Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness

***Musaddag Elrayah*[1]**
King Faisal University, Saudi Arabia.

***Saima Jamil*[2]**
Virtual University of Pakistan, Pakistan

Abstract

Purpose: This study investigates the impact of digital literacy, citizenship, curation practices, connectedness, and online privacy concerns on cybersecurity behaviour. It specifically examines the moderating role of cybersecurity awareness in these factors. The objective is to examine the relationship between these elements and individuals' cybersecurity behaviours, offering valuable insights to guide training programmes and interventions. Methodology: A survey was conducted on a sample of 235 individuals living in different cities in Saudi Arabia to collect data. Confirmatory factor analysis was used to assess the measuring scales, while regression analysis was employed to analyse the relationships between the variables under investigation. Additionally, a moderation test was performed to evaluate the influence of cybersecurity awareness on the associations between predictor variables and cybersecurity behaviour. Findings: The regression analysis reveals significant correlations between digital literacy (specifically copyright, citizenship, curation, and connectedness), online privacy concerns, and cybersecurity behaviour. The understanding of cybersecurity significantly influenced the level and trajectory of these relationships. A deeper comprehension of cybersecurity enhances the positive effects of digital literacy, including copyright awareness, responsible citizenship, content curation, and connectedness, on cybersecurity behaviour. Implications: This study highlights the importance of tailored educational efforts that consider individuals' levels of expertise and specific concerns. Organisations and governments can utilise these findings to create customised cybersecurity training programmes, improve digital literacy, and tackle issues related to online privacy. The report highlights the significance of integrating cybersecurity knowledge into wider digital literacy initiatives. Originality/Novelty: To the best of the

[1] Department of Management, School of Business, King Faisal University, Al-Ahsa 31982, Saudi Arabia. Email: melrayah@kfu.edu.sa
[2] Department of Computer Sciences, Virtual University of Pakistan, Peshawar Campus. Pakistan. Email: saima.jamil@vu.edu.pk

researcher's knowledge, previous studies have not examined the relationship between these variables. This study contributes to current knowledge by investigating the combined influence of digital literacy, citizenship, curation practices, connectedness, and online privacy concerns on cybersecurity behaviour. Furthermore, this study examines the potential moderating impact of cybersecurity awareness.

Keywords: Copyright, Citizenship, Curation, Connectedness, Online Privacy Concerns, Cybersecurity Awareness and Cybersecurity Behaviour.

1. Introduction

Digital literacy refers to the capacity to effectively search, organise, analyse, evaluate, and generate data. Proficiency in the digital realm and technical expertise are necessary. Digital literacy encompasses various essential skills for navigating the digital realm. Technical competency is crucial, encompassing proficiency and familiarity with diverse computer software, hardware, and Internet applications. Proficiency in digital tools and platforms enables individuals to enhance their overall digital skills by utilising them efficiently and effectively. Proficiency in cybersecurity is crucial for formulating effective strategies in this domain. Lee and Chua (2023) found that gender, income, education level, and information and communication technology are influential factors in determining cybersecurity awareness. According to Simonet and Teufel (2019), the key factors in domestic cybersecurity awareness and behaviour are human initiative and understanding of information systems. Information literacy is an essential aspect of digital literacy, in addition to technological proficiency.

It is crucial to thoroughly evaluate and investigate digital data to determine its credibility and validity. Enhancing media literacy can cultivate a discerning approach to information consumption, enabling individuals to navigate the media-rich digital landscape more effectively. Alfalah (2023) found that awareness of Internet security affects the relationship between individuals' perceptions of cyber security and their attitudes towards using a learning management system. Lee and Chua (2023) highlighted the significance of cybersecurity knowledge and awareness in shaping individuals' cybersecurity intentions and behaviours. Key predictors encompass factors associated with information and communications technology, education, income, and gender. Quayyum (2023) emphasised the importance of parental involvement in cybersecurity education, particularly in the early stages of children's development. Also, AlSobeh et al. (2023) highlights the importance of establishing national cybersecurity initiatives in Jordan to improve teenagers' understanding of cybersecurity. This is particularly important given the impact of the cyberscale and individual factors. The rise in online activities in the contemporary digital environment has resulted in heightened concerns regarding cybersecurity. Digital literacy and privacy concerns impact individuals' behaviours in the digital environment.

This study aims to investigate the impact of digital literacy scales, including Copyright Citizenship, Curation, and Connectedness, on cybersecurity behaviour and online privacy concerns. Furthermore, this study aims to examine the impact of

cybersecurity knowledge on the correlations. Sindermann et al. (2021) examined the impact of crystallised intelligence and personality factors on individuals' online privacy literacy and behaviour. The results indicated a positive correlation between these factors and the implementation of data protection measures. Trepte et al. (2015) created the Online Privacy Literacy Scale (OPLIS) to assess individuals' knowledge of organisational protocols, technical elements, legal factors, and user strategies related to privacy management.

Similarly, Epstein and Quinn (2020) identifies a digital divide in privacy literacy that is shaped by traditional socio-economic factors and their impact on privacy-related behaviours. Promoting diversity, offering tools to address information overload, emphasising the importance of cybersecurity measures, and prioritising skill development are crucial for addressing challenges and enhancing digital literacy programmes. Establishing an inclusive, knowledgeable, and safe digital environment necessitates overcoming multiple challenges. Prior research has predominantly overlooked the potential moderating influence of cybersecurity awareness. Instead, it has primarily focused on examining the direct associations between digital literacy and different dimensions of cybersecurity behaviour. The issue lies in the insufficient examination of how consciousness governs or impacts these relationships.

The existing literature may have insufficient information regarding the specific effects of different aspects of digital literacy, such as Copyright, Citizenship, and Curation, on cybersecurity behaviour. Gaining a thorough understanding of the specific impact of each factor can aid in the development of targeted interventions and educational initiatives. Additionally, there is a lack of research examining the contextual factors that could influence the relationship between digital literacy and cybersecurity behaviour. These factors include cultural, educational, and organisational elements that may moderate the observed associations. Therefore, this study aims to examine the impact of various dimensions of digital literacy, including copyright knowledge, citizenship curation, connectedness, and online privacy concerns, on individuals' cyber security behaviour. This study also examines the moderating effect of cybersecurity awareness.

2. Literature Review and Hypothesis Development

2.1 Digital Literacy and Cybersecurity Behaviour

Digital literacy encompasses the proficient and ethical utilisation of digital technologies, and it significantly influences users' comprehension of cybersecurity issues. Gaining digital skills enables individuals to navigate specialised online platforms. Numerous studies have consistently demonstrated a positive correlation between high levels of digital literacy and safe online behaviour (Belanger & Crossler, 2011). To enhance security, it is necessary to employ robust and distinct passwords, regularly update software to mitigate vulnerabilities, and exercise caution when encountering potentially harmful links and information. This paper provides an overview of the various components of digital literacy and outlines the necessary measures for ensuring cybersecurity.

