applied sciences

MDPI

Review

The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0

Kitty Kioskli [1,2,*], Theofanis Fotis [3], Sokratis Nifakos [4] and Haralambos Mouratidis [1]

[1] Institute of Analytics and Data Science (IADS), School of Computer Science and Electronic Engineering, University of Essex, Colchester SO4 3SQ, UK
[2] Trustilio B.V., 681017 Amsterdam, The Netherlands
[3] Centre for Secure, Intelligent and Usable Systems (CSIUS), School of Sport & Health Sciences, University of Brighton, Brighton BN2 4AT, UK
[4] Department of Learning, Management and Ethics, Karolinska Institute, 17177 Solna, Sweden; sokratis.nifakos@ki.se
* Correspondence: kitty.kioskli@essex.ac.uk

Abstract: The cyberspace depicts an increasing number of difficulties related to security, especially in healthcare. This is evident from how vulnerable critical infrastructures are to cyberattacks and are unprotected against cybercrime. Users, ideally, should maintain a good level of cyber hygiene, via regular software updates and the development of unique passwords, as an effective way to become resilient to cyberattacks. Cyber security breaches are a top priority, and most users are aware that their behaviours may put them at risk; however, they are not educated to follow best practices, such as protecting their passwords. Mass cyber education may serve as a means to offset poor cyber security behaviours; however, mandatory education becomes a questionable point if the content is not focused on human factors, using human-centric approaches and taking into account end users' behaviours, which is currently the case. The nature of the present paper is largely exploratory, and the purpose is two-fold: To present and explore the cyber hygiene definition, context and habits of end users in order to strengthen our understanding of users. Our paper reports the best practices that should be used by healthcare organisations and healthcare professionals to maintain good cyber hygiene and how these can be applied via a healthcare use case scenario to increase awareness related to data privacy and cybersecurity. This is an issue of great importance and urgency considering the rapid increase of cyberattacks in healthcare organisations, mainly due to human errors. Further to that, based on human-centric approaches, our long-term vision and future work involves facilitating the development of efficient practices and education associated with cybersecurity hygiene via a flexible, adaptable and practical framework.

Keywords: cyber hygiene; cyberattacks; healthcare; human factors

Citation: Kioskli, K.; Fotis, T.; Nifakos, S.; Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Appl. Sci.* **2023**, *13*, 3410. https://doi.org/10.3390/app13063410

Academic Editors: Stefano Silvestri and Francesco Gargiulo

Received: 7 February 2023
Revised: 3 March 2023
Accepted: 6 March 2023
Published: 7 March 2023

1. Introduction

The rapid evolution of cyberspace, over the last two decades, has had an impact on every facet of human life. The increase in the range, volume and speed of communications, which are offered within the cyberspace, have beyond doubt affected the way people are governed, how companies deliver their services and, overall, how societies interact. The cyberspace also depicts an increasing number of difficulties related to security. This is evident from how vulnerable critical infrastructures are to cyberattacks, while the global economy is unprotected against cybercrime and cyber-espionage. Damages of great value occur from spam, sophisticated Distributed Denial of Service (DDoS) attacks, viruses and worms. As a result, member states have a well-defined cyberspace in their security doctrines and military as a new domain of protection, investigation and conflict. Organisations, for

example EU and NATO, treat cybersecurity as an issue of great importance affecting the defence and security of member states and the organisations per se [1].

The terms Healthcare 4.0, Health 4.0, Medical Industry 4.0 and Healthcare Industry 4.0 are associated with 4IR in healthcare [2]. Technologies related to 4IR are manufacturing systems, cloud-based design and the industrial Internet of Things. The common major challenge with these internet technologies is the applicability of cyber security and data privacy [3].

Users, ideally, should maintain a good level of cyber hygiene, via regular software updates and development of unique passwords, as an effective way to become resilient to cyberattacks. Cyber hygiene refers to keeping proper guidelines and norms and involves establishing healthy cyber behaviours within the cyberspace to protect any available data from hackers [4]. However, it is evident from the high volume of attacks that many users keep poor cyber hygiene, as they share personal information via social networks and freely share passwords as well [5]. Hackers know well that the easiest way to access a system is to find a technical vulnerability or steal an individual's information. There is an urgent need to help individuals improve their behavioural responses and cyber hygiene.

Weak cybersecurity has a detrimental financial cost on society. More specifically, the Ponemon Institute [6] conducted the Second Annual Cost of Cyber Crime Study showing that US organisations' average cost of cyberattacks is $17.36 million, Japan's is 8.39 million, Germany's $7.84 million, United Kingdom's $7.21 million, Brazil's $5.27 million and Australia's $4.3 million. These average estimated values of the attacks are only increasing since 2014. The study indicated that the reasons that the organisations experience the attacks are 98% associated with malware, 70% associated with social engineering and phishing, 63% web-based attacks, 61% associated with malicious code, 55% associated with botnets, 50% associated with stolen devices, 49% associated with denial of services and 41% associated with malicious insiders. It is worth noting that the organisations that experienced social engineering and phishing-related attacks have risen by 8% from 2015 to 2016.

Besides organisations, which are clearly affected by cyberattacks, end users are also greatly impacted by major losses from these cybersecurity breaches. The FBI's Internet Crime Complaints Center (IC3) [7] has provided useful data on cybercrimes reported by American citizens. Only in 2015, 288,012 complaints of cybercrimes were filed in by the FBI and more than 40% of those complaints were followed by monetary losses. The same year, the total amount of losses was officially reported as $1,070,711,522, with $8421 being the average report of a loss. Even though gender and age are not detrimental factors influencing cybercrimes, it has been recorded that males aged 50–59 years had a high victim count of 31,473 and for females aged 40–49 years, 29,559 reported cybercrimes. Meanwhile, there were 1648 women and men in all age groups, who reported over $100,000 in losses.

Humans are often characterised as the weakest link in cyber security [8,9]. This is particularly accurate when it comes to personal computing environments since they are the target of 95% of the malicious attacks [10]. This may be explained by the fact that personal and home computing devices are not guarded by security staff, who also keep software and hardware up to date [11]. The rapid increase of cyber threats and cyberattacks make defensive behaviours from users extremely important. This is because, regardless of how secure a system may be, the user is frequently a critical backdoor into the data and entire network [12]. Hackers look for vulnerabilities to exploit, which may come from end users who are maintaining poor cyber hygiene, such as, for example, by revealing personal information or not complying with best practices [5].

