applied sciences

MDPI

Review

Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories

Afrah Almansoori [1,2], Mostafa Al-Emran [1,3,*] and Khaled Shaalan [1]

[1] Faculty of Engineering & IT, The British University in Dubai, Dubai P.O. Box 345015, United Arab Emirates; almansoori.afrah@gmail.com (A.A.); khaled.shaalan@buid.ac.ae (K.S.)
[2] General Department of Forensic Science and Criminology, Dubai Police G.H.Q., Dubai P.O. Box 1493, United Arab Emirates
[3] Department of Computer Techniques Engineering, Dijlah University College, Baghdad 00964, Iraq
* Correspondence: mustafa.n.alemran@gmail.com

Abstract: Cybersecurity procedures and policies are prevalent countermeasures for protecting organizations from cybercrimes and security incidents. Without considering human behaviors, implementing these countermeasures will remain useless. Cybersecurity behavior has gained much attention in recent years. However, a systematic review that provides extensive insights into cybersecurity behavior through different technologies and services and covers various directions in large-scale research remains lacking. Therefore, this study retrieved and analyzed 2210 articles published on cybersecurity behavior. The retrieved articles were then thoroughly examined to meet the inclusion and exclusion criteria, in which 39 studies published between 2012 and 2021 were ultimately picked for further in-depth analysis. The main findings showed that the protection motivation theory (PMT) dominated the list of theories and models examining cybersecurity behavior. Cybersecurity behavior and intention behavior counted for the highest purpose for most studies, with fewer studies focusing on cybersecurity awareness and compliance behavior. Most examined studies were conducted in individualistic contexts with limited exposure to collectivistic societies. A total of 56% of the analyzed studies focused on the organizational level, indicating that the individual level is still in its infancy stage. To address the research gaps in cybersecurity behavior at the individual level, this review proposes a number of research agendas that can be considered in future research. This review is believed to improve our understanding by revealing the full potential of cybersecurity behavior and opening the door for further research opportunities.

Keywords: cybersecurity; human behavior; information system theories; systematic review

Citation: Almansoori, A.; Al-Emran, M.; Shaalan, K. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Appl. Sci.* **2023**, *13*, 5700. https://doi.org/10.3390/app13095700

Academic Editor: Christos Bouras

Received: 20 March 2023
Revised: 2 May 2023
Accepted: 3 May 2023
Published: 5 May 2023

1. Introduction

The Internet and computers are working together to connect people worldwide [1]. Hence, cybersecurity became a must-have framework. As a result, all communications and information sharing will remain safe. Cybersecurity covers the Internet, computer networks, and computing systems. Technological and organizational elements of cybercrime, such as databases, software administration, and computer programming, are essential for individuals' understanding [2,3]. Organizations and individuals utilize cybersecurity to prevent illegal access to data centers and computerized systems. A robust cybersecurity strategy is typically provided through solid security procedures.

Cybersecurity threats come in three forms: cybercrimes, cyberattacks, and cyberterrorism. Cybercrimes refer to crimes committed through the Internet and other digital means and more conventional crimes enabled or sustained by these means [4]. Cyberattacks refer to cyberspace-based assaults aimed at disrupting, disabling, damaging, or maliciously managing a computer environment/infrastructure, ruining data integrity, or stealing sensitive information [5]. Cyberterrorism involves the disruption of crucial national infrastructure, encompassing transportation, energy, and governmental operations, through employing

computer network tools to coerce or intimidate a government or civilian population [6]. These threats result from malware, phishing, social engineering, SQL injection, man-in-the-middle attack, and distributed denial-of-service attacks [7,8]. Additionally, malicious efforts to harm or destroy computing systems or networks are included in the definition of cybersecurity [9,10]. Hence, cybersecurity attacks and threats can affect various industries, such as healthcare, manufacturing, financial services, government agencies, and education [11]. Cybersecurity must consider technological, regulatory, legal, ethical, and social factors.

Individuals' behavior toward cybersecurity is a concern for both end-users and organizations. This is because most cybersecurity incidents are caused by human mistakes or inadequate knowledge [12–14]. Therefore, promoting cybersecurity behavior is essential to protecting organizations and individuals from security threats [15]. Cybersecurity behavior refers to the users' actions and reactions in the cyber realm [16]. One major limitation is the lack of a clear definition and understanding of how individuals differ in their awareness, knowledge, and cybersecurity behavior when confronted with adaptable cyber hazards [17].

The literature indicates that cybersecurity in general, particularly cybersecurity behavior, plays a critical role in supporting the application of many information system (IS) theories and models. By analyzing cybersecurity behavior research, it has been observed that existing review studies have overlooked studying cybersecurity behavior from the lens of IS theories and models. Psychologists employ various theories to explain and predict human behavior in preparation for cybersecurity programs. For instance, cybersecurity professionals may rely on the protection motivation theory (PMT), which mainly explains the impact of threat perception and self-efficacy on security behaviors or attitudes among the population [18]. In addition, the theory of planned behavior (TPB) indicates that behavioral intention is influenced by subjective norms and attitudes [19]. These theories and models help to decide which behavioral elements are most predictive to be included in the prevention plan or intervention.

While understanding cybersecurity behavior mainly relies on several technical, social, and human factors that can be identified through different IS theories and models, the existing research ignores reviewing this research topic from the perspective of those theories and models. Moreover, most of the current review studies have concentrated on the technical aspects of cybersecurity, with little attention paid to human behaviors. For example, Ref. [20] analyzed the progress of information security awareness (ISA) and provided the current state of the art in the content development of ISA in both the private and public sectors by understanding the different ISA content development methodologies and variables that impact employees' ISA. Additionally, Ref. [21] comprehended the current level of cybersecurity education and its associated research. Moreover, Ref. [22] investigated which qualitative research methodologies have been used the most to study different aspects of cybersecurity.

Therefore, this review systematically examines and synthesizes cybersecurity behavior studies from the perspective of IS theories and models. This is because these theories and models provide a better understanding of user behavior toward a particular technology or service by identifying the underlying drivers and barriers [23]. Identifying the drivers and barriers would improve cybersecurity behavior by allowing researchers to investigate the technical, social, and cultural aspects and understand the correlation between those factors and users' willingness to improve their cybersecurity behavior when using any technology or service. The review also intends to identify the common research themes, external factors, dominant technologies and services, main research methods, active countries, and participants. Analyzing common research themes in cybersecurity behavior is crucial because it helps to identify the most widely studied and significant areas of this field. This can guide future research efforts, ensuring that resources focus on the most critical and impactful areas. Additionally, understanding external factors that affect cybersecurity behavior is crucial because these factors can influence an individual's behavior regarding how they approach and engage with cybersecurity issues [24]. Moreover, researchers and

organizations can better understand the root causes of cybersecurity behavior and develop strategies to encourage positive behavior and minimize risk.

Further, being aware of which technologies are prevalent in the field helps researchers and practitioners understand the current landscape and identify areas for further development or improvement [25]. Moreover, analyzing research methods can inform future studies by highlighting areas where new and different techniques may be needed to address gaps or limitations in the current body of knowledge [26]. In addition, knowing which countries are active in this area of research can help identify regional trends and disparities in knowledge, resources, and expertise. It also provides a sense of the global reach of cybersecurity behavior research and highlights areas where additional research may be needed. Furthermore, analyzing the participants is crucial because the demographic characteristics and behavior of the participants can significantly impact the results and conclusions of the study. Understanding the background, experience, and perspectives of the participants can help to contextualize the findings and provide insights into the generalizability of the results. Additionally, identifying the type of participants, such as individuals, organizations, or communities, can highlight the scope and focus of the study and shed light on the potential biases and limitations in the research. Consequently, this review study intends to address the following research questions:

RQ1: What are the prominent IS theories and models in the context of cybersecurity behavior?
RQ2: What are the common themes in the articles under analysis?
RQ3: What are the common external factors affecting cybersecurity behavior?
RQ4: What is the relationship between the cybersecurity research themes and external factors?
RQ5: What are the dominant technologies and services used in cybersecurity behavior?
RQ6: What are the leading research methods used?
RQ7: What are the active countries in cybersecurity behavior research?
RQ8: What is the relationship between the cybersecurity research themes and study regions?
RQ9: Who are the participants in cybersecurity behavior research?

Following this section, Section 2 provides a background on cybersecurity behavior and previous reviews on cybersecurity. Section 3 presents the review methodology, in which inclusion and exclusion criteria, data sources and search strategies, and data coding and analysis, are discussed. Section 4 shows the results by responding to all the formulated research questions, while Section 5 discusses these results in detail. Section 6 concludes the review and provides a number of research gaps that require further examination.

2. Background

2.1. Cybersecurity Behavior

The continued adoption of information technologies has been accompanied by the need to enhance systems and data security [27]. Effective cybersecurity programs consider the human element the weakest link in cybersecurity [28,29]. Implementing administrative safeguards focusing on behavior is imperative to address people-related vulnerabilities. Cybersecurity behavior refers to the individual practices that attenuate or minimize the risk and likelihood of cyber threats. According to [30], focusing on social and behavioral issues can help deal with cybersecurity. As such, identifying behaviors that can either enhance or reduce the level of security is an essential consideration in creating and implementing a cybersecurity strategy [17]. More importantly, fostering a solid cybersecurity culture in which every member of the organization behaves appropriately reduces people-related cyber vulnerabilities [31]. The idea is to discourage negative behaviors while encouraging positive ones.

Various examples of negative security behaviors should be discouraged in organizational settings. One such behavior is visiting unsafe websites [12]. In workplace environments, it is common for employees to visit potentially dangerous websites. Such websites contain exploits targeting the organization's systems [32]. Another negative behavior relates to falling victim to social engineering. Social engineering techniques are the most utilized avenues for infecting and intruding into computer networks [33]. These

techniques leverage human weaknesses such as greed, fear, negligence, and ignorance to obtain sensitive information from people. For instance, an employee could be tricked into opening a phishing link to win a present. Employees can also fail to back up data or secure their portable devices. For example, the loss of a smartphone containing company data can result in a major data breach.

2.2. Related Work

Lately, the review studies to investigate different domains in the context of cybersecurity behavior have increased. Table 1 lists the previous reviews on cybersecurity-related literature. It is evident that earlier reviews have focused on specific aims, including cybersecurity awareness [34,35], cybersecurity vulnerability and risk assessment policies and strategies [36–38], and determinants affecting cybersecurity behavior, including human factors [37,39–44].

Table 1. Previous review studies on cybersecurity.

Source	Review Type	Number of Reviewed Studies	Domain	Aim
[36]	Narrative review	1249	Healthcare	Understanding and identifying the vulnerabilities and cybersecurity threats and their effect on healthcare.
[43]	Systematic review	35	Software Engineering	Understanding user differences related to good or bad cyber hygiene behavior, and what users can do to support good cyber hygiene.
[37]	Systematic review	70	Healthcare	Uncovering the prevalent factors affecting a healthcare organization's cybersecurity posture due to a lack of awareness of the cyber threat to healthcare, identifying healthcare organizations' cyber defense strategy through studying human behavior, and examining the organization's risk assessment approach and cybersecurity policies that have been enacted.
[41]	Systematic review	27	Social Science	Investigating human factors in cybersecurity, which are subjective and often complex.
[34]	Taxonomy review	56	Global	Reviewing the existing literature on cybersecurity awareness among young people.
[39]	Systematic review	21	Global	Consolidating a paradigm that examines the influence of temporal constraints on human cybersecurity behaviors.
[40]	Systematic review	60	Social sciences	Understanding the underlying human behavioral factors influencing cyber-information security compliance from theoretical perspectives.
[38]	Systematic review	107	Social sciences	Investigating trends in cybersecurity behavioral research by synthesizing secondary literature.
[35]	Systematic review	43	Computer science	Reviewing research on the recommended cybersecurity practices for social media users from the user's point of view.
[42]	Systematic review	33	Computer science	Identifying strategies to address human factors in cybersecurity.
[44]	Systematic review	32	Computer science	Identifying information security policy compliance behavior factors, models, and theories.

Table 1. *Cont.*

Source	Review Type	Number of Reviewed Studies	Domain	Aim
[45]	Meta-analysis	9	Social science-es	Investigating the impact of cyber optimistic bias on an individual's security risk perception and its subsequent influence on their decision-making process.
[46]	Systematic review	54	Computer science	Analyzing teenagers' behavior and its potential susceptibility to exploitation on social media platforms.
[47]	Systematic review	26	Social science	Evaluating common approaches utilized in examining cybersecurity-related behavior.
This Study	Systematic review	39	Global	Conducting a systematic review of cybersecurity behavior from the perspective of IS theories and models to examine the main research themes, influential factors, dominant technologies and services, research methods, active countries, and the interrelationships among these characteristics.