2.2 Copyright and Cybersecurity Behaviour

An individual's cybersecurity practices are influenced by their level of digital literacy, which encompasses various skills for proficiently utilising and manipulating digital technologies. Understanding and adhering to copyright laws that regulate the lawful utilisation and dissemination of digital content is a crucial aspect of digital literacy, particularly in relation to cybersecurity practices. Improving one's digital skills enhances their comprehension of copyright implications in online activities. The users acknowledge the cybersecurity risks linked to copyright infringement and emphasise the significance of honouring intellectual property rights and complying with copyright restrictions while dealing with digital content.

Gibson and Smith (2018) found that knowledge of copyright law is integral to digital literacy and promotes responsible internet usage. Their research demonstrates a positive correlation between individuals' comprehension of digital concepts, such as copyright, and the likelihood of adopting safe online practices. Zhu et al. (2021) found a strong correlation between knowledge of copyright regulations and precautions in acquiring and sharing digital content, which is relevant to cybersecurity. It is important to consider the influence of general cybersecurity awareness when examining the relationship between digital skills, copyright awareness, and cybersecurity behaviour. Sharma et al. (2022) pointed out that cyber security awareness and digital literacy have a synergistic impact, leading individuals to adopt proactive cybersecurity measures and influencing their online behaviour. Corallo et al. (2022) explained that individuals with knowledge of cybersecurity demonstrate a higher propensity to adhere to copyright regulations in safeguarding sensitive online information.

A solid grasp of copyright law, a crucial aspect of digital literacy, enhances responsible behaviour in cybersecurity. A comprehensive comprehension of cybersecurity matters enhances this association. The results emphasise the necessity of inclusive digital literacy initiatives that integrate copyright education and general cybersecurity awareness to promote online safety.

H1: *Copyright positively influences cybersecurity behaviour.*

2.3 Citizenship and Cybersecurity Behaviour

Digital literacy encompasses the crucial aspect of engaging in digital citizenship, which entails the responsible and ethical utilisation of technology. Understanding one's role and responsibilities as a participant in an online community extends beyond basic self-awareness. Digital citizenship is a crucial concept in cybersecurity, as it plays a significant role in influencing individuals' behaviour to create a secure and trustworthy online environment. Emphasises the importance of ethical conduct and responsible utilisation of digital resources in the online environment. Practitioners of good digital citizenship recognise the collective responsibility for cybersecurity and endeavour to enhance internet safety by advocating for secure practices among users.

Ribble and Park (2022) explained that digital citizenship and ethical behaviour online may correlate with each other. Individuals with a strong understanding of digital citizenship are more inclined to adopt measures that ensure their own and others' online safety. Livingstone and Blum-Ross (2020) emphasised the significance

of digital citizenship in promoting responsible internet use. The authors posited that individuals with a digital citizen mindset are more inclined to identify cybersecurity risks and proactively address them. Being a responsible digital citizen entails actively engaging in online communities and contributing knowledge to others. Data transfer safeguards prove essential for individuals who prioritise digital citizenship. It is important to exercise caution when sharing personal information online and to promote the same behaviour among individuals with whom you interact online. Ribble and Bailey (2015) found that individuals who exhibit responsible digital citizenship are at a reduced risk of falling prey to cybercrime due to their cautious approach towards online information sharing. Individuals with a higher level of digital citizenship comprehension are more inclined to participate in secure online collaboration, such as exchanging information on methods to enhance cybersecurity (Sá et al., 2021).

Digital citizenship programmes emphasise responsible online behaviour and are commonly integrated into educational initiatives. Engaging in these programmes increases individuals' awareness of cybersecurity and encourages them to prioritise it. Consequently, participants are more inclined to adopt safe online practices. Ohler (2011) examines the relationship between education, the formation of digital citizenship, and its influence on cybersecurity. Educational strategies that prioritise the importance of digital citizenship can promote cyber awareness and responsible thinking. Individuals with a comprehensive comprehension of digital citizenship are more inclined to embrace and implement cybersecurity best practices. Active participation in the establishment of a secure digital society is imperative, necessitating information sharing, collaboration, and responsible utilisation of digital resources.

H2: *Citizenship positively influences cybersecurity behaviour.*

2.4 Curation and Cybersecurity Behaviour

In the domain of digital literacy, curation encompasses the adept selection, organisation, and administration of digital resources. This significantly influences individuals' cybersecurity behaviours and their utilisation of digital information. Effective curators possess expertise in evaluating digital content, enabling them to make informed decisions and discern between reliable sources and sources that may pose risks to users. Individuals proficient in curation often prioritise the utilisation of reputable sources and exercise caution when encountering unfamiliar or dubious digital content, thereby enhancing their online safety. Bawden (2001) emphasise the significance of curation in the digital era and its influence on information activities. They argue that digital content curators possess expertise in cybersecurity risks and exercise selectivity in managing information. They are more inclined to possess consumer expertise.

Effective curation involves the responsible management of sensitive data. Experienced curators possess knowledge of users' privacy settings, comprehend the potential consequences of revealing personal information, and actively regulate access to sensitive materials. These tactics are effective for organising and safeguarding your online presence. Van Dijck (2014) discovered that people's ability to curate personal data affects their privacy practices in the digital age. Individuals

proficient in curation tend to exhibit a higher propensity for implementing measures aimed at safeguarding their personal information. Bottoni et al. (2020) found that individuals who actively participate in the selection of their online content are more inclined to adopt privacy measures. The organisation of personal information has a direct influence on the implementation of cybersecurity measures.

Digital environment users are more inclined to utilise tools and techniques that enhance their online security, such as: To ensure the security of your digital devices, it is essential to employ reliable security software, regularly update passwords, and take proactive measures. van Leersum et al. (2022) highlighted that individuals who possess a strong comprehension of and adherence to cybersecurity best practices demonstrate enhanced curation skills. In conclusion, individuals with strong curation skills tend to display greater proactive cybersecurity behaviours. This entails implementing proactive security measures to safeguard one's online presence, making well-informed choices regarding the digital information one engages with, and appropriately managing personal data.

H3: *Curation positively influences cybersecurity behaviour.*

2.5 Connectedness and Cybersecurity Behaviour

Connectedness in digital literacy refers to the capacity to establish and sustain significant relationships within digital settings. This entails understanding the interplay between individuals, technology, and online platforms. The interdependence among individuals in cyberspace enhances the likelihood of mutual assistance through the sharing of tips and warnings regarding potential threats. Online communities provide information and support that enhance individuals' sense of belonging, thereby promoting the adoption of safe behaviours (Payne, Cross, & Vandecar-Burdin, 2022). According to Sarker et al. (2019), individuals who actively participate in online communities demonstrate a greater awareness of the significance of cybersecurity and exhibit a higher tendency to adopt protective measures.