Cyber security breaches are a top priority, and most users are aware that their behaviours may put them at risk; however, they are not educated to follow best practices, such as protecting their passwords. Even though there is a vast variety of available security options, users often do not know how to access those options, understand them and implement them [13]. Furthermore, end users lack an understanding of the essential cyber security actions that can be taken, and this can feed inappropriate behaviours and

attitudes [14]. Nevertheless, good cyber hygiene can enhance safe behaviours and can protect against upcoming threats and attacks [15].

Mass cyber education may serve as a means to offset poor cyber security behaviours; however, mandatory education becomes a questionable point if the content is not focused on human factors, using human-centric approaches and taking into account end users' behaviours, which is currently the case [16]. Many cybersecurity, information system and computer science courses do not include content, particularly addressing the weaknesses related to human factors in end users. On the one hand, in several institutions, coursework associated with human behaviour and cognition is not required of information systems or computer science students. This is frankly problematic since a human user will be the handler in a computer-based product. On the other hand, there is an evident shift, in many programs of study, in multidisciplinary approaches [17]. This significant shift in the cyber educational system represents a unique opportunity to set frameworks and guidelines related to good cyber hygiene, human-centric and multidisciplinary approaches. This will strengthen the content of the curricula and make their delivery more effective, while it will further provide practical implications in other fields where training in cybersecurity remains essential for all members of staff, such as governance [18].

It is worth noting that there is a strong connection between cybersecurity and the deep learning approach, as deep learning has shown significant potential in addressing many cybersecurity challenges. Deep learning is a subset of machine learning that involves training artificial neural networks with multiple layers to learn patterns and features from large amounts of data [19]. In the context of cybersecurity, deep learning algorithms can be used to identify and classify threats based on patterns and behaviours that are difficult to detect using traditional signature-based approaches.

One of the key applications of deep learning in cybersecurity, for example, is in the area of threat detection. Deep learning models can analyse large volumes of network traffic, log data and other security data to identify patterns and anomalies that may indicate a security threat. This can help security teams to detect and respond to threats more quickly and effectively. Deep learning is also being used in the development of advanced authentication and access control systems. These systems use deep learning algorithms to analyse user behaviour and identify anomalies that may indicate unauthorised access. This can help organisations to prevent insider threats and protect sensitive data.

Previous research has investigated this topic from various angles, such as by identifying attack paths and showing how a recommendation method can be used to classify potential future cyberattacks, from a risk management perspective [20]. Other additions from the literature include a contribution towards vulnerabilities and effective threats analysis by using machine learning models (i.e., BERT neural language model and XGBoost) to withdraw the most relevant information from the Natural Language documents mostly available online [21]. Another useful proposal is a deep learning technique presented for reliable classification and accurate detection of organic pollutants. This paper refers to water pollutants [19].

Overall, the deep learning approach has shown great promise in addressing many of the challenges associated with cybersecurity. As cyber threats continue to evolve and become more sophisticated, deep learning algorithms will likely play an increasingly important role in helping organisations to detect and respond to these threats.

The nature of the present paper is largely exploratory, and the purpose is two-fold: to present and explore the cyber hygiene definition, context and habits of end users in order to strengthen our understanding of users. Our paper reports the best practices that should be used by healthcare organisations to maintain cyber hygiene. To our knowledge, this is the first paper which collects and presents a concrete set of best practices and directly addresses healthcare organisations and the healthcare staff. Further to that, based on human-centric approaches, to facilitate the development of efficient practices and education associated with cybersecurity hygiene via a flexible, adaptable and practical framework.

2. Cyber Hygiene in the Cyberspace

Cyber hygiene originates from the concept of personal hygiene in the public health domain. In an extensive report exploring cyber hygiene practices across various nations, the European Union Agency for Network and Information Security (ENISA) [22] introduced that "cyber hygiene should be viewed in the same manner as personal hygiene and, once properly integrated into an organisation will be simple daily routines, good behaviours and occasional check-ups to make sure the organisations online health is in optimum condition".

Research in social sciences on cyber security has been focused on the security behaviours and risk factors of the end–end users, while there is limited research on developing measurements of cyber hygiene. In particular, according to previous approaches that assume that the end users are aware of cyber safety behaviours, they, therefore, focus on measuring the frequency of enactment of these behaviours [23].

It is of high importance to understand the role of how end users are processing information and their interpretation within a cybersecurity framework in an organisation. For instance, researchers have empirically demonstrated that individuals who systematically process information are less likely to get victimised during a spear phishing attack [24]. Therefore, plenty of cybersecurity awareness programs aim to enhance the ability of the users to process better information.

The lack of cyber hygiene leads to a number of cyber threats and cyberattacks, as described below. The recent WannaCry Ransomware cyberattack [25], which targeted, on a large scale, the Microsoft Windows operating system, had a severe impact on the systems. This occurred due to the organisations and individuals not having updated their software security versions as of the month of March, even though the more recent version had been released in 2014. This is why unlicensed Windows software and systems with outdated software versions became vulnerable and easy to exploit in this attack. The healthcare ecosystem was particularly affected by CT and MRI scanners being exploited in hospitals, among banking, business and corporate sectors worldwide. Around 300,000 computer systems in 150 countries were affected.

Ransomware refers to a cyber malware, which blocks the access to data and related information. However, it impaired the access over data with vulnerable ports. Sometimes, a ransomware needs an amount to be paid in order to access the infected data and when the individual clicks on that attachment or link, it activates on that email. In addition, it can infiltrate the system when the individual visits some webpages. A cyber malware blocks the internal files, encrypts according to itself and makes the documents inaccessible or inactive for the user while it may infect the server attached to that system and also lock up the whole computer network system.

Firstly, in this process, the attacker develops a key pair and puts the public key in the malware, and following that, the malware is released. Then, the malware develops a random symmetric key, which then encrypts the individual's data with it. This is referred to as hybrid encryption in which the public key is used in the malware in order to encrypt the symmetric key. This procedure results in the formulation of small symmetric and asymmetric ciphertext of the individual's data. It also places a message to the individual involving the asymmetric ciphertext and the amount that should be paid as ransom by the individual to get rid of this attack. If the end user sends back the asymmetric ciphertext along with the ransom amount to the cyber attacker, then the hacker decrypts the asymmetric ciphertext with his/her private key and sends back the symmetric key to the end user. Following that, the end user, with the help of the symmetric key, will be able to decrypt the encrypted data. Lastly, this crypto virological attack will have been completed [4].

However, there is no such evidence of computer systems getting deciphered after making the required ransom payments. There has been a recorded mitigation of one attack by Marcus Hutchin battling accusations of involvement in a malware scam. They discovered a "kill switch", which the malware itself had coded [26]. For the DNS sinkhole, he registered a space name; a DNS provides inaccurate data about a domain and made the spreading of the infection work, such as a worm. At the same time, the spread of

malware was backing off and offering time to the end users to prepare protective measures. After that, Adrian Guinet created a solution to the WannaCry Ransomware cyberattack by providing a "wannakey", which was based on its flaws. This worked only if the decryption key was not overwritten by any malware, or the infected computer was not being rebooted.