Although numerous review studies have been conducted in recent years, providing scholars with valuable information on cybersecurity behavior. It has been noticed that research has neglected the review of cybersecurity behavior from the lenses of IS theories and models. This issue was the driving force behind the decision to conduct this systematic review.

3. Method

This review is based on the results of studies published in digital journals and databases to debate and empirically analyze IS theories and models in cybersecurity behavior. A literature review is crucial to every scientific study [48]. It lays the groundwork for information accumulation, promoting the development and refinement of ideas, filling gaps in existing research, and discovering places past research has missed [49]. A systematic review assists researchers in gaining a deeper understanding of the research topic under investigation [50,51]. Systematic reviews are distinct from traditional or narrative reviews since they are more thorough and provide a well-defined methodology for reviewing a particular topic [52]. This study intends to comprehensively review past studies on cybersecurity behavior involving IS theories and models, focusing on the common research themes, external factors, dominant technologies and services, main research methods, active countries, participants, and the interrelationships among these characteristics. The systematic review is divided into three stages: determining inclusion and exclusion criteria, data sources and search methods, and data coding and analysis.

3.1. Inclusion and Exclusion Criteria

The inclusion/exclusion criteria filter out the collected data and determine which papers to include or exclude, as shown in Table 2. The inclusion criteria cover articles that focus on IS theories and models in cybersecurity behavior and must be written in English. On the other hand, the excluded studies were articles written in languages other than English, did not focus on cybersecurity behavior, and did not involve using theories and models.

Table 2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Addresses cybersecurity behavior.	Behavior is covered but not cybersecurity.
Discusses a theoretical model.	Cybersecurity behavior is described without presenting a theoretical model.
Should be written in English.	Articles written in a language other than English.

3.2. Data Sources and Search Strategies

The data were collected through different online databases, such as Emerald, Springer, Taylor, and Francis, IEEE Explore, SAGE, Science Direct, and Google Scholar. The studies were searched in these databases between June–August of 2021. The retrieved studies were restricted to journal articles and conference proceedings. The search string for the studies was ((“cybersecurity” OR “cyber security”) AND (“behavior” OR “behaviour”)). The selection of relevant keywords is critical since it influences the retrieval of relevant articles from databases [53].

The search results retrieved 2210 articles by using the mentioned search string. A total of 227 were found as duplicate articles, and thus, were discarded. The remaining articles become 1983. The inclusion and exclusion criteria were applied strictly for the remaining articles. The entire review process followed the preferred reporting items for systematic reviews and meta-analysis (PRISMA), as depicted in Figure 1. The first and second authors of this research independently analyzed each of the gathered papers to conduct the analysis. The two authors reconciled their discrepancies in analyzing the studies through conversation and further examination of the contested papers. The total number of articles consulted for this study is 39.

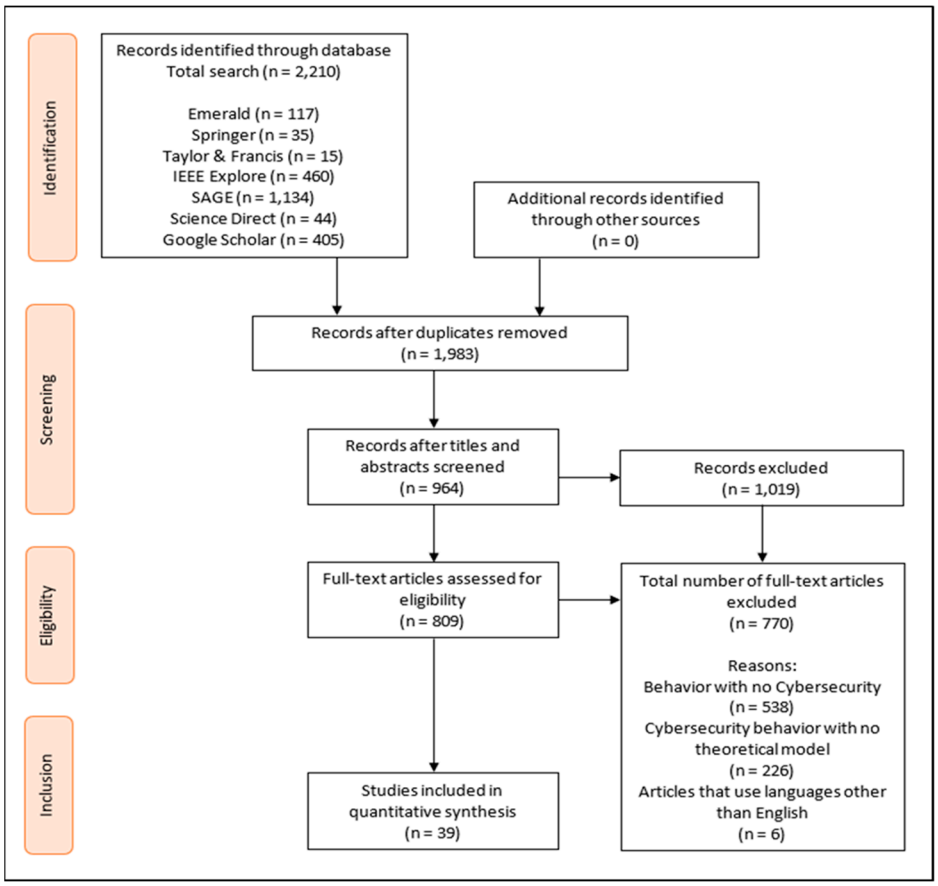

Figure 1. PRISMA flowchart.

3.3. Data Coding and Analysis

The data extracted from the included articles involved different characteristics, such as (a) publication year, (b) theoretical model, (c) independent variables, (d) dependent variables, (e) technologies or services, (f) method, (g) participants, and (h) country. These characteristics correspond to the research questions of this systematic review.

4. Results

The outcomes of this systematic review are provided based on the research questions through analyzing the included studies (N = 39). Table A1 (Appendix A) shows the classification analysis of the analyzed research articles on cybersecurity behavior. Figure 2 depicts the distribution of the examined articles throughout the years they were published. These studies span the years 2012 to 2021. Most cybersecurity research articles were published in the last three years (2019, 2020, 2021), clearly showing the research community's increasing interest in this research topic.

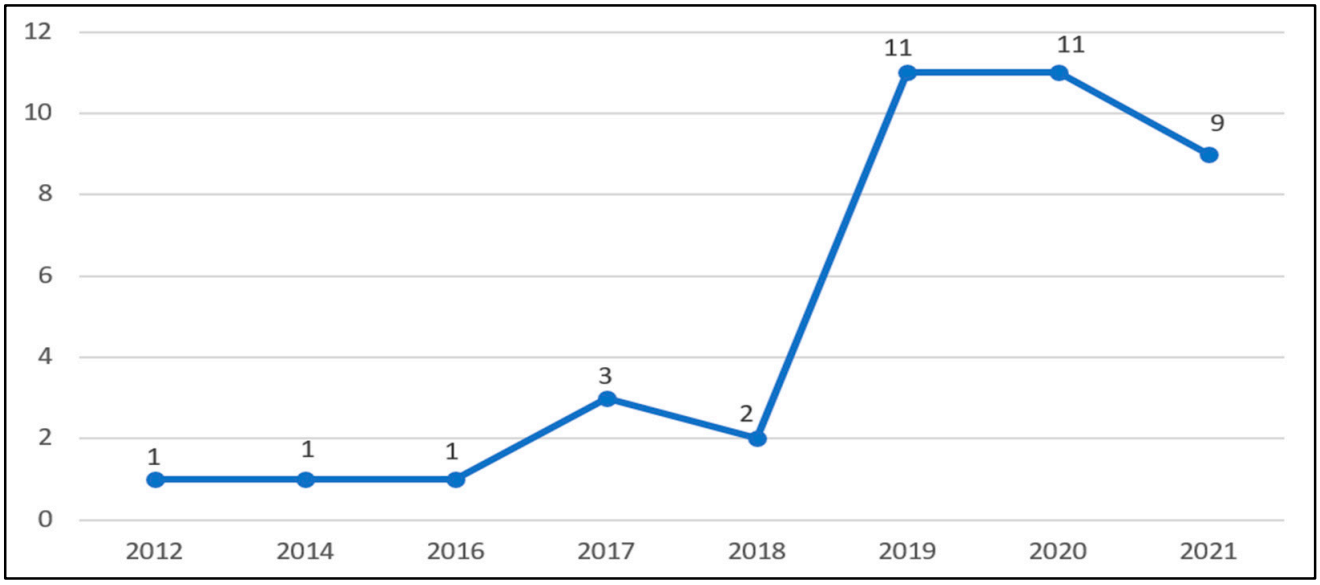

Figure 2. Articles distribution by publication years.

4.1. Prominent Theories and Models in Cybersecurity Behavior

Numerous research studies investigated cybersecurity behavior through different theories and models. Table 3 illustrates the prominent theories and models used in understanding what impacts cybersecurity behavior. The protection motivation theory (PMT), with 17 studies, dominates the list of theories and models, followed by the technology threat avoidance theory (TTAT), with 6 studies. In addition, the theory of planned behavior (TPB) and the general deterrence theory (GDT) represent the third and fourth categories in the list with four studies each, followed by the threat avoidance motivation (TAM) (N = 3) and health belief model (HBM) (N = 2). However, the other theories and models appeared only once in the analyzed studies, as shown in Table 3.

Table 4 highlights the strengths and limitations of the significant theories and models that appeared at least twice in the analysis. While PMT considers factors related to threat appraisal and coping appraisal, it fails to acknowledge the impact of social norms. In addition, TTAT adopts a broad perspective in identifying the determinants of threat avoidance in cybersecurity. However, it fails to cover individual threat motivations sufficiently. Further, the GDT emphasizes rationality in modeling behavior. The downside of this approach is that people can be irrational sometimes. TPB's main strength is that it considers subjective norms, perceived behavioral control, and attitudes in affecting behavior. However, it fails to consider personal factors that influence motivation and intention. Although TAM

explains avoiding threats, evaluating cybersecurity behavior in organizations with large and complex security environments can also be challenging. Further, HBM is broad and considers cognitive elements influencing behavior. Still, it fails to consider economic and environmental factors affecting behavior. In summary, it can be noticed that there is no single theory that covers all the factors affecting cybersecurity behavior. Understanding the strengths and limitations of each theory enables future research to consider various perspectives through the development of hybrid theoretical models.

Table 3. Prominent theories and models in cybersecurity behavior.

Theories and Models	Frequency
Protection Motivation Theory	17
Technology Threat Avoidance Theory	6
General Deterrence Theory	4
Theory of Planned Behavior	4
Threat Avoidance Motivation	3
Health Belief Model	2
Control Theory	1
Theory of Reasoned Action	1
Decision-making Theory	1
Compliance Theory	1
Donalds and Osei-Bryson Model	1
Knowledge, Attitude, and Behavior Model	1
Actor-network Theory	1
Regret Theory	1
Affect Heuristic Model	1
Theory of Social Preferences	1
Big Five Model	1
Social Cognitive Theory	1
6-T Internet Attitude Model	1
Coping Theory	1
Job Demands-Resources Model	1
Unified Theory of Acceptance and Usage of Technology	1
Individual Cybersecurity Compliance Behavior Model	1
Innovation Diffusion Theory	1

Table 4. Strengths and limitations of prominent theories and models.

Theories/Models	Strengths	Limitations
Protection Motivation Theory (PMT)	PMT explains how people respond to fear appeals. It considers two elements related to protection motivation: threat appraisal and coping appraisal [54]. Cybersecurity behavior studies have shown that PMT effectively changes behavior [55].	PMT fails to consider environmental elements, which affect behavior. For example, it does not consider the effect of social norms. Additionally, it does not consider cognitive variables influencing decision making. For instance, it does not consider the role of experience in behavior [56]. PMT also lacks consideration of individual differences [18]. PMT assumes everyone responds to threats similarly, but this is not always true. This is because individuals have different perceptions of what is threatening, and their reactions may vary based on their past experiences, beliefs, and attitudes.

