized access - these are a few examples.

This chapter concerns the techniques and techniques that start-up companies can utilize to obtain a high degree of digital hygiene. It explains how to use antivirus software, firewalls, password managers, encryption solutions, and data backup systems as the first line of defense against cyber threats. In addition, the chapter discusses the significance of developing a digital hygiene culture within a company. The report highlights those things, for example making sure employees are updated with training and internal systems are processed through the regular updating and monitoring of them. Case studies (for example, SecureTech's successful adoption of digital hygiene practices) and other practical insights are given which explain how start-ups can not only improve their cybersecurity but also use it as a competitive advantage. Through the adoption of these security

[9] Muğla Sıtkı Koçman University, egemenkahraman@mu.edu.tr

[10] Muğla Sıtkı Koçman University, utugba@mu.edu.tr

[11] Muğla Sıtkı Koçman University, cerayaldemir@mu.ed.tr

measures, startups can minimize the risks, fortify the crucial assets, and hence add to the ongoing trust with and between their clients and partners.

5.1. Top Digital Hygiene Tools for Startups

An interconnected world poses risks of broader and more complicated digital threats. That is why it is more important than ever that start-ups place substantial importance on cyber security to protect their valuable assets and confidential information. In this unit, you will learn about some of the key strategies and practices that start-ups should look to undertake to improve their online security. These range from creating strong passwords to implementing thorough data backup solutions. This guide will provide you with the knowledge and tools that start-ups need to know to stay secure online. This unit will take you through the key principles and provide a range of recommendations that will help you build a strong base for your digital hygiene strategy, as well as protect your digital assets effectively.

5.1.1. Maintaining Good Password Hygiene: The Basics

Ticketmaster was sued in January 2021 for hacking a rival company's computer systems after an ex-employee of the rival company used his/her credentials to enable Ticketmaster to have surreptitious access to its competitor's computers. Acting U.S. Attorney DuCharme stated that “Ticketmaster employees have illegally accessed a competitor's computers without permission on numerous occasions to steal business knowledge via unlawfully obtained passwords”. This case singularity led to Ticketmaster being subject to a cash penalty of $10 million under the terms of the Computer Fraud and Abuse Act. (Jones, 2022). Google Cloud's 2023 Threat Horizons Report indicates that 86% of security breaches include the use of stolen credentials, and credential problems are responsible for more than 60% of the underlying causes of the breaches - problems that stronger organizational identity management flanks could help resolve. According to (Keszthely, 2013) the act of taking someone else's password can be completed in four basic ways:

1- Default words: Computers and applications have default passwords built in. Computer and account passwords might be voids or part of a separate set of common words like "123456, " "asdfgh," and "password."

2- Connection between login name and passwords: Password guessing or logic is when the attackers will take the time to systematically guess the username and password. The user may even be helping the attacker guess the username and password. Some examples are “password”, “login-login”, “qwerty” and “letmein”.

3- Method of the dictionary: Hackers will collect some general passwords and select them from the list. They will download them one at a time because the tools work offline and are more likely to succeed if they function more slowly. In

addition, they will still have the opportunity to test each strand without an Internet connection.

To avoid suffering damage caused by password theft, it is necessary to give priority to the selection of strong, secure passwords. (Kato & Klyuev, 2013) suggest some recommended tips for creating strong passwords:

- **Use Uppercase and Punctuation**: Utilize uppercase letters and punctuation marks to create a stronger password.
- **Mix It Up:** Integrate both letters and numbers to generate more secure passwords.
- **Avoid Common Info**: Refrain from using easily guessed words and personal information details in passwords.
- **Consider Longer Passwords:** Aim for longer passwords that are easy for you to remember.
- **Use Password Managers**: Utilize programs that are designed to store passwords safely like LastPass.
- **Unique Passwords**: Formulate different passwords for different accounts.

In addition to practicing safe password habits as an individual, companies need to implement policies that focus on improving password security. (Inglesant & Sasse, 2010) suggests that at the organizational level, password guidelines should center around the user. The guidelines should reflect the unique requirements and skills of the users in their everyday work. Organizations can maximize security while bolstering user effectiveness and efficiency in managing passwords by complying with the principles of human-computer interaction and accounting for specific use. Moreover, enterprises should try to analyze and apply tight password-creation standards by using new password techniques and devices like Telepathwords. In addition, businesses should make sure to assist employees in a preventive effort from using weak or influenced passwords. Outdoing the scheme through these techniques will greatly improve it is safety (Blocki & Liu, 2023).

5.1.2. Safeguarding Vital İnfrastructure with Two-Factor Authentication

Two-factor Authentication (2FA) is a security measure that requires users to provide a secondary component for user confirmation. This method adds a factor of authentication to the password authentication system. There are some advantages that an assessment platform would have with the implementation of 2FA (Tellini & Vargas, 2017):

- **Eliminating the possibility of unauthorized access**: 2FA goes beyond just using a username and password. It utilizes an entirely separate system for authentication, altogether.
- **Protection Against Password Theft:** Usernames and passwords are stolen daily. With 2FA, an attacker would need more than just the user's name and password credentials to gain illegitimate access.

- **Decreased Risk of Unauthorized Access**: With 2FA, unauthorized or unproven access is less likely because of the extra layer of authentication the hacker would need to complete accessing the account and would need possession of the user's phone or a code generated on their phone.
- **Increased User Confidence:** Trust and faith in the platform may increase when users know that their account is protected by more than just a password.
- **Compliance with Security Standards:** Using 2FA can make your log-ins compliant with best practices for online security and might be required by specific regulations or standards in your industry.
- **Mitigation of Common Password Issues:** 2FA helps mitigate common password issues such as poor password choices, and reuse. By reducing our reliance on a single password 2FA can help us use more complex passwords.

2FA is a two-step verification process that requires users to provide two different types of authentication factors before granting access to the end user. The three types of factors are something the user knows (knowledge factor), something the user has (possession factor), and something the user is (inherence factor).(De Cristofaro, Du, Freudiger, & Norcie, 2013). The two-factor Authentication method makes password-centered authentication techniques more secure. Services can use dynamic combinations of factors to greatly increase the assurance of user credentialing by quantifying the risks and benefits (Han, Sun, Shen, Chang, & Shen, 2013).

Table 1: Some classes of authentication factors

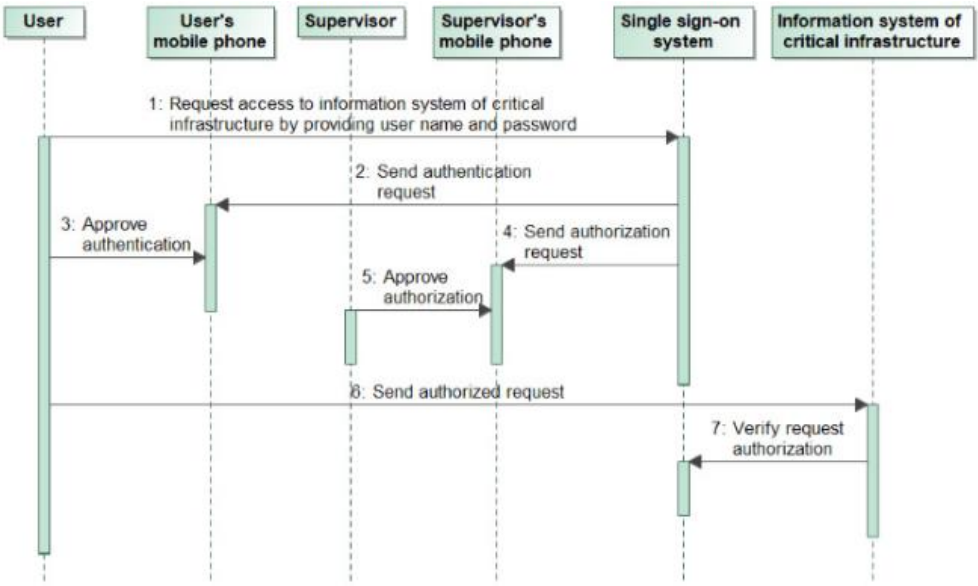
Class type	Class description	Examples
Knowledge	Something known	Password Key phrase Secret question Personal question
Possession	Something held	One time password generator Grid token Smart card
Inherence (biometrics)	Something about the person	Fingerprint scan Iris scan Voice recognition

Source : (Pearce, Zeadally, & Hunt, 2010).

(Bruzgiene & Jurgilas, 2019) provides an authentication method that operates in a three-step process for securing remote access to critical infrastructure information systems. Firstly, the user enters his/her account ID and password. Once the correct information is entered an authentication request from the local security authority (LSA) will be sent to the user's mobile device. Then the user must approve the request by a single touch to the phone's screen; this will enable the mobile device to send an authorization request to the supervisor(s) of the user to determine the level of access rights for the remote system. Once the user request

is approved successfully by the supervisor(s), the requesting user is given access rights to the remote system

Figure 1: The proposed authentication method by (Bruzgiene & Jurgilas, 2019)



Source : (Bruzgiene & Jurgilas, 2019)

5.1.3. Timely Software Updates: Bolstering System Security

Software updates are very important because they fix buggy or enhance the performance of software, such as drivers and operating systems (Mathur, Malkin, Harbach, Péer, & Egelman, 2018). By updating the software, you ensure that it is compatible with other software and hardware systems and keep your systems safe and secure by running the latest version of the software. The updates encompass security updates which are required to safeguard a computer from malicious software and vulnerabilities, feature updates that range in terms of severity as they can include anything from minor bug fixes to significant workflow changes, and the cumulative update that necessitate the installation of all previous updates before reaching the latest update (Vaniea, Rader, & Wash, 2014). These improvements help to maintain the security and functionality of software systems. Making sure you are up to date on all necessary updates is important for this reason.

However, many users tend to avoid updating their software due to perceived factors. These factors include *update costs*, such as time to install, requiring restart

and disk space used; *update necessity*, including satisfaction of user with the current system, clarity of the update reasons and the importance of the update perceived to be by user and *update risk* which involve worries about data loss during updates and that any update might carry some virus or malware that could make a system vulnerable (Mathur, Malkin, Harbach, Péer, & Egelman, 2018). Neglecting to upgrade software may make computer systems susceptible to the actions of hackers who might try to infect the computers with new viruses and worms. It can also produce serious consequences for your computers. Not only will unpatched security flaws make the system less secure, but they are also the reason most viruses are so successful.

A software update delivery policy is a policy developed by organizations that define timelines and methods for assessing and delivering security-related software updates. This policy focuses on the immediate delivery of security updates, within a restricted time interval (constraint) to minimize the vulnerability window, if the constraint allows so. Organizations may adopt a more strategic approach, depending on resource constraints. Innovative solutions could include, for example, peer-to-peer Blockchain-based systems, and large-scale overlay networks, to enable the highly efficient and expedient distribution of security updates to wide networks of end users. (Mugarza, Flores, & Montero, 2020). The policy is to break down different categories of patches, and their associated timelines for assessment and delivery to ensure that updates, at different levels, are assessed in line with their need, cost, and associated risks, before deployment.

