information

MDPI

Article

Smartphone Privacy and Cyber Safety among Australian Adolescents: Gender Differences

Yeslam Al-Saggaf * and Julie Maclean

School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, NSW 2678, Australia; jumaclean@csu.edu.au
* Correspondence: yalsaggaf@csu.edu.au

Abstract: While existing studies explore smartphone privacy setting risks for adolescents, they provide limited insight into the role of gender in these dynamics. This study aims to enhance adolescents' awareness of the security risks associated with smartphone privacy leakage by focusing on how a cyber safety intervention lesson can affect knowledge of smartphone privacy settings, attitudes toward smartphone settings, and concerns about smartphone privacy. This study surveyed 376 high school students before and after a cyber safety lesson. Our study found that before the cyber safety intervention, females reported lower knowledge of smartphone settings than males. After the lesson, this gap narrowed, with both genders demonstrating more consistent understanding. Both genders showed lower attitudes towards smartphone privacy compared to knowledge, with males displaying the largest gap, reflecting the privacy paradox. Females expressed greater concern regarding location privacy, especially when tracked by unknown individuals, indicating that while both genders are aware of risks, females perceive them more acutely. The results suggest that targeted educational programs can effectively enhance adolescents' knowledge, attitudes, and concerns about smartphone privacy, particularly in technical areas where gender gaps exist.

Keywords: smartphones; information security management; privacy; cybersecurity; Internet of Things (IoT); adolescent; gender

Citation: Al-Saggaf, Y.; Maclean, J. Smartphone Privacy and Cyber Safety among Australian Adolescents: Gender Differences. *Information* **2024**, *15*, 604. https://doi.org/10.3390/info15100604

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 29 August 2024
Revised: 28 September 2024
Accepted: 29 September 2024
Published: 2 October 2024

1. Introduction

A recent survey revealed that 95% of U.S. teens have access to smartphones, with 94% of adolescent boys and 97% of adolescent girls reporting smartphone ownership [1]. While this widespread access enables connectivity and learning, it also introduces significant privacy risks, especially if smartphone data leakage is not properly managed. Research shows that privacy behaviour in online environments is shaped by various factors, including privacy concerns, attitudes, knowledge, skills, experience, education, gender, and age [2,3], trust and risk perceptions [4] and offline expected social norms [5]. Children primarily use their smartphones to pass the time, connect with others, and learn new things [6]. However, frequent use of apps for social media, gaming, and communication often leads to the neglect of critical privacy settings, thereby increasing the risk of personal information leakage [7,8].

Studies in child psychology reveal that children's impulsive behaviour and strong desire for social connectivity often overshadow their privacy concerns [9]. Male and female teenagers exhibit significantly different attitudes toward privacy, influenced by socialization, personal experiences, and perceived risks [10]. Despite being aware of risks such as exposure to inappropriate content, interactions with strangers, and oversharing, children often struggle to take effective steps to address privacy issues and prevent data tracking [11]. This behaviour reflects the "privacy paradox", where children express concern for privacy but engage in actions that compromise it. Therefore, effective educational interventions are crucial to raising children's awareness of privacy risks and encouraging protective behaviours.

In this study, smartphone privacy refers to the protection of sensitive personal information that smartphones collect, store, and share. It focuses on the awareness and behaviours of adolescents in managing privacy settings to prevent unauthorized access or exposure of their data, such as location, and personal identifiers. Specific privacy risks include leaving Wi-Fi and Bluetooth enabled, sharing real names for device identification, and failing to manage location tracking settings. This study examines the knowledge and behaviours of adolescents regarding these risks and how targeted educational interventions can improve their understanding and practices to better protect their privacy.

Despite the importance of safeguarding children's smartphone privacy, there is limited research on how educational interventions can effectively protect children, particularly in the context of gender differences. This study aims to enhance adolescents' awareness of the security risks associated with smartphone privacy leakage by focusing on three key areas: (1) knowledge of smartphone privacy settings, (2) attitudes toward smartphone settings, and (3) concerns about smartphone privacy. Critically, this study investigates gender differences in adolescents' responses to a hands-on cyber safety lesson they attended in their school to raise their awareness about these security areas.

Although existing studies examine adolescent risk-taking in relation to privacy [9], online privacy perceptions [10], and general privacy attitudes [11], they offer limited insight into the specific role gender plays in smartphone privacy dynamics. This study builds on the protection motivation theory (PMT) [12], which posits that individuals are motivated to protect themselves based on their perceived severity and vulnerability to a threat. This theoretical framework is particularly relevant to online privacy, as it helps identify factors that may deter individuals from engaging in protective behaviours. PMT may be instrumental in addressing gender disparities in adolescent privacy behaviours and in developing targeted strategies to reduce the risk of smartphone privacy leakage across different genders. As technology continues to evolve and new privacy threats emerge, it is imperative to continuously update educational content to effectively safeguard children's privacy.

This paper is structured into five key sections. The Section 2 reviews the existing literature on smartphone privacy, cyber safety education, and gender differences in digital literacy among adolescents. In Section 3, we describe the survey methodology, the educational interventions delivered, and the approach used to measure data leakage and student knowledge before and after the lessons. The Section 4 presents the key findings from the surveys and data leakage analysis, highlighting improvements in smartphone privacy knowledge and behavioural changes post-intervention. In Section 5, we analyse these findings in the context of prior research, exploring the implications for educational practices and policies. Finally, Section 6 summarizes the key takeaways and suggests directions for future research, emphasizing the importance of targeted interventions in enhancing cyber safety for adolescents.

2. Related Work

2.1. Knowledge of Smartphone Privacy Settings

Male and female attitudes towards privacy often diverge due to various factors, including early exposure to technology, societal expectations, and career aspirations. Males are frequently encouraged to engage with programming, hardware, and gaming from a young age, which contributes to their advanced technological skills and confidence in these areas [13]. In contrast, females typically develop proficiency in communication tools, social media, and creative applications, favouring technology that enhances productivity and collaboration [14]. These differences influence how each gender approaches online privacy, data sharing, and the protection of personal information.

Males' higher likelihood of pursuing STEM (science, technology, engineering, mathematics) careers further cultivates their technological expertise [15]. On the other hand, females often gravitate towards fields such as education, healthcare, and social sciences, where the use of technology is more focused on application rather than development [16,17].

This divergence in career interests may impact their knowledge of and attitudes toward technical privacy settings.

Males also tend to report higher confidence in performing technological tasks [18,19], which could contribute to a perception of greater technological proficiency among younger males. This confidence, potentially bolstered by frequent engagement with video games and other technology-intensive activities, might lead to higher levels of perceived knowledge [20]. However, despite having comparable abilities, females may exhibit lower self-efficacy in traditionally male-dominated areas [21,22]. This discrepancy in confidence can result in females perceiving themselves as less knowledgeable, even if their actual skills are equivalent.