Table 4. *Cont.*

Theories/Models	Strengths	Limitations
Technology Threat Avoidance Theory (TTAT)	TTAT adopts a broad perspective in explaining the users' awareness of technology threats and their motivation to avoid them [57]. In addition to threat and coping appraisal, it considers elements related to coping. More importantly, it includes factors related to risk tolerance and social influence [58]. It has been found to be a valid framework for examining users' cybersecurity behavior toward malware [59].	TTAT does not cover individual threat motivations adequately [58]. Individual characteristics, such as the propensity for risk and impulsivity, influence people's actions. Its broad nature also makes implementing it in practical settings difficult. Additionally, TTAT focuses mainly on technical measures to prevent cyber threats and overlooks other critical aspects of cybersecurity, such as policy, governance, and organizational culture.
General Deterrence Theory (GDT)	GDT adopts a rational approach to deterring negative behavior by using countermeasures, such as sanctions and other disincentives [60]. Increasing the perception that offenders will be caught and punished can promote positive behavior.	GDT fails to consider that negative actions are often irrational. In addition to personal factors, other environmental variables can influence an individual to engage in harmful behavior [60]. Offenders might feel that they can get away by committing an offense. This is particularly common in cybersecurity, as attackers can remain anonymous. Similarly, if the sanction is minor, attackers can agree to bear the risk.
Theory of Planned Behavior (TPB)	TPB considers the role of subjective norms in influencing the initiation and maintenance of behavior [61]. It also considers the role of perceived behavioral control and attitudes in affecting the intention to use technology [62]. This theory has also been used to model behavior in cybersecurity [61].	While the TPB considers the availability of the resources needed to perform the required behavior [61], it fails to consider personal factors that influence motivation and intention. Although the theory considers normative influences, it fails to consider environmental factors. It posits that the decision-making process is linear, which might not be the case in all situations. The TPB assumes that attitudes and intentions are the primary determinants of behavior [19]. However, there may be a significant gap between individuals' attitudes and actual behavior, particularly in examining cybersecurity behavior. Additionally, the TPB assumes that individuals have control over their behavior. However, in cybersecurity behavior, individuals may not have complete control over their actions due to other factors, such as technical constraints or external threats.
Threat Avoidance Motivation (TAM)	TAM posits that the motivation to avoid a threat is premised on perceived vulnerability and severity [55]. Its main strength is that it offers a framework for describing how individuals avoid threats. It also adopts a rational approach to explaining the behavior of people.	The theory adopts a narrow approach to explaining the motivation to avoid threats. Another limitation of the theory is that it may be based on an incomplete or inaccurate understanding of the existing threats. This can result in individuals focusing on the wrong threats or failing to prepare for potential attacks adequately. The theory can also be challenging to evaluate cybersecurity behavior in organizations with large and complex security environments. This is due to the limitations of effective threat avoidance strategies. In general, it has not been examined sufficiently in cybersecurity behavior research.
Health Belief Model (HBM)	HBM considers cognitive elements that influence behavior. This is based on four factors: susceptibility, benefits, severity, and barriers [63]. This broad examination of an individual's beliefs enables the adoption of holistic strategies for changing behavior. HBM can be leveraged to promote positive cybersecurity behavior.	HBM is a psychological model, which means that other external factors influencing behavior, such as economic and environmental factors, are not considered. Additionally, it does not explain routine factors that routinely influence decision making. It also lacks an explanation of the beliefs and attitudes affecting behavior. It does not account for peer pressure and social norms controlling behavior.

4.2. Common Research Themes

To understand the research themes of the analyzed articles, we have relied on surveying the dependent variables measured in each study. Table 5 shows the research themes

in the analyzed articles. It can be seen that the cybersecurity behavior and intention behavior counted the highest purpose for conducting most of the studies, with 14 studies for each. This is followed by avoidance behavior and avoidance motivation, with five studies each. Further, the analysis also shows four studies for usage behavior and three for each compliance behavior and cybersecurity awareness.

Table 5. Research themes in cybersecurity behavior.

Research Themes	Frequency
Intention behavior	14
Cybersecurity behavior	14
Avoidance behavior	5
Avoidance motivation	5
Usage behavior	4
Compliance behavior	3
Cybersecurity awareness	3
Attitude	2
Procrastination	1
Perceived usefulness	1
Value for personalization	1
Assurance behavior	1
Perseverance of effort	1
Behavioral comprehensiveness	1
Cooperate intention	1
Psychological detachment	1
Behavioral habits	1
Compliance intention	1
Peer behavior	1

Compliance behavior refers to individual practices related to adhering to laws and regulations. Compliance behavior adheres to cybersecurity laws, regulations, and procedures [64]. An example of a regulation that must be complied with within the cybersecurity realm is the Gramm-Leach-Bliley Act, which requires financial institutions to explain their information-sharing practices and safeguard sensitive information [65]. On the contrary, cybersecurity behavior is specific to cybersecurity but not limited to laws and regulations. In other words, cybersecurity behavior goes beyond the law to include acting in a manner that aligns with best practices, industry values, and standards.

4.3. External Factors Affecting Cybersecurity

External factors refer to those that are not a part of the original theories/models and were used to extend these theories/ models to examine the users' cybersecurity behavior in specific technologies or services. The role of external factors has a significant positive or negative impact on individuals' behaviors. Therefore, we have analyzed the included studies through the lenses of the external factors affecting cybersecurity behavior, as shown in Table 6. It is imperative to report that only the factors that appeared at least twice in the analyzed studies were depicted. It can be observed that the most influential factor is self-efficacy (N = 16), followed by perceived severity (N = 12), response efficacy (N = 10), perceived vulnerability (N = 7), and five studies for subjective norm, response costs, and perceived susceptibility.

Table 6. External factors affecting cybersecurity behavior.

External Factors	Frequency
Self-efficacy	16
Perceived severity	12
Response efficacy	10
Perceived vulnerability	7
Perceived susceptibility	5
Response costs	5
Subjective norm	5
Cues to action	4
Peer behavior	4
Perceived barriers	4
Perceived risk	3
Perceived benefit	3
Habit	3
Security self-efficacy	3
Computer skills	3
Perceived cost	3
Severity	2
Perceived certainty of sanction	2
Psychological ownership	2
Perceived response efficacy	2
Safeguard cost	2
Neuroticism	2
Perceived effectiveness	2
Perceived risk vulnerability	2
Agreeableness	2
Openness	2
Risk-taking	2
Perceived severity of sanction	2
Safeguard effectiveness	2
Extraversion	2
Conscientiousness	2
Perceived usefulness	2
Familiarity	2
Perceived ease of use	2
Decision-making style	2

4.4. Relationship between Cybersecurity Research Themes and External Factors

Mind mapping is believed to be a suitable way to represent the relationship between cybersecurity research themes and external factors. Mind mapping, also known as concept mapping, visually represents links between ideas or concepts [66]. Figure 3 presents the mind map of the research themes (i.e., dependent variables) in the analyzed articles and the external factors affecting different behaviors. The relationship is assessed based on the significance of the results in the analyzed articles. In that, only the factors that showed significant differences were considered in the mind map.

It can be observed that self-efficacy, response efficacy, response cost, subjective norms, perceived usefulness, and perceived ease of use significantly impact intention behavior. Moreover, perceived severity, self-efficacy, perceived vulnerability, cues to action, response efficacy, peer behavior, and perceived barriers significantly affect cybersecurity behavior. Moreover, self-efficacy, perceived susceptibility, perceived severity, perceived cost, safeguard effectiveness, safeguard cost, and perceived effectiveness have substantial effects on avoidance behavior. In addition, it was found that self-efficacy, perceived susceptibility, perceived severity, perceived cost, safeguard effectiveness, safeguard cost, and perceived effectiveness have significant impacts on avoidance motivation. Furthermore, perceived ease of use, facilitating conditions, self-efficacy, trust, and habit considerably impact usage behavior. Moreover, attitude, response cost, subjective norms, and self-efficacy significantly

impact compliance behavior. Additionally, it was noticed that perceived costs, response efficacy, self-efficacy, perceived severity, and perceived vulnerability have significant impacts on cybersecurity awareness.

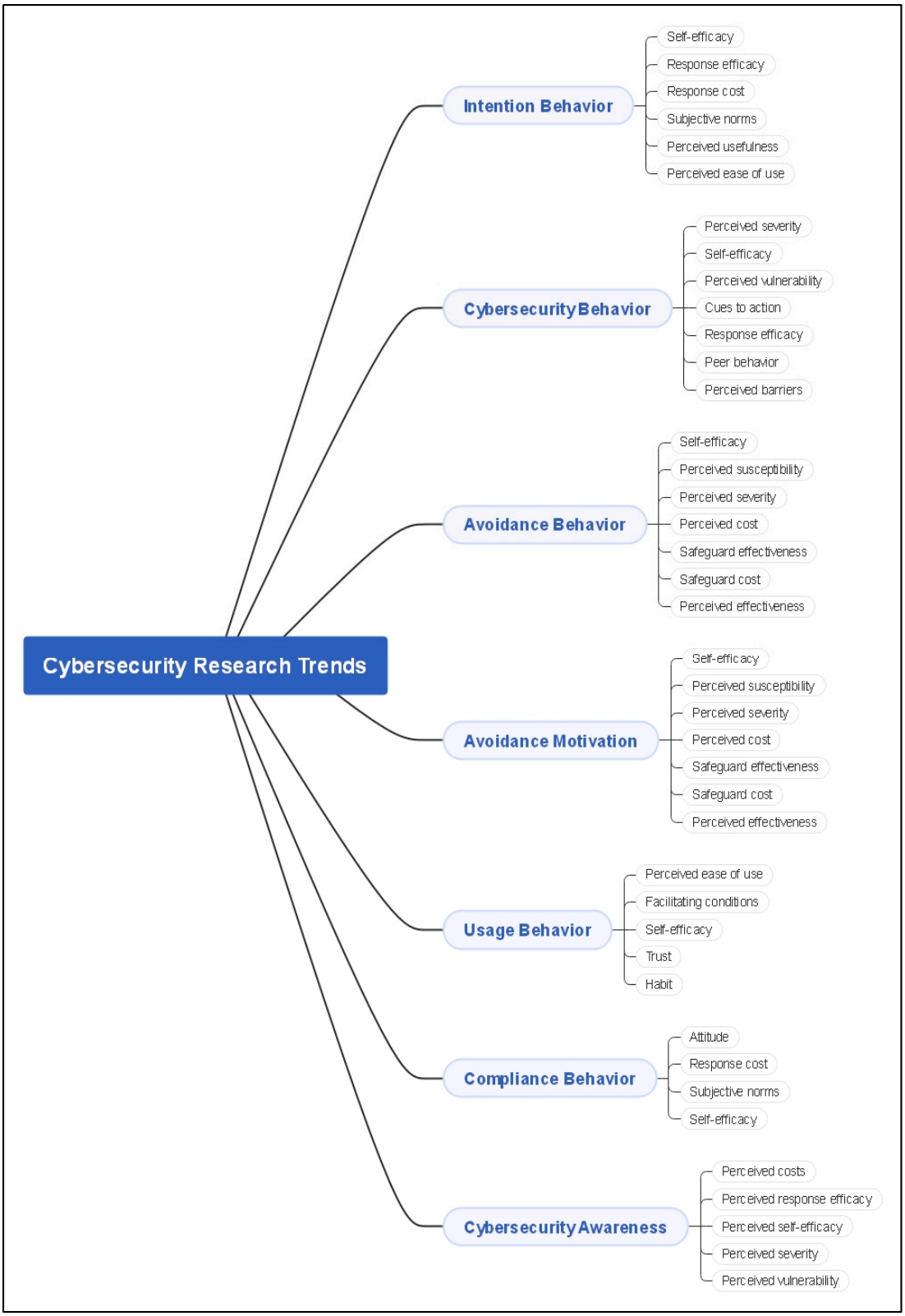

Figure 3. Mind map of cybersecurity research themes and external factors.

4.5. Dominant Technologies and Services in Cybersecurity

It is imperative to report that cyber threats can affect several technologies and services. Therefore, this systematic review considers analyzing the dominant technologies and services studied in the previous cybersecurity behavior research. Table 7 shows the prevailing technologies and services used in cybersecurity behavior research. It is observed that smartphones (N = 5) are the most common technology used in the analyzed studies. This is followed by information systems (N = 4), social networking sites, and games, with three studies each, and e-mail, malware, and Internet threats, with two studies each. It is also essential to indicate that 12 studies did not report the technology or service used.

Table 7. Dominant technologies and services in cybersecurity.