Individuals who perceive themselves as members of a broader online community are inclined to exhibit greater cooperation towards cybersecurity initiatives. Connectivity is crucial due to its significance. This encompasses the dissemination of information regarding emerging threats, collaborative efforts in combating cybercrime, and the promotion of enhanced cybersecurity standards. Ertz, Lecompte, and Durif (2017) found that individuals who experience a sense of connection are more inclined to collaborate in efforts to enhance cybersecurity on a collective level. This particularly applies to individuals who experience a sense of online community.

Connectivity greatly enhances the efficacy of cybersecurity decision-making. Individuals who maintain a constant online presence derive advantages from the availability of diverse perspectives, ideas, and data pertaining to emerging cybersecurity risks. This extensive knowledge base enables users to make informed decisions regarding their online activities, leading to safer behaviour. Livingstone and Blum-Ross (2020) found that individuals who are well-connected actively search for and exchange information regarding cybersecurity best practices. This tool facilitates improved decision-making in the online realm. According to Sulaiman et al. (2022), individuals who have a strong sense of connection tend to prioritise online security

when making decisions. Digital networks have an impact on the collective knowledge and opinions exchanged within them. Connection positively impacts cybersecurity behaviour through increased community knowledge, enhanced collaborative security measures, and improved decision-making. As the digital sphere experiences exponential growth, the likelihood of attracting and retaining users in virtual spaces increases when they are safe and welcoming.

H4: *Connectedness positively influences cybersecurity behaviour.*

3. Online Privacy Concerns and Cybersecurity Behaviour

Individuals' attitudes towards internet privacy significantly influence their behaviours in relation to cybersecurity. Anxious individuals tend to be cautious when it comes to disclosing personal information (Chau, 1996). Individuals demonstrate vigilance in various ways, including actively managing privacy settings, employing encryption techniques to safeguard communications, and exercising caution when sharing personal information on social media platforms. The correlation between an individual's concern for online privacy and their inclination to adopt cybersecurity measures demonstrates the interconnection between personal privacy perspectives and proactive actions against cyber threats. Privacy concerns greatly influence individuals' online behaviour and actions, particularly in the realm of cybersecurity.

To comprehend the factors that impact cybersecurity activities, it is imperative to grasp these concerns. This study aims to examine the relationship between cybersecurity awareness and the connection between digital literacy levels and online privacy concerns. Multiple studies have identified notable privacy concerns within the realm of cybersecurity. Hamid et al. (2020) and Basahel and Yamin (2020) emphasise the challenges associated with safeguarding user privacy and security in social media and the Internet of Things (IoT), respectively. Toch et al. (2018) categorises privacy issues by identifying potential infringements on privacy resulting from cybersecurity technology. Aziz, Siraj, and Rehman (2021) examines the issue of privacy concerns within the context of cybercrime in the field of digital forensics. The author proposes the use of a classification matrix and a control system as potential remedies to address these concerns.

Similarly, Riebe et al. (2023) suggests that the perceived significance of Open-Source Intelligence (OSINT) adoption is closely tied to the perception of cyber risks. Privacy concerns were found to have a negative association. This highlights the importance of transparency and accuracy in open-source intelligence (OSINT) systems. In the same vein, Ali et al. (2023) suggested implementing a consortium blockchain strategy to safeguard sensitive data in cyber-physical systems, particularly emphasising the resolution of privacy concerns. Kim (2023) identified privacy concerns in the PACMAN authentication system utilised in cybertown-based 6G networking, emphasising the critical requirement for strong security prerequisites. Huo and Liu (2021) proposed a method that combines encryption, decentralisation, and multi-agent optimisation to safeguard privacy in cyber-physical systems. The methodology was found to be highly effective in ensuring participant confidentiality.

H5: *Online Privacy Concerns positively influence Cybersecurity Behaviour.*

4. Moderating Role of Cybersecurity Awareness

Promoting understanding of cyber threats and fostering a commitment to secure online practices are crucial for strengthening cybersecurity awareness. Awareness programmes improve users' decision-making abilities by providing knowledge on common cyber threats, the importance of strong passwords, recognising phishing attempts, and promoting effective security measures. Heightened cybersecurity awareness plays a crucial role in strengthening the link between digital literacy, concerns about online privacy, and the translation of information into tangible cybersecurity measures. Digital literacy, online privacy concerns, and cybersecurity awareness are interconnected factors that collectively shape an individual's cybersecurity stance. The interaction of these elements emphasises the significance of a comprehensive strategy for cybersecurity education and promotion in cultivating a more secure digital environment.

Studies on cyber security awareness, knowledge, and behaviour indicate that while many internet users are aware of cyber threats, they frequently fail to implement appropriate preventive measures (Klein, Zwilling, & Lesjak, 2022; Zwilling et al., 2022). This is especially relevant for students who may feel insecure online and lack the necessary knowledge to protect themselves (Kovačević, Putnik, & Tošković, 2020). Cybersecurity awareness may undermine the link between knowledge of cyber threats and the adoption of protective behaviours, particularly when the information is limited to IT security courses (Klein et al., 2022). According to Alfalah (2023), internet security knowledge influences the connection between various factors related to perceptions of cyber security and attitudes towards using a learning management system. These findings indicate that increased awareness of Internet security can result in a more positive attitude towards cyber security. Almansoori, Al-Emran, and Shaalan (2023) emphasised the significance of cybersecurity conduct, particularly the protection incentive theory. This theory proposes that individuals are more likely to engage in cyber-secure behaviour when they possess awareness of potential risks and are motivated to protect themselves. Huraj et al. (2023) conducted a study on cyber security awareness among computer science and media studies students. The study revealed both similarities and differences in their perspectives.

The study's key findings include the factors strongly associated with cybercrime victimisation, the heightened vulnerability of women to cybercrime, and the perspectives of the industrial sector on cybercrime. The study reveals a deficiency in cybersecurity awareness among TVTC trainees. It highlights the necessity for enhanced awareness and training initiatives, as well as the importance of enhancing decision-making skills in privacy and security matters. The study primarily focuses on three key aspects: understanding internet usage patterns and purposes, evaluating college students' familiarity with cybersecurity awareness and countermeasures, and providing recommendations to mitigate cybercrime in the future. The paper presents additional findings, including a systematic review of 55 research papers that evaluate the privacy and security risks associated with smartphone sensors. It also includes a survey of 23 human end-users through questionnaires, which reveals different levels of familiarity with smartphone sensors and a lack of awareness regarding potential threats and preventive measures. These findings have the potential to contribute to the development of effective solutions for addressing security and privacy concerns. According to Malandrino, Scarano,

and Spinelli (2013), increased awareness is associated with a greater tendency for cautious online behaviour, particularly among individuals with limited ICT expertise. Bubaš, Orehovački, and Konecki (2008) identified conscientiousness and risk engagement as significant indicators of online security and privacy behaviours. Mamonov and Benbunan-Fich (2018) demonstrated that exposure to information security threats can lead individuals to take automatic defensive measures, such as limiting the dissemination of personal information and using stronger passwords.