The perception that technology settings are a "male activity" could further influence females' enthusiasm for learning about technology [19], particularly if smartphone privacy settings are seen as more technical [23]. This societal bias might discourage females from engaging deeply with privacy settings, reinforcing the gender gap in perceived technological expertise. Based on these gender differences that are likely to result in differences for adolescent male and female knowledge of smartphone settings, we propose the following hypothesis:

Hypothesis 1: *Adolescent males are expected to have higher levels of knowledge of smartphone privacy settings than adolescent females.*

2.2. Attitude towards Smartphone Privacy Settings

Male and female teenagers exhibit differing levels of privacy practices, influenced by factors such as social acceptance and peer approval. Male teenagers generally perceive lower risks related to online privacy, often prioritizing convenience over security. This behaviour is reflected in their tendency to share personal information more freely on social media, potentially leading to less effective use of privacy settings [24]. Social acceptance and peer approval often take precedence over privacy concerns for males, which may cause them to underestimate the potential consequences, such as privacy breaches or data misuse [10].

In contrast, female teenagers tend to be more proactive in protecting their privacy. They are more likely to utilize simple privacy protection settings on social media (e.g., untagging photos), limit the sharing of personal information, and carefully select their online interactions [24,25]. Females are more inclined to manage their online social media presence with greater caution, sharing content primarily with trusted friends and family while being vigilant about what they disclose [24,26]. This contrasts with males, who are more inclined to share personal data with third-party apps, often prioritizing convenience and enhanced functionality over informed consent [27]. The gender differences for attitudes towards privacy may translate into differences in attitudes for male and female adolescent attitudes towards smartphone settings. We propose the following hypothesis:

Hypothesis 2: *Adolescent females are expected to have a more cautious attitude towards smartphone privacy settings than adolescent males.*

2.3. Concerns About Smartphone Privacy

While female teenagers are more likely to seek privacy-enhancing tools and value informed consent [28], their strong motivation for social connection can sometimes lead to compromises in privacy for the sake of maintaining online interactions [29]. Despite their general caution, the desire for social connection may cause them to occasionally overlook privacy risks. Females are more likely than males to adopt protective practices, such as limiting contact with strangers and using stronger privacy settings, due to a heightened awareness of issues like online harassment [30]. Additionally, females often prioritize physical safety in their online behaviour, employing strategies like using pseudonyms

and avoiding the sharing of real-time locations to mitigate potential risks [31]. Given the anticipated gender differences, where adolescent females are more likely to worry about smartphone privacy due to concerns related to physical safety and location risks than adolescent males, we propose the following hypothesis:

Hypothesis 3: *Adolescent females are expected to have higher levels of concerns about smartphone privacy than adolescent males.*

2.4. Privacy Paradox

The privacy paradox describes a phenomenon where individuals express concerns about their privacy yet engage in behaviours that contradict these concerns, often compromising their privacy in online environments [32]. This paradox is especially evident in digital spaces, where users claim to value their privacy but still share personal information freely, use weak passwords, or neglect to adjust privacy settings [33].

For adolescents, the privacy paradox is particularly pronounced due to their still-developing capacity to fully comprehend long-term consequences and risks [34]. Adolescents are more susceptible to impulsive behaviour, especially in the context of peer interactions or social validation [9]. This impulsivity can lead to sharing personal information online without fully considering the associated privacy risks [9]. While they may be aware of privacy concerns such as cyberbullying, identity theft, or unwanted attention and express anxiety about these threats, they frequently engage in risky behaviours like sharing personal details, using weak passwords, or failing to log out of shared devices [35].

Gender differences are likely to influence how the privacy paradox manifests among adolescents. These differences are shaped by variations in socialization, risk perception, and the ways in which boys and girls interact with technology [24]. Males, who may be less concerned about privacy breaches related to physical safety, such as stalking or harassment, often focus more on cybersecurity threats like hacking and identity theft, employing tools like two-factor authentication to protect themselves [36].

Females, on the other hand, typically perceive higher risks regarding privacy, especially concerning personal data being accessed and misused by third parties, potentially leading to safety issues and harassment [24,37]. However, despite their heightened awareness of these risks, they may paradoxically expose themselves to harm by freely using real names and profiles across platforms for social connection purposes [38]. This behaviour exemplifies the privacy paradox, where high-risk perception does not always translate into protective actions. Given these observations, where adolescent males are likely to have higher levels of knowledge of smartphone settings and a less cautious attitude to smartphone privacy settings than adolescent females, we propose the following hypothesis:

Hypothesis 4: *The privacy paradox between levels of knowledge of smartphone privacy settings and levels of attitudes toward smartphone privacy settings will be more pronounced for adolescent males than for adolescent females.*

2.5. Targeted Educational Intervention

Addressing gender differences in privacy through inclusive education for technological skills may help bridge gaps in knowledge, attitudes, and concerns related to smartphone privacy settings by encouraging all teenagers to explore and develop a diverse range of competencies. While many studies have applied theories such as communication privacy management [39] and the privacy calculus model [40,41], this study leverages PMT to examine how threat and coping appraisals influence protective behaviour. PMT suggests that individuals are motivated to protect themselves when they perceive a threat as both severe and credible (perceived threat) and believe they have the capability and efficacy to respond effectively (perceived efficacy) [12]. This framework is particularly relevant

to smartphone privacy, as it helps identify the factors that may deter individuals from engaging in protective behaviours.

Linking PMT with educational programs has proven critical for enhancing cyber privacy protection [42]. Research indicates that educational interventions can significantly improve children's digital skills and self-efficacy [43]. However, much of the current cybersecurity privacy messaging lacks proper evaluation regarding its effectiveness in being learned, applied, and the actual safety it provides [44] and differences between genders. Understanding how PMT can address gender disparities in privacy attitudes is essential, as these differences highlight the need for tailored education that addresses specific concerns and behaviours. Considering that targeted educational interventions are expected to reduce gender differences in privacy threat perceptions and efficacy based on PMT, we propose the following hypothesis:

Hypothesis 5: *A targeted educational intervention is expected to reduce gender disparities in knowledge, attitudes, and concerns regarding smartphone privacy among adolescent males and females.*

3. Materials and Methods

3.1. Procedure

The presenters delivered a one-off hands-on lesson of approximately one hour duration in five Australian high schools. The lesson demonstrated how smartphones can inadvertently share sensitive information, how easily this information can be captured by others, and how students can manage their devices to prevent such data leaks. The lesson included practical demonstrations where students learned how to turn off Bluetooth, switch off Wi-Fi, change their Bluetooth name, and disable location services.

Before and after the lesson, students were invited to complete a short online survey to assess changes in their awareness of online safety. Participation was voluntary and not targeted by gender or ethnicity. Each student received a QR code linked to a unique identifier for survey access. All participants received an AUD 20 gift card, regardless of survey completion. Ethical approval was obtained from the university's Human Research Ethics Committee (Protocol No. H23489). Of 574 responses, 79 were excluded due to incomplete surveys, leaving 495 valid responses for analysis.