Technologies and Services	Frequency
Not specified	12
Smartphones	5
Information systems	4
Games	3
Social networking sites	3
Internet threats	2
E-mail	2
Malware	2
Computer	1
Ecosystem	1
Web browser	1
Internet security software	1
Anti-malware software	1
Internet of Things	1

Social networking sites collect large quantities of data daily [67,68]. Therefore, appropriate cybersecurity behavior among social media users is critical to preserving privacy. Some security best practices on social media include managing privacy settings, maintaining personal information, using secure devices, and being cautious [69]. For instance, Addae et al. [70] devised a personal data attitude assessment instrument by employing psychometric principles, enabling the reliable quantification and comparison of attitudes. The research involved administering an online questionnaire to 247 participants. The results indicate that factors shaping individuals' attitudes toward personal data encompass privacy concerns, protective practices, awareness, cost-benefit analysis, security, and responsibility. Consequently, the trustworthiness of social networking can be evaluated based on these six constructs for both individuals and organizations. Another study [71] employed principles derived from the TPB to investigate the mediating effect of information security awareness on users' intentions to examine privacy settings on Facebook. The results indicate that information security awareness does, indeed, mediate security behavior in certain personality traits, particularly openness, and conscientiousness. The study highlights that openness and conscientiousness can shape individuals' and organizations' perceptions of social networks' trustworthiness, particularly when those in decision-making roles exhibit these traits. In addition, Van Schaik et al. [72] demonstrated that the "affect heuristic" significantly shapes risk perception within the cybersecurity domain. This indicates that an individual's perception of the risk associated with a specific technology is directly influenced by the affective response elicited by that technology. Consequently, if individuals perceive using a typical social networking platform as advantageous, they will likely regard it as beneficial and trustworthy. A parallel perception can be anticipated within organizational contexts.

Smartphones also collect highly confidential data from users, including location, messages, phone calls, images, and personal information. Hence, positive cybersecurity behavior can help secure the data on these devices. Web browsers, which are utilized to surf the web, can be exploited, resulting in cyberattacks. Therefore, users must exhibit

positive behavior when visiting websites and updating their browsers and extensions [73]. Computer games, like other applications, can be conduits for attacks. Gamers, therefore, must be careful not to divulge sensitive information on these platforms. In addition, malware and Internet threats are often successful due to negative cybersecurity behavior. Failure to update applications could increase the impact of threats.

4.6. Leading Research Methods

Identifying the research methods used in the analyzed articles assists further research in selecting the suitable method for the intervention. Therefore, we have examined the research methods used in the analyzed studies. We observed that the majority of the analyzed studies have relied on the quantitative method of questionnaire surveys (N = 37). On the other hand, only two of the analyzed studies exposed a mixed method of questionnaire surveys and focus groups. It is imperative to mention that none of the analyzed studies have relied on the qualitative approach.

4.7. Active Countries in Cybersecurity Behavior Research

Analyzing the countries in any behavioral research helps determine those active and inactive in the domain, highlight the existing challenges, and suggest further research opportunities. The determinants affecting cybersecurity behavior vary between developing and developed countries. Therefore, it is worth analyzing the countries in this research arena. Figure 4 shows the active countries in cybersecurity behavior research. It is evident that studies were carried out mainly in the United States (USA) (N = 12), followed by Malaysia (N = 5), and Australia, China, and the United Kingdom (U.K.), with four studies each. Additionally, New Zealand, Taiwan, and the United Arab Emirates (UAE), with two studies each. It is imperative to mention that seven of the analyzed studies did not specify the country of study.

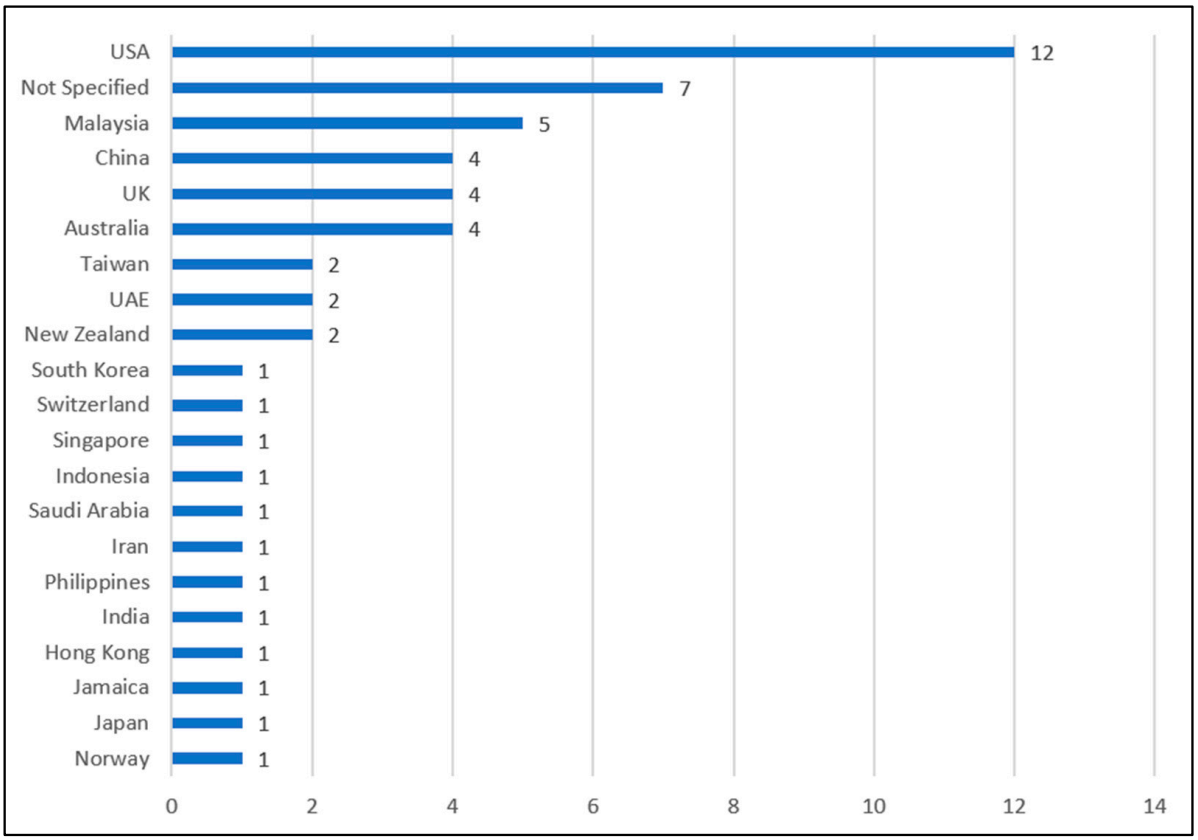

Figure 4. Active countries in cybersecurity behavior research.

4.8. Relationship between Cybersecurity Research Themes and Study Regions

Identifying the relationship between research themes, which were characterized through the dependent variables in each study, and study regions helps understand each region's focus and suggests further research in the domain. Figure 5 shows the cybersecurity research trends among active countries. It can be noticed that intention behavior toward a specific technology/service was mostly studied in the USA (N = 4), followed by the UAE, U.K., Australia, and Malaysia, with two studies each. Moreover, the cybersecurity behavior was mainly examined in the USA (N = 5), followed by the U.K. (N = 3), and China (N = 2). Moreover, avoidance motivation and avoidance behavior were intensively studied in three studies carried out in the USA and one in Australia. Further, the usage behavior was mainly studied in Australia (N = 3), followed by Taiwan (N = 2), and a single study was conducted in other countries. Furthermore, compliance behavior was researched in the USA (N = 2), followed by China, U.K., Jamaica, and the UAE, with one study each. In addition, cybersecurity awareness was scarcely studied, with one study in Australia and Switzerland.

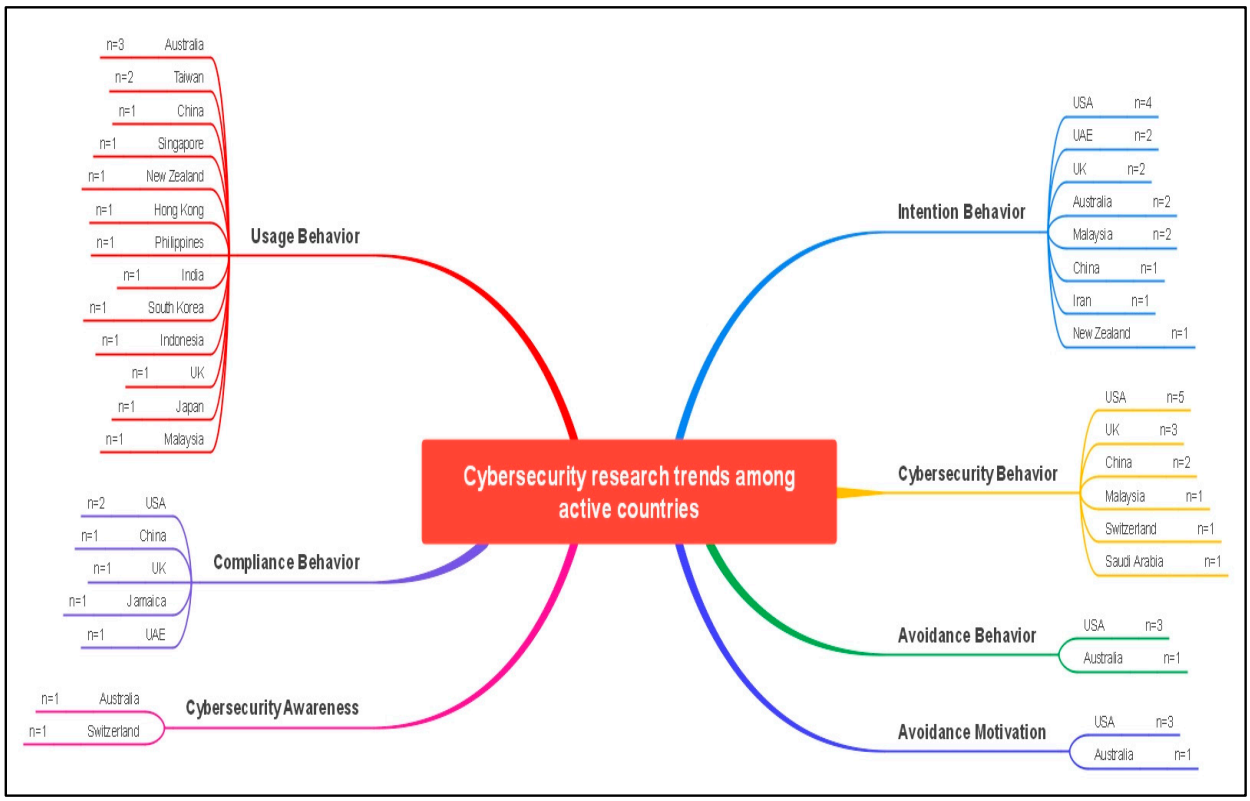

Figure 5. Cybersecurity research trends among active countries.

4.9. Main Participants in Cybersecurity Behavior Research

Understanding the participants in previous cybersecurity behavior research assists in conducting future trials. The analysis also helps us to understand whether the existing research has emphasized the individual or organizational level. Figure 6 demonstrates the distribution of the analyzed studies in terms of participants. It can be observed that cybersecurity behavior studies were primarily focused on organizational employees (N = 22), including managers, decision-makers, IT experts, and end-user employees. This is followed by students (N = 13), consumers (N = 4), academics (N = 3), including researchers and lecturers, and parents (N = 1).

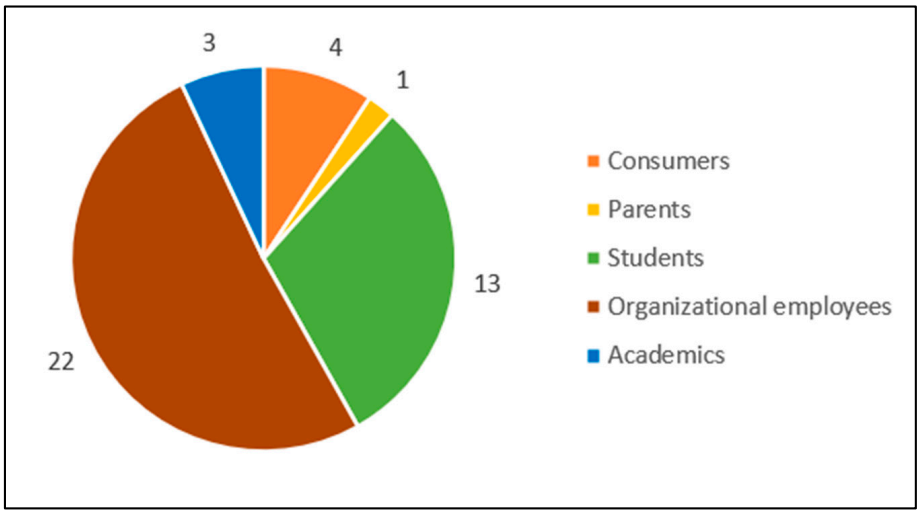

Figure 6. Articles distribution by study participants.