These are just examples highlighting how ignorance in cyber hygiene could lead to critical cyber threats and cyberattacks [27,28]. Some of the prevention measures that should be adopted are as follows: in order to avoid unwanted searches, activate Google Opt-Out while logged into Google, delete cookies on a daily basis, use PayPal and credit cards instead of debit cards, turn off Google's web history, use a hard drive to back up your data, and bring counterfeit for your online purchases. If the end users keep updating their software regularly, such major cyberattacks would have been avoided efficiently and easily.

3. Human Behaviours: The Weakest Link in Cyberattacks

A significant number of cyberattacks are directed towards the users through distorted means, such as malicious emails and masqueraded applications. Though cyberattacks are aiming to exploit either the technical vulnerabilities of networks and systems, or the errors due to human behaviour, it is the latter that remains as the weakest link in these cyberattacks [29,30]. Attackers most often employ methods exploiting weak cyber behaviours, defined as social engineering.

Studies historically confirm that social engineering approaches account for the majority of total cyber security attacks. Bowen et al. [31] showed that 28% of the total attacks were due to social engineering, and in 2016, 97% of malware attacks targeted human behaviour. A more recent report estimated that 95% of cyberattacks were again attributed to human errors and risky behaviour [32].

Looking in the literature at the types of risky behaviours and human errors, one can identify the most common, including the use of infected memory disks, sharing of passwords, reusing the same passwords for different platforms, not updating software, unauthorised disclosure of personal information, accessing fake emails and installing software from unverified sources [33–37].

Early research exploring the reasons for risky behaviour found these to be due to an employee's lack of knowledge and poor decision making due to staff shortage, fatigue and heavy workload, as well as avoidance of human behaviour where the end user does not perceive the risk as related to them [37].

Exploring further the human behaviours that raise the risks of errors and increase the cybersecurity vulnerabilities, it seems there is a direct link between individual personalities and behavioural traits. Moustafa et al. [38] identified the following traits playing a key role in behavioural cybersecurity: (a) procrastination, where research has shown that individuals who procrastinate are less likely to adhere to security policies; (b) impulsivity, where research demonstrated that addictive behaviour is directly linked to risky cyber behaviour and ignorance of information security policies [14]; (c) future thinking, where it was shown that individuals who are interested in their future have higher rates on following cybersecurity guidelines [39–41], but at the same time those that are more optimistic may fall easier victims to cybersecurity attacks; and (d) risk taking behaviours, where it seems that according to some research studies, individuals that are taking high risks in their lives, are more likely to make cybersecurity errors.

4. Cyber Threats and Countermeasures in Healthcare 4.0

There are several attacks that occur daily within healthcare 4.0. However, as found in the literature, there are six main types of cyber threats that can be identified in the cyberspace, and are directly applied in healthcare 4.0, accompanied by appropriate countermeasures [4], which are presented in detail in Table 1.

Table 1. Cyber Threats in the Cyberspace.

Cyber Threat	Description
Attacks on Hosted Components	These types of attacks include destructive software injection to a targeted system, for example, cross-site scripting, SQL injection and related techniques, which threaten the access and/or authentication controls. This may occur in cloud-based control systems handling big volumes of sensitive data. Here, the countermeasures include mainly role-based approaches, creating awareness in order to protect towards impersonation at the cloud level and API authentication.
Social Engineering	It refers to the attacks performed on the "weakest link" in the security supply chain. This is achieved by psychologically manipulating individuals to perform malicious actions or share confidential information. Common techniques used for this manipulation are shoulder surfing, diversion theft, "dumpster diving", impersonation of help desk calls, phishing and/or personal blackmailing [38,39]. Social engineering is one of the major reasons why even security-aware and well-equipped companies fall victims to cyberattacks. Hackers identify the weakest link in the security supply chain in which they can insert the malicious software or the virus into the targeted system. Therefore, it is of great importance to identify and further secure the weakest link in the security chain. Some of the initial countermeasures, which can be adopted to prevent upcoming attacks, include block Wi-Fi connections to unsecured networks, block network connections related to malicious content, stop using non-secure web pages and websites and performing actions on them. Further approaches, which can be taken to reduce the high level of cyberattacks, include mitigating known threats in the systems and applications, regularly patching vulnerable systems and/or keeping the company's devices up-to-date with the latest version.
Physical Attack	Physical attacks are mostly carried out in fields involving several Internet of Things (IoT) applications since they are connected to a number of components and hardware devices. These are easily located by hackers since they cannot be monitored at a single location and are kept far away from each other [42,43]. The main countermeasures in such cases include trusted platform modules to enable storage of the data on separate platforms securely, file system encryption meaning proper algorithms and encryption decryption techniques shall be used so the data can be stored and secured properly, and lastly remote attestation meaning attesting a remote to each hardware device, which is located far in order to be controlled from faraway locations as well.
Network Compromise	These attacks are known as 'middle way attacks' where the hackers use a number of techniques, for example, altering or blocking communications between hardware devices and their cloud-based controller session and/or hijacking to enter and disrupt a network. The countermeasures that can be offered here include performing regular updates on the software and use of proper file decryption and encryption techniques while sending and receiving sensitive data between the end-to-end users.
Hacked Device Software	In these attacks, the hacker accesses the software at the device level and then it carries out several fraudulent activities and techniques. Such activities and techniques target to take control of the data in the system and include elevation of privileges, denial of service, malware injection and/or false identification [44]. These types of attacks can be tackled by carrying out countermeasures, as for example, software isolation; "secured boot", meaning that when any malicious activities are carried out in the system, after rebooting the system, it then does not turn on and all the available data in the system becomes resilient to the attacker; and/or software update, which maintains the software and its system updated with the latest version available on the market.
Security Misconfiguration	This type of attack is being performed due to inattentiveness or carelessness. The moment when it has been observed to occur is when handling the security changes of the software, as the security changes become misconfigured and provide the attackers with the right opportunity to attack the devices and extract the available data from them. Hence, the most significant countermeasure is that the security changes ought to be carried out with extreme care and with proper decryption encryption techniques as well [42].

It is essential to ensure aspects, such as higher confidentiality, resilience, and integrity levels, to tackle such attacks. Consideration of the human aspects would be key to build these aspects within healthcare 4.0.