3.2. Participants

To confirm the validity of the survey responses, the data were analysed to identify duplicate participant IDs among the high school students who had shared the same QR code. To differentiate between unique responses, different IP addresses suggested that the survey was accessed from different devices. Gender, age, and high school information were also used as unique identifiers to differentiate between responses.

Where all information was valid between the responses and there was a time difference that aligned to before and after the presentation, these were classified as "Before" responses, where the timeframe aligned to prior to the cyber safety lesson, and "after" responses, where the timeframe aligned to after the cyber safety lesson. The dataset included 376 "before" responses and 100 "after" responses.

Table 1 presents the sociodemographic statistics for the before and after groups, including age, gender, school, and device ownership. Gender distribution remained relatively consistent, with males comprising 41.2% of the before group and 47.0% of the after group, and females making up 58.8% and 53.0%, respectively. Participants ranged in age from 13 to 19 years, with a mean age of 14.96 years (SD = 1.07) in the before group and 14.76 years (SD = 0.94) in the after group. Most students were between 14 and 16 years old (>90% in both groups), and 93% owned a smartphone. Smartphones accounted for 44.5% of all devices owned, with 42% of students indicating they owned only one type of digital device.

Table 1. Summary of sociodemographic statistics for the before and after groups.

		Before		After	
		n	**%**	***n***	**%**
Age	13	8	2.1	1	1.0
	14	155	41.2	54	54.0
	15	88	23.4	15	15.0
	16	100	26.6	28	28.0
	17	19	5.1	2	2.0
	18	5	1.3	-	-
	19	1	0.3	-	-
Gender	Male	155	41.2	47	47.0
	Female	221	58.8	53	53.0
Devices Owned	Smartphone	342	44.5	92	43.2
	Smartwatch	113	14.7	34	16.0
	iPad	125	16.3	34	16.0
	Android Tablet	25	3.3	5	2.3
	Fitness Tracker	52	6.8	14	6.6
	Clothing with "Smart Tags"	7	0.9	5	2.3
	Dumb Phone	15	2.0	2	0.9
	None	3	0.4	27	12.7
	Other	87	11.3	92	43.2
Number of Devices Owned	0	3	0.8	2	1.9
	1	159	42.3	39	37.5
	2	99	26.3	26	25.0
	3	70	18.6	24	23.1
	4	35	9.3	12	11.5
	5	7	1.9	1	1.0
	6	1	0.3	2	1.9
	7	2	0.5	39	37.5

3.3. Measures

Knowledge of smartphone privacy settings was measured using 13 questionnaire items rated on a four-point Likert scale from one (Strongly disagree) to four (strongly agree). The questions asked students about their knowledge of smartphone names, location services, Bluetooth, Wi-Fi, IP address, and SSID settings. This questionnaire received a total of 476 responses from students. There were 375 "before" responses and 101 "after" responses.

Attitudes towards smartphone privacy settings were measured using 6 questionnaire items rated on a four-point Likert scale from one (strongly disagree) to four (strongly agree). The questions asked students about their attitude towards accessing public Wi-Fi's, using their real name, switching off location services, Bluetooth and Wi-Fi, and whether or not they worry about their cybersecurity. This questionnaire received a total of 476 responses from students. There were 367 "before" responses and 96 "after" responses.

Concerns about smartphone privacy was measured using 13 questionnaire items rated on a four-point Likert scale from one (strongly disagree) to four (strongly agree). The questions were grouped into four main privacy concern categories with an additional two questions for each category outlining whether their concern was heightened "if the person monitoring their privacy was a stranger" and "if the monitoring was happening without their awareness". A total of 448 responses were included in the analysis. There were 358 "before" responses and 90 "after" responses.

3.4. Data Analysis

Data analysis was conducted using IBM SPSS Statistics for Windows, Version 26. To explore intergroup differences in responses before and after the intervention, as well as potential gender-related variances, we employed *t*-tests and one-way ANOVA. Data were collected via an online survey tool, extracted, and tabulated using Microsoft Excel Version 2406 (Microsoft Corporation, Redmond, WA, USA). An independent sample *t*-test was used to compare gender differences and evaluate before and after intervention outcomes. The mean (M) and standard deviation (SD) values were also calculated. Additionally,

analysis of variance (ANOVA) was used to assess the magnitude of changes within each group, determining t-values (t) and statistically significant *p*-values (*p*). Eta-squared (η^2) was calculated as a measure of effect size. Tukey's post hoc test was conducted to facilitate pairwise comparisons between mean scores, particularly in assessing differences between before and after intervention results across schools. Statistical significance was set at * $p < 0.05$ and ** $p < 0.01$.

4. Results

Figure 1 presents the mean differences between males and females for each question set before and after the intervention. Females had the highest overall mean scores for the concerns about smartphone privacy questions, while males had the highest mean scores for knowledge of smartphone privacy settings and attitude towards smartphone privacy settings.

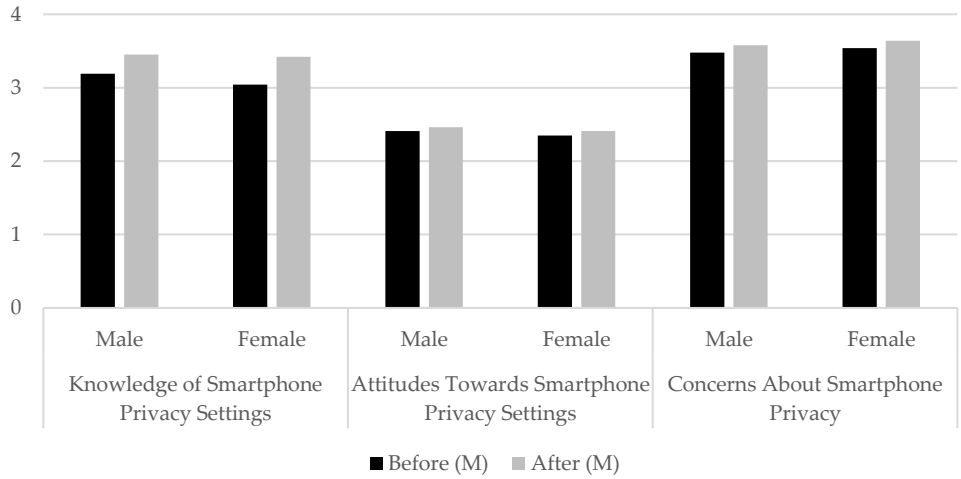

Figure 1. Gender before and after mean results for each survey questionnaire.

Table 2 presents the overall mean scores for each question set, comparing gender results for the before and after groups. Notably, all mean scores for both males and females increased in the after group compared to the before group.

Table 2. Overall mean statistics for each question set relating to each gender for the before and after groups.