5. Discussion

Cybersecurity behavior and human characteristics are correlated [74]. Cybersecurity is essential for preserving privacy and avoiding illegal monitoring, and information exchange and intelligence collection can be valuable tools for implementing cybersecurity [75]. The primary purpose of this research was to conduct a systematic review to critically analyze and synthesize the articles published on cybersecurity behavior to improve the understanding of the common research themes, external factors, dominant technologies and services, main research methods, active countries, and participants. Understanding these characteristics would provide more insights into the existing challenges in cybersecurity behavior and offer opportunities for future research trials. Figure 7 summarizes the main review findings through a mind map, depicting the relationship between each characteristic and its main conclusions.

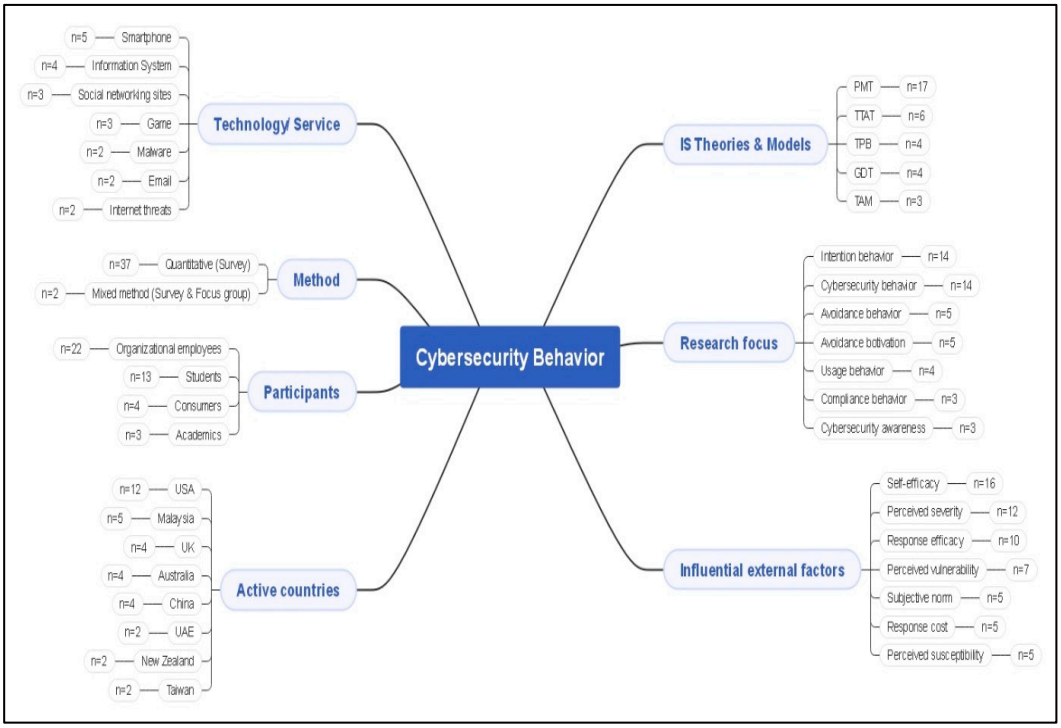

Figure 7. Mind map of cybersecurity behavior research findings.

5.1. Rapid Growth in Cybersecurity Behavior Research

The results showed that there had been a rise in the number of articles published between 2012 and 2021, with a significant boom between 2019 and 2021. The considerable number of publications, specifically during the last few years, contributes to the increasing research interest in examining what impacts cybersecurity behavior. The growing interest stems from several reasons. For instance, individual errors cause 95% of cybersecurity incidents [76]. In 2019, 88% of organizations worldwide were exposed to spear-phishing attacks [77]. Thus, it is believed that the number of publications on cybersecurity behavior will be doubled in the next few years. This belief is due to the expectation that the number of IoT-connected devices will reach 75 billion in 2025 [76], which requires individuals and organizations to make cybersecurity behavior a part of their culture.

5.2. Analysis of Theories and Models in Cybersecurity Behavior

For the IS theories and models, the results showed that PMT is the most frequently used theory, with 17 studies. The prominent use of PMT stems from the theory's aim to explain fear appeals and suggests that individuals protect themselves through several factors, such as perceived severity and perceived vulnerability [78,79]. In addition, PMT assists in explaining individual differences in protective cybersecurity behaviors, as action-based decisions are built on individual risk perceptions [72]. By critically analyzing the PMT-related studies, it has been found that most of them focused on exploring the cybersecurity behavior (N = 10) and the intention behavior (N = 7). For example, some studies used the PMT to study the factors affecting cybersecurity behavior in social networking sites [70,72], web browsers [55], and computers [80]. Moreover, other studies employed the PMT to study the intention behavior toward smartphone use [81,82] and malware [56]. This is followed by TTAT-related studies (N = 6) that mainly focused on analyzing avoidance motivation and avoidance behavior. For instance, the TTAT is used to analyze the avoidance motivation and avoidance behavior in playing games [54], dealing with Internet threats [83], and malware [59]. The TPB and GDT-related studies (N = 4) also focused on analyzing the intention behavior. For example, the TBP is utilized to study the intention behavior toward using social networking sites [71] and anti-malware software [61]. Moreover, the GDT is employed to analyze the intention behavior toward using e-mail [60] and smartphones [81,82]. Moreover, the TAM-related studies (N = 3) mainly focused on exploring cybersecurity behavior. For example, the TAM is used to study the cybersecurity behavior toward using web browsers [55] and social networking sites [70]. In addition, the HBM-related studies (N = 2) focused on analyzing cybersecurity behavior [63,84] where the technology or service is not specified. Since we are dealing with 'behavior', more theories need to be explored to further understand what impacts cybersecurity behavior by individuals and organizations. The existing literature sheds inadequate exposure to the social, psychological, and technical determinants.

5.3. Cybersecurity Research Themes and Key Factors

This review analyzed the research themes of the collected articles by examining the dependent variables in each study. The findings showed that 'intention behavior' and 'cybersecurity behavior' were the most common purposes for conducting the studies. The studies that relied on the 'intention behavior' aimed to examine the users' behavior toward using different technologies and services from the perspective of security incidents. The studies that examined 'cybersecurity behavior' aimed to investigate the determinants affecting users' behavior toward cybersecurity. The findings also indicated that the extant literature has not adequately addressed the aspects of cybersecurity awareness and compliance behavior, thereby presenting opportunities for additional investigative endeavors. A recent systematic review corroborates this observation [85].

For the external factors, the results indicated that self-efficacy is the most influential factor affecting cybersecurity behavior, followed by perceived severity, response efficacy, and perceived vulnerability. Undoubtedly, these are the factors derived from the PMT

theory. These results suggest that further research needs to consider the role of social, technical, and psychological factors in understanding cybersecurity behavior. While analyzing the external factors, it has been noticed that the role of moderators is neglected in the extant literature. This issue was also discussed in a recent study conducted on employees' security behavior [86].

This review also analyzed the relationship between the cybersecurity research themes and the external factors, technologies/services, and active countries. In terms of 'intention behavior', it was found that self-efficacy, response efficacy, response cost, subjective norms, perceived usefulness, and perceived ease of use significantly impact intention behavior. The studies mainly focused on examining the intention behavior toward using several technologies/services, such as information systems [87,88], Internet security software [71], malware [56], anti-malware software [61], social networking sites [70,71], web browsers [55], games [89,90], e-mails [60], and smartphones [81,82]. The 'intention behavior' has been primarily studied in the USA, UAE, U.K., Australia, and Malaysia, respectively.

In terms of cybersecurity behavior, the results showed that perceived severity, self-efficacy, perceived vulnerability, cues to action, response efficacy, peer behavior, and perceived barriers were the most influential factors. The technologies/services under this theme include information systems [91], social networking sites [70,72], web browsers [55], computers [80], smartphones [92], and Internet threats [93]. Understanding what impacts cybersecurity behavior was mainly studied in the USA, U.K., and China, respectively.

For avoidance behavior and avoidance motivation, the results indicated that self-efficacy, perceived susceptibility, perceived severity, perceived cost, safeguard effectiveness, safeguard cost, and perceived effectiveness were the dominant influential factors. The leading technologies/services investigated under this theme include Internet threats [83], games [54], smartphones [94], and malware [59]. The USA and Australia were the only active countries conducting studies on avoidance behavior and avoidance motivation. The increasing interest in these two countries stems from the COVID-19 pandemic-related cybercrime reported cases, which have increased to 300% in the USA [95] and 75% in Australia [96].

Concerning the 'usage behavior', the findings showed that perceived ease of use, facilitating conditions, self-efficacy, trust, and habit have significant impacts on using several technologies/services from the perspective of cybercrimes and security incidents. These technologies/services include web browsers [59], games [89], smartphones [97], and e-mails [98]. This theme has been mainly studied in Australia and Taiwan.

In terms of 'compliance behavior', the results found that attitude, response cost, subjective norms, and self-efficacy were the most influential factors. Smartphones were the primary technology examined under this cluster [81]. The other studies that examined compliance behavior specified neither the technology nor the service used [99,100]. The USA has dominated the list for conducting studies related to this cluster.

For 'cybersecurity awareness', the results indicated that perceived costs, response efficacy, self-efficacy, perceived severity, and perceived vulnerability were the most common determinants affecting the individuals' cybersecurity awareness. The main technologies/services examined under this theme include computers [80], IoT [101], and social networking sites [71]. This has been mainly studied in Australia and Switzerland.

5.4. Cybersecurity Research Trends in Diverse Cultural and Socioeconomic Settings

Understanding the relationship between cybersecurity research themes and influential factors on the one hand and the active countries on the other hand assists further research in the domain. For instance, the majority of the examined studies were conducted in individualistic contexts with limited exposure to collectivistic societies. This phenomenon encourages further empirical research to be carried out in those contexts. Moreover, most of the analyzed studies were carried out in developed countries. Understanding the determinants affecting cybersecurity might differ in developing countries from those in developed

countries due to the differences in technology infrastructure, participants' awareness, culture, etc. This observation, in turn, encourages more research in those countries.

5.5. Research Methodologies in Cybersecurity Behavior

The results showed that 95% of the analyzed articles relied on quantitative research methods through questionnaire surveys, while the rest used mixed research methods involving questionnaire surveys and focus groups. This result suggests considering the mixed research method in future studies as relying on questionnaire surveys only might not be adequate to explain the causal relationships among the variables in the research model.

5.6. Participants in Cybersecurity Behavior Research

This review also analyzed the participants involved in each study. This classification helps understand whether the existing research has emphasized the individual or organizational level. The results found that 56% of the analyzed studies focused on organizational employees, followed by students with 33%. This observation provides evidence that understanding what impacts cybersecurity behavior at the individual level is still in its infancy stage, which opens the door for further research.

6. Conclusions and Future Research Agendas

The increasing number of cybercrimes and security incidents has promoted the concept of cybersecurity behavior to protect individuals and organizations from such threats efficiently. However, this topic is still in its infancy stage and requires further investigation. Therefore, this systematic review was conducted to gain deeper insights into the common research themes, external factors affecting cybersecurity behavior, dominant technologies and services, main research methods, active countries, and participants. We believe this review will be a valuable guide for scholars and practitioners in providing the existing gaps and suggesting opportunities for further research.

This review sheds light on several gaps in research. First, the PMT was the most frequently used theory in understanding the determinants influencing cybersecurity behavior. Most of the examined studies concentrated on the role of security determinants, such as perceived severity, response efficacy, and perceived vulnerability, in understanding cybersecurity behavior, with little attention paid to the role of social, psychological, and technical determinants. This phenomenon requires the need for more research that involves theories covering these factors. Second, insufficient knowledge of what affects cybersecurity awareness and compliance behavior opens the door for further research trials. Third, we have noticed that the role of moderators is neglected in the extant literature. Therefore, we suggest that further research involves the role of moderators as their absence might raise inconsistent effects of the factors across studies [102]. Fourth, most of the examined studies were conducted in individualistic contexts with limited exposure to collectivistic societies. This issue encourages further empirical research to be conducted in those contexts. Fifth, 95% of the analyzed articles have relied on quantitative research methods through questionnaire surveys for data collection. Therefore, further empirical research is encouraged to consider mixed methods as relying on questionnaire surveys only might not be adequate to explain the causal relationships among the variables in the research model. Sixth, since most of the reviewed studies have relied on conventional analysis techniques, such as SEM, more advanced analytical methods can be used in future studies. For example, machine learning algorithms can analyze large amounts of data and identify interesting patterns in these data [103,104]. Machine learning and deep learning play essential roles in securing computer systems from unauthorized access and managing system penetration by anticipating and comprehending the behavior and traffic of harmful software [105]. Therefore, future research might use machine learning algorithms to analyze individual cybersecurity behavior by processing large amounts of data to identify patterns and correlations that could indicate potential security threats. Seventh, 56% of the analyzed studies have focused on organizational employees in explaining what affects cy-

bersecurity behavior. This observation provides evidence that understanding what impacts cybersecurity behavior at the individual level is still in short supply, which requires further investigation.