H6: *Cyber security Awareness moderates the relationship between Copyright of digital literacy scale and Cyber security Behaviour.*
H7: *Cyber security Awareness moderates the relationship between Citizenship of digital literacy scale and Cyber security Behaviour.*
H8: *Cyber security Awareness moderates the relationship between Curation of digital literacy scale and Cyber security Behaviour.*
H9: *Cyber security Awareness moderates the relationship between Connectedness of digital literacy scale and Cyber security Behaviour.*
H10: *Cyber security Awareness moderates the relationship between Online Privacy Concerns of digital literacy scale and Cyber security Behaviour.*

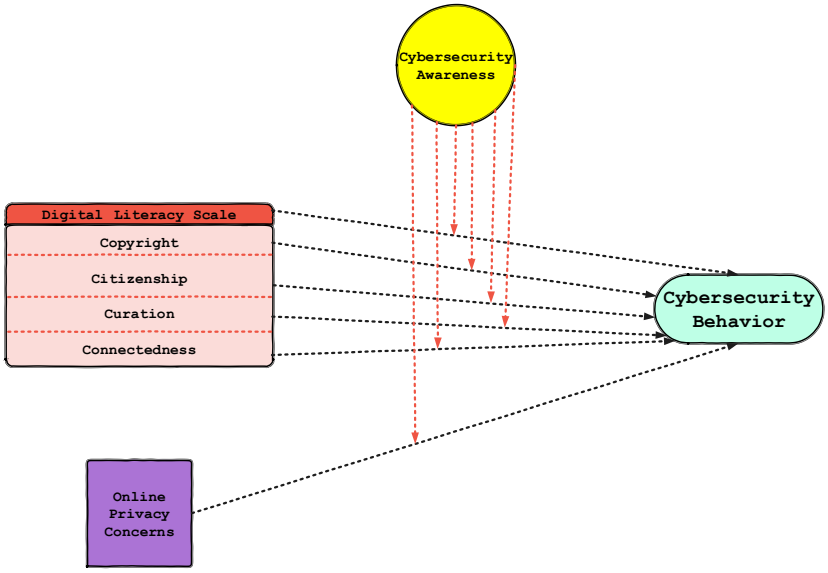

Figure 1: Proposed Framework.

5. Methodology and Sample and Data Collection

This study aims to examine the impact of digital literacy and online privacy concerns on cybersecurity behaviour, taking into consideration the moderating influence of cybersecurity awareness. The study collected data from a sample of 235 individuals residing in different cities in Saudi Arabia. Examining the sample's demographics, education levels, and professional backgrounds can offer further insights into the generalizability of the findings. This study examines the digital literacy, online privacy concerns, cybersecurity behaviour, and awareness of Saudi citizens, considering the potential influence of regional or cultural factors. The primary independent factors in this study are digital literacy and online privacy

concerns, while the dependent variable is cybersecurity behaviour. Cybersecurity knowledge is included as a moderating variable. The study is expected to employ statistical analysis techniques such as regression analysis or structural equation modelling to examine the relationships between variables and explore the moderating effect of cybersecurity knowledge. It is important to acknowledge any limitations of the study, such as potential sample bias, reliance on self-reported data, or other factors that may impact the generalizability of the findings.

Table 1: Descriptive Statistics.

Variable	Mean	SD	Cronbach's alpha	1	2	3	4	5	6
Copyright	3.11	0.54	0.77	0.21**					
Citizenship	3.64	0.48	0.71	0.38*	0.49*				
Curation	2.98	0.56	0.69	0.46	0.58	0.61*			
Connectedness	3.68	0.66	0.74	-0.53	0.42**	0.54	0.47		
Online Privacy Concerns	3.01	0.60	0.80	0.44*	-0.50	0.33**	-0.36**	0.46	
Cybersecurity Awareness	3.54	0.57	0.86	0.67	0.27**	0.29**	0.69	0.52	0.19*
Cybersecurity Behaviour	3.78	0.49	0.74	0.40*	-0.41*	0.34**	0.55	-0.18**	-0.51

** Correlation is significant at the 0.01 level (2 tailed)
* Correlation is significant at the 0.05 level (2 tailed)

6. Confirmatory Factor Analysis

Table 2 presents the outcomes of a confirmatory factor analysis (CFA) conducted on the questionnaire data. The table includes the Kaiser-Meyer-Olkin (KMO) statistics for each variable as well as the percentage of variation that each factor accounts for. The Explained column and the Variance Percentage indicate the proportion of variability in each variable that can be attributed to the underlying factors. The identified components explain a substantial amount of the variability in Copyright Citizenship, as evidenced by the CFA's explanation of 28.34% and 48.64% of the variance in this concept. Curation demonstrates significant explanatory power, accounting for 53.64% of the variance. Online privacy and connectivity concerns explain 39.55% and 44.50% of the variance, respectively.

In contrast, the KMO statistics provide an assessment of the adequacy of the factor analysis sampling. Factor analysis can be conducted on variables with a KMO value approaching 1.0. The factors of copyright citizenship, curation, connectedness, and online privacy concerns were measured with respective scores of 0.54, 0.61, 0.62, and 0.48. The KMO scores indicate that the sample adequacy in this case is moderate to acceptable. While KMO levels above 0.5 are generally deemed acceptable, researchers often strive for values of 0.7 or higher to ensure a more robust factor analysis.

In conclusion, the confirmatory factor analysis results indicate that the identified factors (Curation, Connectedness, Copyright Citizenship, and Online Privacy Concerns) explain a significant amount of the variability in their

respective variables. The measurement model used in the study seems valid, as indicated by the moderate KMO values. These values suggest that the variables are reasonably suitable for factor analysis. To improve the explanatory capacity of the analysis, scientists may consider augmenting the model or exploring alternative components.

Table 2: Results of Confirmatory Factor Analysis of Questionnaire Data.

	% of Variance	KMO Statistics
Copyright	28.34	0.54
Citizenship	48.64	0.48
Curation	53.64	0.61
Connectedness	44.50	0.62
Online Privacy Concerns	39.55	0.48

7. Regression Results

Table 3 presents the results of a regression analysis involving the variables of online privacy concerns, connectedness, citizenship, copyright, curation, and cybersecurity behaviour.

Interpretation of regression findings:

• Beta Standardised Coefficients:

• Cybersecurity activity is dramatically reduced by copyright (Beta = -0.269, $p < 0.05$). Reduced cybersecurity conduct may result from more copyright.