		Before			After		
		n	**M**	**SD**	***n***	**M**	**SD**
Knowledge of Smartphone Privacy Settings	Male	147	3.19	0.53	46	3.45	0.44
	Female	213	3.04	0.55	51	3.42	0.45
Attitudes towards Smartphone Privacy Settings	Male	142	2.41	0.65	43	2.46	0.65
	Female	210	2.35	0.71	50	2.41	0.87
Concerns About Smartphone Privacy	Male	138	3.48	0.54	38	3.58	0.51
	Female	206	3.54	0.56	49	3.64	0.46

4.1. Knowledge of Smartphone Privacy Settings

Table 3 shows the mean and standard deviation for the knowledge of smartphone privacy settings questions based on both the male and female responses for the before and after groups. For the before group, males scored higher than females in 11 out of 13 knowledge of smartphone privacy settings questions. For the after group, males scored higher on seven out of 13 knowledge of smartphone privacy settings questions, which indicated a reduction in the differences between male and female knowledge levels post

the cyber safety lesson. The results indicate that both males and females possess a generally high level of knowledge regarding smartphone settings, with mean scores predominantly above 3. This suggests that both genders had a solid understanding of essential smartphone functionalities post the cyber safety intervention lesson.

Table 3. Mean results for knowledge of smartphone settings for male and female before and after groups.

			Before			After		
	Question	**Gender**	***n***	**M**	**SD**	***n***	**M**	**SD**
1	I know how to change my name on my smartphone	Male Female	147 213	3.39 3.41	0.73 0.76	46 51	3.76 3.76	0.43 0.47
2	I know how to switch off my location services	Male Female	147 213	3.48 3.50	0.66 0.69	46 51	3.63 3.67	0.57 0.59
3	I know what an SSID is	Male Female	147 213	2.53 2.01	0.97 0.93	46 51	2.93 2.47	0.93 0.99
4	I know how to switch off my Wi-Fi connection	Male Female	147 213	3.79 3.74	0.46 0.54	46 51	3.76 3.73	0.43 0.57
5	I know what my Wi-Fi is broadcasting	Male Female	147 213	3.07 2.77	0.87 0.93	46 51	3.50 3.35	0.66 0.72
6	I know what Bluetooth advertisement is	Male Female	147 213	2.90 2.81	0.89 0.92	46 51	3.30 3.29	0.73 0.78
7	I know how to switch off my Bluetooth connection	Male Female	147 213	3.76 3.71	0.49 0.55	46 51	3.67 3.75	0.47 0.48
8	I know how to prevent apps from tracking my activities	Male Female	147 213	3.31 3.05	0.70 0.84	46 51	3.43 3.49	0.69 0.67
9	I know how to prevent IP Address Tracking	Male Female	147 213	2.67 2.50	0.87 0.99	46 51	3.00 3.12	0.84 0.89
10	I know what my Bluetooth device is Broadcasting	Male Female	147 213	2.91 2.74	0.87 0.97	46 51	3.33 3.27	0.70 0.87
11	I know how to change my Bluetooth name	Male Female	147 213	3.21 3.08	0.85 0.89	46 51	3.52 3.57	0.66 0.67
12	I know how to manage my smartphone settings	Male Female	147 213	3.48 3.34	0.58 0.70	46 51	3.59 3.57	0.54 0.54
13	I know that my smartphone continually leaks information	Male Female	147 213	3.02 2.88	0.88 0.87	46 51	3.48 3.43	0.59 0.61

Before intervention, both male and female participants displayed a reasonably high level of knowledge about smartphone settings, with males generally scoring slightly higher across most questions. Males showed a higher familiarity with concepts like SSID (M = 2.53, SD = 0.97) and what their Wi-Fi is broadcasting (M = 3.07, SD = 0.87) compared to females (SSID: M = 2.01, SD = 0.93; Wi-Fi broadcasting: M = 2.77, SD = 0.93). Both genders had the highest confidence in knowing how to switch off their Wi-Fi connection (males: M = 3.79, SD = 0.46; females: M = 3.74, SD = 0.54). On average, males reported higher knowledge than females in nearly all aspects of smartphone settings. The most significant gaps were observed in technical areas, such as knowing what an SSID is and understanding what their Wi-Fi or Bluetooth devices broadcast.

After intervention, knowledge levels improved across all items for both genders, with noticeable increases in understanding complex concepts like preventing IP address tracking (males: M = 3.00, SD = 0.84; females: M = 3.12, SD = 0.89) and what Bluetooth devices broadcast (males: M = 3.33, SD = 0.70; females: M = 3.27, SD = 0.87). The gap between male and female knowledge narrowed after the intervention, particularly in areas like

changing Bluetooth names (males: M = 3.52, SD = 0.66; females: M = 3.57, SD = 0.67) and managing smartphone settings (males: M = 3.59, SD = 0.54; females: M = 3.57, SD = 0.54). Both genders saw increases in their mean scores, with the most substantial gains in areas where knowledge was initially lower, such as understanding SSID and IP address tracking.

The variability in responses was generally higher among females than males before the intervention, particularly in knowledge areas that were more technical, such as SSID and what their devices broadcast via Bluetooth or Wi-Fi. This suggests a broader range of understanding within the female group. Post the intervention, standard deviations generally decreased, indicating a more consistent level of knowledge across participants, with some areas showing significant convergence between males and females. For example, knowledge about preventing IP address tracking saw a notable reduction in variability for both genders, suggesting the intervention was effective in standardizing this understanding.

A two-sample *t*-test and ANOVA means analysis were performed to compare knowledge of smartphone privacy settings questions results between males (n = 147) and females (n = 213) in the before group. There was a significant difference in the means for question three relating to students "knowing what an SSID is" between males (M = 2.53, SD = 0.97) and females (M = 2.01, SD = 0.93); t(304) = 5.038, p = 0.000, η^2 = 0.067. There was a significant difference in the means for question five relating to students "knowing what their Wi-Fi is broadcasting" between males (M = 3.07, SD = 0.87) and females (M = 2.77, SD = 0.93); t(358) = 3.083, p = 0.002, η^2 = 0.026. There was a significant difference in the means for question eight relating to students "knowing how to prevent apps from tracking their activities" between males (M = 3.31, SD = 0.70) and females (M = 3.05, SD = 0.84); t(358) = 3.094, p = 0.002, η^2 = 0.026. There was a significant difference in the means for question 12 relating to students 'knowing how to manage their smartphone settings' between males (M = 3.48, SD = 0.58) and females (M = 3.34, SD = 0.70); t(358) = 2.003, p = 0.046, η^2 = 0.011.

A two-sample *t*-test and ANOVA means analysis were performed to compare knowledge of smartphone privacy settings questions results between males (n = 46) and females (n = 51) in the after group. There was only one significant difference in the means post the cybersecurity lesson and that was for question three relating to "students knowing what an SSID is" between males (M = 2.93, SD = 0.93) and females (M = 2.47, SD = 0.99); t(95) = 2.386, p = 0.019, η^2 = 0.056. There was no significant difference in the means for the remaining knowledge of smartphone privacy settings questions post the cybersecurity lesson, which indicates the cybersecurity lesson was effective in increasing both male and female knowledge of smartphone privacy settings.