To address the gaps in cybersecurity behavior research at the individual level, this review proposes a number of future research agendas. Future research should focus on the impact of social and psychological factors, such as peer influence, cultural values, and individual beliefs and attitudes, on cybersecurity behavior. Technical determinants, such as technology literacy and accessibility, should also be considered. Additionally, further research should be conducted to understand the factors influencing awareness and compliance with cybersecurity best practices and policies. This can include studies on the impact of training and education programs and the role of incentives and consequences. The role of moderators, such as age, sex, and technical experience, in shaping the effects of other determinants on cybersecurity behavior should also be investigated at the individual level. This can help to explain inconsistencies in the existing literature. Moreover, research at the individual level should be conducted in collectivistic societies to understand how cultural values and group norms shape cybersecurity behavior. Future research needs to be conducted longitudinally to understand how cybersecurity behavior changes over time and in response to different factors and events. Comparative studies can also be suggested across different cultures and regions to understand how cultural and regional factors influence cybersecurity behavior.

In summary, cybersecurity is crucial for both organizations and individuals. It has been observed that an increasing number of non-expert social media users are becoming aware of the significance of various security measures [106]. Furthermore, individuals are less inclined to divulge personal information due to privacy concerns [107]. As stated in [108], security, privacy, and resilience are vital components of healthcare applications. Additionally, the Metaverse is not immune to security and privacy violations linked to human behavior, as noted in [109,110]. Consequently, Kannelønning and Katsikas [47] underscored the necessity for implementing policies to regulate employee conduct within organizations. Enhanced education and awareness contribute to improved cybersecurity behavior [111,112]. Therefore, raising information security awareness can foster positive behavior among employees [113].

Author Contributions: Conceptualization, A.A. and M.A.-E.; methodology, A.A. and M.A.-E.; validation, A.A. and M.A.-E.; formal analysis, A.A.; investigation, A.A.; resources, A.A.; writing—original draft preparation, A.A.; writing—review and editing, M.A.-E. and K.S.; supervision, M.A.-E. and K.S.; project administration, M.A.-E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the authors.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. List of analyzed studies.

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S01	[83]	2021	Technology Threat Avoidance Theory	"Perceived susceptibility", "Perceived severity", "Perceived effectiveness", "Perceived cost", and "Self-efficacy"	"Avoidance Motivation" and "Avoidance Behavior"	Internet threats	Quantitative (survey)	Organizational employees	USA
S02	[114]	2019	Social Cognitive Theory	"Information security policy", "Subjective norm", "Perceived inconvenience", "Self-efficacy", "Outcome expectation", and "Information security monitoring"	Assurance Behavior	Information system	Mixed method (survey and focus group)	Organizational employees	Malaysia
S03	[91]	2019	Coping Theory	"Perceived externality" and "Triage"	"Procrastination", "Psychological detachment", and "Cybersecurity Behavior"	Information system	Quantitative (survey)	Organizational employees	China
S04	[88]	2020	Job Demands-Resources Model	"Continuity demand", "Mandatory demand", "Trust enhancement", and "Professional development"	"Perseverance of effort" and "Intention Behavior"	Information system	Quantitative (survey)	Organizational employees	Not Specified
S05	[100]	2021	Compliance Theory and Control Theory	"Reward expectancy", "Punishment expectancy", and "Organizational commitment"	"Compliance Behavior"	Not Specified	Quantitative (survey)	Organizational employees	China
S06	[87]	2021	Decision-making Theory	"Punishment likelihood", "Reward likelihood", and "Neutralization scenarios"	"Intention Behavior"	Information system	Quantitative (survey)	Students	USA
S07	[115]	2018	Innovation Diffusion Theory	"Compatibility", "Ease of use", "images", "intention", "Relative advantage", "Results demonstrability", "Trialability", "Visibility", and "Voluntariness"	"Intention Behavior"	Internet security software	Quantitative (survey)	Students	Malaysia

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S08	[61]	2019	Theory of Planned Behavior	"Perceived price level", "Information security awareness", "Subjective norms", and "Perceived behavioral control"	"Attitude" and "Intention Behavior"	Anti-malware software	Quantitative (survey)	Students	Malaysia
S09	[70]	2017	Protection Motivation Theory and Threat Avoidance Motivation	"Attitude to personal data", "Perceived risk", and "Perceived ease of use"	"Perceived usefulness", "Intention Behavior", and "Cybersecurity Behavior"	Social networking sites	Mixed method (survey and focus group)	Consumers	Not Specified
S10	[55]	2019	Protection Motivation Theory and Threat Avoidance Motivation	"Self-efficacy", "Security breach concern level", "Perceived risk", "Domain knowledge", "System characteristics", "Perceived ease of use", "Perceived usefulness", "Value for personalization" and "Attitude to personal data"	"Intention Behavior", "Cybersecurity Behavior", "Usage Behavior", "Value for personalization", and "Attitude"	Web browser	Quantitative (survey)	Students and academics	China and U.K.
S11	[54]	2020	Technology Threat Avoidance Theory	"Fear", "Safeguard effectiveness", "Safeguard cost", "Self-efficacy", "Perceived severity", "Perceived susceptibility", and "Decision-making style"	"Avoidance Motivation" and "Avoidance Behavior"	Game	Quantitative (survey)	Students	Australia
S12	[89]	2020	Unified Theory of Acceptance and Usage of Technology	"Performance expectancy", "Effort expectancy", "Facilitating conditions", "Hedonic motivation", "Social influence", "Habit", and "Gamification feature"	"Intention Behavior" and "Usage Behavior"	Game	Quantitative (survey)	Students	Australia
S13	[80]	2019	Protection Motivation Theory	"Perceived vulnerability", "Perceived severity", "Perceived self-efficacy", "Perceived response efficacy", "Perceived costs", "Organizational determinants", "Social determinants", and "Personal determinants"	"Cybersecurity Awareness" and "Cybersecurity Behavior"	Computer	Quantitative (survey)	Organizational employees	Switzerland

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S14	[101]	2020	Knowledge, Attitude, and Behavior Model	"Greater employment level", "Grater perception of personal risk", "Grater dread and unfamiliarity of InfoSec risks", and "Greater organizational commitment"	"Cybersecurity Awareness"	Internet of Things	Quantitative (survey)	Organizational employees	Australia
S15	[116]	2019	Theory of Social Preferences	"Cyber attack experience", "Perceived cybersecurity risk", "Perceived cybersecurity value", and "Social preferences"	"Cooperate Intention"	Ecosystem	Quantitative (survey)	Organizational employees	Norway
S16	[117]	2020	Theory of Planned Behavior and Threat Avoidance Motivation	"Subjective norm", "Attitude", "Hardness", "Habit", "Perceived severity", and "Perceived vulnerability"	"Compliance Intention"	Not Specified	Quantitative (survey)	Organizational employees	USA
S17	[60]	2020	Protection Motivation Theory, Theory of Planned Behavior, and General Deterrence Theory	"Perceived vulnerability", "Perceived severity", "Rewards", "Perceived shame", "Response efficacy", "Self-efficacy", "Response cost", "Habit", "Subjective norms", "Procedural countermeasures", "Preventive countermeasures", and "Detective countermeasures"	"Intention Behavior"	E-mail	Quantitative (survey)	Organizational employees	New Zealand
S18	[92]	2020	Technology Threat Avoidance Theory and Protection Motivation Theory	"Security intention", "Self-efficacy", and "Psychological ownership"	"Cybersecurity Behavior"	Smartphone	Quantitative (Survey)	Organizational employees	Not Specified
S19	[90]	2021	Big Five Model	"Risk-taking" and "Decision-making styles"	"Intention Behavior"	Game	Quantitative (Survey)	Students and academics	Iran
S20	[118]	2014	Protection Motivation Theory	"Explicit cybersecurity policy"	"Peer Behavior" and "Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	USA

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S21	[119]	2017	Protection Motivation Theory	"Computer skills", "Information seeking skills", "Experience with cybersecurity practice", "Perceived susceptibility", "Perceived severity", "Self-efficacy", "Perceived barriers", "Perceived benefits", "Response efficacy", "Cues to action", and "Peer behavior"	"Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	Not Specified
S22	[97]	2019	6-T Internet attitude model	"Social networking sites", "Communication", "Video-watching", "Game-playing", "Photo-sharing", "Academy", "Recreational info. searching", "Friends making", "Transaction", "Individual factors", and "Parental factors"	"Usage Behavior"	Smartphone	Quantitative (Survey)	Students and parents	Taiwan
S23	[12]	2021	Protection Motivation Theory	"Situational support", "Self-efficacy", and "Response efficacy"	"Behavioral comprehensiveness" and "Behavioral habits"	Not Specified	Quantitative (Survey)	Students	China
S24	[71]	2021	Theory of Planned Behavior	"Agreeableness", "Conscientiousness", "Extraversion", "Neuroticism", and "Openness"	"Intention Behavior" and "Cybersecurity Awareness"	Social networking sites	Quantitative (Survey)	Consumers	Not Specified
S25	[81]	2021	Protection Motivation Theory, Theory of Reasoned Action, and General Deterrence Theory	"National smartphone cybersecurity policies", "Response cost", "Top management participation", "Technology (smartphone-specific) security threats", "Attitude", "Self-efficacy", "Subjective norms", "Perceived risk vulnerability", "Perceived response efficacy", "Perceived severity of sanction", and "Perceived certainty of sanction"	"Intention Behavior" and "Compliance Behavior"	Smartphone	Quantitative (Survey)	Organizational employees	U.K., USA, and UAE

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S26	[64]	2019	Protection Motivation Theory	"Peer behavior", "Cues to action", "Prior experience with information security practice", "Perceived severity", "Perceived vulnerability", "Perceived barriers", "Response efficacy", and "Self-efficacy"	"Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	USA
S27	[94]	2019	Technology Threat Avoidance Theory and Regret Theory	"Anti-Phishing self-efficacy" and "Anticipated regret"	"Avoidance Motivation" and "Avoidance Behavior"	Smartphone	Quantitative (Survey)	Consumers	Not Specified
S28	[82]	2020	Protection Motivation Theory and General Deterrence Theory	"Self-efficacy", "Perceived severity of sanction", "Perceived risk vulnerability", "Response cost", "Perceived certainty of sanction", "Severity of the adverse consequences", "Response efficacy", "Uncertainty avoidance", "Power distance", "Individualism vs. collection", and "Masculinity vs. femininity"	"Intention Behavior"	Smartphone	Quantitative (Survey)	Organizational employees	USA and UAE
S29	[56]	2018	Protection Motivation Theory	"Severity", "Susceptibility", "Self-efficacy", "Response efficacy", "Response costs", "Experience", "Workplace information sensitivity appraisal", "Responsibility", "Psychological ownership", and "Organisational citizenship behaviors"	"Intention Behavior"	Malware	Quantitative (Survey)	Organizational employees	Not Specified
S30	[99]	2020	Individual cybersecurity compliance behavior model and Donalds and Osei-Bryson model	"Dominant decision style", "General security orientation", "General security awareness", "Dominant orientation", and "Security self-efficacy"	"Compliance Behavior"	Not Specified	Quantitative (Survey)	Students and academics	Jamaica