Here are the software update suggestions for business[12]:

- **Timely Installation:** Getting security updates installed on time can help protect your systems from vulnerabilities and threats.
- **Clear Communication:** Users are often resistant to updates because they do not understand why you need them. It is important to communicate why the update is important and that it is not just a random patch provided by the vendor. It is also beneficial to mention in your email that some updates are patches to security holes that may already be exploited
- **Minimize Disruption:** Enable silent installations or configurations to the system which would make it easier to apply updates. Another way to minimize disruption is to distribute and deploy updates during non-peak hours.
- **User Education:** Educate end-users on the importance of software updates in maintaining system security and functionality to promote proactive update behavior
- **Testing Procedures:** Improve testing procedures to ensure that updates are rigorously tested for compatibility and potential risks before deployment.
- **Differentiate Updates:** Distinguish security updates from feature updates so users understand the value of each kind of update and prioritize them accordingly.

[12] (compiled from (Mathur, Malkin, Harbach, Péer, & Egelman, 2018), (Di Tizio, Armellini, & Massacci, 2022), (Vaniea, Rader, & Wash, 2014))

- **Cumulative Updates:** Consider the implications of cumulative updates and encourage the user to install the critical security patches.

5.1.4. Antivirus Protection: Safeguarding System Integrity

According to (Rohith & Kaur, 2021), anti-virus software is a specialized program that protects the operating system from viruses, spyware, hacker attacks, and other unauthorized computer access to prevent valuable personal data stolen, or the computer unauthorized control is another computer application (freeware, shareware, and commercial). Anti-virus software is used to detect computer viruses that can implicate computer files, application programs, and the operating systems of the computer. For this reason, it can also be set up to conduct regular reviews of the files and memory of the computer, to detect any known virus signature thereby preventing possible contagion of the computer system and its files. Is important to regularly update the anti-virus software with the latest definitions and virus signatures because new viruses and variations keep coming out regularly. By detecting the latest virus threats, updating the anti-virus software provides a robust defense against the constant evolution of computer threats as it works (Naie & Teymournejad, 2012).

Several signs are associated with the presence of computer viruses on your computer, a few of which are detailed below. Each of these symptoms can indicate a virus problem. Therefore, it is very important to scan the system with antivirus software as soon as possible (Kumar, 2008):

- Slower computer
- Basic tasks take longer
- Lock ups and crashes
- Constant disk activity
- Excessive CPU usage
- Internet browsing is much slower than before.
- Applications won’t start.
- Pop-ups and uninvited messages featuring adult content.
- Hard drives pencil numbers.
- CD-ROM drive opening and closing.

If you encounter one or more of these situations unexpectedly, contact your IT administrator or perform the necessary virus checks. It is important to note that having an antivirus installed on all systems is crucial even if it’s not the best. This helps give a higher level of difficulty for attackers trying to compromise the security of a system (Min & Varadharajan, 2015). Moving forward, (Ncube & Maiden, 2004) provides valuable insights into the challenges, and considerations to investigate during the selection of antivirus software for an organization:

1. Use a questionnaire together with other elicitation techniques

2. Make sure questions are short and to the point of getting good responses from suppliers.

3. Ask for documentation with questionnaire responses so we can better match the product description with the actual product.

4. Clearly define what you are saying in the product and how far will you test will help you define the test case better.

5. Understand that we are going to be limited with time while we are selecting COT software and look into process description templates to be faster on different occasions.

6. Know that you can't test everything. Some requirements might have restrictions.

5.1.5. Data Backups: A Shield Against Loss

Although unforeseen, unexpected events and cyber incidents are capable of causing a significant amount of damage to an organization's data. This is where data backups come into play. Data backups are a critical component of cyber security and maintaining a safe digital environment. Data backups can be a great tool for organizations in case of security breaches. Along with the protection of data from loss backup systems provide the capability to restore the past versions of files, so that the file history is protected. Most of the backup tools can keep multiple instances of the same file in many formats, each of them associated with a time stamp. Also, compression and encryption are common features of almost all backup systems. Compression helps users transfer files across a network or the Internet when sharing them (Sampaio & Bernardino, 2015).

Techniques of data backup systems involve full backup which makes a full copy of all data, differential backup which stores data changes since the last full backup, and incremental backup which only saves the data portions that have changed since the previous backup was taken. (Nadee & Somwang, 2021). Each method yields different consequences and suitability for backup operations. Reliable backups are noteworthy because some data is invaluable, and recreating additional is time/money-consuming (Traeger, Joukov, Sipek, & Zadok, 2006). Backup data is not only to save data loss but also to restore an old version (Sampaio & Bernardino, 2015). This dual functionality is important for both data recovery and compliance with certain legal standards. Here are some best practices for small business backup (Rock, 2023):

Data Protection Strategy: Small businesses need to design a detailed plan for data protection, which will be part of their BCP (Business Continuity Plan) or DRP (Disaster Recovery Plan).

Backup Solutions: Businesses should not use simple backup solutions but rather they should pick some robust BC/DR (Business Continuity /Disaster Recovery) solutions, which guarantee minimal operational interruption.

Backup Frequency and Storage: Regular backups are essential and modern backup solutions do frequent backups. It is recommended to have hybrid backup protection, which stores data both on-site and in the cloud.

Security and Compliance: It's important to protect the backups from Cyber-attacks and also comply with data retention policies. Encrypting backups in transit and at rest would be an additional security.

Backup data on secure devices: Configure backup devices for outbound communication only within a secure local area network. This approach will help prevent a cybercriminal from taking control of your backups.

Backup data on separate devices: Make sure to keep backup devices separate from the local network to avoid backups being affected when ransomware occurs on the local network. One of the benefits of backing up data to the cloud is that it can be done from any connected place, away from the main organization offices.

Use encrypted backups: Use encrypted storage and transmission to protect critical data from unauthorized access, tampering, and corruption.

Back up all endpoint data using recovery software: A very important source of data loss is lost, stolen, or corrupt laptops/desktops. As a result, your inability to backup or restore the lost data. Knowing that backup devices take the form of desktops and servers, always select recovery solutions to protect all the data on any computer and select endpoint backup accordingly.

5.1.6. Guardians Against Malicious Code: Understanding Anti-Malware Solutions

Malicious executables are unauthorized programs created to infest or damage a computer system, which constitutes a great hazard to the computer's security (Ye, Wang, Lİ, & Ye, 2007). Users are typically victims of malicious software without even knowing it. It's the program that runs in the background on a user's computer without their knowledge and does things such as steal information, viruses that will wipe your devices clean, or trojans that may or may not delete your files. Spyware, Viruses, worms, Trojan horses, ransomware, and adware are the common versions of malware. Every business should be backing up their systems more than once a day and be using a robust anti-malware solution. Several factors need to be considered when choosing anti-malware software for a business, to ensure that the solution fits the organization's needs or goals (Alharbi, Alzahrani, Asseri, & Taramisi, 2020):

Security Features: Real-time access, firewall protection, and intrusion detection are key security features that need to be included in an anti-malware program.

These features are vital for effective threat management and to make sure that there are no threats that get missed.

Operational Features: Operational features of anti-malware software that you should look for include how easy it is to deploy and use the software, what management capabilities the software has, and how it will integrate with your existing systems.

Efficiency: Evaluate the efficiency of the anti-malware software in discovering and removing harmful software. Look for solutions that have a high detection percentage of up to 100% and a minimal false positive percentage.

Scalability: Choose a solution that can scale with the needs of the business as it grows. Ensure that the anti-malware software solution can handle your organization's current needs and can address future needs.

Check Vendor Reputation: A good reputation is a rare commodity in the software industry, but it's one of the most valuable traits of any software vendor. Look for anti-malware vendors with a long history of high-quality security solutions. Have they been recognized by independent testing organizations?

Cost: The first thing to consider is the price of the anti-malware software. Different vendors provide their software at different price points and licensing options, so make sure it falls within your budget. Some organizations may classify this as an important factor, while others might classify this as not very important.

Support and Updates: Evaluate the vendor's record of support and updates. Find a vendor that provides regular updates and technical support should problems arise.

Compatibility is one of the things that an organization has to check off a list since no software can be effective if you are having compatibility issues. Compatibility issues are one of the biggest reasons an organization's software becomes ineffective.

5.2. How to Make Digital Hygiene a Habit in Startup Operations

Making a culture Cyber Security and Cyber-hygiene practices in the everyday operations of a start-up operation is crucial. Cyber hygiene practices are the same as personal hygiene they provide the necessary protocols to follow to keep personal and company data/information safe and secure (Alkhaledi & Hawamdeh, 2023). Start-ups, with their lack of funds, cannot afford the setbacks of a cyber incident. The business implications are not limited to just a financial impact but include loss of customer trust, reputational damage, and potential legal consequences, which in a start-up could mean the difference between successfully scaling or failing prematurely. Many organizations still lack good cyber hygiene behavior even though a lot has been done to address cyber hygiene issue (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021).

Good cyber hygiene behavior is essential to reduce cyber threats and daily challenges to addressing cyber hygiene issues. This chapter serves to outline and expand upon the strategies set in place daily for start-up companies to create a daily digital hygiene routine.

5.2.1. Assessing Your Startup's Digital Health

Cybersecurity risk assessment is an essential part of business planning; it involves identifying, evaluating, and estimating risks to an organization's digital assets and operations. The cybersecurity risk assessment method applied enables the organization to evaluate its security postures, assign value to its information and its systems, estimate the effectiveness of its current security infrastructure and activities, and also estimate the magnitude of damage that would occur if the specific risks are realized. By prioritizing identified risks, organizations can effectively allocate resources to strengthen their defenses and ensure business continuity.

Numerous studies offer valuable findings regarding the different aspects of cyber security risk assessment, which can be helpful in a business. (Chavez, ve diğerleri, 2020) indicates the assessment of information needs also as one of the main steps in effective deviation handling in SMEs with the use of digital tools. Deciding the types of information that need to be collected for the procedures and the level of criticality of the data will help in minimizing the risk of integrating the digital systems. (Elmarady & Rahouma, 2021) summarized the risk assessment process in aviation cyber security, but these practices can be used as a general framework in risk assessment in SMEs :

1. Identify the systems that need protection. With an understanding of what the systems were defined to do, identifying the potential threats to those systems sounds simple.

    • Recognize potential threats by understanding the systems.

    • Define the boundaries of the systems to be assessed and describe them.

2. List all the things that could happen to cause loss or harm to the system. Understand what could directly or indirectly cause a security objective to not be carried out and what the difference is between a threat and a vulnerability.

    • Determine scenarios that could harm the system directly or indirectly.

    • Evaluate threats that may affect the system's integrity, confidentiality, and availability.

3. Assess the likelihood and impact of threats. In assessing the seed at which a threat can be carried out, many factors must be addressed.

    • Evaluate the probability of threats.

• Assess the potential impact of threats on safety, efficiency, economy, politics, and public confidence.