The results indicate that Hypothesis 1 was supported, as males were found to have a higher level of knowledge of smartphone privacy settings than females. The intervention appears to have effectively elevated knowledge in these more technical aspects, reducing the gender gap observed before the intervention.

4.2. Attitudes towards Smartphone Privacy Settings

Table 4 presents the mean and standard deviation for responses to the attitude towards smartphone privacy settings questions, comparing male and female responses before and after the cyber safety lesson. In both the before and after groups, males and females scored three out of six questions higher. Females reported higher scores than males in the following areas: regularly switching off location services, regularly switching off Wi-Fi, in the after group only, switching off Bluetooth radio regularly and, in the before group only, concerns about smartphone security not being adequately addressed by their device.

Table 4. Mean results for attitude towards smartphone settings questions for male and female before and after groups.

			Before			After		
	Question	**Gender**	***n***	**M**	**SD**	***n***	**M**	**SD**
1	I don't use public Wi-Fis whenever they are available	Male	142	2.77	1.03	43	2.88	1.00
		Female	210	2.60	0.95	50	2.62	1.10
2	I don't use my real name as my smartphone name	Male	142	2.35	0.98	43	2.79	0.97
		Female	210	2.10	0.98	50	2.40	0.97
3	I switch off my location services regularly	Male	142	2.32	0.89	43	2.21	0.89
		Female	210	2.38	0.89	50	2.28	0.97
4	I switch off my Wi-Fi connection regularly	Male	142	2.15	0.85	43	2.07	0.74
		Female	210	2.22	0.92	50	2.30	1.04
5	I switch off my Bluetooth radio regularly	Male	142	2.43	0.96	43	2.28	0.80
		Female	210	2.31	0.95	50	2.40	1.01
6	I worry about smartphone security because my smartphone does not take care of it	Male	142	2.42	0.89	43	2.53	0.96
		Female	210	2.47	0.94	50	2.44	1.01

Before intervention, both males and females exhibited moderate levels of protective behaviours regarding smartphone use. Males were slightly more likely than females to avoid using public Wi-Fi (M = 2.77, SD = 1.03) and to not use their real name as their smartphone name (M = 2.35, SD = 0.98). However, neither group consistently engaged in practices like switching off location services or Bluetooth regularly, with mean scores around 2.3 for both genders. In comparison, in the post-intervention group, there were modest improvements in privacy protective behaviours. Both genders reported slight increases in not using their real name as their smartphone name (Males: M = 2.79, SD = 0.97; Females: M = 2.40, SD = 0.97). However, behaviours such as regularly switching off Wi-Fi and location services remained relatively unchanged, indicating persistent habits that may be harder to shift.

Males generally reported slightly higher protective behaviours than females across most questions before the intervention, particularly in avoiding public Wi-Fi and not using their real name as a smartphone name. The differences were small but consistent. Both genders showed small improvements in their protective behaviours, with males continuing to report slightly higher levels of these behaviours than females in the after group. The most notable improvement was in the practice of not using real names for smartphone identification, especially among males (M = 2.79, SD = 0.97).

The variability in responses was similar between males and females in the before group, with standard deviations indicating a moderate spread in protective behaviours. The highest variability was observed in the use of public Wi-Fi and the switching off of Bluetooth, suggesting diverse attitudes and practices within each gender group. Standard deviations remained relatively stable post-intervention, with no significant reductions in variability. This indicates that while mean behaviours improved slightly, the range of attitudes and practices among participants did not become more uniform.

A two-sample *t*-test and ANOVA means analysis were performed to compare knowledge of smartphone privacy settings questions results for males (n = 142) and females (n = 210) in the before group. There was a significant difference in the means for question two relating to whether students "didn't use their real name as their smartphone name" between males (M = 2.35, SD = 0.98) and females (M = 2.10, SD = 0.98); t(350) = 2.339, p = 0.020, η^2 = 0.048. There were no statistically significant differences for the attitudes towards smartphone privacy settings questions for after group between males and females indicating the educational intervention led to more consistent levels of privacy attitudes post the cybersecurity lesson.

The results indicate that Hypothesis 2 was not supported, as both males and females exhibited cautious attitudes toward smartphone settings, albeit in different areas. In the preintervention group, males showed more caution in technical aspects, while females

were more cautious regarding location privacy and general security concerns, aligning with expected gender differences in knowledge of smartphone settings and concerns about privacy.

The results supported Hypothesis 4, as the results underscore gender differences in knowledge and attitudes toward smartphone privacy and security, leading to increased privacy paradox for males. While both genders expressed moderate concern, males tended to score slightly higher on most measures. However, mean attitude scores were lower than knowledge scores, indicating a gap between awareness and behaviour. In the post-intervention group, this gap narrowed for means for both genders, with the difference between male and female scores decreasing from 0.09 to 0.02, though males continued to exhibit larger gaps between knowledge and attitudes.

4.3. Concerns About Smartphone Privacy

Table 5 shows the mean and standard deviation for concerns about smartphone privacy questions for males and females within the before and after group. Females scored higher means than males across the majority of the questions in the before and after group. Both male and female respondents exhibited a strong awareness of privacy concerns regarding their location data, with average scores consistently around 3.5 on a scale of one to four.

Table 5. Mean results for concerns about smartphone privacy for male and female before and after groups.

			Before			After		
	Question	**Gender**	***n***	**M**	**SD**	***n***	**M**	**SD**
1.	I would be concerned if someone knew where I was at any particular point in time	Male Female	138 206	3.24 3.23	0.80 0.80	38 49	3.47 3.49	0.65 0.65
1.1	I would be more concerned if that someone was a stranger	Male Female	138 206	3.49 3.64	0.70 0.62	38 49	3.55 3.69	0.69 0.51
1.2	I would be even more concerned if I didn't know it was happening	Male Female	138 206	3.54 3.59	0.62 0.65	38 49	3.61 3.67	0.64 0.47
2	I would be concerned if someone knew where I was at the same time every day	Male Female	138 206	3.43 3.44	0.66 0.70	38 49	3.55 3.59	0.60 0.54
2.1	I would be more concerned if that someone was a stranger	Male Female	138 206	3.56 3.66	0.64 0.64	38 49	3.61 3.71	0.50 0.50
2.2	I would be more concerned if I didn't know it was happening	Male Female	138 206	3.57 3.60	0.60 0.66	38 49	3.55 3.69	0.69 0.47
3	I would be concerned if someone knew what my regular travel route to school was	Male Female	138 206	3.25 3.34	0.74 0.80	38 49	3.55 3.55	0.65 0.58
3.1	I would be more concerned if that someone was a stranger	Male Female	138 206	3.50 3.60	0.66 0.69	38 49	3.68 3.71	0.47 0.50
3.2	I would be more concerned if I didn't know it was happening	Male Female	138 206	3.52 3.57	0.61 0.66	38 49	3.58 3.65	0.60 0.48
4	I would be concerned if someone was able to plot my location on a Google map at a particular point in time	Male Female	138 206	3.49 3.56	0.64 0.65	38 49	3.53 3.59	0.65 0.57
4.1	I would be concerned if someone could plot my location on a Google map over a period of time	Male Female	138 206	3.53 3.55	0.63 0.69	38 49	3.61 3.67	0.60 0.47
4.2	I would be more concerned if that someone was a stranger	Male Female	138 206	3.54 3.64	0.64 0.65	38 49	3.58 3.67	0.55 0.52
4.3	I would be more concerned if I didn't know it was happening	Male Female	138 206	3.56 3.61	0.62 0.66	38 49	3.63 3.61	0.54 0.61