5. Towards a Human-Centric Approach to Security

As we discussed earlier, human behaviour is the weakest link in cybersecurity; it is the employees of any organisation that should be involved and engaged within cybersecurity awareness and the development of mitigation approaches. Furthermore, it is important to accept that these individuals can be simultaneously the point of risk but also the point of success. Holland (2020), suggests as a response, the development of an interaction of trust between the end user and the systems especially as the cybersecurity landscape is vast and continuously expanding with the proliferation of new smarter and interconnected devices and networks [45].

Furthermore, as a result of the global COVID-19 pandemic, new working trends have been introduced, where employees working flexibly use their own devices or are using work devices outside the office, resulting in blurred lines between personal and business limits, exacerbating the risky behaviours. As a result, any measures to mitigate the cyber risks need to go beyond the software updating and hardware maintenance to a more human-centric approach.

Human-centric cyber security is still a new domain, which is an intangible concept and is challenging to define and to be understood, not only by the lay end user, but also by specialists in cyberspace. The reason is that it sits at the intersection of human behaviour, computing and security systems. Grobler et al. (2021) [46] defined human-centric cyber security as involving all aspects of cyber security, with a particular focus on the human involvement in the system and processes. They propose for the design, implementation and assessment of holistic human centric cyber security systems, three components of what they define as the 3U's, User, Usage and Usability, with each one of them including further subsections, as seen in Table 2.

Table 2. Design, implementation and assessment of holistic human-centric cyber security systems.

Component	Description
User	• Demography and Culture • Situational Awareness • Psychology and Behaviour • Cognitive Factors
Usage	• Functional Measures • Technical Measures • Legislation, Regulations and Policies
Usability	• Experience Factors • Interaction Factors

The authors suggest that the consideration of all these factors in the development of human-centric cybersecurity approaches can lead to automated functions and, at the same time, keep the end user engaged with the technology in an interaction of what they call 'collaborative intelligence'.

Furthermore similar and relevant components are proposed to be considered when organisations wish to build a human-centred security culture by following specific steps, including the assessment of the organisation's information handling, the testing of the employee's awareness, the review of their interactions and the promotion of their critical thinking, the identification of threats, the reflection on past mistakes, the revision of the processes and training and the automation of security functions [47].

Regarding the future and the way forward, similarly to Grobler et al. (2021) [46], relevant literature suggests that further research and a paradigm shift is required to validate and test such approaches (i.e., 3Us) addressing the need for a human-centric approach to cybersecurity. The paradigm shift suggests moving away from quantitative data collection of human behaviour to an observational approach, increasing the number of participants in projects with diverse samples rather than segmented groups and be 'Belief-Driven'

where the cybersecurity researchers start considering end users perspectives rather than instructing them only what to do [48].

A human-centric, co-produced approach would lead and inform:

(a) Education tailormade to the demographics and needs of the audience with regularly updated messages to avoid desensitisation of the audience [49].
(b) Automation, whereby users would not need to proactively undertake cyber practices, reducing their workload and resulting in increased engagement and adherence to regulations [50].

This approach will inform the development of both best practices and education for cybersecurity hygiene that we will discuss below.

6. Best Practices and Education of Cybersecurity Hygiene for Healthcare Professionals

Cyber threats are rapidly increasing across various business sectors and the incidents in data privacy and cybersecurity breaches are also rising alongside them, particularly in the healthcare domain. In response to the rising threats and incidents, healthcare organisations adopt technical measures, such as the use of firewalls, antivirus and software/firmware patches, aiming to preserve and protect the business continuity of healthcare services. Regardless of such efforts, cybersecurity threats are rising, and the adopted measures have been proven insufficient to respond to cyberattacks. This is often because the important role that the personnel play in this supply chain, related to cyber defence, is not being considered.

In practice, healthcare organisations are encouraged to adopt general data privacy and cybersecurity guidelines that have, as a focal point, the human factor. Nevertheless, there is limited research within the literature on collective practical cyber hygiene guidelines and best practices, which can help healthcare organisations to apply specific interventions, such as training programs and awareness activities, which at the same time are measurable to the healthcare professionals. With that being said, structured best practices that would assist the higher management to choose the optimal number of security controls that will be most efficient for healthcare organisations and professionals are yet not available and, at the same time, are highly desirable.

The importance of developing best practices in order to maintain cybersecurity hygiene has been highlighted with the COVID-19 pandemic through the increased usage of cyberspace and worldwide connection via a simple click [51]. In similar ways, cyberspace has become the main means of working, which makes businesses and individuals particularly vulnerable to cyber threats and risks [4]. The high usage levels of cyberspace make individuals' lives easy; meanwhile, it exposes their personal and professional information to cyber threats. It is beyond doubt that end users are vulnerable to a number of cyber risks [51]. The most optimal way to secure cyberspace usage requires education and proper adoption of the cyber hygiene best practices. Acceptable and accessible practices are necessary to proactively protect, improve, monitor, secure and maintain user's information on the Internet [14,19]. The continuous development and application of such best practices should be the standard route that ensures user's safety, identity and information. These best practices help reduce the impact of corruption and loss of information, resource damage and data breach while improving cyber hygiene [17]. The repeated use of the best practices to maintain proper cybersecurity hygiene results in peace of mind with the prospective of reaching an excellent outcome overall.

Cybersecurity hygiene best practices and education are linked to individual differences aiming to improve cybersecurity. Even though Internet security guidelines for users are widely available, it is doubtful how many consumers understand and apply these reports and if the available security guidelines are written in a lay language for both tech laggards and tech savvy users [52]. One feasible solution in order to overcome the educational gap in cybersecurity would be to establish best practices and mandatory cyber hygiene education for users, including both non-cyber and cyber professionals [17,53].

Best practices and mass cyber education may contribute to discourage poor cybersecurity behaviours; however, to achieve the most optimal results, the content should shift its focus to human factors and use behaviours. It is evident that most available courses and/or training do not address explicitly human cognition and behaviours. In this section, we will present best practices for cyber hygiene, as found in the literature, which are suggested to be applied in the context of healthcare to improve security overall.

The baseline cyber hygiene involves several basic steps that are required for cyber defence. The baseline practices are mostly rooted in frameworks, such as, for example, the NIST cybersecurity framework. It helps organisations, including the healthcare supply chain, to have a detailed and clear set of best practices to show and modify how cybersecurity is being performed and measured regularly [19]. While there are not standardised best practices for healthcare, a basic set of methods to maintain cyber hygiene in business has been presented in the literature [54,55]. All organisations and cyber users need to take responsibility for their browsing in both their personal and professional space. Individuals must take ownership of maintaining sufficient cyber hygiene and safeguarding, by using best practices, against cyberattacks [4]. Best practices, as collected from the literature, are presented in Figure 1.