4. Determine risk levels. Assess the risk levels.

• Analyze the risk profile using likelihood, vulnerability assessments, and threat impact.

• Convert risk levels into qualitative terms and determine risk tolerability.

• Categorize risk levels using a standardized methodology.

Implement mitigation measures required to reduce risks to acceptable levels. By following these steps, organizations can effectively assess cybersecurity risks, identify threats, and implement policies to protect critical systems.

5.2.2. Establishing a Culture of Digital Hygiene

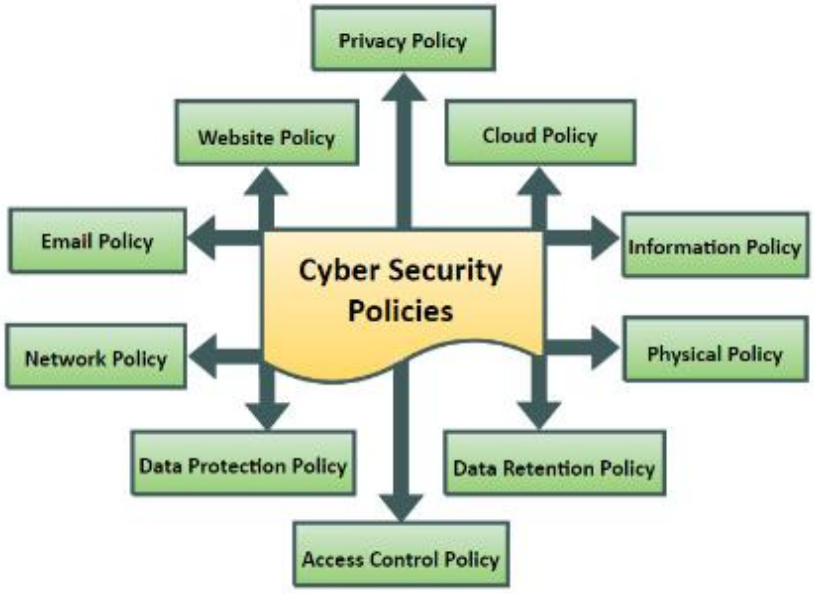
The culture of digital hygiene, the making of a thriving digital ecosystem, must first be embedded within the organization as a first condition. This has to be driven top-down by management. It is not only sufficient to talk about digital wellbeing but has to be practiced by the top management. It starts with developing policies. Leaders should drive and develop a comprehensive policy that governs data management and increases security. A regular training session is highly required. It should be taken as a regular program to create awareness among the employees on how to remain safe and the latest best practices of Digital Security. Open communication is highly critical. It's very important to have a transparent culture in an organization where employees are comfortable communicating, can raise their concerns, and also can report if they find anything suspicious that would cause any security problems. This is the only way we can ensure a culture in place to maintain digital hygiene and security.

Policy Development

Having a strong cyber security policy is very important for Small and Medium Enterprises (SMEs) to secure their digital assets and ensure operational continuity. Research has shown that SMEs face several challenges including the lack of budget, unavailability of specialists, and increase in cyber threats (Neri, Niccolini, & Martino, 2023)Therefore SMES need to improve their cyber awareness and readiness posture. Having cyber security measures in place can also significantly reduce data breaches and improve internal process security in addition to building a reliable system with sufficient information processing capacity (Hasani, O'Reilly, Dehghantanha, Rezania, & Levallet, 2023). Additionally, the resilience of SMEs to cyber-attacks could be improved through their cybersecurity policies. implementation of a holistic approach to cyber resilience could improve the capability of MSMEs to anticipate, detect, withstand, recover from, and evolve after a cyber attack (Carias, Borges, Labaka, Arrizabalaga, & Hernantes, 2020).

Businesses should consider different areas when designing cyber security policies and produce cyber security policies in the appropriate field according to their needs. To advance their cybersecurity policies and practices associations can use the parts to develop the taxonomy of cybersecurity policies. The components of the cybersecurity policies taxonomy mentioned by (Mishra, Alzoubi, Gill, & Anwar, 2022) are illustrated in Figure 2:

Figure 2: Cybersecurity policies taxonomy



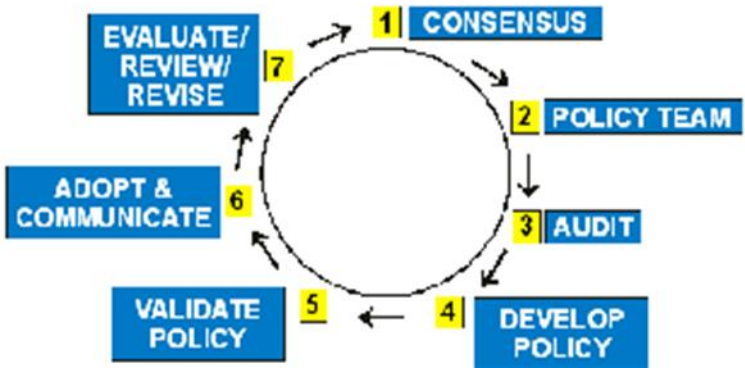
Source: (Mishra, Alzoubi, Gill, & Anwar, 2022)

1. Privacy Policy: Focuses on protecting sensitive personal data and ensuring compliance with data protection regulations.
2. Website Security: Involves securing websites from cyber threats and vulnerabilities to protect user data.
3. Cloud Computing Security: Addresses security measures for cloud-based services to safeguard data stored in the cloud.
4. Email Security: Focuses on securing email communications and preventing email-based cyber threats.
5. Physical Security: Involves securing physical access to IT infrastructure and critical assets to prevent unauthorized access.
6. Network Security: Focuses on protecting computer networks from cyber threats and unauthorized access.

7. Information Security: Encompasses measures to protect sensitive information
8. Access Control: Involves managing user access to systems and data to prevent unauthorized access.
9. Data Retention: Addresses policies for storing and managing data throughout its lifecycle.
10. Data Protection: Focuses on safeguarding data from loss, theft, or unauthorized access through encryption and security controls.

Once you know the deficiencies and targets, you can design the cyber security policies to cover these areas. A useful framework for policy design has been outlined by (Lubua & Pretorius, 2019) shown in Figure 3. The Policy Development Cycle includes recognizing issues that will require some sort of policy to be developed, forming a policy team, getting together with, and gathering the stakeholders, validating the policy, adopting the policy with every valued resolution, handling the policy not after three years, reducing your policy also having the feedback and by the change. Throughout the process, it is important to have stakeholder engagement, gaining input from diverse groups of people. The policy also has to be formalized, making sure it is in line with our organizational goals and any of the law requirements. Policies have to be reviewed regularly, updating the policy when it is outdated. Regular reviews should be in place and the updates were necessary. Policies will accordingly challenge and also operate environmental changes in an organization or a particular context.

Figure 3: Policy development cycle



Source: (Lubua & Pretorius, 2019)

Regular Training

A vital consideration in educating employees on the best practices in cyber hygiene is to examine the numerous factors that influence their behavior and knowledge. In a recent study by (Cain, Edwards, & Still, 2018) pints to the fact that users are often not aware of key actions they should take and their impacts thus influencing their behaviors. Most users lack the understanding of what exactly would mean to follow best security practices when they are aware of the risks involved. A significant number of users may also be aware of the risks but still cannot take the appropriate precautions to better grasp the concept of security. Another study by (Neigel, Claypoole, Waldfogle, Acharya, & Hancock, 2020) provides the factors such as human factors that contribute to cyber breaches and risks. Poor cyber hygiene practices, lack of awareness, behavioral biases, educational gaps, and inadequate training significantly contribute to human factors that can be addressed by education and awareness can reduce the vulnerability to a large extent and thus enhance cyber resilience as well.

Cybersecurity training for employees is essential so that organizations can proactively take an approach to protect their information. Employee training not only trains workers but also raises awareness among all employees about the type of cyber threats that exist, what could be the consequences of a successful attack from a cybercriminal, and how to counteract it if it were to destabilize an organization. The organization needs to train all of its employees to make them well-informed about cyber security and explain any threat to the company's valuable assets (Singh, Mohanty, Swagatika, & Kumar, 2020).

Here are some best practices for cyber cybersecurity training (Mughal, 2019) :

- Regular Training: Keep providing security training to end-users of the company to keep them informed and updated about the new threats that always appear within their responsibilities.
- Tailored or Custom Content: Always use custom or tailored training content that is based on the risk of the IoT device and end-user role concern.
- Interactive Learning: It is important to know what engages the end users and their learning process of the knowledge of the rip it helps to interact and simulate workshops to keep engaging the user like this.
- Clear Communication: Always communicate the policy regarding the IoT security and limitations based on its practices best and the user is aware of it.
- Reinforcement and Reminders: Keep reminding the end user regarding the security and always keep ensuring the awareness of the end-users.
- Incentives and Rewards: Ensure and encourage good practice of cyber security by rewards and incentives encouraging end-users to complete the training or the report Incidents.
- Evaluation and Feedback: Monitor the user behavior and how the program officer works if it has been shown any involvement.

Organizational Culture

How can the concept of cultural readiness be applied to your own organization's cyber security preparedness? Research has shown that organizations with a strong culture for cyber security are better prepared to handle cyber threats (Berlilana,Noparumpa, Ruangkanjanases, Hariguna, & Sarmini, 2021). Cybersecurity culture is an integral element in the overall organization culture, which shapes the risk management frameworks, governance, policies, and employee behaviors that are related to cybersecurity (AL-Nuaimi, 2024). Moreover, organizations may promote employee compliance with information security policies by leveraging top management support and organizational culture by leveraging top management leadership by championing security initiatives, effective communication, and actively engaging employees (Hu, Dinev, Hart, & Cooke, 2012). A common security culture helps all employees, regardless of department or job role, to understand the risks of cyber threats. This helps to better align their strategies for mitigating those information security risks (Fritzvold, 2017).

Technology-Organization-Environment (TOE) framework, which was developed by Tornatzky and Fleischer (1990), is a comprehensive framework that provides a foundation for examining the adoption of a variety of Information Systems (IS) and Information Technology (IT) products and services by organizations (Gangwar, Date, & Ramaswamy, 2015). This framework represents not just only the technical aspect of the innovation, but also the organizational and environmental view to explain and examine the adoption of a technology (Rahayu & Day, 2015). Consequently, the TOE framework encompasses these three dimensions to illustrate a clear overall picture of the factors that influence the adoption of innovations in organizations. According to (Hasan, Ali, Kurnia, & Thurasamy, 2021) the key factors influencing cyber security readiness in organizations based on the TOE framework include:

Technological Factors

The maturity of Organizational IT Infrastructure plays a significant role in enhancing an organization's readiness to counter cyber-attacks. Being mature in IT infrastructure by having the required resources cautionary of its experts, IT devices, and user software applications can result in enhancing readiness.

Organizational factors

Top management support of cyber security, Organizational structure, and Organizational Culture are important factors for readiness of cyber-attacks. Top management support has a positively significant impact on cyber security readiness.