The highest concerns were related to the involvement of strangers and the lack of knowledge about being tracked, with males and females both expressing significant unease about these scenarios (e.g., "I would be more concerned if that someone was a stranger": males M = 3.49, SD = 0.70; females M = 3.64, SD = 0.62). There was a slight increase in concern levels, post-intervention, especially among females. For example, female concern

about someone knowing where they were at any particular point in time increased slightly (M = 3.49, SD = 0.65), as did concern about strangers having access to their location data over time (M = 3.67, SD = 0.47). Males also showed slight increases, but the changes were generally smaller.

The means indicate that females were generally more concerned about location privacy than males, particularly when considering scenarios involving strangers or unknown tracking in the before group. For instance, females reported higher concern about a stranger knowing their location (M = 3.64) compared to males (M = 3.49). Both genders exhibited small increases in concern levels post-intervention, with females maintaining slightly higher concern levels than males across most variables. Notably, the concern about location tracking by strangers remained one of the highest-rated items for both groups (males: M = 3.58; females: M = 3.67).

Standard deviations across the board were relatively low in the before group, suggesting a consensus among participants regarding their concerns about location privacy. The highest variability was observed in responses to concerns about what a stranger might know, indicating some differences in perception among participants. The standard deviations remained stable post-intervention, with only minor changes, indicating that the intervention did not significantly alter the distribution of responses. Females, in particular, showed a slight decrease in variability, suggesting a more uniform concern level post-intervention.

A two-sample *t*-test and ANOVA means analysis were performed to compare concerns about smartphone privacy questions results for males (n = 138) and females (n = 206) in the before group. There was a significant difference in the means for the second question in the first category of whether students "would be more concerned if a stranger knew where they were at any particular point in time" between males (M = 3.49, SD = 0.70) and females (M = 3.64, SD = 0.62); t(271) = −2.015, p = 0.045, η^2 = 0.048. There was no significant difference in the means for any of the other questions in the male and female groups for concerns about smartphone privacy. There were no statistically significant differences for the concerns about smartphone privacy questions for after group between males and females, indicating the educational intervention had some effect on consistency in attitude towards privacy post the cybersecurity lesson.

The results support Hypothesis 3, with females exhibiting higher levels of concern about smartphone privacy settings, especially related to personal safety and strangers, compared to males. The intervention successfully increased perceived threats for both genders, narrowing the preintervention gender gap.

The results also supported Hypothesis 5, as the targeted educational intervention reduced gender differences in knowledge, attitudes, and concerns regarding smartphone privacy. Post-intervention, responses from male and female adolescents were more consistent across all question sets, suggesting that educational interventions can effectively reduce gender disparities in smartphone privacy risk.

5. Discussion

5.1. Knowledge of Smartphone Privacy Settings

The results revealed that, prior to the intervention, females reported lower knowledge of smartphone settings compared to males. However, after the cyber safety lessons, both genders exhibited significant improvements in knowledge, leading to more consistent levels across genders. This finding highlights the effectiveness of the intervention in enhancing students' understanding of smartphone security settings, aligning with PMT [12], which suggests that perceived threat and efficacy can drive behavioural change.

Despite overall improvements in knowledge across both genders, technical aspects like SSIDs and broadcasting settings remained challenging, particularly for females. Males exhibited slightly better technical understanding, supporting previous findings on gender differences in confidence and technical knowledge [13]. The results suggest that targeted interventions may be necessary to bridge this gap. Interestingly, even males—who initially

reported higher confidence in their knowledge—demonstrated significant improvement, suggesting the value of continual reinforcement of PMT concepts for addressing ongoing behaviour change [12].

While the results showed that the intervention helped equalize knowledge between genders, the results also indicate that post-intervention, females rated their knowledge on par with males, highlighting that when equipped with equal knowledge, both genders can perform similarly. This suggests that prior to the lesson, females may have lacked confidence rather than ability. This finding aligns with previous research, which suggests that a lack of confidence may lead females to perceive themselves as less knowledgeable, even when their actual skills are comparable to males [21]. Social biases often portray men as being more proficient in technology and this is likely to contribute to females self-reporting lower confidence in technological skills [19,20].

5.2. Attitudes towards Smartphone Privacy Settings

Despite increased awareness, the persistence of behaviours like keeping Wi-Fi and Bluetooth enabled underscores the privacy paradox [32], where knowledge does not always translate into protective actions. These results emphasize the need for educational programs to not only increase knowledge but also actively change behaviours regarding smartphone privacy management. The gender differences observed in attitudes toward privacy management suggest that education should target specific concerns and behaviours. Programs should focus not only on increasing knowledge of smartphone privacy settings but also on shaping attitudes toward actively managing these settings.

Future research could explore the psychological or contextual factors that contribute to the persistence of risky behaviours, such as the reluctance to disable Wi-Fi or Bluetooth. Additionally, evaluating the impact of different educational interventions, such as gamified learning or peer-led discussions, could provide valuable insights into improving behaviours. Additionally, evaluating whether these risky behaviours correlate with actual privacy breaches would offer a more comprehensive understanding of the practical effectiveness of these educational interventions in promoting cyber safety. Although targeted interventions resulted in modest improvements in behaviours, such as avoiding real-name use for smartphone identification, other behaviours—like regularly disabling location services or Wi-Fi connections—remained more resistant to significant change. This suggests that ongoing education is crucial to not only raise awareness but also to motivate more consistent behavioural changes. Tailoring educational messages to address specific misconceptions or barriers could significantly enhance the effectiveness of these interventions.

The results underscore gender differences in the privacy paradox [32]. While both genders expressed moderate concern, males tended to score slightly higher on most measures. However, mean attitude scores were lower than knowledge scores, indicating a gap between awareness and behaviour. This aligns with previous research showing that while females perceive greater privacy risks, especially related to personal data misuse and harassment, their attitudes may not always translate into protective actions [24,37], and males have a tendency to share personal information more freely on social media, potentially leading to less effective use of privacy settings [24].

5.3. Concerns About Smartphone Privacy

The findings highlight gender differences in privacy concerns related to location data. Both genders showed moderate concern about their whereabouts being known, with males slightly more concerned overall, but females expressing greater concern when strangers were involved, aligning with other research on gender and physical safety concerns [30]. This concern persisted across scenarios, such as being tracked daily or having their travel route known.