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S31	[120]	2021	Protection Motivation Theory	"Perceived severity", "Perceived vulnerability", "Perceived barriers", "Response efficacy", and "Security self-efficacy"	"Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	Saudi Arabia
S32	[58]	2020	Technology Threat Avoidance Theory	"Perceived susceptibility", "Perceived severity", "Perceived effectiveness", "Perceived cost", and "Self-efficacy"	"Avoidance Motivation", "Avoidance Behavior", and "Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	USA
S33	[93]	2017	Actor-network Theory	"Familiarity" and "Internet experience proxies"	"Cybersecurity Behavior"	Internet threats	Quantitative (Survey)	Students	U.K. and USA
S34	[72]	2020	Protection Motivation Theory and Affect heuristic model	"Affect", "Perceived risk", and "Perceived benefit"	"Cybersecurity Behavior"	Social networking sites	Quantitative (Survey)	Consumers	U.K.
S35	[63]	2019	Protection Motivation Theory and Health Belief Model	"Perceived vulnerability", "Prior experience with computer security", "Perceived severity", "Security self-efficacy", "Response efficacy", "Cues to action", "Peer behavior", "Computer skills", and "Familiarity with cyber threats"	"Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Students	Malaysia
S36	[59]	2016	Technology Threat Avoidance Theory	"Perceived susceptibility", "Perceived severity", "Perceived threat", "Safeguard effectiveness", "Safeguard cost", and "Self-efficacy"	"Avoidance Motivation" and "Avoidance Behavior"	Malware	Quantitative (Survey)	Students	USA
S37	[84]	2019	Protection Motivation Theory and Health Belief Model	"Computer skills", "Experience with cybersecurity practice", "Perceived vulnerability", "Perceived severity", "Self-efficacy", "Perceived barriers", "Perceived benefits", "Response efficacy", "Cues to action", and "Peer behavior"	"Cybersecurity Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	USA

Table 1. *Cont.*

#	Source	Year	Theoretical Model	Independent Variables	Dependent Variables	Technology/Service	Methodology	Participants	Country
S38	[121]	2012	Protection Motivation Theory and General Deterrence Theory	"Threat severity", "Threat vulnerability", "Self-efficacy", "Response efficacy", "Response cost", "Sanction severity", "Sanction certainty", "Agreeableness", "Conscientiousness", "Extraversion", "Neuroticism", and "Openness"	"Intention Behavior"	Not Specified	Quantitative (Survey)	Organizational employees	USA
S39	[98]	2021	Not Specified	"Human Intention and Perception", "Perceived Trust and beliefs", "Perceived e-mail security", "Perceived Privacy", and "Information Sharing"	"Usage Behavior"	E-mail	Quantitative (Survey)	Organizational employees	Japan, South Korea, India, Australia, Hong Kong, Taiwan, Singapore, New Zealand, Malaysia, Indonesia, and the Philippines

References

1. Seki, T.; Çimen, F.; Dilmaç, B. The Effect of Emotional Intelligence on Cyber Security: The Mediator Role of Mindfulness. *Bartın Univ. J. Fac. Educ.* **2023**, *12*, 190–199. [CrossRef]
2. González-Manzano, L.; de Fuentes, J.M. Design recommendations for online cybersecurity courses. *Comput. Secur.* **2019**, *80*, 238–256. [CrossRef]
3. NIST. *NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
4. Donalds, C.; Osei-Bryson, K.M. Toward a cybercrime classification ontology: A knowledge-based approach. *Comput. Hum. Behav.* **2019**, *92*, 403–418. [CrossRef]
5. NIST. *Cyber Attack—Glossary*; CSRC: Gaithersburg, MD, USA, 2012.
6. Lewis, J.A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*; Center for Strategic & International Studies: Washington, DC, USA, 2002.
7. Almomani, O.; Almaiah, M.A.; Alsaaidah, A.; Smadi, S.; Mohammad, A.H.; Althunibat, A. Machine Learning Classifiers for Network Intrusion Detection System: Comparative Study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 440–445. [CrossRef]
8. Mohammad, A.H. Intrusion Detection Using a New Hybrid Feature Selection Model. *Intell. Autom. Soft Comput.* **2021**, *30*, 65–80. [CrossRef]
9. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
10. Smadia, S.; Almomanib, O.; Mohammadc, A.; Alauthmand, M.; Saaidahe, A. VPN Encrypted Traffic classification using XGBoost. *Int. J. Emerg. Trends Eng. Res.* **2021**, *9*, 960–966.
11. Cybersecurity Education Guides. Cybersecurity Industries and Domains | Careers and Jobs. Available online: https://www.cybersecurityeducationguides.org/industries-and-domains/ (accessed on 19 March 2023).
12. Hong, Y.; Furnell, S. Understanding cybersecurity behavioral habits: Insights from situational support. *J. Inf. Secur. Appl.* **2021**, *57*, 102710. [CrossRef]
13. Reeves, A.; Calic, D.; Delfabbro, P. "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Comput. Secur.* **2021**, *106*, 102281. [CrossRef]
14. Al-Emran, M.; Griffy-Brown, C. The role of technology adoption in sustainable development: Overview, opportunities, challenges, and future research agendas. *Technol. Soc.* **2023**, *73*, 102240. [CrossRef]
15. Chowdhury, N.H.; Adam, M.T.P.; Teubner, T. Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Comput. Secur.* **2020**, *97*, 101931. [CrossRef]
16. Mashiane, T.; Kritzinger, E. Cybersecurity Behaviour: A Conceptual Taxonomy. In *Information Security Theory and Practice*; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Cham, Switzerland, 2019; Volume 11469, pp. 147–156.
17. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
18. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook*; Guilford Press: New York, NY, USA, 1983; pp. 153–176.
19. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
20. Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
21. Svabensky, V.; Vykopal, J.; Celeda, P. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE 2020, Portland, OR, USA, 11–14 March 2020; pp. 2–8. [CrossRef]
22. Fujs, D.; Mihelič, A.; Vrhovec, S.L.R. The power of interpretation: Qualitative methods in cybersecurity research. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; ACM: New York, NY, USA, 2019.
23. AlShamsi, M.; Al-Emran, M.; Shaalan, K. A Systematic Review on Blockchain Adoption. *Appl. Sci.* **2022**, *12*, 4245. [CrossRef]
24. Al-Qaysi, N.; Mohamad-Nordin, N.; Al-Emran, M. Factors Affecting the Adoption of Social Media in Higher Education: A Systematic Review of the Technology Acceptance Model. In *Recent Advances in Intelligent Systems and Smart Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 571–584.
25. Alqudah, A.A.; Al-Emran, M.; Shaalan, K. Technology Acceptance in Healthcare: A Systematic Review. *Appl. Sci.* **2021**, *11*, 10537. [CrossRef]
26. Alsharida, R.A.; Hammood, M.M.; Al-Emran, M. Mobile Learning Adoption: A Systematic Review of the Technology Acceptance Model from 2017 to 2020. *Int. J. Emerg. Technol. Learn.* **2021**, *15*, 147–162. [CrossRef]
27. Baraković, S.; Husić, J.B. The Importance of Security Matters for Quality of Experience in Mobile Web Context. *Int. J. Hum.–Comput. Interact.* **2022**, *39*, 1712–1722. [CrossRef]
28. Rahman, T.; Rohan, R.; Pal, D.; Kanthamanon, P. Human Factors in Cybersecurity: A Scoping Review. In Proceedings of the 12th International Conference on Advances in Information Technology, Bangkok, Thailand, 29 June 2021–1 July 2021; ACM: New York, NY, USA, 2021. [CrossRef]

29. Mc Mahon, C. In Defence of the Human Factor. *Front. Psychol.* **2020**, *11*, 2–5. [CrossRef]
30. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
31. Alshaikh, M. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Comput. Secur.* **2020**, *98*, 102003. [CrossRef]
32. Edkrantz, M.; Truve, S.; Said, A. Predicting Vulnerability Exploits in the Wild. In Proceedings of the 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015; pp. 513–514. [CrossRef]
33. Klimburg-Witjes, N.; Wentland, A. Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Sci. Technol. Hum. Values* **2021**, *46*, 1316–1339. [CrossRef]
34. Quayyum, F.; Cruzes, D.S.; Jaccheri, L. Cybersecurity awareness for children: A systematic literature review. *Int. J. Child-Comput. Interact.* **2021**, *30*, 100343. [CrossRef]
35. Herath, T.B.G.; Khanna, P.; Ahmed, M. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 1. [CrossRef]
36. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* **2018**, *113*, 48–52. [CrossRef]
37. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors* **2021**, *21*, 5119. [CrossRef]
38. Khan, N.F.; Yaqoob, A.; Khan, M.S.; Ikram, N. The cybersecurity behavioral research: A tertiary study. *Comput. Secur.* **2022**, *120*, 102826. [CrossRef]
39. Chowdhury, N.H.; Adam, M.T.P.; Skinner, G. The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behav. Inf. Technol.* **2019**, *38*, 1290–1308. [CrossRef]
40. Sulaiman, N.S.; Fauzi, M.A.; Wider, W.; Rajadurai, J.; Hussain, S.; Harun, S.A. Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. *Soc. Sci.* **2022**, *11*, 386. [CrossRef]
41. Jeong, J.; Mihelcic, J.; Oliver, G.; Rudolph, C. Towards an improved understanding of human factors in cybersecurity. In Proceedings of the 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; pp. 338–345. [CrossRef]
42. Hakami, M.; Alshaikh, M. Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2022**, *22*, 299–309.
43. Kalhoro, S.; Rehman, M.; Ponnusamy, V.A.P.; Shaikh, F. Extracting Key Factors of Cyber Hygiene Behaviour among Software Engineers: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 99339–99363. [CrossRef]
44. Kuppusamy, P.; Samy, G.N.; Maarop, N.; Shanmugam, B.; Perumal, S. Information Security Policy Compliance Behavior Models, Theories, and Influencing Factors: A Systematic Literature Review. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 1536–1557.
45. Alnifie, K.M.; Kim, C. Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. *J. Inf. Secur.* **2023**, *14*, 93–110. [CrossRef]
46. Chang, V.; Golightly, L.; Xu, Q.A.; Boonmee, T.; Liu, B.S. Cybersecurity for children: An investigation into the application of social media. *Enterp. Inf. Syst.* **2023**, *17*, 2188122. [CrossRef]
47. Kannelønning, K.; Katsikas, S.K. A systematic literature review of how cybersecurity-related behavior has been assessed. *Inf. Comput. Secur.* **2023**. [CrossRef]
48. Al-Saedi, K.; Al-Emran, M. A Systematic Review of Mobile Payment Studies from the Lens of the UTAUT Model. In *Recent Advances in Technology Acceptance Models and Theories*; Springer: Cham, Switzerland, 2021; Volume 335, pp. 79–106.
49. Marangunić, N.; Granić, A. Technology acceptance model: A literature review from 1986 to 2013. *Univers. Access Inf. Soc.* **2015**, *14*, 81–95. [CrossRef]
50. Fatehah, M.; Mezhuyev, V.; Al-Emran, M. A Systematic Review of Metamodelling in Software Engineering. In *Recent Advances in Intelligent Systems and Smart Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–27.
51. Al-Qaysi, N.; Granić, A.; Al-Emran, M.; Ramayah, T.; Garces, E.; Daim, T.U. Social media adoption in education: A systematic review of disciplines, applications, and influential factors. *Technol. Soc.* **2023**, *73*, 102249. [CrossRef]
52. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Software Engineering Group, School of Computer Science and Mathematics, Keele University: Newcastle, UK, 2007; pp. 1–57.
53. Costa, V.; Monteiro, S. Key knowledge management processes for innovation: A systematic literature review. *VINE J. Inf. Knowl. Manag. Syst.* **2016**, *46*, 386–410. [CrossRef]
54. Alqahtani, H.; Kavakli-Thorne, M. Does Decision-Making Style Predict Individuals' Cybersecurity Avoidance Behaviour? In *HCI for Cybersecurity, Privacy and Trust*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 12210, ISBN 9783030503086.
55. Addae, J.H.; Sun, X.; Towey, D.; Radenkovic, M. Exploring user behavioral data for adaptive cybersecurity. *User Model. User-Adapt. Interact.* **2019**, *29*, 701–750. [CrossRef]
56. Blythe, J.M.; Coventry, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Comput. Hum. Behav.* **2018**, *87*, 87–97. [CrossRef]
57. Al-Emran, M.; AlQudah, A.A.; Abbasi, G.A.; Al-Sharafi, M.A.; Iranmanesh, M. Determinants of Using AI-Based Chatbots for Knowledge Sharing: Evidence From PLS-SEM and Fuzzy Sets (fsQCA). *IEEE Trans. Eng. Manag.* **2023**. [CrossRef]