Environmental factors

Vendor / Partner Relationships, governmental regulations, and industrial policies are external environmental conditions that are positively helping to increase organization readiness to counter cyber-attack

Developing a cyber security culture is a complex process that considers organizational culture, subcultures, and frameworks. Organizational culture has been identified as an essential factor in shaping security cultures and security culture has been defined as a subculture within an organization. To establish a security culture that is part of the organization, the organization can explore the culture through dimensions such as artifacts and propose values, shared assumptions, organizational knowledge, and the required operational practices (Uchendu, Nurse, Bada, & Furnell, 2021).

5.3. Daily Habits for Better Digital Hygiene

A robust digital hygiene culture is a must in the ever-evolving ecosystem of start-ups. Driven by management from the top down, this culture emphasizes the importance of cybersecurity and data protection. To help foster this culture, start-ups must implement regular backups with hybrid protection, whereby data is stored both on-site and in the cloud. This will help protect against cyber-attacks and system failures and will ensure that the data is safe at all times. Encrypted backups are also of paramount importance, especially for industries such as healthcare where data protection compliance is non-negotiable.

It is essential to deploy anti-malware software that provides a comprehensive suite of features including real-time scanning, behavior monitoring, email protection, and web filtering to protect systems from getting infected with malicious software. On the other hand, start-ups should conduct proactive cyber security risk assessments regularly to determine possible threats and evaluate their likelihood and impacts, and the risk levels. The assessments will guide the implementation of effective mitigation measures to protect critical systems.

Developing comprehensive data management policies and protocols to enable the safe handling of data is a priority. Policies should describe policies and procedures for best practices in data protection, secure communication, and good Digital Hygiene. Regular training for employees The staff needs to be better informed about the digital threats and what they can do to help prevent them. This will keep your staff up to date with the latest Threats and Security measures.

Open communications organizationally allowing employees to raise security concerns comfortably, report suspicious activities, and discuss potential threats is vital to securing the environment. Having good cyber hygiene daily practices such as creating strong passwords, keeping up with software patches, encrypting data, and using secure communication channels must become a habit for employees.

Another cost-effective element to consider is looking at different anti-malware solutions, the cost, support, updates, and compatibility with your budget and the

way you operate. Just as startups should not be considering adding the above elements as add-ons, startups should not be treating these elements as add-ons. Startups need to be secure online, protect their assets, and build trust with their customers and partners so to do this, startups need to make digital Hygiene and Cybersecurity part of their DNA. Startups need to weave digital maintenance and cyber hygiene throughout their daily operational activity is the only true way of raising startups' online security thereby making them cyber resilient. Cyber Hygiene is brushing your teeth and secure digital practices, whereas Cybersecurity is having a Mouth Guard on top of brushing your teeth. Deposit you have one you cannot have the other, both are very much required.

5.4. Digital Hygiene Integration: Case Study and 1 Good practice from startups

Best Practices: Top Digital Hygiene Tools for Startups

Context: In this digital age, start-ups and any special business if highly reliant on technology for their operational activities then it is very important to keep digital hygiene in place to keep safe from all digital threats and breaches of data. Every start-up should have certain digital hygiene tools that will help them protect their digital assets so they can continue their operational activities without any interruption.

Identifying Top Digital Hygiene Tools: Startups must equip themselves with a suite of digital hygiene tools to address various aspects of cybersecurity. Here is a list of a few tools from businesses and organizations trusted by large numbers of people.

1. **Antivirus Software**: Antivirus software is a system of controls that blocks detects & eliminates viruses and other malware in a particular software as well as protects the data from online threats.
2. **Firewalls**: Another network security system is the firewalls that are for Internet security devices designed to prevent unauthorized access to a network.
3. **Password Managers**: These will assist in creating and maintaining strong, unique passwords for all sites.
4. **Encryption Tools**: Encrypt data both at rest and in transit ensuring that sensitive data is unreadable to unauthorized users.
5. **Two-Factor Authentication (2FA)**: Adds extra security during a login process.
6. **Virtual Private Networks (VPN)**: Provides secure and encrypted connections to maintain privacy and data security over public networks.
7. **Secure Cloud Storage**: offers a place where you can back up your files in a safe spot. By only allowing certain people to get to it.

Testing the Effectiveness of Digital Hygiene Tools

First, we need to make sure the tools we chose were helpful:

1. **Compatibility Check**: Be sure that the tools that have been picked are compatible with the startup's current systems and additionally shall not interfere with workflows.
2. **Usability Assessment**: We need to perform tasks using the tools. To be successful in performing daily tasks using the tool does not consume too much time and data input
3. **Security Audit**: To test the effectiveness, the tools will be run regularly to notice if they are truly secure from the latest forms of cyber threats
4. **Training and Awareness**: Educating the team on the importance of digital hygiene and ethical and proper use of the tools.

Establishing a Culture of Digital Hygiene

Context Creating a culture of cyber hygiene in each startup is as important as the technology itself. Cybersecurity awareness and readiness is the idea of fostering an environment where each employee in each start-up recognizes the importance of cybersecurity and their role in protecting against a threat.

Setting up a Culture of Digital Hygiene In Your Business:

1. **Leadership Example**: Direct leaders need to lead by example and have good digital hygiene.
2. **Regular Training**: Educate employees as new threats arise.
3. **Clear Policies**: Have clear and well-defined internal policies for good digital hygiene.
4. **Encouraging Open Communication**: Create a culture where employees are rewarded for knowing or seeing digital hygiene issues.
5. **Rewarding Compliance**: Reward employees who show they exceed the baseline in digital hygiene.

Results and Impact Expected results of a culture of digital hygiene for a Startup:

- **Reduced Risk of Cyber Attacks**: A well-informed team is the first line of defense.
- **Enhanced Data Protection**: Protect your and your customer's businesses with appropriate digital hygiene.
- **Regulatory Compliance** Follow cybersecurity regulations and avoid financial and other penalties.

Key Takeaways: Start-ups need to be getting the basics right if they want to succeed long-term. Using top digital hygiene tools and getting a cyber resilience culture embedded in the business is essential to reduce the long-term costs of a breach and quicken the recovery period if the worst happens.

Case Study: SecureTech Start-up - Embracing Digital Hygiene for Cybersecurity

Executive Summary: SecureTech is a fintech start-up that realized the importance of digital hygiene as part of securing their company. This case study will provide an outline of the different tools and cultural shifts they made in their organization to create an even bigger gap for attackers to break through in their digital space.

Introduction: In an era of rapid evolution in cyber threats, SecureTech has a very tough task to do thereby protecting its digital assets and customer data. During the early stages of the start-up, company management understands the fact that robust digital hygiene isn't just a necessity for them but also a very critical competitive advantage.

Situation Analysis: After an initial cyber security assessment, the company discovered that they have a lot of areas to improve. SecureTech improved the tools to be used as regards digital hygiene and overall employee cyber security awareness.

Identifying Digital Hygiene Tools: After evaluating numerous tools associated with Digital Hygiene, SecureTech has identified a suite that will address their specific situation.

1. **BitDefender**: Protects all of your devices from various threats.
2. **Cisco Firewalls**: Monitors and controls network traffic.
3. **LastPass**: Password Manager of choice.
4. **VeraCrypt**: Encrypts all of your data.
5. **Duo Security**: Used for two-factor authentication.
6. **NordVPN**: Protects your remote connection and work from prying eyes.
7. **Dropbox Business**: Securely stores your backups and files in the cloud.

Establishing a Culture of Digital Hygiene: SecureTech leadership designed and introduced a digital hygiene program to the company.

CEO Commitment: Support for using the program companywide was aided by the CEO giving it his stamp of approval.

1. **Monthly cybersecurity training**: Workshops were held to keep the team informed of the latest threats and trends.

2. **Digital Hygiene Handbook:** A comprehensive set of policies and processes was provided as a Desk Drop to all associates.

3. **Security Champions:** Selected associates were trained to be Cybersecurity Advocates for their respective departments.

4. **Reward and Recognition for Secure Habits:** Individuals with excellent digital hygiene were recognized and rewarded.

Challenges and Solutions: The objections to our change: adoption of new tools, cultural shift in our digital hygiene practices.

1. Reduction of Roadblocks: Made sure our new digital toolkits increased each of our teams' efficiencies as opposed to slowing them down.

2. Making Security Training Fun: Implemented a game-based security training program that would rank teams according to their cyber skills.

3. **Keeping our Troops Informed:** Continually communicated the progress TeamSecureTech was making and the IMPACT their digital hygiene efforts were having on their company's security.

Results: Within a year, SecureTech reported:

100% Digital Hygiene Tool Adoption – The tools chosen had full adoption by staff

80% Reduction in Phishing Attempts – Increased staff awareness allowed for quicker recognition and reporting of suspicious emails

Improved Compliance Posture – All regulatory standards were met, and no fines were encountered

Conclusion

One of the complex issues thus far which Facebook has to negotiate with the adoption of a digitalized world is the observance of the right digital hygiene. This chapter has demonstrated that by adopting a holistic approach to cybersecurity, incorporating tools such as antivirus software, two-factor authentication, encryption, and secure cloud storage, start-ups can significantly reduce their vulnerability to cyber-attacks. However, tools alone are insufficient. A good internal culture of digital cleanliness with constant training and easy communication is the only thing that will add every member of an organization to the creation of such a secure digital environment.

Start-up SecureTech is an example of a company that set a new digital hygiene paradigm and it further showed that setting up the plan in the company resulted in improved compliance through curtailing the phishing attempts and the overall security was amped up. In the final analysis of a semi-technical requirement of a start-up, e.g. the cyber-hygiene, the issue is that the humanities' link to it is a distinct strategy. Enterprises that respect cybersecurity and integrate it into their culture are the ones that remain relevant to the digital-age society and it provides them a platform to be accountable for their business and also to the customer in the digital economy. SecureTech's highly proactive stance on digital hygiene has greatly improved its cybersecurity and developed a culture of vigilance and responsibility. This case study illustrates how a complex threat environment can be defeated through an effective control framework working in unison with a company's transformation in culture.

Chapter 6

Implications of Digital Hygiene in Startups

Anca Mustea[13]

Lucia Panea[14]

Like keeping good physical health, maintaining robust digital hygiene is key to being safer online. Digital hygiene should turn into a routine for all of us, both in our personal online lives and professional activities. As start-ups, when defining internal rules and policies you must include also digital hygiene rules and best practices to be followed by all the employees. Most of our work activities are performed using online digital environments. So, you must be aware of the possible risks and implement specific policies to mitigate them and maintain good digital hygiene in your startup.

Before considering implementing a digital hygiene policy, just a formal task that you must check, think of all the benefits it can bring. So, implementing a digital hygiene policy for your startup is not nice, but a must-have to protect your employees' professional and personal lives. If you need some reasons to emphasize the need for digital hygiene practices in startups, let's review a few reasons why digital hygiene is crucial for them. Startups are small organizations, with limited resources and without the strong security infrastructure of larger organizations. This makes them attractive targets for cybercriminals and more susceptible to cyber threats. A digital hygiene policy helps implement efficient security measures and mitigate possible risks. In conclusion, for startups, a digital hygiene policy serves as a foundational element for security, trust-building, scalability, cost-effectiveness, and operational efficiency. It helps set the tone for responsible and secure digital practices, which is crucial for the sustained success and growth of the startup in today's digital business landscape.