Both genders consistently demonstrated awareness of location tracking risks. Females were particularly worried about being tracked via Google Maps, especially by strangers or without their knowledge. These results suggest that females' concerns are often linked

to personal safety, emphasizing the need for education that addresses both privacy and physical security risks.

The findings highlight the need for tailored cyber education that not only addresses knowledge gaps but also focuses on motivating protective behaviours, particularly where privacy concern gaps persist. Future interventions should prioritize educating adolescents about location privacy, especially in relation to personal safety concerns for being tracked by unknown individuals. While self-reported concern levels were already high, targeted education can further increase awareness and promote safer behaviours. Future interventions should not only raise awareness but also teach practical strategies for managing location privacy, like effective use of privacy settings and understanding the implications of location sharing. Further research could explore whether increased concern leads to more cautious use of location services, the factors driving higher concern among females, and how peer influence shapes attitudes toward location privacy. This could help in designing more impactful educational programs. Teaching practical strategies for managing location privacy and emphasizing the implications of location sharing will be essential for fostering safer digital practices among adolescents.

6. Conclusions

This study contributes to the understanding of how gender differences influence privacy behaviours among adolescents and underscores the need for tailored educational interventions to address these disparities. Our study found that before the cyber safety intervention, females reported lower knowledge of smartphone settings than males. After the lesson, this gap narrowed, with both genders demonstrating more consistent understanding. Males still had a slight edge in technical areas like SSIDs and broadcasting settings, highlighting the need for targeted interventions to support female students in these areas. Both genders showed lower attitudes towards smartphone privacy compared to knowledge, with males displaying the largest gap, reflecting the privacy paradox. Females expressed greater concern regarding location privacy, especially when tracked by unknown individuals, indicating that while both genders are aware of risks, females perceive them more acutely.

The results suggest that targeted educational programs can effectively enhance adolescents' knowledge, attitudes, and concerns about smartphone privacy, particularly in technical areas where gender gaps exist. The narrowing of the knowledge gap across both genders post-intervention underscores the importance of such programs in building essential digital literacy skills, though persistent differences highlight the need for continued, focused efforts. Educational interventions should not only address the knowledge gap but also focus on changing behaviours related to privacy. Adolescents need practical skills to manage privacy settings, understand data-sharing risks, and recognize phishing attempts. By acknowledging gender differences, digital literacy programs can be tailored to meet distinct needs. These differences are influenced by education, cultural norms, access to technology, and personal interests.

These findings highlight the potential for targeted educational interventions to significantly improve smartphone privacy knowledge and reduce risky behaviours among adolescents. Schools can incorporate cyber safety lessons into their curricula, supported by policies that mandate regular education on managing smartphone privacy settings and mitigating data leakage. The demonstrated reduction in data leakage post-lesson suggests real behavioural change, with implications for shaping broader government and advocacy programs. Tailored interventions, particularly for female students who were found to be more at risk, can further enhance the effectiveness of these initiatives. Ultimately, these efforts could lead to a generation of digitally literate adolescents better equipped to navigate online risks, informing both school policies and national cyber safety strategies.

A limitation of this study was the small size of the post-lesson survey group and the lack of long-term impact assessment. Future research should ensure that all prelesson survey participants also complete the post-lesson survey and conduct longitudinal studies

to evaluate the lasting effectiveness of cyber safety education. Another limitation is understanding existing levels of technology use and psychological or contextual factors that contribute to the persistence of certain risky behaviours, such as the reluctance to switch off Wi-Fi or Bluetooth. Further research might also examine whether these behaviours correlate with actual incidents of privacy breaches, offering a more comprehensive understanding of the effectiveness of these practices. Future investigations could shed light on persistent knowledge gaps, especially concerning SSIDs and technical aspects, and understanding students' prior technology experiences could provide valuable insights.

Author Contributions: Conceptualization, Y.A.-S.; methodology, Y.A.-S.; software, Y.A.-S.; validation, Y.A.-S.; formal analysis, J.M.; investigation, Y.A.-S.; resources, Y.A.-S.; data curation, Y.A.-S. and J.M.; writing—original draft preparation, J.M.; writing—review and editing, Y.A.-S.; visualization, J.M.; supervision, Y.A.-S.; project administration, Y.A.-S.; funding acquisition, Y.A.-S. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded through the Australian eSafety Commissioner's Online Safety Grants Program.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Charles Sturt University Human Research Ethics Committee (protocol code H23489 and date of approval 4/4/2023).

Informed Consent Statement: I confirm that "Informed consent was obtained from all subjects involved in the study".

Data Availability Statement: The datasets presented in this article are not readily available because the study involved children. Requests to access the datasets should be directed to yalsaggaf@csu.edu.au.

Acknowledgments: The authors wish to thank Alan Ibbett and acknowledge his contribution to this study. This study builds on his earlier work for his doctoral thesis project.

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

References

1. Taylor, P. Percentage of Teenagers in the United States Who Have Access to a Smartphone at Home as of October 2023, by Gender. 28 February 2024. Available online: https://www.statista.com/statistics/256501/teen-cell-phone-and-smartphone-ownership-in-the-us-by-gender/ (accessed on 14 August 2024).
2. Boerman, S.; Kruikemeier, S.; Borgesius, F. Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data. *Commun. Res.* **2021**, *48*, 953–977. [CrossRef]
3. Smit, E.G.; Van Noort, G.; Voorveld, H.A.M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Comput. Hum. Behav.* **2014**, *32*, 15–22. [CrossRef]
4. Baruh, L.; Secinti, E.; Zeynep, C. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *J. Commun.* **2017**, *67*, 26–53. [CrossRef]
5. Chai, S.; Das, S.; Rao, H. Factors Affecting Bloggers' Knowledge Sharing: An Investigation across Gender. *J. Manag. Inf. Syst.* **2011**, *28*, 309–341. [CrossRef]
6. Richter, A.; Adkins, V.; Selkie, E. Youth Perspectives on the Recommended Age of Mobile Phone Adoption: Survey Study. *JMIR Pediatr. Parent.* **2022**, *5*, e40704. [CrossRef]
7. 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]
8. Radesky, J.; Weeks, H.M.; Schaller, A.; Robb, M.; Mann, S.; Lenhart, A. *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*; Common Sense: San Francisco, CA, USA, 2023.
9. Romer, D. Adolescent risk taking, impulsivity, and brain development: Implications for prevention. *Dev. Psychobiol.* **2010**, *52*, 263–276. [CrossRef]
10. Youn, S.; Hall, K. Gender and Online Privacy Among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. *Cyberpsychol. Behav.* **2008**, *11*, 763–765. [CrossRef]
11. Dempsey, J.; Sim, G.; Cassidy, B. Designing for GDPR—Investigating Children's Understanding of Privacy: A Survey Approach, In Proceedings of the BCS-HCI'18: 32nd Human Computer Interaction Conference, Belfast, UK, 2–6 July 2018.
12. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *J. Psychol. Interdiscip. Appl.* **1975**, *91*, 93–114. [CrossRef]
13. Saunders, M.A. The Role of Video Game Play, Gender Roles, and Career Decision Self-Efficacy in Development of STEM Career Interests & Motivation. Doctoral Dissertations, Louisiana Tech University, Ruston, LA, USA, 2021.

