Journal of
*Cybersecurity and Privacy*

MDPI

*Article*

# Individual Differences in Psychological Stress Associated with Data Breach Experiences

**Christopher R. Sears * and Daniel R. Cunningham**

Department of Psychology, University of Calgary, 2500 University Drive N.W., Calgary, AB T2N 1N4, Canada; daniel.cunningham1@ucalgary.ca
* Correspondence: sears@ucalgary.ca

**Abstract:** Data breach incidents are now a regular occurrence, with millions of people affected worldwide. Few studies have examined the psychological aspects of data breach experiences, however, or the individual differences that influence how people react to these events. In this study, we examined the psychological stress associated with a personal experience with a data breach and several individual differences hypothesized to modulate such stress (age, gender, digital security awareness and expertise, trait anxiety, negative emotionality, and propensity to worry). A student sample (*N* = 166) and a community sample (*N* = 359) completed an online survey that asked participants to describe their most serious data breach and then complete the Impact of Events Scale—Revised (IES-R) to answer specific questions about the nature of the stress they experienced after the breach. Standard measures of trait anxiety, negative emotionality, and propensity to worry were also completed. A Data Breach Severity Index (DBSI) was created to quantify the invasiveness and consequences of each participant's data breach. Hierarchical multiple regression analyses were used to identify demographic variables and psychological characteristics predictive of IES-R scores while controlling for DBSI scores. As expected, more invasive and consequential data breaches were associated with higher IES-R scores (greater data-breach-induced stress). Women had higher IES-R scores than men, and this difference persisted after controlling for gender differences in anxiety, negative emotionality, and propensity to worry. Greater daily social media use was associated with higher IES-R scores, whereas higher digital security expertise was associated with lower IES-R scores. The results illuminate several relationships between demographic and psychological characteristics and data-breach-induced stress that should be investigated further.

**Keywords:** data breach; psychology; stress; anxiety; digital security

check for updates

**Citation:** Sears, C.R.; Cunningham, D.R. Individual Differences in Psychological Stress Associated with Data Breach Experiences. *J. Cybersecur. Priv.* **2024**, *4*, 594–614. https://doi.org/10.3390/jcp4030028

Academic Editor: Danda B. Rawat

Received: 14 April 2024
Revised: 10 August 2024
Accepted: 13 August 2024
Published: 20 August 2024

## 1. Introduction

A data breach can be defined as an intentional or unintentional release of confidential information to an untrusted environment [1] or when unauthorized individuals access and/or remove personal information from where it is stored [2]. Most modern data breaches involve unauthorized access to protected information stored electronically. Examples include the hacking of bank and credit accounts, social media profiles, smartphone applications, and online shopping accounts. Data breach events are becoming more common as online banking, shopping, record-keeping, and social media use become ubiquitous [3]; the increase in personal information stored online has increased the risk of unauthorized access to personally identifiable information and other sensitive data. Recent reports indicate that data breaches have become a significant security issue in the United States, with estimates reaching 38 billion records exposed in the last decade and over 300 million persons affected in 2023 alone [4]. Many large and well-known companies such as Facebook, Equifax, Capital One, Target, Marriott, and Ticketmaster have had their customer data stolen. In Canada, the Office of the Privacy Commissioner reported that over 28 million Canadians were affected by a data breach between November 2018 and

November 2019 [5]. A data breach can have serious negative consequences for an organization, and several studies have examined the impact of data breaches on a company's market value [6–8] and customer perceptions and behavior [9–11].

Although there has been widespread media attention to many data breach incidents, few studies have examined the psychological aspects of these events. Media reports suggest that some data breach incidents are linked to significant psychological distress. One example is the 2015 Ashley Madison data breach [12]. The customer database of the extramarital dating website was stolen, and the company's 32 million user records included subscriber names, home addresses, email addresses, credit card transactions, private messages, and other personally identifying information, as well as sexual preferences and fantasies [13,14]. The database was subsequently available online, and the public shaming, embarrassment, and extortion attempts had detrimental effects on many careers and relationships and were linked to several suicides [15,16].

One of the first studies to consider the psychological aspects of a data breach experience was published in 2009 [17]. The purpose of the study was to examine factors that influenced adolescent internet users' private information-sharing behavior. The researchers administered a survey to 285 American adolescents (the average age was 13.6 years) who were attending technology camps in 2006 and 2007. The researchers created a measure of "information privacy anxiety" and examined whether it was related to previous experience with online privacy breaches (a "hacking incident"). Information privacy anxiety was defined as "anxiety toward becoming a target for bullying on the internet, and anxiety toward computer and privacy incidents". Being a victim of a hacking incident significantly predicted anxiety about possible future hacking, as measured by the information privacy anxiety measure.