[13] eLearning & Software, anca.mustea@elearningsoftware.ro

[14] eLearning & Software, lucia.panea@elearningsoftware.ro

6.1. Benefits of Implementing Digital Hygiene Practices in Startups

For startups, implementing strong digital hygiene practices isn't just about ticking off a checklist—it's about building a foundation for long-term success. Startups often face the challenge of juggling many priorities with limited resources, making them more vulnerable to cyber threats like data breaches, phishing attacks, and ransomware. By embedding good digital hygiene from the start, startups can protect sensitive information like customer data, employee records, and intellectual property. Simple practices like using strong, unique passwords, enabling multi-factor authentication, and keeping software up-to-date can prevent many common cyberattacks that might otherwise derail a startup before it even gets off the ground.

In today's digital landscape, startups frequently handle large amounts of data, whether it's customer information, financial transactions, or proprietary technology. Ensuring this data is secure not only maintains operational integrity but also builds trust with clients and investors, who need to feel confident that the company takes cybersecurity seriously. This trust is invaluable, especially for a startup trying to carve out its place in a competitive market.

Good digital hygiene also boosts productivity. A well-secured and maintained digital environment reduces the risk of disruptions caused by malware or security breaches. Employees can work more efficiently when they're not dealing with preventable IT issues, and founders can focus on what matters most—growing the business. Additionally, startups that prioritize digital hygiene are more likely to comply with important regulations, such as GDPR. This helps avoid hefty fines and demonstrates to customers and partners that the company is not only innovative but also responsible and trustworthy.

Moreover, establishing a culture of digital hygiene can enhance a startup's reputation. In industries driven by technology, clients and investors are more likely to engage with companies that show they take security seriously. By emphasizing digital hygiene, startups position themselves as credible, reliable partners, which can help them stand out from competitors who might overlook this critical aspect of modern business. Ultimately, good digital hygiene is about protecting the startup's present and future. It ensures security, supports growth, and builds a positive reputation—helping startups navigate the complex digital world and thrive in the long run. Here is the main areas of the main benefits:

- **Security and maintenance:**

Implementing good digital hygiene policies and best practices will keep your workplace (and personal) digital environment secure. Do not forget to define maintenance rules, to be sure that all employees are aware of the internal policy, and that the rules are up to date with new possible threats. It is recommended to

perform periodic cybersecurity awareness training, to be sure that your team has the necessary knowledge to respond properly to possible new cyber threats. How can we sum up the main benefits for startups when they implement and maintain good digital hygiene practices to protect their security in the digital environment?

- **Security and data privacy compliance**

The protection of sensitive information is crucial. Regularly updating software, using strong passwords, and implementing encryption techniques can help safeguard sensitive data from cyber threats. Good digital hygiene helps in safeguarding sensitive information and prevents unauthorized access, reducing the risk of data breaches. Adhering to data protection regulations ensures that the startup avoids legal issues and builds trust with customers. Also, protecting financial and customer data is paramount for startups. Digital hygiene ensures secure online transactions and financial data integrity.

- **Reputation management and building trust**

Customers and partners trust businesses that prioritize digital security. Demonstrating a commitment to digital security and privacy can enhance the startup's reputation and build trust with customers, investors, and partners. Also, the negative impact of security incidents can be avoided. Well-maintained digital assets, including a user-friendly website and secure online transactions, contribute to a professional image.

- **Compliance and legal protection: meeting regulatory requirements**

Many industries have strict regulations regarding data protection and privacy. Adhering to industry-specific regulations and compliance standards helps startups avoid legal complications, fines, and reputational damage. Adopting these regulations not only protects the start-up from legal consequences but also helps in building a trustworthy brand image. Audits and reviews are another important aspect. Regularly auditing digital practices ensures that the startup remains compliant with evolving regulations and industry standards.

- **Operational continuity: mitigating downtime**

Cybersecurity incidents, such as malware attacks or data loss, can lead to significant downtime. Digital hygiene measures help in preventing and mitigating such incidents, ensuring uninterrupted business operations.

- **Cost Savings: avoiding financial losses**

Recovering from a cybersecurity incident can be expensive. Regular backups and secure storage methods can prevent data loss, saving the startup from the potentially high costs associated with recovering lost information. Investing in digital security measures early on is a proactive approach that helps prevent potential financial losses due to cyberattacks, such as ransomware or data breaches.

- **Innovation and growth: fostering innovation**

A secure digital environment allows startups to focus on innovation without being constantly distracted by cybersecurity concerns. This fosters creativity and accelerates business growth. By automating routine tasks and optimizing digital workflows, startups can free up time and resources to focus on innovation and strategic initiatives. Good digital hygiene ensures that the startup is technologically prepared to adopt new tools and technologies, staying competitive in the market.

- **Customer trust and loyalty: protecting customer information**

Customers are more likely to engage with businesses that prioritize the security of their personal information. Digital hygiene builds customer trust and loyalty, contributing to long-term relationships.

- **Supply chain security: ensuring vendor and partner security**

Good digital hygiene practices extend beyond the startup's internal systems to include secure communication and data exchange with vendors and partners, ensuring a secure end-to-end supply chain.

- **Adaptability to emerging threats: staying ahead of threats**

Digital hygiene involves staying informed about the latest cybersecurity threats and implementing measures to counteract them. This adaptability is crucial in the ever-evolving landscape of cyber threats.

We are overwhelmed by the numerous digital technologies, and online platforms that we spend our time during the day. We should not neglect the impact they may have on our mental health. If during work time we follow the existing rules from our organizations, in our personal lives we should also implement good digital hygiene. Being careful with your screen time, avoiding over-exposure and over-time on social media, and using a password manager and two-factor authentication for your accounts will bring you only safety.

Implementing good digital hygiene practices has only benefits for the employees' productivity and morale. Distractions are reduced and employees can be more productive when they are not constantly dealing with security issues. A secure digital environment promotes a positive workplace atmosphere and boosts morale. Also, we can mention as additional benefits of implementing and maintaining digital hygiene practices:

- **Efficient workflow.** Proper organization of digital assets and files can streamline work processes, enabling employees to find information quickly and complete tasks more efficiently.
- **Collaboration.** Digital hygiene practices, such as using collaborative tools and cloud storage, enhance teamwork by providing a centralized platform for communication and file sharing.

- **Easy adaptation to growth and scalability**. Implementing scalable digital solutions from the beginning allows startups to grow without significant disruptions or the need for major overhauls of digital infrastructure.
- **Flexibility.** Maintaining a clean and organized digital environment provides the flexibility to adapt to **changing business needs and market trends.**
- **Agility.** Startups, known for their agility, benefit from efficient workflows and collaboration enabled by a well-implemented policy.

To sum up, for startups, a digital hygiene policy serves as a foundational element for security, trust-building, scalability, cost-effectiveness, and operational efficiency. It helps set the tone for responsible and secure digital practices, which is crucial for the sustained success and growth of the startup in today's digital business landscape.

6.2. Potential Threats and Consequences of Neglecting Digital Hygiene

In March 2023, the European Union Agency for Cybersecurity (ENISA) published an extensive report on cybersecurity threats and challenges for 2030 to increase the awareness of future threats and countermeasures among its member states and stakeholders (Mattioli et al., 2023). Many of the threats identified are already relevant today, and in the following years, they will remain pressing. In October 2023, the same agency published a report on threats that were reported during July 2022 and June 2023: ENISA Threat Landscape 2023 (Lella, 2023).

Though the audience and the stakeholders of these reports are wide, from both the public and private sectors, they are particularly relevant in the context of startups. The latter are particularly vulnerable to cyber threats due to a combination of factors, often related to their structure, resource constraints, and the rapidly evolving nature of the business environment. As emerging businesses increasingly rely on technology and online platforms for their operations, they become more susceptible to cyberattacks. As pointed out previously, the potential consequences of falling victim to cyber threats include data breaches, financial losses, damage to reputation, and even business interruption. Start-ups often handle sensitive information while lacking the infrastructure and resources bigger organizations have, making them attractive targets for cybercriminals seeking to exploit vulnerabilities.

The vulnerability of startups to cyber threats can also have significant impacts on the economy at large and various other public structures. For example, several ways in which startup vulnerabilities can influence broader economic and societal aspects can include economic losses, job losses and unemployment, innovation slowdown, loss of intellectual property, customer trust erosion, supply chain disruptions, regulatory and legal ramifications, increased government intervention, and even national security concerns. Therefore, startups need to

acknowledge and increase awareness regarding all existing and potential future threats to protect themselves and society at large.

A comprehensive understanding of cyber threats and the implementation of robust security measures are imperative for start-ups to mitigate risks and establish a resilient foundation for long-term success in the digital realm. To help raise awareness of the variety of cyber threats, we will present below the ones included in the „ENISA Threat Landscape 2023" report (Lella, 2023).

The main threats included in the report are Ransomware, Malware, Social Engineering, Threats against data, Denial of Service, Internet threats, Information Manipulation, and Supply Chain Attacks. We defined them shortly and then included the definitions from the „ENISA Threat Landscape 2023" report.

1. **Ransomware.** Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money, or ransom, is paid to the attacker. It can encrypt files, making them inaccessible to the victim.
2. **Malware.** Malware, short for malicious software, is a term used to describe any software or code created with the intent to harm a computer system, steal data, or disrupt normal operations. It includes various types such as viruses, worms, and trojan horses.
3. **Social Engineering.** Social engineering is a method of manipulating individuals to disclose sensitive information or perform actions that may compromise security. Techniques include phishing, impersonation, and psychological manipulation to exploit human behavior.
4. **Threats against data.** Threats against data encompass intentional or unintentional actions that compromise the confidentiality, integrity, or availability of data. This includes data breaches, leaks, or any unauthorized access or disclosure of sensitive information.
5. **Denial of Service (DoS).** Denial of Service is an attack that aims to disrupt or disable the normal functioning of a computer system, network, or service, making it temporarily or indefinitely unavailable to users. Distributed Denial of Service (DDoS) involves multiple systems coordinating the attack.
6. **Internet threats.** Internet threats refer to intentional or unintentional disruptions of Internet or electronic communications, causing outages, blackouts, shutdowns, or censorship. These threats can result from various factors, including cyberattacks, technical problems, or government-directed actions.
7. **Information Manipulation.** Information Manipulation involves intentional, coordinated efforts to negatively impact values, procedures, and political processes. This can include spreading misinformation, fake news, or conducting activities that manipulate public opinion or disrupt normal information flows.
8. **Supply Chain Attacks.** Supply Chain Attacks target the relationship between organizations and their suppliers. These attacks involve

compromising the security of the supply chain to gain unauthorized access or influence over a target organization. Examples include the compromise of software updates or hardware components.