58. Gillam, A.R.; Foster, W.T. Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Comput. Hum. Behav.* **2020**, *108*, 106319. [CrossRef]
59. Young, D.; Carpenter, D.; McLeod, A. Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication. *AIS Trans. Replication Res.* **2016**, *2*, 1–17. [CrossRef]
60. Shahbaznezhad, H.; Kolini, F.; Rashidirad, M. Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *J. Comput. Inf. Syst.* **2020**, *61*, 539–550. [CrossRef]
61. Vafaei-Zadeh, A.; Thurasamy, R.; Hanifah, H. Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes* **2019**, *48*, 1565–1585. [CrossRef]
62. Al-Emran, M.; Al-Nuaimi, M.N.; Arpaci, I.; Al-Sharafi, M.A.; Anthony Jnr, B. Towards a wearable education: Understanding the determinants affecting students' adoption of wearable technologies using machine learning algorithms. *Educ. Inf. Technol.* **2022**, *28*, 2727–2746. [CrossRef]
63. Fatokun, F.B.; Hamid, S.; Norman, A.; Fatokun, J.O. The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *J. Phys. Conf. Ser.* **2019**, *1339*, 12098. [CrossRef]
64. Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int. J. Inf. Manag.* **2019**, *45*, 13–24. [CrossRef]
65. Ryle, P.; Yan, J.; Gardiner, L.R. Gramm-Leach-Bliley Gets a Systems Upgrade: What the Ftc'S Proposed Safeguards Rule Changes Mean for Small and Medium American Financial Institutions. *EDPACS* **2022**, *65*, 6–17. [CrossRef]
66. Buzan, T. Tony Buzan | Inventor of Mind Mapping.
67. Al-Qaysi, N.; Mohamad-Nordin, N.; Al-Emran, M. What leads to social learning? Students' attitudes towards using social media applications in Omani higher education. *Educ. Inf. Technol.* **2020**, *25*, 2157–2174. [CrossRef]
68. Al-Qaysi, N.; Mohamad-Nordin, N.; Al-Emran, M.; Al-Sharafi, M.A. Understanding the differences in students' attitudes towards social media use: A case study from Oman. In Proceedings of the 2019 IEEE Student Conference on Research and Development (SCOReD), Bandar Seri Iskandar, Malaysia, 15–17 October 2019; pp. 176–179.
69. Jain, A.K.; Sahoo, S.R.; Kaubiyal, J. Online social networks security and privacy: Comprehensive review and analysis. *Complex Intell. Syst.* **2021**, *7*, 2157–2177. [CrossRef]
70. Addae, J.H.; Brown, M.; Sun, X.; Towey, D.; Radenkovic, M. Measuring attitude towards personal data for adaptive cybersecurity. *Inf. Comput. Secur.* **2017**, *25*, 560–579. [CrossRef]
71. Van der Schyff, K.; Flowerday, S. Mediating effects of information security awareness. *Comput. Secur.* **2021**, *106*, 102313. [CrossRef]
72. Van Schaik, P.; Renaud, K.; Wilson, C.; Jansen, J.; Onibokun, J. Risk as affect: The affect heuristic in cybersecurity. *Comput. Secur.* **2020**, *90*, 101651. [CrossRef]
73. Varshney, G.; Misra, M.; Atrey, P. Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks. *J. Inf. Secur. Appl.* **2018**, *42*, 1–17. [CrossRef]
74. Gratian, M.; Bandi, S.; Cukier, M.; Dykstra, J.; Ginther, A. Correlating human traits and cyber security behavior intentions. *Comput. Secur.* **2018**, *73*, 345–358. [CrossRef]
75. Fischer, E.A. *Cybersecurity Issues and Challenges: In Brief*; Congressional Research Service: Washington, DC, USA, 2016.
76. Cybint 15 Alarming Cyber Security Facts and Stats. Available online: https://www.cybintsolutions.com/cyber-security-facts-stats/ (accessed on 28 October 2021).
77. Proofpoint. *An In-Depth Look at User Awareness, Vulnerability and Resilience*; Proofpoint: Sunnyvale, CA, USA, 2020.
78. Katsikeas, S.; Johnson, P.; Ekstedt, M.; Lagerström, R. Research communities in cyber security: A comprehensive literature review. *Comput. Sci. Rev.* **2021**, *42*, 100431. [CrossRef]
79. Al-Emran, M.; Granić, A.; Al-Sharafi, M.A.; Ameen, N.; Sarrab, M. Examining the roles of students' beliefs and security concerns for using smartwatches in higher education. *J. Enterp. Inf. Manag.* **2021**, *34*, 1229–1251. [CrossRef]
80. Simonet, J.; Teufel, S. The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. *IFIP Adv. Inf. Commun. Technol.* **2019**, *562*, 194–208. [CrossRef]
81. Ameen, N.; Tarhini, A.; Shah, M.H.; Madichie, N.; Paul, J.; Choudrie, J. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Comput. Hum. Behav.* **2021**, *114*, 106531. [CrossRef]
82. Ameen, N.; Tarhini, A.; Shah, M.H.; Madichie, N.O.; Hussain Shah, M.; Madichie, N.O. Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Comput. Hum. Behav.* **2020**, *104*, 106184. [CrossRef]
83. Gillam, A.R.; Waite, A.M. Gender differences in predictors of technology threat avoidance. *Inf. Comput. Secur.* **2021**, *29*, 393–412. [CrossRef]
84. Anwar, M.; We, H.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender Difference and Employees' Cybersecurity Behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
85. Alsharida, R.A.; Al-rimy, B.A.S.; Al-Emran, M.; Zainal, A. A systematic review of multi perspectives on human cybersecurity behavior. *Technol. Soc.* **2023**, *73*, 102258. [CrossRef]
86. Alshaikh, M.; Adamson, B. From awareness to influence: Toward a model for improving employees' security behaviour. *Pers. Ubiquitous Comput.* **2021**, *25*, 829–841. [CrossRef]
87. Bansal, G.; Muzatko, S.; Shin, S. Il Information system security policy noncompliance: The role of situation-specific ethical orientation. *Inf. Technol. People* **2021**, *34*, 250–296. [CrossRef]

88. Li, Y.; Pan, T.; Zhang, N. From hindrance to challenge: How employees understand and respond to information security policies. *J. Enterp. Inf. Manag.* **2020**, *33*, 191–213. [CrossRef]
89. Alqahtani, H.; Kavakli-Thorne, M.; Alrowaily, M. The Impact of Gamification Factor in the Acceptance of Cybersecurity Awareness Augmented Reality Game (Cybar). In *HCI for Cybersecurity, Privacy and Trust*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 12210, ISBN 9783030503086.
90. Abroshan, H.; Devos, J.; Poels, G.; Laermans, E. Phishing Happens beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* **2021**, *9*, 44928–44949. [CrossRef]
91. Xu, Z.; Guo, K. It ain't my business: A coping perspective on employee effortful security behavior. *J. Enterp. Inf. Manag.* **2019**, *32*, 824–842. [CrossRef]
92. Verkijika, S.F. Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. In Proceedings of the 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Kimberley, South Africa, 25–27 November 2020. [CrossRef]
93. Jeske, D.; van Schaik, P. Familiarity with Internet threats: Beyond awareness. *Comput. Secur.* **2017**, *66*, 129–141. [CrossRef]
94. Verkijika, S.F. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Comput. Hum. Behav.* **2019**, *101*, 286–296. [CrossRef]
95. Packetlabs Cybersecurity Statistics for 2021. Available online: https://www.packetlabs.net/cybersecurity-statistics-2021/ (accessed on 29 October 2021).
96. ACSC. ACSC Annual Cyber Threat Report 2020–21. Available online: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (accessed on 29 October 2021).
97. Chou, H.L.; Chou, C. A quantitative analysis of factors related to Taiwan teenagers' smartphone addiction tendency using a random sample of parent-child dyads. *Comput. Hum. Behav.* **2019**, *99*, 335–344. [CrossRef]
98. Sivarethinamohan, R.; Sujatha, S. Behavioral Intentions towards adoption of Information Protection and Cyber security (Email Security and Online Privacy): SEM model. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 56–68. [CrossRef]
99. Donalds, C.; Osei-Bryson, K.M. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *Int. J. Inf. Manag.* **2020**, *51*, 102056. [CrossRef]
100. Liu, C.; Liang, H.; Wang, N.; Xue, Y. Ensuring employees' information security policy compliance by carrot and stick: The moderating roles of organizational commitment and gender. *Inf. Technol. People* **2021**, *35*, 802–834. [CrossRef]
101. Reeves, A.; Parsons, K.; Calic, D. Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness? In Proceedings of the International Conference on Human-Computer Interaction, Copenhagen, Denmark, 19–24 July 2020; Springer: Cham, Switzerland, 2020; pp. 232–249.
102. Sun, H.; Zhang, P. The role of moderating factors in user technology acceptance. *Int. J. Hum. Comput. Stud.* **2006**, *64*, 53–78. [CrossRef]
103. Arpaci, I.; Huang, S.; Al-Emran, M.; Al-Kabi, M.N.; Peng, M. Predicting the COVID-19 infection with fourteen clinical features using machine learning classification algorithms. *Multimed. Tools Appl.* **2021**, *80*, 11943–11957. [CrossRef]
104. Zaza, S.; Al-Emran, M. Mining and exploration of credit cards data in UAE. In Proceedings of the 2015 5th International Conference on e-Learning, ECONF 2015, Manama, Bahrain, 18–20 October 2015; IEEE: New York, NY, USA, 2015; pp. 275–279.
105. Mijwil, M.M.; Salem, I.E.; Ismaeel, M.M. The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. *Iraqi J. Comput. Sci. Math.* **2023**, *4*, 87–101. [CrossRef]
106. Pattnaik, N.; Li, S.; Nurse, J.R.C. Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. *Comput. Secur.* **2023**, *125*, 103008. [CrossRef]
107. Liu, B.; Wei, L. Unintended effects of open data policy in online behavioral research: An experimental investigation of participants' privacy concerns and research validity. *Comput. Hum. Behav.* **2023**, *139*, 107537. [CrossRef]
108. Lin, W.; Xu, M.; He, J.; Zhang, W. Privacy, security and resilience in mobile healthcare applications. *Enterp. Inf. Syst.* **2023**, *17*, 1–15. [CrossRef]
109. Huang, Y.; Li, Y.J.; Cai, Z. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Min. Anal.* **2023**, *6*, 234–247. [CrossRef]
110. Koohang, A.; Nord, J.; Ooi, K.; Tan, G.; Al-Emran, M.; Aw, E.; Baabdullah, A.; Buhalis, D.; Cham, T.; Dennis, C.; et al. Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation. *J. Comput. Inf. Syst.* **2023**, *63*, 735–765. [CrossRef]
111. Hong, W.C.H.; Chi, C.Y.; Liu, J.; Zhang, Y.F.; Lei, V.N.L.; Xu, X.S. The Influence of Social Education Level on Cybersecurity Awareness and Behaviour: A Comparative Study of University Students and Working Graduates. *Educ. Inf. Technol.* **2023**, *28*, 439–470. [CrossRef]
112. Limna, P.; Siripipattanakul, S. The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *Int. J. Comput. Sci. Res.* **2022**, *7*, 1–19. [CrossRef]
113. Rohan, R.; Pal, D.; Hautamäki, J.; Funilkul, S.; Chutimaskul, W.; Thapliyal, H. A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon* **2023**, *9*, e14234. [CrossRef]
114. Ahmad, Z.; Ong, T.S.; Liew, T.H.; Norhashim, M. Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Inf. Comput. Secur.* **2019**, *27*, 165–188. [CrossRef]

115. Vafaei-Zadeh, A.; Ramayah, T.; Wong, W.P.; Md Hanifah, H. Modelling internet security software usage among undergraduate students: A necessity in an increasingly networked world. *VINE J. Inf. Knowl. Manag. Syst.* **2018**, *48*, 2–20. [CrossRef]
116. Kianpour, M.; Øverby, H.; Kowalski, S.J.; Frantz, C. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In *HCI for Cybersecurity, Privacy and Trust*; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2019; Volume 11594, pp. 149–163. [CrossRef]
117. Aigbefo, Q.A.; Blount, Y.; Marrone, M. The influence of hardiness and habit on security behaviour intention. *Behav. Inf. Technol.* **2020**, *41*, 1151–1170. [CrossRef]
118. Li, L.; He, W.; Xu, L.; Ivan, A.; Anwar, M.; Yuan, X. Does explicit information security policy affect employees' cyber security behavior? A pilot study. In Proceedings of the 2nd International Conference on Enterprise Systems, Shanghai, China, 2–3 August 2014; pp. 169–173. [CrossRef]
119. Anwar, M.; He, W.; Yuan, X. Employment status and cybersecurity behaviors. In Proceedings of the 2016 International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC), Durham, NC, USA, 11–13 November 2016; IEEE: New York, NY, USA, 2016; pp. 1–2.
120. Alghamdi, M.I. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Mater. Today Proc.* **2021**. [CrossRef]
121. McBride, M.; Carter, L.; Warkentin, M. *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies*; RTI International: Research Triangle Park, NC, USA, 2012; ISBN 3312021278.