Research findings indicate a significant positive relationship between individuals' strong belief in their citizenship rights and their adherence to cybersecurity practices ($\beta = 0.354$, $p < 0.01$). The study found a positive relationship between curation and improved cybersecurity behaviour (Beta = 0.297, $p < 0.05$), suggesting that content curators may have more robust cybersecurity policies. Research findings indicate that individuals who experience a stronger sense of online connectedness are more likely to adopt positive cybersecurity practices. This relationship is statistically significant (beta = 0.314, $p < 0.01$). Research findings indicate a positive correlation between individuals who prioritise their online privacy and their likelihood to adopt effective cybersecurity practices (Beta = 0.211, $p < 0.05$). The R-squared (R2) and Adjusted R-squared values were calculated to assess the explanatory power of the independent variables on cybersecurity behaviour. The obtained R2 value of 0.348 indicates that the independent variables account for approximately 34.8% of the variance in cybersecurity behaviour. The adjusted R2 value (0.301) provides a more accurate representation of the model's explanatory capacity due to its adjustment for the number of predictors.

• The regression model fits the data well, as evidenced by the F-statistic of 21.64 ($p < 0.01$), which shows that at least one predictor significantly affects the dependent variable.

The regression analysis results indicate that copyright, citizenship, curation, connectedness, and online privacy concerns are significant factors in explaining cybersecurity behaviour. The findings indicate that cybersecurity behaviours can be predicted by factors such as citizenship, curation, connection, and concerns related to online privacy.

Table 3: Regression Results.

	Standardized Coefficients Beta	R2	Adjusted R2	F
Copyright	-0.269*	0.348	0.301	21.64**
Citizenship	0.354**			
Curation	0.297*			
Connectedness	0.314**			
Online Privacy Concerns	0.211**			

a. Dependent Variable: Cyber Security Behaviour

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4: Results of Hypothesis Testing.

Hypothesis	P-Value	Testing Result
Copyright	0.064	Rejected
Citizenship	0.021	Supported
Curation	0.001	Supported
Connectedness	0.016	Supported
Online Privacy Concerns	0.000	Supported

8. Examining Moderation

Table 5 investigates the impact of Cybersecurity Awareness on the association between Copyright, Citizenship, Curation, Connectedness, Online Privacy Concerns, and Cybersecurity Behaviour.

• *Moderation Coefficients*

Cybersecurity Awareness (Coefficient = 0.314, p 0.01) moderates copyright and cybersecurity behaviour.

• At the 0.05 level, the moderation coefficient for citizenship is 0.268, which is statistically significant.

• At the 0.05 level, Curation's moderation coefficient of -0.288 is statistically significant.

• At the 0.01 level of significance, the connection moderation coefficient is 0.260.

• At the 0.01 level of significance, concerns regarding online privacy have a moderation coefficient of 0.347.

• Adjusted R-squared and R-squared (R2):

• With an R2 score of 0.301, the model can account for roughly 30.1% of the variation in cybersecurity behaviour. With the number of predictors taken into consideration, the adjusted R2 (0.291) provides a more cautious evaluation of the explanatory power of the model.

• *F-statistic*

• At least one interaction term significantly affects the dependent variable, and the entire regression model fits the data well, as shown by the statistically significant (p 0.01) F-statistic of 8.97.

The relationship between independent variables and cybersecurity behaviour is influenced by the levels of cybersecurity awareness, as reflected by the moderation coefficients for each variable. The positive and significant coefficient for copyright suggests a positive relationship between copyright and cybersecurity behaviour, as well as higher levels of cybersecurity awareness.

The findings of the moderation analysis indicate that Cybersecurity Awareness plays a moderating role in the associations between Cybersecurity Behaviour, Copyright, Citizenship, Curation, Connectedness, and Online Privacy Concerns. This emphasises the significance of considering individuals' awareness levels when examining the impact of traits such as connectivity, digital literacy, and concerns about online privacy on their actual cybersecurity behaviours.

Table 5: Testing Moderation (Cyber Security Awareness).

Variable	Copyright	Citizenship	Curation	Connectedness	Privacy Concern	R^2	Adjusted R^2	F
Cybersecurity Awareness	0.314**	0.268*	-0.288*	0.260**	0.347**	0.301	0.291	8.97**

a. Dependent Variable: Cybersecurity Behaviour
**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

9. Discussion

Understanding digital movement is crucial due to the prevalence of digital devices in people's daily lives. Digital literacy significantly influences online behaviour by impacting various aspects such as copyright awareness, material selection, and online networking skills. The increasing importance of online privacy necessitates an examination of its potential impact on cybersecurity practices. Digital literacy is essential in the current digital landscape, yet it poses challenges. The digital divide, which refers to disparities in technology and internet access, poses a significant barrier. The acquisition of digital skills may differ based on economic, geographical, and demographic factors.

Closing this gap is crucial to achieve equal and equitable access to information and tools for digital participation. Internet data poses a significant challenge. Individuals face challenges in locating reliable, precise, and beneficial information within the vast volume of accessible data. The abundance of information necessitates the development of information literacy skills, such as critical thinking and filtering. This enables purchasers to efficiently navigate extensive digital datasets and make well-informed choices. Cybersecurity impedes digital literacy. As our online presence increases, it is imperative for users to comprehend and implement secure measures to safeguard their personal information. Cyberattacks encompass criminal data breaches and phishing scams. Understanding cybersecurity is crucial for reducing vulnerabilities and safeguarding online privacy and personal information. This study examines the relationship between digital literacy characteristics and cybersecurity behaviours, specifically focusing on the moderating effect of cybersecurity awareness. Initially, we proposed several hypotheses to investigate the impact of digital competency components on cybersecurity behaviours.

H1 of the study indicates that copyright law has a positive impact on cybersecurity behaviour. There is a significant negative association, indicating that knowing copyright laws is linked to a decrease in proactive cybersecurity behaviours. This serendipitous finding necessitates further investigation into the nuanced impact of copyright awareness on cybersecurity. The unexpected negative correlation between copyright awareness and cybersecurity behaviour could be explained by slight differences in copyright awareness and its influence on proactive cybersecurity behaviour, contradicting hypothesis H1. The potential impact on individual engagement should be taken into consideration. This unexpected outcome could potentially be attributed to the level of awareness and comprehension surrounding copyright law.

Enhancing knowledge of copyright laws, although essential for digital literacy, may not necessarily lead to an improvement in cybersecurity practices. Copyright awareness can lead individuals to exercise caution and impose restrictions when engaging in online activities due to their recognition of legal boundaries and the potential repercussions. This perspective aligns with existing literature that argues a strict interpretation of copyright law can impede technological progress and creative expression in the digital realm (Lessig, 2004). Individuals who prioritise cybersecurity and have a cautious attitude towards risk may choose to refrain from participating in online activities that they believe could potentially infringe upon copyright laws. Despite the inherent dangers of those activities.