Prime Threats defined in the “ENISA Threat Landscape 2023” report
„Ransomware
According to ENISA’s Threat Landscape for Ransomware Attacks report, ransomware is defined as a type of attack where threat actors take control of a target’s assets and demand a ransom in exchange for the return of the asset’s availability. This action-agnostic definition is needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques, and the various goals, other than solely financial gains, of the perpetrators. Ransomware has been, once again, one of the prime threats during the reporting period, with several high-profile and highly publicized incidents.

Malware
Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system.

Social Engineering
Social engineering encompasses a broad range of activities that attempt to exploit human error or human behavior with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured to open documents, files, or e-mails, to visit websites, or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful. This threat canvas consists mainly of the following attack vectors: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps, and scareware. While social engineering techniques are often used to gain initial access, they may also be used at later stages in an incident or breach. Notable examples are business e-mail compromise (BEC), fraud, impersonation, counterfeiting, and, more recently, extortion.

Threats against data
A data breach is defined in the GDPR as any breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed (article 4.12 GDPR). Technically speaking, threats against data can be mainly classified as data breaches or data leaks. Though often used

as interchangeable concepts, they entail fundamentally different concepts that mostly lie in how they happen. A data breach is an intentional cyber-attack brought by a cybercriminal with the goal of gaining unauthorized access and releasing sensitive, confidential, or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organization with the intention to steal data. A data leak is an event (e.g. misconfigurations, vulnerabilities, or human errors) that can cause the unintentional loss or exposure of sensitive, confidential, or protected data (intentional attacks are sometimes referred to as data exposure).

Threats against availability: Denial of Service
Availability is the target of a plethora of threats and attacks, among which DDoS stands out. DDoS targets system and data availability and, though it is not a new threat, it plays a significant role in the cybersecurity threat landscape6 7. Attacks occur when users of a system or service are not able to access relevant data, services, or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure8.

Threats against availability: Internet threats
Threats to Internet availability refer to intentional or unintentional disruptions of the Internet or electronic communications that result in Internet outages, blackouts, shutdowns, or censorship. Internet disruptions can be due to government-directed Internet shutdowns, cyclones, massive earthquakes, power outages, cable cuts, cyberattacks, technical problems, and military actions. These threats are diversifying and growing, having reached a new record in this reporting period and having caused huge monetary losses to national economies.

Information Manipulation
Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character and conducted in an intentional and coordinated manner. FIMI can be carried out by state or non-state actors, including their proxies inside and outside of their territory, whereas in this report we study the threat regardless of its origin.

Supply Chain Attacks
A supply chain attack targets the relationship between organizations and their suppliers. For this ETL report, we use the definition as stated in the ENISA Threat Landscape for Supply Chain Attacks10 in which an attack is considered to have a supply chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets. SolarWinds was one of the first revelations of this kind of attack and

> showed the potential impact of supply chain attacks. It was observed that threat actors are continuing to feed on this source to conduct their operations and gain a foothold within organizations, to benefit from the widespread impact and large victim base of such attacks."
>
> Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA, pp. 6-8

In addition to the cyber threats defined above (Ransomware, Malware, Social Engineering, Threats against data, Denial of Service, Internet threats, Information Manipulation, and Supply Chain Attacks), startups may face various other cybersecurity threats. Some additional threats to be aware of are:

1. **Phishing Attacks.** Phishing involves the use of deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as usernames, passwords, or financial details. Phishing attacks can be highly targeted (spear-phishing) or more widespread.
2. **Man-in-the-Middle (MitM) Attacks.** In MitM attacks, an unauthorized entity intercepts and potentially alters communication between two parties. This can lead to data theft, eavesdropping, or injection of malicious content into the communication stream.
3. **Zero-Day Exploits.** Zero-day vulnerabilities are software vulnerabilities that are unknown to the vendor and have not been patched. Threat actors may exploit these vulnerabilities before a fix is developed, posing a risk to any organization using the affected software.
4. **Advanced Persistent Threats (APTs).** APTs are sophisticated and targeted cyberattacks typically orchestrated by well-funded and organized threat actors. These attacks often involve a prolonged and stealthy infiltration of a network, aiming to steal sensitive information.
5. **IoT (Internet of Things) Vulnerabilities.** As startups increasingly integrate IoT devices into their operations, these devices can become potential targets for cyberattacks. Insecure IoT devices may be exploited to gain unauthorized access to networks or launch attacks.
6. **Cryptojacking.** Cryptojacking involves the unauthorized use of a computer or network's resources to mine cryptocurrency. Cybercriminals may infect systems with malware that silently mines cryptocurrency, impacting system performance.
7. **Cross-Site Scripting (XSS).** XSS attacks involve injecting malicious scripts into web pages viewed by other users. This can lead to the theft of user data, session hijacking, or the spreading of malware to other users.
8. **SQL Injection.** SQL injection attacks occur when malicious SQL code is injected into input fields, allowing attackers to manipulate a database. This can lead to unauthorized access, data manipulation, or data extraction.

9. **Fileless Malware.** Fileless malware operates in memory rather than relying on executable files. This makes it more challenging for traditional antivirus solutions to detect, as there may be no physical file to analyze.
10. **Credential Stuffing.** In credential stuffing attacks, cybercriminals use stolen username and password combinations from one service to gain unauthorized access to another service where users have reused credentials.
11. **DNS Spoofing and Cache Poisoning.** DNS spoofing involves redirecting domain name system (DNS) queries to malicious sites. Cache poisoning manipulates DNS cache data, leading users to unintended and potentially harmful destinations.

As mentioned, the „ENISA Threat Landscape 2023" report (Lella, 2023) shows that the primary threats worldwide and in the EU are: Ransomware, Malware, Social Engineering, Threats against data, Denial of Service, Internet threats, Information Manipulation, and Supply Chain Attacks.

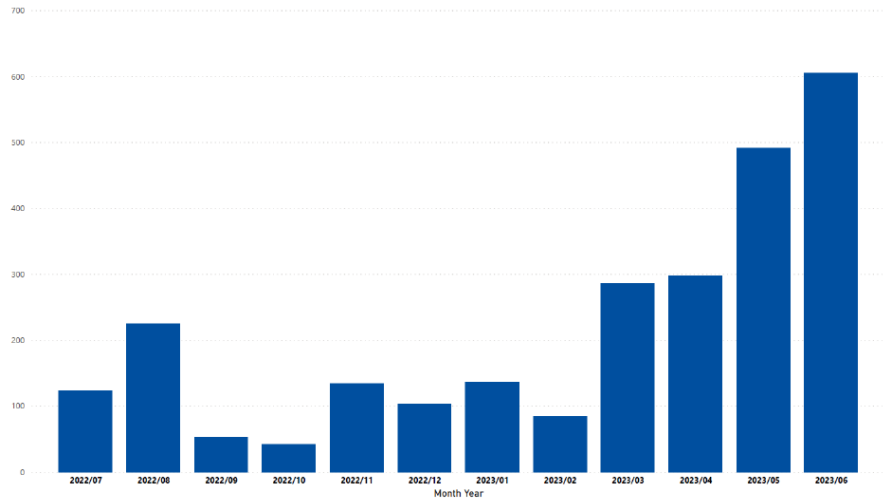


Figure 1. Timeline of EU events (count of number of observed incidents per month) (Lella, 2023)

The report illustrates (Figure 1) the increase in cyberattacks in the first part of 2023. This increase is reflected both at the global and EU level. The increase might not reflect only the increase in numbers, but also the awareness of such events happening. Nonetheless, the trend is worrisome.

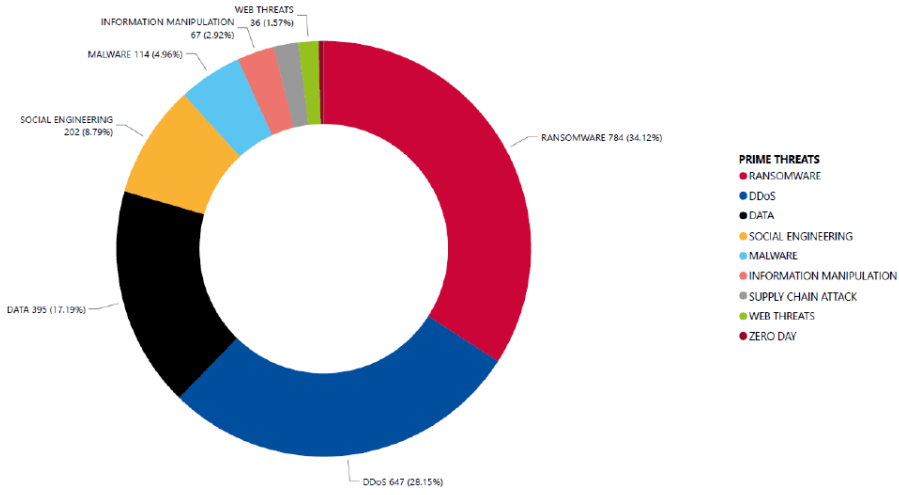


Figure 2. EU breakdown of number of threats by threat group (Lella, 2023)

We can see in Figure 2 that the most frequent threats were: Ransomware, Denial of Service, Threats against data, Social Engineering, and Malware. These were followed by Information Manipulation, Supply Chain Attacks, Internet threats, and Zero Day.

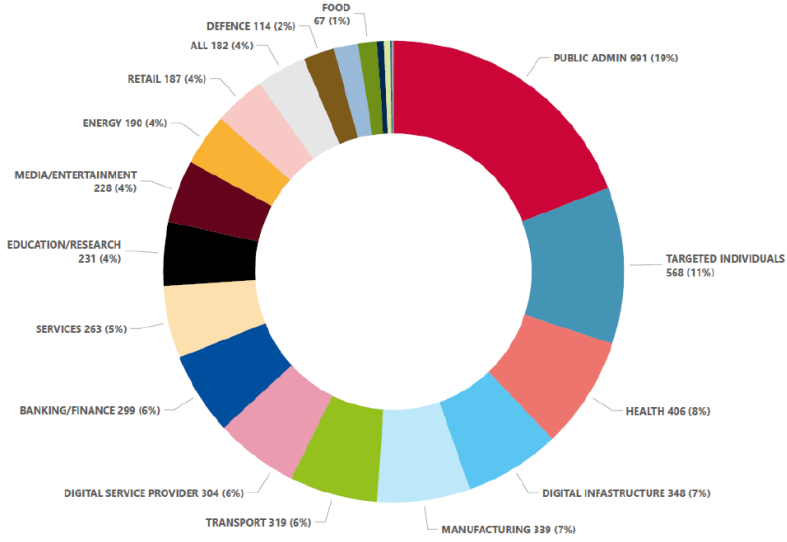


Figure 3. Targeted sectors per number of incidents (July 2022 - June 2023) (Lella, 2023)

A sectorial analysis reveals that threats transcend the boundaries of specific industries or sectors, exerting their influence across a broad spectrum of areas (Lella, 2023). This might be due to the high interconnectivity of today's digital world.