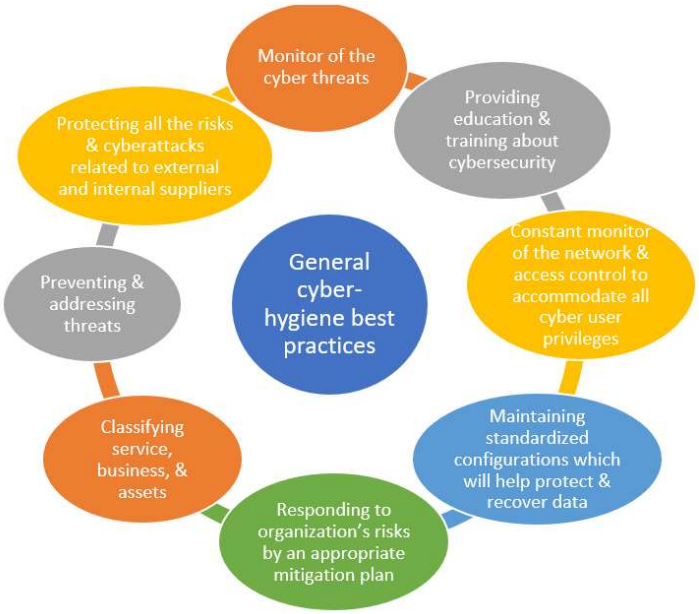

Figure 1. Best practices for general cyber hygiene.

Jointly with other best practices, the deficiency of essential techniques, such as the above, may lead to poor cyber hygiene. Additional recommended set of best practices for small business enterprises targeting cyber risks have been introduced [53]. Meanwhile, cyber hygiene best practices, which can be used by healthcare staff to maintain privacy and security, are illustrated in Figure 2 [56,57].

These practices should be constantly implemented to prevent data breach, unauthorised access and loss of information. The effects of using best practices for cyber hygiene will ultimately provide safe cyber surfing and improve cyber health. The baseline practice as compiled with the National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF) will be explained below.

The current literature suggests the need [54,55] for organisations to align and comply with the NIST's cybersecurity framework in order to promote cyber hygiene. The NIST Framework's main aim is to provide a detailed outline for businesses and organisations to improve ways to identify, prevent and mitigate various cyber incidents [58]. The NIST framework includes five fundamental categories and functions for cyber threats, which are to identify, detect, protect, respond and recover [59].

Figure 2. Cyber hygiene best practices for healthcare staff.

Every fundamental component plays a crucial role in promoting good practice while maintaining a balanced cyber hygiene at all levels. In order to comply with the "identify" main element, the asset's responsibility, leading role and vulnerability and risks to cyberattacks need to be understood. With this implementation of this fundamental function, each organisation would more easily establish the rules and policies that will help them improve good cyber hygiene and remain protected against cyber threats [54,55].

The second fundamental element is to "protect" the organisations by applying sufficient counter measures to safeguard against potential malicious cybersecurity attacks. In this phase, organisations should provide essential education and training related to cybersecurity measures. The third phase includes steps to continuously "detect" cybersecurity incidents and to monitor cyber threats. The fourth phase involves the development of a "response" plan, which will establish the communication channels, clearly mitigating the cyber incidents. The last phase is to "recover" the damaged services whose damages were caused by cyber incidents and to prioritise cyber-related activities [60].

When organisations and businesses are not compliant with the five fundamental elements of the NIST CSF, it becomes extremely challenging to properly handle cyber incidents. In addition, organisations and businesses tend to become vulnerable to cyber incidents, which could potentially affect their continuity. It is suggested that all organisations adopt human-centric approaches alongside with a detailed and clear mitigation plan to promote cyber hygiene and address cyber incidents.

From the analysis above, it is evident that cybersecurity is important for healthcare professionals because they deal with sensitive patient information and medical records, which must be kept confidential and secure. To deepen and summarise our analysis, the best hands-on practices for cyber hygiene are identified as follows:

- Use strong passwords: Healthcare professionals should use strong passwords for all their accounts, including their electronic medical record (EMR) system. Passwords should be long and include a mix of uppercase and lowercase letters, numbers and special characters.
- Use two-factor authentication: Two-factor authentication provides an extra layer of security for healthcare professionals. They should enable two-factor authentication for all their accounts, especially for EMR systems.

- Keep software updated: Healthcare professionals should keep all software, including operating systems and applications, up to date with the latest security patches and updates. This helps to protect against known vulnerabilities and exploits.
- Use secure networks: Healthcare professionals should only use secure networks, such as their workplace network or a trusted VPN, when accessing sensitive patient information or medical records. They should avoid using public Wi-Fi networks or unsecured networks.
- Be cautious of phishing scams: Healthcare professionals should be cautious of phishing scams, which are fraudulent emails or messages designed to steal personal information or infect computers with malware. They should avoid clicking on links or downloading attachments from unknown sources.
- Encrypt sensitive data: Healthcare professionals should encrypt sensitive patient information and medical records to protect against unauthorised access. Encryption helps to ensure that only authorised individuals can access the data.
- Regularly backup data: Healthcare professionals should regularly backup their data, including patient information and medical records, to ensure that it can be recovered in the event of a data breach or system failure.
- Use secure messaging: Healthcare professionals should use secure messaging platforms to communicate with colleagues and other healthcare professionals. They should avoid using unsecured messaging apps or SMS messages, which can be intercepted and read by unauthorised individuals.
- Educate staff: Healthcare professionals should educate their staff on cybersecurity best practices and provide regular training to ensure that everyone is aware of the risks and how to prevent them.
- Use a reputable IT provider: Healthcare professionals should work with a reputable IT provider to ensure that their systems and networks are secure and up to date with the latest security protocols. The IT provider can also provide support and guidance on cybersecurity best practices.

It is important to also highlight the advantages and disadvantages of the existing methods. Advantages of existing cyber hygiene methods are as follows:

1. Regular updates and patches—Keeping software, operating systems and applications up to date with the latest patches and updates can help prevent cyberattacks that exploit vulnerabilities in the system.
2. Strong passwords and authentication—Using strong and unique passwords, along with multi-factor authentication, can help prevent unauthorised access to accounts and data.
3. Backups—Regular backups of important data can help ensure that data is not lost in the event of a cyberattack or system failure.
4. Security awareness training—Educating employees about cybersecurity risks and best practices can help prevent human errors that could lead to cyberattacks.
5. Firewall and antivirus protection—Firewalls and antivirus software can help prevent unauthorised access to a network and protect against viruses and malware.

Disadvantages of existing cyber hygiene methods:

1. Complexity—Some cybersecurity practices can be complex and require technical expertise to implement and maintain, which can be challenging for small businesses or individuals.
2. Cost—Implementing robust cybersecurity measures can be costly, especially for small businesses or individuals with limited budgets.
3. False sense of security—Relying solely on cybersecurity measures can create a false sense of security and lead to complacency, which could make an organisation or individual more vulnerable to cyberattacks.