The study provides evidence in support of Hypothesis 2 (H2), which suggests that citizenship enhances cybersecurity behaviour. Our empirical research aligns with existing literature that underscores the importance of responsible digital citizenship in promoting safe online practices. According to Ribble and Bailey (2015), digital citizenship refers to the appropriate and responsible behaviour norms associated with technology usage. Respecting the rights of others, understanding the legal consequences of digital actions, and prioritising online safety and security are integral aspects of responsible digital citizenship. The survey findings suggest that individuals who prioritise copyright protection are more likely to exhibit responsible behaviour on the internet. Respecting intellectual property rights, understanding copyright laws, and practicing safe online habits are essential for safeguarding both personal and shared digital environments. The positive influence of citizenship on cybersecurity behaviour highlights the correlation between ethical conduct and online safety. Practicing responsible digital citizenship enhances individuals' inclination to participate in digital networks and increases their awareness of potential security risks.

The study provides support for Hypothesis 3 (H3), which suggests that curation enhances cybersecurity behaviours. This finding aligns with existing literature that highlights the importance of proactive content management in the context of online security. Jenkins' book, "Convergence Culture: Where Old and New Media Collide" (2006), is a valuable source. Jenkins discusses a digital culture characterised by active participation and curation of content as opposed to passive consumption. Content curators are responsible for organising and presenting digital material, demonstrating proficiency in digital literacy. Content curation enhances digital literacy, thereby enhancing online safety. Curators exhibit a higher degree of

scepticism towards the material they present, possess a comprehensive understanding of the potential consequences associated with disseminating it across various online platforms, and demonstrate a proactive approach to safeguarding their online presence. Curation positively impacts cybersecurity behaviours, highlighting the interconnectedness of digital literacy components. Responsible content curation encompasses copyright citizenship, information literacy, and privacy concerns. These factors contribute to a comprehensive digital literacy approach that encompasses content curation and cybersecurity.

The findings confirm Hypothesis 4 (H4), which posits that networking enhances cybersecurity behaviour by highlighting the social dimensions of online conduct. Boyd and Ellison's influential publication, "Social Network Sites: Definition, History, and Scholarship" (2007), could provide insights into this matter. The authors investigate the impact of social networking sites on online interactions, specifically focusing on the role of social connections. The study suggests that individuals are more susceptible to the influence of their social networks, including their cybersecurity practices, after establishing connections on social media and other online communities. Boyd and Ellison (2007) discuss the role of social networks in facilitating the expression and visualisation of interpersonal relationships. Networks enhance cybersecurity behaviour through the influence of social impact and the establishment of shared norms within online communities. Individuals who experience a sense of connection in online environments are more likely to adopt cybersecurity best practices because of peer influence, information sharing, and adherence to social norms. The literature on social influences and norms in the field of cybersecurity could provide valuable assistance. Kirlappos, Sasse, and Harvey (2012) investigate the impact of social norms on safety behaviour and decision-making.

The research findings confirm Hypothesis 5 (H5), which suggests that there is a positive relationship between online privacy concerns and cybersecurity behaviour. Additionally, the study establishes a connection between privacy attitudes and cybersecurity practices. The article by Acquisti and Grossklags (2005) provides evidence for the connection between privacy and rationality in individual decision-making. This study investigates the impact of privacy concerns on decision-making in the online context. Privacy-conscious individuals prioritise data protection, which is closely associated with cybersecurity. In this context, Norberg, Horne, and Horne's (2007) analysis of the privacy paradox is pertinent. The privacy paradox refers to the phenomenon in which individuals express concerns about their privacy but do not consistently engage in behaviours that align with those concerns. This study demonstrates a positive correlation between an individual's online privacy concerns and their cybersecurity behaviour, indicating that individuals are inclined to act based on their worries. The literature on privacy calculus and perceived risk is in support of the study's findings. Dinev and Hart (2006) found that "An Extended Privacy Calculus Model for E-Commerce Transactions". Individuals who have higher levels of privacy concerns are more likely to perceive greater risks to online security and are more inclined to take proactive measures to mitigate these risks.

The study discovered that cybersecurity awareness (H6 to H10) significantly moderates the relationship between digital literacy variables and cybersecurity behaviour, in addition to other significant effects. Enhanced cybersecurity awareness promotes the development of digital literacy skills, including understanding copyright laws, practicing good digital citizenship, engaging in content curation, fostering connectedness, and addressing online privacy concerns. Developing a strong sense of awareness is essential for effectively translating digital skills into secure online practices.

10. Implications

This study investigates the multifaceted aspects of digital literacy, specifically focusing on copyright citizenship, curation, networking, and online privacy. This expansion of the digital literacy framework incorporates additional elements that impact online behaviour, thereby enhancing its previous focus on general abilities. This study highlights the interconnectedness of digital capability components and underscores the importance of considering them collectively. The interconnections among citizenship, curation, networking, and online privacy concerns demonstrate the multifaceted nature of digital literacy. The positive correlation between concerns about online privacy and cybersecurity behaviour contributes to our understanding of the relationship between privacy and security. This study demonstrates the interconnection between privacy and security in the digital realm, indicating that individuals who prioritise privacy are more inclined to engage in security practices.

This study demonstrates that the relationship between digital literacy components and cybersecurity behaviours is influenced by cybersecurity awareness. These theoretical findings highlight the importance of incorporating awareness into digital literacy frameworks to enhance safe online behaviours. The unexpected inverse relationship observed between copyright knowledge and cybersecurity behaviour challenges conventional assumptions and highlights the dynamic nature of cybersecurity behaviour. This finding encourages scholars to reconsider theoretical frameworks and investigate contextual factors that could influence digital perceptions and behaviours. The cross-sectional design of the study hinders the establishment of causal relationships and raises concerns regarding the temporal dynamics of digital literacy and cybersecurity behaviour. Future studies could investigate how technology and societal norms influence these correlations in the long run. The positive relationship between networking and cybersecurity behaviour suggests that social factors play a role in influencing online security.

The results highlight the importance of digital citizenship, curation, networking, and online privacy in shaping cybersecurity behaviours. Organisations and policymakers can customise online behaviour and digital literacy education programmes. Cybersecurity awareness plays a moderating role in the relationship between public education efforts and cybersecurity behaviours. Efforts focused on copyright enforcement, protection of civil rights, curation, and internet privacy awareness can yield improved results. This study proposes the customisation of cybersecurity education based on the individual's level of awareness and specific topics. Tailoring cybersecurity training to address these aspects enhances its efficacy. There is a positive correlation between individuals' cybersecurity concerns and their

behaviour, indicating that individuals who prioritise online privacy are more inclined to adopt advanced cybersecurity measures. This insight can aid in the development of privacy-centric design principles for digital platforms and services by promoting the use of user-friendly, privacy-secure technologies.