14. Campbell, K. Gender and Technology: Social Context and Intersectionality. In *Handbook of Research in Educational Communications and Technology*; Bishop, M.J., Boling, E., Elen, J., Svihla, V., Eds.; Springer: Cham, Switzerland, 2020. [CrossRef]
15. Wang, M.; Degol, J.L. Gender Gap in Science, Technology, Engineering, and Mathematics (STEM): Current Knowledge, Implications for Practice, Policy, and Future Directions. *Educ. Psychol. Rev.* **2017**, *29*, 119–140. [CrossRef]
16. Stewart-Williams, S.; Halsey, L.G. Men, women and STEM: Why the differences and what should be done? *Eur. J. Personal.* **2021**, *35*, 3–39. [CrossRef]
17. Carranza, E.; Das, S.; Kotikula, A. *GenderBased Employment Segregation: Understanding Causes and Policy Interventions*; World Bank: Washington, DC, USA, 2023.
18. Christensen, M.A. Tracing the Gender Confidence Gap in Computing: A Cross-National Meta-Analysis of Gender Differences in Self-Assessed Technological Ability. *Soc. Sci. Res.* **2023**, *111*, 102853. [CrossRef] [PubMed]
19. He, J.; Freeman, L. Are Men More Technology-Oriented Than Women? The Role of Gender on the Development of General Computer Self-Efficacy of College Students. *J. Inf. Syst. Educ.* **2019**, *21*, 672.
20. Marja, L.; Overå, S. Are There Differences in Video Gaming and Use of Social Media among Boys and Girls?-A Mixed Methods Approach. *Int. J. Environ. Res. Public Health* **2021**, *18*, 6085. [CrossRef]
21. Robinson, K.A.; Perez, T.; White-Levatich, A.; Linnenbrink-Garcia, L. Gender Differences and Roles of Two Science Self-Efficacy Beliefs in Predicting Post-College Outcomes. *J. Exp. Educ.* **2022**, *90*, 344–363. [CrossRef]
22. Denejkina, A. Generative AI—Gender Gap Identified in Skills and Confidence. 25 August 2023. Available online: https://youthinsight.com.au/education/generative-ai-gender-gap-identified-in-skills-and-confidence/#:~:text=Here,%20men%20were%20more%20likely,62%20per%20cent%20of%20girls (accessed on 14 August 2024).
23. Sebastián-Tirado, A.; Félix-Esbrí, S.; Forn, C.; Sanchis-Segura, C. Are gender-science stereotypes barriers for women in science, technology, engineering, and mathematics? Exploring when, how, and to whom in an experimentally-controlled setting. *Front. Psychol.* **2023**, *14*, 1219012. [CrossRef]
24. Tifferet, S. Gender differences in privacy tendencies on social network sites: A meta-analysis. *Comput. Hum. Behav.* **2018**, *93*, 1–12. [CrossRef]
25. Gruzd, A.; Hernández-García, Á. Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media. *Cyberpsychol. Behav. Soc. Netw.* **2018**, *21*, 418–428. [CrossRef]
26. eSatefy Commissioner. State of Play—Youth, Kids and Digital Dangers, Australian Government. 3 May 2018. Available online: https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf (accessed on 14 August 2024).
27. Office of the Australian Information Commissioner. Australian Community Attitudes to Privacy Survey 2020. Australian Government. September 2020. Available online: https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020 (accessed on 14 August 2024).
28. Office of the Australian Information Commissioner. Australian Community Attitudes to Privacy Survey 2023, Australian Government. 8 August 2023. Available online: https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023 (accessed on 14 August 2024).
29. Savoia, E.; Harriman, N.W.; Su, M.; Cote, T.; Shortland, N. Adolescents' Exposure to Online Risks: Gender Disparities and Vulnerabilities Related to Online Behaviors. *Int. J. Environ. Res. Public Health* **2021**, *18*, 5786. [CrossRef]
30. Livingstone, S.; Stoilova, M.; Nandagiri, R. *Children's Data and Privacy Online: Growing Up in a Digital Age. An Evidence Review*; London School of Economics and Political Science: London, UK, 2019.
31. Coopamootoo, K.; Ng, M. "Un-Equal Online Safety?" A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns. In Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, USA, 9–11 August 2023.
32. Solove, D. The Myth of the Privacy Paradox. *Georg. Wash. Law Rev.* **2021**, *89*, 1. [CrossRef]
33. Svirsky, D. Why Do People Avoid Information About Privacy? *J. Law Innov.* **2021**, *2*, 2.
34. Hargittai, E.; Marwick, A. "What Can I Really Do?": Explaining the Privacy Paradox with Online Apathy. *Int. J. Commun.* **2016**, *10*, 21.
35. Quayyum, F.; Cruzes, D.S.; Jaccheri, L. Cybersecurity awareness for children: A systematic literature review. *Int. J. Child-Comput. Interact.* **2021**, *30*, 100343. [CrossRef]
36. Pratama, A.R.; Firmansyah, F.M. Until you have something to lose! Loss aversion and two-factor authentication adoption. *Appl. Comput. Inform.* 2021; *ahead-of-print*.
37. Dhir, A.; Torsheim, T.; Pallesen, S.; Andreassen, C.S. Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? *Front. Psychol.* **2017**, *8*, 815. [CrossRef]
38. Kaarakainen, M.; Hutri, H. Participating with a Real Name, a Nickname or by Being Anonymous?—Anonymous and Identifiable Users' Skills and Internet Usage Habits, 2016. Available online: http://urn.fi/URN:ISBN:978-952-03-0307-5 (accessed on 1 August 2024).
39. Petronio, S.; Caughlin, J.P. Communication Privacy Management Theory: Understanding Families. In *Engaging Theories in Family Communication: Multiple Perspectives*; Braithwaite, D.O., Baxter, L.A., Eds.; Routledge: New York, NY, USA, 2006; pp. 35–49. [CrossRef]

40. Meier, Y.; Krämer, N.C. The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. *Commun. Res.* **2024**, *51*, 178–202. [CrossRef]
41. Peng, Z. A privacy calculus model perspective that explains why parents sharent. *Inf. Commun. Soc.* **2023**, 1–24. [CrossRef]
42. Khan, N.F.; Ikram, N.; Murtaza, H.; Javed, M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Comput. Secur.* **2023**, *125*, 103049. [CrossRef]
43. Lee, A.Y.; Hancock, J.T. Developing digital resilience: An educational intervention improves elementary students' response to digital challenges. *Comput. Educ. Open* **2023**, *5*, 100144. [CrossRef]
44. Finkelhor, D.; Jones, L.; Mitchell, K. Teaching privacy: A flawed strategy for children's online safety. *Child Abus. Negl.* **2021**, *117*, 105064. [CrossRef]