4. Lack of standardisation—Cybersecurity practices and standards are not always consistent across different organisations and industries, which could create gaps in cybersecurity coverage.
5. Evolving threat landscape—The threat landscape is constantly evolving, and new cyber threats are emerging all the time. Cybersecurity measures that were effective in the past may not be sufficient to protect against new threats.

Overall, cyber hygiene is critical in today's digital world, and adopting best practices and measures can help individuals and organisations protect themselves against cyber threats; this is why this piece of research is considered essential as a complete review of the literature on the topic has not been conducted before. However, it is important to be aware of the limitations of existing methods and to continuously evaluate and update cybersecurity practices to stay ahead of evolving threats.

7. Deployment, Demonstration and Implementation of a Healthcare Use-Case Scenario for Raising Data Privacy and Cybersecurity Awareness

The chosen scenario, which is described in this section, is mainly based on a user-centred Digital Health Living lab. This Living Lab provides a real-life setting with a systematic co-production and user co-creation approach while incorporating research and innovation processes. The key involved stakeholders are councils, residents, service providers, technology companies and academic institutions, and are active in every step from the creation to commercialisation of a product or service. This scenario aims to demonstrate the real-world applicability of best cybersecurity hygiene practices, aiming to raise data privacy and cybersecurity awareness.

More specifically, the involved stakeholders in the Living Lab are contributing to health innovation in an innovative way and have the opportunity to help individuals and society. They are being key partners in inspiring and creating health innovations based on their perceptions, needs and user experience. This is characterised as an open innovation ecosystem and the Living Lab plays the role of a unique testbed for the development and testing of prototypes or mature digital healthcare solutions. The scenario, presented here, is based on Tier 3 test and trial category in accordance with the UK National Institute for Health and Care Excellence (NICE) for Digital Health Technologies (DHTs). Particularly, Tier 3 is targeted on helping people who are diagnosed with a long or short-term condition with treatment and management. It involves clinical management tools for treatment and diagnosis via active monitoring or calculation. For example, a symptom tracking function, which transfers patients' records to the healthcare team to support the clinical decision process.

All involved stakeholders, such as service providers, patients, residents, and healthcare practitioners, are engaging with the Living Lab using their own network connections and infrastructures. As an extent, they connect to the internet through their own routers (WiFi) and communicate through online means, such as emails via their personal devices (i.e., PCs, mobile devices, tablets, laptops). It is worth noting that there is a lot of big data involved, such as personal information. In addition, the Living Lab includes several medical healthcare devices, such as infusion and/or insulin pumps and IoT devices for healthcare diagnosis, management and treatment. The scenario presented below is used to demonstrate the importance to maintain and promote cybersecurity hygiene in such an environment.

Vulnerabilities in the healthcare sector differentiate compared to the other sectors. This is due to the lack of security measures related to connectivity of the network and medical devices. The healthcare information infrastructure includes a huge number of legacy systems and threat actors are always looking for ways to exploit the systems. It has been noted in the literature that the most common attack path is found by hackers via social engineering and lack of cybersecurity hygiene by the involved actors. For example, healthcare professionals collect patient data (i.e., financial, personal), hence breaches of this data would provide additional benefits to the attackers.

This scenario is making a number of assumptions for the purpose of implementation. More specifically, the home patients use an insulin pump for their diabetes treatment and the pump is configured and managed by their healthcare practitioner. In addition, there are IT devices, such as servers and applications software, computers, operating systems and routers that are essential for the system infrastructure as a whole. The security of medical devices mainly relies on the cybersecurity hygiene and best practices adopted by the patient, healthcare professional and IT staff involved. Security is required to protect patient data and to safeguard the healthcare service delivery, as the medical devices are connected to the internet.

8. Conclusions

This paper shows the importance of human-centric and multidisciplinary approaches in cyber hygiene education and practices, and how specific end users are targeted through social engineering attacks. For example, males have the tendency to show greater trust in technological tools, which could act as a bias in their cyber hygiene practices and behaviours. Even though there is not a single theoretical framework or model for best practices in cyber hygiene, this piece of work, in combination with previous studies performed (i.e., [61]), is a start to develop and apply a holistic empirical educational framework. The present research sets the scene to utilise an articulated and flexible model of cyber hygiene education, which connects behaviours, human factors, knowledge, individual differences and attitudes. It is an extension of the existing literature and may be employed to cultivate and support current theories of cyber hygiene.

For reasons as such, the findings of the present research could better inform information technology courses, cybersecurity, computer science and didactical approaches in cybersecurity practices. This would be achieved by providing awareness of possible biases, and students may become prepared for future social engineering attacks in their professional and personal lives, while also grasping a better understanding of these principles as a whole.

Individual differences and human-centric approaches associated with cyber hygiene are essential to disseminate in mathematics (STEM), science, health, technology and engineering classes. They are an important addition into the curriculum of cyber education, since humans are the biggest threat to efficient cybersecurity. Hence, the practical application of this piecework is its application to education. Last, but not least, by personalising cyber hygiene training to fit the individual's needs based on their attitudes, behaviours and knowledge [62], greater efficacy and transfer are expected, especially related to the protection of confidential and personal information [63].

In conclusion, cyber education, at the moment, is not effectively preparing individuals to take into consideration human factors, which are strongly associated with cybersecurity. The human factor can be the main cause of security violations and malicious attacks and remains the weakest link in cyber resiliency.

The novelty of the present research is:

- As far as we are concerned, this is the first research paper that presents a holistic, hands-on set of best practices in cyber hygiene, specifically addressing the healthcare staff.
- It facilitates the identification as to why humans are the weakest link, due to their lack of awareness, training, education, errors and complexity of technology.
- It accomplishes the presentation of important theoretical and practical applications within cyber education.

Author Contributions: Conceptualization, H.M., T.F. and K.K.; methodology, H.M., T.F. and K.K.; investigation, T.F. and K.K.; resources, T.F., S.N. and K.K.; writing—original draft preparation, K.K.; writing—review and editing, T.F., S.N. and K.K.; visualization, H.M., T.F. and K.K.; supervision, H.M. and T.F.; project administration, K.K.; funding acquisition, H.M. All authors have read and agreed to the published version of the manuscript.

Funding: The research conducted in this paper was funded by the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No. 883273. The project was funded by the European Union's Horizon 2020 research and innovation programme.

Institutional Review Board Statement: Ethical approval was not required for this study.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful for the financial support of this project that has received funding from the European Union's Horizon 2020 research and innovation programme. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned project.