11. Limitations and Future Research Directions

The study sample comprises individuals from multiple cities in Saudi Arabia. Future research should aim to enhance the generalizability of findings by expanding the sample size and incorporating greater diversity, thereby increasing the applicability of results across various regions and cultural contexts. Response bias may occur when self-reported data is used. Future studies could utilise objective measurements or observational data to corroborate and enhance self-reported findings. Given the cultural diversity of the sample, it is important to recognise that digital literacy, concerns about online privacy, and knowledge of cybersecurity may vary across cultures.

Comparative studies conducted in diverse cultural contexts may enhance our understanding of these dynamics in a more comprehensive manner. The cross-sectional design of the study limits the ability to establish causal relationships. Longitudinal studies, which track individuals over time, can provide valuable insights into the temporal dynamics of the variable interactions being investigated. This study explores relationships and moderation effects, suggesting that further research should explore the underlying processes that mediate these interactions. Studying the influence of digital literacy, citizenship, curation, connectedness, and online privacy on cybersecurity behaviour can enhance our understanding of the underlying dynamics. As technology advances, cybersecurity issues also evolve. Future research could explore emerging technologies and their impact on digital literacy, concerns related to privacy, and awareness of cybersecurity. This would help maintain the relevance of the findings in the context of technological advancements.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under grant number (GRANT5374)

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences, 10*(4), 136-144. https://doi.org/10.21833/ijaas.2023.04.017

Ali, A., Al-Rimy, B. A. S., Almazroi, A. A., Alsubaei, F. S., Almazroi, A. A., & Saeed, F. (2023). Securing secrets in cyber-physical systems: A cutting-edge privacy approach with consortium blockchain. *Sensors, 23*(16), 7162. https://doi.org/10.3390/s23167162

Alissa, K. A., AlDeeb, B. A., Alshehri, H. A., Dahdouh, S. A., Alsubaie, B. M., Alghamdi, A. M., & Alsmadi, M. K. (2021). Developing a simulated intelligent instrument to measure user behavior toward cybersecurity policies. *International Journal of Communication Networks and Information Security, 13*(1), 82-91. http://dx.doi.org/10.17762/ijcnis.v13i1.4923

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences, 13*(9), 5700. https://doi.org/10.3390/app13095700

AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies, 13*(2), e202312. https://doi.org/10.30935/ojcmt/12942

Amin, H., Malik, M. A., & Akkaya, B. (2021). Development and validation of digital literacy scale (DLS) and its implication for higher education. *International Journal of Distance Education and E- Learning (IJDEEL), 7*(1), 24-43. http://dx.doi.org/10.36261/ijdeel.v7i1.2224

Aziz, O., Siraj, M. A., & Rehman, A. (2021). Privacy challenges in cyber security against cybercrime in digital forensic. A systematic literature review in Pakistan. *Journal of Computing & Biomedical Informatics, 2*(02), 158-164. https://doi.org/10.56979/202/2021/31

Basahel, A. M., & Yamin, M. (2020). Cyber Security and Privacy in Internet of Things. *International Journal of Human Potentials Management, 2*(1), 43-53.

Bawden, D. (2001). Information and digital literacies: a review of concepts. *Journal of Documentation, 57*(2), 218-259. https://doi.org/10.1108/EUM0000000007083

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *Management Information Systems Quarterly, 35*(4), 1017-1041. https://doi.org/10.2307/41409971

Bottoni, P., Gessa, N., Massa, G., Pareschi, R., Selim, H., & Arcuri, E. (2020). Intelligent smart contracts for innovative supply chain management. *Frontiers in Blockchain, 3*, 52. https://doi.org/10.3389/fbloc.2020.535787

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication, 13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62-70. https://courses.ischool.berkeley.edu/i271b/f12/readings/Brown_2004.pdf

Bubaš, G., Orehovački, T., & Konecki, M. (2008). Factors and predictors of online security and privacy behavior. *Journal of Information and Organizational Sciences, 32*(2), 79-98. https://jios.foi.hr/index.php/jios/article/view/63

Chau, P. Y. (1996). An empirical assessment of a modified technology acceptance model. *Journal of Management Information Systems, 13*(2), 185-204. https://doi.org/10.1080/07421222.1996.11518128

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media+Society, 6*(2), 1-13. https://doi.org/10.1177/2056305120916853

Ertz, M., Lecompte, A., & Durif, F. (2017). Dual roles of consumers: Towards an insight into collaborative consumption motives. *International Journal of Market Research, 59*(6), 725-748. https://doi.org/10.2501/IJMR-2017-040

Gibson, P. F., & Smith, S. (2018). Digital literacies: Preparing pupils and students for their information journey in the twenty-first century. *Information and Learning Science, 119*(12), 733-742. https://doi.org/10.1108/ILS-07-2018-0059

Hamid, A., Alam, M., Sheherin, H., & Pathan, A.-S. K. (2020). Cyber security concerns in social networking service. *International Journal of Communication Networks and Information Security, 12*(2), 198-212. https://www.proquest.com/openview/3213fc00de03a053b6e2802a98373161

Huo, X., & Liu, M. (2021). Encrypted decentralized multi-agent optimization for privacy preservation in cyber-physical systems. *IEEE Transactions on Industrial Informatics, 19*(1), 750-761. https://doi.org/10.1109/TII.2021.3132940

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal, 12*(2), 623-633. https://doi.org/10.18421/TEM122-05

Jenkins, H. (2006). *Convergence Culture: Where Old and New Media Collide*. New York University Press. https://www.jstor.org/stable/j.ctt9qffwr

Kim, S. S. (2023). Motivators and concerns for real-time online classes: focused on the security and privacy issues. *Interactive Learning Environments, 31*(4), 1875-1888. https://doi.org/10.1080/10494820.2020.1863232

Kirlappos, I., Sasse, M. A., & Harvey, N. (2012). Why trust seals don't work: A study of user perceptions and behavior. In *Trust and Trustworthy Computing: 5th International Conference, TRUST 2012, Vienna, Austria, June 13-15, 2012. Proceedings 5* (pp. 308-324). Springer. https://doi.org/10.1007/978-3-642-30921-2_18

Klein, G., Zwilling, M., & Lesjak, D. (2022). A comparative study in israel and slovenia regarding the awareness, knowledge, and behavior regarding cyber security. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 424-439). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch020

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access, 8*, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*. https://doi.org/10.1177/00111287231180093

Lessig, L. (2004). The Creative Commons. *Montana Law Review, 65*(1), 1. https://scholarworks.umt.edu/mlr/vol65/iss1/1

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives*. Oxford University Press, USA. https://doi.org/10.1093/oso/9780190874698.001.0001