In the overall global landscape, a large number of events were targeting organizations in the public administration (19%) and health (8%) sectors. We can see that one of the main actors threatened are individuals (11%). Even though this might appear unrelated to startups and the private sector, these individuals might be employees in some startup companies, and they might unintentionally put the companies at risk.

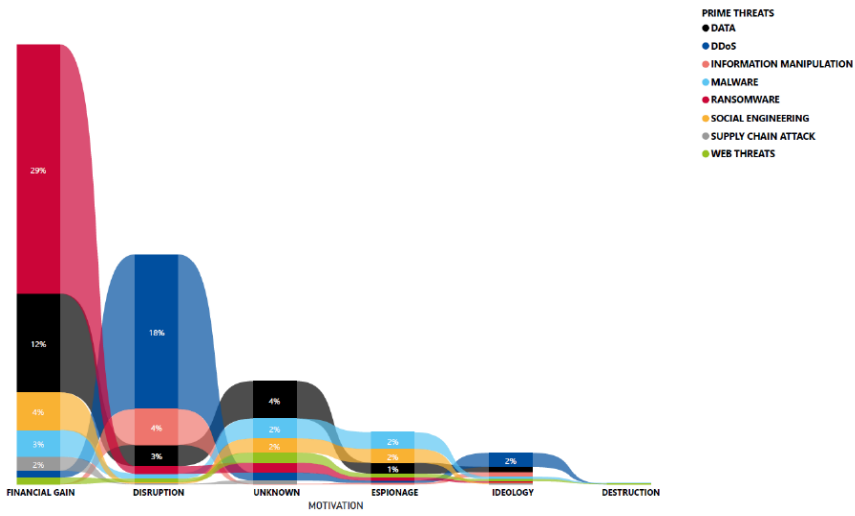


Figure 4. Motivation of threat actors per threat category (Lella, 2023)

The report also presents the motivations behind the cyber-attacks during the set period (Lella, 2023). As can be seen from Figure 4, most attacks had financial gain, followed by disruption, unknown, espionage, and ideology. Ransomware accounts for almost 30% of attacks conducted for financial gain, followed by threats against data, social engineering, and malware.

Being aware of the reasons behind cyber threats and the types of threats could inform and guide the strategy used by startups to develop and implement digital hygiene practices. For example, startups and the private sector are mostly targeted for financial gains. Knowing that Ransomware, Threats against data, Social

Engineering, and Malware were predominantly used for such purposes, start-ups might focus their digital hygiene strategy on protecting access to data and the education of clients and employees to protect themselves from Social Engineering threats.

To help understand how a startup should approach cyber threats and what they need to do to protect themselves, we prepared an example of good practice. This will illustrate how a company should deal with possible threats and how should prepare to prevent cyber events from happening.

6.3. The Good Practice from Startups

To better understand how to identify threats and how to handle the situation beforehand, let's consider the following example. We focused the example on the vulnerability that can arise from online payment, which is a widespread and common situation that can affect both the company and the clients in the situation of a cyber-attack.

Digital Hygiene in Online Payment Security

Context

In the fast-evolving landscape of mobile app development, where innovation intersects with financial transactions, ensuring the security of an app that processes online payments becomes paramount. An example is one of a company that offers a mobile app subscription, which might raise a vulnerability associated with their payment processing. The potential vulnerability in their online payment processing system could expose both the company and its clients to risks of financial fraud.

The startup needs to analyze the situation, identify the risks, and implement solutions to prevent any vulnerabilities and financial fraud situations.

Step 1. The Situation Analysis

As a first step in the digital hygiene process, we have the situation analysis. During this phase, it's important to identify the vulnerabilities and to assess the risk and implication of these vulnerabilities in the case of a security breach.

Identifying the Payment Security Vulnerability:

The company conducted a thorough analysis of the app's payment processing functionality to identify potential weak points, including insecure payment gateways, vulnerabilities in transaction encryption, and potential points of unauthorized access.

Conducting a comprehensive analysis of a payment app to identify potential weak points involves a systematic and thorough examination of various components within the application. A general guideline for conducting such an analysis could include:

1. **Risk Assessment:** Identify and understand the critical components of the payment app, including user authentication, data storage, payment processing, and communication with external servers.
2. **Regulatory Compliance Check:** Ensure that the payment app adheres to relevant regulatory standards and compliance requirements in the industry, such as the Payment Card Industry Data Security Standard (PCI DSS).
3. **Data Flow Mapping:** Map out the flow of sensitive data (e.g., credit card information) within the app, from input to storage and transmission. Identify potential points of vulnerability in this data flow.
4. **Network Security:** Assess the security of network communications, including the use of secure protocols (HTTPS), encryption, and secure sockets layer (SSL) certificates.
5. **Authentication Mechanisms:** Evaluate the strength of user authentication mechanisms. Implement multi-factor authentication to add an extra layer of security.
6. **Payment Gateway Security:** Examine the integration with payment gateways, ensuring that secure and reputable services are used. Regularly update and patch payment gateway software.
7. **Data Encryption:** Implement end-to-end encryption to protect sensitive user data throughout the entire transaction process.
8. **Vulnerability Scanning and Penetration Testing:** Conduct regular vulnerability scans and penetration tests to identify potential weaknesses and simulate real-world attack scenarios. This can involve using automated tools or hiring third-party security firms with expertise in penetration testing.
9. **Code Review:** Perform a thorough code review to identify any vulnerabilities or weaknesses in the app's source code. Ensure that coding practices follow security best practices.
10. **Incident Response Plan:** Develop and implement an incident response plan to address and mitigate potential security breaches promptly. This includes having procedures in place for notifying users in the event of a security incident.
11. **Third-Party Security Audits:** Consider engaging third-party security firms that specialize in application security audits. These firms can bring an independent perspective and specialized expertise to identify vulnerabilities.

You can use these points as a checklist to perform your analysis.

Security is an ongoing process, and regular reviews and updates are crucial to staying ahead of emerging threats. The points on the checklist mentioned above can change over time, according to the possible threats and the cyber security landscape. Engaging with third-party security firms or consultants can provide additional expertise and insights, particularly when it comes to thorough security audits and penetration testing. It's essential to prioritize the security of payment apps to protect both the business and its users from potential risks and breaches.

Let's assume that during a routine security audit, the startup security team identifies a potential weakness in the encryption protocol used for transmitting payment data within their mobile app. Next, the team needs to assess the vulnerability and its implications for the company and the users.

Assessing Risks and Implications:

After identifying the payment security vulnerabilities, it is important to consider risks and implications for both the company and the users. This part of the process involves evaluating the risks for the company, and the users, and prioritizing the identified vulnerabilities according to the potential impact.

1. **Impact assessment:** Evaluate the potential impact of a security breach on both the company and its users, considering financial losses, reputational damage, and potential legal consequences.
2. **Prioritization:** Prioritize vulnerabilities based on the severity of the potential impact and the likelihood of exploitation.

During the evaluation of the risks associated with the weakness in the encryption protocol, the security team evaluates the extent of the vulnerability, considering factors such as the type of encryption algorithm in use, the scope of potential exploitation, and the impact on user data security.

The risk analysis aims to understand the potential consequences of the encryption vulnerability, including the risk of unauthorized access to sensitive payment information and the potential impact on the company's reputation.

Step 2. Finding a Solution

The solutions for possible payment security vulnerabilities would include:

1. **Secure Payment Gateway Integration:** Upgrade the payment processing system to integrate with a secure payment gateway, ensuring that all transactions are encrypted and protected from interception during transmission.
2. **End-to-end Encryption:** Implement end-to-end encryption for all payment transactions, protecting sensitive user data from unauthorized access at every stage of the transaction process.
3. **User Authentication Enhancements:** Strengthen user authentication measures, incorporating multi-factor authentication to ensure that only authorized users can access and conduct transactions within the app.
4. **Regular Security Audits and Compliance Checks:** Institute routine security audits specifically focused on the payment processing functionality, conducting compliance checks with industry standards and regulations.

In the more specific care of the weakness in the encryption protocol we used as an example, the response and mitigation would include:

1. **Immediate Containment:** The company takes immediate action to contain the vulnerability by temporarily disabling the affected encryption protocol to prevent any further potential exploitation.
2. **Communication with Stakeholders:** The company initiates transparent communication with its users, notifying them about the identified encryption vulnerability, the temporary suspension of the affected feature, and the ongoing efforts to address the issue.
3. **Engagement of Security Experts:** The company engages the services of external cybersecurity experts to conduct an in-depth analysis of the encryption vulnerability and provide recommendations for a more robust and secure encryption solution.
4. **Development of a Patch:** Based on the recommendations from the security experts, the development team creates a patch that addresses the encryption vulnerability. This includes implementing a more secure encryption algorithm and ensuring compatibility with existing systems.
5. **Internal Testing:** Before deploying the patch, the company conducts thorough internal testing to ensure that the updated encryption measures do not introduce any new vulnerabilities or disrupt the functionality of the payment app.
6. **Deployment of the Patch:** Once the patch is deemed effective and secure, the company deploys the update across all users' devices, reinstating the payment functionality with enhanced encryption measures.
7. **Post-Implementation Monitoring:** The company closely monitors the app's performance post-implementation to ensure that the encryption patch successfully mitigates the vulnerability and does not introduce any unforeseen issues.
8. **User Education:** To rebuild user trust, the company could launch an educational campaign within the app, informing users about the encryption vulnerability, and the steps taken to address it, and providing tips on maintaining secure usage practices.

The steps in this response are specific to the identified problem. If the security audit identifies a different problem, then specific responses for that problem would be deployed.

Step 3. Results and Impact

The company’s targeted approach to digital hygiene in app security for online payments yielded positive outcomes:

- Zero instances of unauthorized transactions or security breaches over one year.
- Increased user confidence and trust in the app, leading to a rise in the number of transactions and positive user reviews.
- Compliance with industry regulations, positioning the company as a secure and trustworthy platform for online payments.

Key Takeaways

Start-ups offering payment processing apps can draw valuable insights from this example:

- Prioritize the integration of secure payment gateways to protect transaction data.
- Implement end-to-end encryption to safeguard user data throughout the payment process.
- Enhance user authentication measures, incorporating multi-factor authentication for added security.
- Conduct regular security audits and compliance checks to stay ahead of potential vulnerabilities and ensure alignment with industry standards.

By adopting these digital hygiene practices, payment processing app developers can contribute to creating a secure and reliable platform, fostering trust among users engaging in online financial transactions.

Conclusion

In conclusion, fostering strong digital hygiene practices is not just a protective measure but an essential part of ensuring the long-term success and growth of any startup. Startups, often operating with limited resources and a focus on rapid growth, face unique risks when it comes to cybersecurity threats. By adopting digital hygiene—such as secure payment systems, robust data encryption, and regular security checks—startups can safeguard their sensitive information, build trust with clients and investors, and prevent costly cyberattacks that could threaten their progress.