Conflicts of Interest: The authors declared no potential conflict of interest with respect to the research, authorship and/or publication of this article.

References

1. Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. *J. Inf. Warf.* **2015**, *14*, 15–24.
2. Javid, T.; Faris, M.; Beenish, H.; Fahad, M. Cybersecurity and data privacy in the cloudlet for preliminary healthcare big data analytics. In Proceedings of the 2020 International Conference on Computing and Information Technology, Tabuk, Saudi Arabia, 9–10 September 2020; pp. 1–4. [CrossRef]
3. Thuemmler, C.; Bai, C. Health 4.0: Application of industry 4.0 design principles in future asthma management. In *Health 4.0: How Virtualization and Big Data Are Revolutionizing Healthcare*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 23–37.
4. Singh, D.; Mohanty, N.; Swagatika, S.; Kumar, S. Cyber-hygiene: The key Concept for Cyber Security in Cyberspace. *Test Eng. Manag.* **2020**, *83*, 8145–8152.
5. Cain, A.; Edwards, M.; Still, J. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. [CrossRef]
6. Ponemon Institute. 2016. Available online: http://www.ponemon.org/li-brary/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation (accessed on 1 January 2023).
7. FBI. 2015. Available online: https://www.ic3.gov/media/annualreports.aspx (accessed on 15 December 2022).
8. Long, R. Using Phishing to Test Social Engineering Awareness of Financial Employees. Ph.D. Thesis, Eastern Washington University, Cheney, WA, USA, 2013.
9. Russell, J.D.; Weems, C.F.; Ahmed, I.; Richard, G.G. Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors. *J. Cyber Secur. Technol.* **2017**, *1*, 1–12. [CrossRef]
10. Talib, S.; Clarke, N.L.; Furnell, S.M. An analysis of information security aware-ness within home and work environments. In Proceedings of the International Conference on Availability, Reliability, and Security, Krakow, Poland, 15–18 February 2010; Volume 1, pp. 196–203.
11. Anderson, C.L.; Agarwal, R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
12. Konieczny, F. USAFR NJT. SEADE: Countering the futility of network security. *Air Space Power J.* **2015**, *29*, 1–11.
13. Furnell, S. Why users cannot use security. *Comput. Secur.* **2005**, *24*, 274–279. [CrossRef]
14. Henshel, Q.; Hart, P.; Cooke, D. The role of external influences on organizational information security practices: An institutional perspective. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences 2006, Kauia, HI, USA, 4–7 January 2006; Volume 6, pp. 1–10. [CrossRef]
15. Almeida, V.A.F.; Doneda, D.; Abreu, J.S. Cyberwarfare and digital governance. *IEEE Internet Comput.* **2017**, *21*, 68–71. [CrossRef]
16. Neigel, A.R.; Claypoole, V.L.; Waldfogle, G.E.; Acharya, S.; Hancock, G.M. Holistic cyber hygiene education: Accounting for the human factors. *Comput. Secur.* **2020**, *92*. [CrossRef]
17. Dupuis, M.J. Cyber security for everyone: An introductory course for nontechnical majors. *J. Cybersecur. Educ. Res. Pract.* **2017**, *3*, 1–17.
18. Cone, B.D.; Irvine, C.E.; Thompson, M.F.; Nguyen, T.D. A video game for cyber security training and awareness. *Comput. Secur.* **2007**, *26*, 63–72. [CrossRef]
19. Molinara, M.; Cancelliere, R.; Di Tinno, A.; Ferrigno, L. A Deep Learning Approach to Organic Pollutants Classification Using Voltammetry. *Sensors* **2022**, *22*, 8032. [CrossRef] [PubMed]
20. Polatidis, N.; Pimenidis, E.; Pavlidis, M.; Papastergiou, S.; Mouratidis, H. From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *Evol. Syst.* **2020**, *11*, 479–490. [CrossRef]
21. Silvestri, S.; Islam, S.; Papastergiou, S.; Tzagkarakis, C.; Ciampi, M. A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. *Sensors* **2023**, *23*, 651. [CrossRef] [PubMed]