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviors toward online privacy protection. In *2013 international conference on social computing* (pp. 57-62). IEEE. https://doi.org/10.1109/SocialCom.2013.15

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44. https://doi.org/10.1016/j.chb.2018.01.028

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Ohler, J. (2011). Digital citizenship means character education for the digital age. *Kappa Delta Pi Record, 47*(sup1), 25-27. https://doi.org/10.1080/00228958.2011.10516720

Payne, B. K., Cross, B., & Vandecar-Burdin, T. (2022). Faculty and Advisor Advice for Cybersecurity Students: Liberal Arts, Interdisciplinarity, Experience, Lifelong Learning, Technical Skills, and Hard Work. *Journal of Cybersecurity Education, Research and Practice, 2021*(2). https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/5

Quayyum, F. (2023). Collaboration between parents and children to raise cybersecurity awareness. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference* (pp. 149-152). ACM. https://doi.org/10.1145/3590777.3590802

Ribble, M., & Bailey, G. (2015). *Digital Citizenship in Schools: Nine elements all students should know*. International Society for technology in Education. https://epale.ec.europa.eu/sites/default/files/digcit-excerpt.pdf

Ribble, M., & Park, M. (2022). *The digital citizenship handbook for school leaders: Fostering positive interactions online*. International Society for Technology in Education. https://www.everand.com/book/441102567/The-Digital-Citizenship-Handbook-for-School-Leaders-Fostering-Positive-Interactions-Online

Riebe, T., Bäumler, J., Kaufhold, M.-A., & Reuter, C. (2023). Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response: A Value Sensitive Design Perspective. *Computer Supported Cooperative Work (CSCW)*, 1-47. https://doi.org/10.1007/s10606-022-09453-4

Sá, M. J., Santos, A. I., Serpa, S., & Miguel Ferreira, C. (2021). Digitainability—Digital competences post-COVID-19 for a sustainable society. *Sustainability, 13*(17), 9564. https://doi.org/10.3390/su13179564

Sarker, A., Shen, H., Rahman, M., Chowdhury, M., Dey, K., Li, F., Wang, Y., & Narman, H. S. (2019). A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles. *IEEE Transactions on Intelligent Transportation Systems, 21*(1), 7-29. https://doi.org/10.1109/TITS.2019.2892399

Sharma, S., Kar, A. K., Gupta, M., Dwivedi, Y. K., & Janssen, M. (2022). Digital citizen empowerment: A systematic literature review of theories and development models. *Information Technology for Development, 28*(4), 660-687. https://doi.org/10.1080/02681102.2022.2046533

Simonet, J., & Teufel, S. (2019). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34* (pp. 194-208). Springer. https://doi.org/10.1007/978-3-030-22312-0_14

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online privacy literacy and online privacy behavior–the role of crystallized intelligence and personality. *International Journal of Human–Computer Interaction, 37*(15), 1455-1466. https://doi.org/10.1080/10447318.2021.1894799

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences, 11*(9), 386. https://doi.org/10.3390/socsci11090386

Tirumala, S., Valluri, M. R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCI.2019.8821951

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR), 51*(2), 1-27. https://doi.org/10.1145/3172869

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In *Reforming European data protection law* (pp. 333-365). Springer, Dordrecht. https://doi.org/10.1007/978-94-017-9385-8_14

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

van Leersum, C. M., Jaschinski, C., Bults, M., & van der Zwart, J. (2022). Citizen involvement in research on technological innovations for health, care or well-being: a scoping review. *medRxiv*. https://doi.org/10.1101/2022.11.03.22281892

Zhu, S., Yang, H. H., Wu, D., & Chen, F. (2021). Investigating the relationship between information literacy and social media competence among university students. *Journal of Educational Computing Research, 59*(7), 1425-1449. https://doi.org/10.1177/0735633121997360

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Appendix 1: Measurement Scales

Digital Literacy Scale	
Copyright	
1. I know online plagiarism policy of my institute.	
2. I know the consequences of using copyright work online without permission.	
3. I give acknowledgement/reference in my online work while using collusion (copying from fellow students).	
4. I use Turnitin or other similar software to check and avoid unintentional plagiarism.	
Citizenship	
1. I communicate with others in a respectable way while using technology.	
2. I know the consequences for violating cyber laws in digital world.	
3. I accept and follow the terms and conditions for accessing any information.	
4. I respect the cultural differences in online world, and respond accordingly.	Amin, Malik, and Akkaya (2021)
Curation	
1. I search for material from renowned websites.	
2. I try to add value to the existing pieces of information available online.	
3. I play my part in adding to, and updating online information.	
Connectedness	
1. I am involved in different online communities for volunteer work.	
2. I participate in different online projects at national level.	
3. I actively take interest in different online campaigns for community development.	
4. I actively participate in online polls/surveys.	
5. I encourage and help my community to post their problems and issues on social media for getting attention.	
Online Privacy Concerns	
1. I detest the fact that the web is becoming a haven for electronic junk mail.	
2. My personal details are safe with online companies.	
3. I wish I had more control over unwanted messages sent by businesses on the web.	
4. I dislike the fact that marketers are able to find out personal information about online shoppers.	
5. I believe the information I share with online companies will not be shared with other companies.	Brown and Muchira (2004)
6. Online companies will keep confidential what they learn about me from my activities on their site.	
7. I have dealt with over the Internet passed on your personal details to a third party.	
8. My personal details have been incorrectly altered or modified in some way without your approval by companies you have dealt with over the Internet.	
9. I actually purchased something via the Internet and made full payment online.	
Cybersecurity Behavior	
1. I never open when I receive an e-mail with an attachment	
2. When constructing a password, you should	
o Use a family member's name, sports name, and pet name with a number at the end.	
o Use misspelled words or phrases with embedded numbers and special characters.	
o Use sequenced numbers and letters from your keyboard.	
3. I never allow a (trusted/untrusted) person to use your e-mail account to send an urgent and important message	
4. I never leave sensitive data in open areas (copiers, faxes, printers, desktops)	Alissa et al. (2021)
I never follow the physical security practices	
I physically secure your computing devices (desktops, laptops, portable drives, and smart devices)	
5. I never text or post sensitive data on a social site	
6. I have a personal laptop, and I would protect it with virus protection and software patches	
7. I normally take backup of my sensitive/critical data on a routine basis	
Cybersecurity Awareness	
1. Common Password: I have a password that I use for more than one device / system	
2. Password Strength: I have a password contains number, alphabet in more than once case and a special character	
3. Change of Password I change your password over a period of time before being alerted	Tirumala, Valluri, and Babu (2019)
4. Parental lock I use parental lock on my devices	
5. Safe Search: I use any software for blocking illegitimate sites	
6. Awareness: I am aware that some of my data will be collected by websites and apps irrespective of my consent Protection: I am aware of security features in browsers	