But it's not only about security. Creating a culture that prioritizes digital hygiene helps a startup operate more smoothly while ensuring compliance with important regulations. This not only helps avoid potential legal issues but also strengthens the company's credibility, making it a more reliable and trusted partner in the eyes of customers and investors.

As startups continue to grow and innovate, maintaining these digital hygiene practices becomes a continuous process. It's not just about staying safe in the present, but being prepared to face future challenges in the digital world. By doing so, startups can set themselves up for sustainable growth, protecting both their own interests and the trust of the people they rely on.

BIBLIOGRAPHY

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

Alharbi, B., Alzahrani, H., Asseri, A., & Taramisi, K. (2020). Anti-malware efficiency evaluation framework. 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (s. 1-4). IEEE.

Alkhaledi, R., & Hawamdeh, S. (2023). Electronic health records and cyber hygiene: a qualitative study of the awareness, knowledge, and experience of physicians in Kuwait. Proceedings of the Association for Information Science and Technology, 60(1), s. 21-30.

Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional.

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. Global Knowledge, Memory and Communication, 73 ((1/2)), 1-23.

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

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.

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.

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]

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]

Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.

Berlilana,Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761.

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

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

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

Bishop, M. (2018). *Computer Security: Art and Science*. Addison-Wesley.

Blocki, J., & Liu, P. (2023). Towards a rigorous statistical analysis of empirical password datasets. 2023 IEEE Symposium on Security and Privacy (SP), 606-625.

Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill Osborne Media.

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

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)

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]

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]

Bruce Schneier's Blog, Website: https://www.schneier.com/

Bruzgiene, R., & Jurgilas, K. (2019). Securing remote access to information systems of critical infrastructure using two-factor authentication. Electronics, 10(15), 1819.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications, 42, 36-45.

Caloyannides, M. A. (2010). *Privacy Protection and Computer Forensics* (2nd ed.). Artech House.

Carias, J. F., Borges, M. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). a systematic approach to cyber resilience operationalization in SMEs. IEEE Access, 8, s. 174200-174221.

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

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

Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8th ed.). Sybex.

Chavez, Z., Hauge, J. B., Bellgran, M., Gullander, P., Johansson, M., Medbo, L., & Ström, M. (2020). Digital tools and information need assessment for efficient deviation handling in SMEs. Advances in Transdisciplinary Engineering., 13(SPS2020), 24 - 35.

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

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]

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

Cisco. (n.d.) Cisco Learning Network Store. Retrieved from https://learningnetworkstore.cisco.com/ [Access Date 06.12.2023]

CivicERT. (n.d.). Retrieved from CiviCERT

Clarke, N. L., & Furnell, S. M. (2016). *Cybersecurity Education: Strategies and Best Practices*. Springer.

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

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.

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

CyberSec Europe https://www.cyberseceurope.com/

Cybersecurity & Infrastructure Security Agency (CISA) Website: https://www.cisa.gov/.

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]

Dafoulas, G. A., & Maia, C. (2015). *Global Security, Safety, and Sustainability: Tomorrow's Challenges of Cyber Security*. Springer.

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]

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. arXiv preprint, 1309, 5344.

Di Tizio, G., Armellini, M., & Massacci, F. (2022). Software updates strategies: A quantitative evaluation against advanced persistent threats. IEEE Transactions on Software Engineering, 49(3), 1359-1373.

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

Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [accessed April 15, 2024].

Digital hygiene: the most important unfinished business: https://www.telefonica.com/en/communication-room/blog/digital-hygiene-the-most-important-unfinished-business/

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

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/

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]

Easttom, C. (2019). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education.

Eckert, J. W. (2017). *CompTIA Linux+ Guide to Linux Certification*. Cengage Learning.

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

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. IEEE Access, 9, 143997-144016.

Enck, W. (2011). *Understanding Android Security*. IEEE Security & Privacy Magazine.

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

European e-Competence Framework, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accessed April 15, 2024].

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]

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].

Federal Trade Commision 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]

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.

FinTech Innovations https://www.fintechinnovation.no/

Fritzvold, E. (2017). Cyber Security in Organizations. (Master's thesis, University of Stavanger, Norway).

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management, 28(1), 107-130.

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/

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]

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]

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

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

Goodrich, M. T., & Tamassia, R. (2019). *Introduction to Computer Security*. Pearson.

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

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

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]

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

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

Han, W., Sun, C., Shen, C., Chang, L., & Shen, S. (2013). Dynamic combination of authentication factors based on quantified risk and benefit. Security and Communication Networks, 7(2), 385-396.

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

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business &Amp; Economics, 3(5).

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/ Digital First Aid. (n.d.). Retrieved from Digital First Aid Kit

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

Infosec Institute, Website: https://resources.infosecinstitute.com/

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. Proceedings of the Sigchi conference on human factors in computing system, (s. 383-392).

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]

Jones, C. (2022, 11 24). Expert Insights. https://expertinsights.com/insights/the-most-significant-password-breaches/ Dresden alındı

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behavior among software engineers: a systematic literature review. IEEE Access, 9, s. 99339-99363.

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

Kato, K., & Klyuev, V. (2013). Strong passwords: Practical issues. 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS). 2, s. 608-613. IEEE.

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.

Keszthely, A. (2013). About passwords. Acta Polytechnica Hungarica, 99-118.

Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

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/

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/

Krebs on Security,Website: https://krebsonsecurity.com/

Kumar, P. (2008). Computer virus prevention & anti-virus strategy. Sahara Arts & Management Academy Series.

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.

Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA

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.

Liska, A., & Gallo, T. (2016). *Rethinking the Security of the Internet of Things*. Elsevier.

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organizations. Proceedings of the International Conference on Industrial Engineering and Operations Management, (s. 1-13).

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

Mathur, A., Malkin, N., Harbach, M., Péer, E., & Egelman, S. (2018). Quantifying users' beliefs about software updates., (s. Proceedings 2018 Workshop on Usable Security.).

Mattioli, R.; Malatras, A.; Hunter, E.N.; Biasibetti Penso, M.G.; Bertram, D.; Neubert, I. (2023). Identifying Emerging Cyber Security Threats and Challenges for 2030. ENISA

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

Min, B., & Varadharajan, V. (2015). Design, implementation, and evaluation of a novel anti-virus parasitic malware. Proceedings of the 30th Annual ACM Symposium on Applied Computing, (s. 2127-2133).

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. Sensors, 22(2), 538.

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software update management in the industrial Internet of Things (IoT) era. Sensors, 20(24), Sensor.

Mughal, A. A. (2019). Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. Applied Research in Artificial Intelligence and Cloud Computing, 2(1), 1-31.

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)

Nadee, P., & Somwang, P. (2021). Efficient incremental data backup of unison synchronize approach. Bulletin of Electrical Engineering and Informatics, 10(5), 2707-2715.

Naie, H., & Teymournejad, K. (2012). Choosing the best anti-virus in the world by application of the TOPSIS method. Life Science Journal, 9(4).

National Institute of Standards and Technology (NIST) Cybersecurity Framework, Website: https://www.nist.gov/cyberframework

Ncube, C., & Maiden, N. (2004). Selecting cots anti-virus software for an international bank: Some lessons learned. Proceedings 1st MPEC Workshop.

Ncubukezi T., Mwansa L. Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid-19 Pandemic. Journal of Internet Technology and Secured Transactions (JITST), Volume 9, Issue 1, 2021.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. Computers & Security(92), 101731.

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. Information &Amp; Computer Security, 32(1), 38-52.

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

Open Web Application Security Project (OWASP), Website: https://owasp.org/

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

Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. Information Management & Computer Security, 18(2), 124-139.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.

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

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.

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

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]

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.

Rahayu, R., & Day, J. (2015). Rahayu, R., & Day, J. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia. Procedia-social and behavioral sciences, 195, 142-150.

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

Rock, T. (2023, 10). Invenioit. https://invenioit.com/continuity/10-best-practices-for-small-business-backup/ adresinden alındı

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. 2021 2nd International Conference on Intelligent Engineering and Management (iciem) (s. 429-434). IEEE.

Ross, R. S. (2013). *Managing Information Security Risks: The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Approach*. Addison-Wesley.

Sampaio, D., & Bernardino, J. (2015). Open source backup systems for SMEs. New Contributions in Information Systems and Technologies, 823-832.

Sampaio, D., & Bernardino, J. (2015). Open-source backup systems for SMEs. New Contributions in Information Systems and Technologies: Volume 1, 823-832.

SANS Institute, https://www.sans.org/

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]

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)

SecureHealth https://www.shpg.com/

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

ShareCert Toolkit. (n.d.). Retrieved from Cybersecurity Toolkit

Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. Test Engineering and Management, 8145-8152.

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]

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]

Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

SMEX. (n.d.). Retrieved from SMEX

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

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.

TechGenius https://techgenius.co.in/

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]

Tellini, N., & Vargas, F. (2017). Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform.

The Hacker News, Website: https://thehackernews.com/

Tipton, H. F., & Nozaki, M. K. (2013). *Official (ISC)2 Guide to the CISSP CBK* (4th ed.). CRC Press.

Toigo, J. W. (2009). *Disaster Recovery Planning: Preparing for the Unthinkable* (3rd ed.). Prentice Hall.

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/

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]

Traeger, A., Joukov, N., Sipek, J., & Zadok, E. (2006). Using free web storage for data backup. Proceedings of the Second ACM Workshop on Storage Security and Survivability.

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

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]

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

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

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

Vaniea, K. E., Rader, E., & Wash, R. (2014). Betrayed by updates: how negative experiences affect future security. Proceedings of the SIGCHI conference on human factors in computing systems, (s. 2671-2674).

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/

Vishwanath A., Seng Neo L., Goh P., Lee S., Khader M., Ong G., Chin. J. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, Volume 128, 2020, https://doi.org/10.1016/j.dss.2019.113160.

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.

What is cyber hygiene and why is it important?: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

What is Cyber Hygiene? Definition, Benefits, & Best Practices: https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.

World Economic Forum, “Future of Jobs Report 2023”, https://www.weforum.org/publications/the-future-of-jobs-report-2023/

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

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

Ye, Y., Wang, D., Lİ, T., & Ye, D. (2007). IMDS: Intelligent malware detection system. Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, (s. 1043-1047).

Yegen, C., Kirik, A.M., Çetinkaya, A. (2023). Sustainability, Digital Security, and Cyber Hygiene During the Covid-19 Pandemic. In: Mondal, S.R., Yegen, C., Das, S. (eds) New Normal in Digital Enterprises. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-19-8618-5_5

Zdziarski, J. A. (2015). *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media.

Gazi
κιταβενι

Merkez/Mağaza
53. Sokak No: 29
Bahçelievler / ANKARA
Tel : (0 312) 223 77 73 - 223 77 17
info@gazikitabevi.com.tr • www.gazikitabevi.com.tr

ISBN: 978-625-365-692-8
9 786253 656928

Gazi Kitabevi
Sosyal Bilimler Serisi