22. European Union Agency for Network and Information Security (ENISA). Review of Cyber Hygiene Practices. 2016. Available online: https://www.enisa.europa.eu/publications/cyber-hygiene (accessed on 30 November 2022).
23. Trevors, M. Mapping Cyber Hygiene to the NIST Cybersecurity Framework. 2019. Available online: https://insights.sei.cmu.edu/insider-threat/2019/10/mapping-cyber-hygiene-to-the-nist-cybersecurity-framework.html (accessed on 3 January 2023).
24. Vishwanath, A.; Neo, L.S.; Goh, P.; Lee, S.; Khader, M.; Ong, G.; Chin, J. Cyber hygiene: The concept, its measure, and its initial tests. *Decis. Support Syst.* **2020**, *128*, 113–160. [CrossRef]
25. Ehrenfeld, J.M. Wannacry, cybersecurity and health information technology: A time to act. *J. Med. Syst.* **2017**, *41*, 104. [CrossRef] [PubMed]
26. Independent. 2017. Available online: https://www.independent.co.uk/news/uk/home-news/marcus-hutchins-arrested-latest-us-authorities-wannacry-cyberattack-nhs-las-cegas-mccaran-a7875761.html (accessed on 3 January 2023).
27. Rader, M.; Rahman, S. Exploring Historical And Emerging Phishing Techniques And Mitigating The Associated Security Risks. *Int. J. Netw. Secur. Appl.* **2013**, *4*, 50–69.
28. Aparajita, A.; Swagatika, S.; Singh, D. Comparative Analysis of Clustering Techniques in Cloud for Effective Load Balancing. *Int. J. Eng. Technol.* **2018**, *7*, 47–51. [CrossRef]
29. Kelly, R. Almost 90% of Cyber Attacks Are Caused by Human Error or Behaviour. 2017. Available online: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/ (accessed on 5 December 2022).
30. Annarelli, A.; Nonino, F.; Palombi, G. Understanding the management of cyber-resilient systems. *Comput. Ind. Eng.* **2020**, *149*, 43–59. [CrossRef]
31. Bowen, B.; Devarajan, R.; Stolfo, S. Measuring the human factor of cyber security. In Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–16 November 2011; Volume 1, pp. 198–207.
32. Nobles, C. Botching human factors in cybersecurity in business organizations. *Holistica* **2018**, *9*, 71–88. [CrossRef]
33. Dragana, C.; Pattinson, M.R.; Parsons, K.; Butavicius, M.A.; McCormac, A. Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think. In Proceedings of the 10th International Symposium of Human Aspects of Information Security and Assurance, Frankfurt, Germany, 19–21 July 2016; Volume 1, pp. 32–52.
34. Baillon, A.; Bruin, J.; Emirmahmutoglu, A.; Veer, E.; Dijk, B. Informing, simulating experience, or both: A field experiment on phishing risks. *PLoS ONE* **2019**, *14*, e0224216. [CrossRef] [PubMed]
35. Hakim, Z.; Ebner, N.; Oliveira, D.; Getz, S.; Levin, B.E.; Lin, T.; Wilson, R.C. The phishing email suspicion test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behav. Res. Methods* **2021**, *53*, 1342–1352. [CrossRef] [PubMed]
36. Kobis, P. Human factor aspects in information security management in the traditional IT and cloud computing models. *Oper. Res. Decis.* **2021**, *31*, 61–76. [CrossRef]
37. Richardson, M.D.; Lemoine, P.A.; Stephens, W.E.; Waller, R.E. Planning for Cyber Security in Schools: The Human Factor. *Educ. Plan.* **2020**, *27*, 23–39.
38. Moustafa, A.A.; Bello, A.; Maurushat, A. The Role of User Behaviour in Improving Cyber Security Management. *Front. Psychol.* **2021**, *12*, 224–231. [CrossRef]
39. Moustafa, A.A.; Morris, A.N.; Elhaj, M. A review on future episodic thinking in mood and anxiety disorders. *Rev. Neurosci.* **2018**, *30*, 85–94. [CrossRef]
40. Moustafa, A.A.; Morris, A.N.; Nandrino, J.; Misiak, B.; Szewczuk-Boguslawska, M.; Frydecka, D.; El Haj, M. Not all drugs are created equal: Impaired future thinking in opiate, but not alcohol, users. *Exp. Brain Res.* **2018**, *236*, 2971–2981. [CrossRef]
41. Wikipedia. Available online: https://en.mwikipedia.org/wiki/social_engineering(security) (accessed on 18 January 2023).
42. Chen, H.; Zhongchuan, F.; Dongyan, Z. Security and trust research in M2M system. In Proceedings of the 2011 IEEE International Conference on Vehicular Electronics and Safety, Beijing, China, 10–12 July 2011; Volume 1, pp. 286–290.
43. Sung-Ming, Y.; Kim, S.; Lim, S.; Moon, S. A countermeasure against one physical cryptanalysis may benefit another attack. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Republic of Korea, 6–7 December 2001; pp. 414–427.
44. Gregory, R.G.; Fitzgerald, J.; Hunsperger, N.; Lavine, J.; Nguyen, V.; Tellado, J. Service Processor Configurations for Enhancing or Augmenting System Software of a Mobile Communications Device. U.S. Patent Application 14/083,324, 3 March 2014.
45. Holland, N. The Human-Centered Cybersecurity Stance. 2020. Available online: https://www.bankinfosecurity.com/human-centric-cybersecurity-stance-a-13897 (accessed on 1 October 2022).
46. Grobler, M.; Gaire, R.; Nepal, S. Usage and Usability: Redefining Human Centric Cyber Security. *Front. Big Data* **2021**, *4*, 344–452. [CrossRef]
47. Durbin, S. Eight Steps to Building a Human-Centered Security Culture. 2020. Available online: https://www.forbes.com/sites/forbesbusinesscouncil/2020/11/25/eight-steps-to-building-a-human-centered-security-culture/ (accessed on 5 January 2023).
48. Renaud, K.; Flowerday, S. Contemplating human-centred security & privacy research: Suggesting future directions. *J. Inf. Secur. Appl.* **2017**, *34*, 76–81. [CrossRef]
49. Khader, M.; Chai, W.; Neo, L.S. *Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators*, 1st ed.; World Scientific Publishing: Singapore, 2021; 404p.
50. Blau, A. Better Cybersecurity Starts with Fixing Your Employees Bad Habits. 2017. Available online: https://hbr.org/2017/12/bettercybersecurity-starts-with-fixing-your-employees-badhabits (accessed on 1 December 2022).

51. Ncubukezi, T.; Mwansa, L.; Rocaries, F. A review of the current cyber hygiene in small and medium sized businesses. In Proceedings of the 15th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 8–10 December 2020; Volume 15, pp. 283–288.
52. Symantec, C.D. Internet Security Threat Report: 2011 Trends. *Symantec Corp.* **2012**, *17*, 977–999.
53. Sobiesk, E.; Blair, J.R.; Conti, G.; Lanham, M.; Taylor, H. Cyber education: A multilevel, multi-discipline approach. In Proceedings of the 16th Annual Conference on Information Technology Education, London, UK, 4–8 September 2015; Volume 1, pp. 43–47.
54. Ncubukezi, T.; Mwansa, L. Best practices used by businesses to maintain good cyber hygiene during COVID-19 pandemic. *J. Internet Technol. Secur. Trans.* **2021**, *9*, 714–721. [CrossRef]
55. Trevors, M.; Wallen, C.M. *Cyber Hygiene: A Baseline Set of Practices*; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2017; pp. 1–17.
56. Cyber Essentials. 2020. Available online: https://www.gov.uk/gov (accessed on 26 January 2023).
57. Such, J.M.; Cholas, P.; Rashid, A.; Vidler, J.; Seabrook, T. Basic cyber hygiene: Does it work? *Computer* **2019**, *52*, 21–31. [CrossRef]
58. NIST Special Publication 800–181. 2017. Available online: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center (accessed on 3 October 2022).
59. Mehravari, N. Resilience management through the use of CERT-RMM and associated success stories. In Proceedings of the IEEE, International Conference on Technologies for Homeland Security (HST), Vienna, Austria, 17–20 October 2013; Volume 1, pp. 119–125.
60. Martin, R.A. Non-Malicious Taint: Bad Hygiene Is as Dangerous to the Mission as Malicious Intent. 2014; Volume 1, pp. 19–30. Available online: https://apps.dtic.mil/sti/pdfs/AD1107757.pdf (accessed on 4 November 2022).
61. Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M.; McCormac, A.; Zwaans, T. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Comput. Secur.* **2017**, *66*, 40–51. [CrossRef]
62. Hancock, P.A.; Billings, D.R.; Schaefer, K.E.; Chen, J.Y.C.; Visser, E.J.; Parasuraman, R. A Meta-Analysis of Factors Affecting Trust in Human-Robot Interaction. *J. Hum. Factors Ergon. Soc.* **2011**, *53*, 517–527. [CrossRef]
63. Bansal, G.; Zahedi, F.; Genfen, D. The impact of personal dispositions on in-formation sensitivity, privacy concern and trust in dis-closing health information online. *Decis. Support Syst.* **2010**, *49*, 138–150. [CrossRef]