A more recent study, published in 2016, examined adults' anxiety and stress when thinking about different types of data breach incidents [18]. A community sample of 304 adults completed an online survey, and one of the first questions asked about the participants' resting or baseline anxiety ("How worried, stressed, or anxious do you feel right now?"); responses were made on a scale from 1 ("not at all") to 7 ("very much"). Subsequent questions inquired about anxiety related to specific types of data breaches, which the researchers defined as "data breach anxiety". Participants were asked "How worried, anxious, or stressed do you feel about the following events happening to you?" There were 10 data breach types (e.g., "email hacked"; "financial account hacked into"; "personal information posted by others to the internet"; "theft of internet account password"), and, for each type, the respondent used a seven-point scale ("not at all" to "very much") to rate their anxiety. The researchers' statistical analyses used the difference between the resting anxiety ratings and the ratings for each of the 10 data breach types to assess participants' anxiety for each type of data breach (i.e., the extent to which a data breach anxiety exceeded resting anxiety). For 9 of the 10 data breach types, data breach anxiety was higher than resting anxiety ($M = 2.45$), with higher data breach anxiety ratings for more invasive and potentially consequential breaches (e.g., for "email hacked", $M = 3.96$; for "financial account hacked into", $M = 5.35$). Many participants had personal experience with a data breach: 33% indicated their email had been compromised, and 19% indicated their social media account had been hacked. The researchers examined how such personal experiences influenced data breach anxiety and found no associations. It was also found that various electronic security precautions (e.g., "code on phone"; "encryption on computer") were not predictive of data breach anxiety.

A similar 2017 study sought to identify variables that could predict anxiety about data hacking and the association between this anxiety and the use of digital privacy protection behavior [19]. The study recruited a community sample of 305 adults who completed an online survey. The survey included the Generalized Anxiety Disorder-7 (GAD-7) scale, a widely used clinical measure [20] that the researchers used to measure resting or baseline anxiety. The survey also included a measure of data breach anxiety, which the researchers referred to as a data hacking anxiety scale (GAD-7-HACK). Participants read a short description of recent data breach incidents ("People have had their email, cloud accounts, social media accounts, banking and other internet accounts hacked, as well as sensitive/nude photos released") and were then asked "When thinking about these types of data breaches happening to you, how much are you bothered by the following problems?" There were seven problems listed, and these were taken from the GAD-7 (e.g., "Feeling nervous, anxious, or on edge"; "Not being able to stop or control worrying"; "Worrying too much about different things"). Each problem was rated on a scale from "not at all" to "extremely". Note that this measure of data breach anxiety does not probe a respondent's anxiety about specific types of data breaches (e.g., email hacked vs. financial account hacked). Instead, it asks respondents to think about data breaches in general and to indicate how much they are bothered by specific anxiety symptoms (e.g., "Feeling nervous, anxious, or on edge") while doing so. Prior experience with a data breach was found to be weakly associated with hacking anxiety, such that hacking anxiety (as measured by the GAD-7-HACK) was higher in those who reported such experience. It was also found that hacking anxiety was generally higher in those with IT-related occupations. Hacking anxiety was related to digital privacy protection behavior, and the researchers concluded that some level of anxiety could help motivate online privacy protection without becoming an "overburdening level of anxiety".

One other study used the GAD-7-HACK measure to examine cross-cultural and gender associations with data hacking anxiety [1]. The sample consisted of 389 American and 216 Korean college students who completed an online survey in 2015. Interestingly, the American students' average resting anxiety (GAD-7) scores ($M$ = 10.02) were higher than their mean GAD-7-HACK scores ($M$ = 4.85), suggesting a low level of hacking anxiety among these participants. The researchers inquired about respondents' personal experiences with data hacking and found that 42% of the American students and 52% of the Korean students reported having had their electronic data accessed without authorization or had their email, social media, or bank account compromised or hacked. Their analyses revealed a weak association between personal experience with a data breach and hacking anxiety, with hacking anxiety being higher in students with such experiences.

### *The Present Study*

Only a few studies have examined data breaches from a psychological perspective, but these investigations have contributed to researchers' understanding of some of the individual differences associated with psychological responses to a data breach. Previous studies also share several limitations, however, the first being the difficulty of making cause-and-effect inferences between a data breach incident and subsequent psychological reactions (e.g., increased anxiety). This is because previous studies have not assessed participants' psychological responses to their own data breach experiences. Instead, they have measured anxiety in response to imagined data breaches [18] or media reports of data breach incidents [1,19]. Although some studies did inquire about participants' personal experiences with a data breach [21], participants' psychological reactions to their own experiences were not examined. A second limitation of previous studies is the focus on anxiety. While the possibility of heightened anxiety is a potentially significant consequence of a data breach experience, many other psychological reactions could be evaluated (e.g., stress, worry, depression, fear, and anger). A third limitation is that psychological differences among participants, particularly those that could moderate responses to data breach incidents (e.g., individual differences in propensity to worry), have not been examined. A more multi-dimensional evaluation is necessary to build and expand on previous research and further researchers' understanding of the breadth of reactions to data breach experiences.

With this goal in mind, the present study examined the psychological stress experienced after a personal experience with a data breach incident and individual differences that could moderate that stress. Stress has a significant influence on mood, well-being, and health, and chronic stress is associated with both depression and anxiety [22,23], thus making it an important psychological response to consider. The study recruited individuals who had experienced a data breach and asked them to describe their most serious data breach in detail. They then completed the Impact of Events Scale—Revised (IES-R) [24,25] to answer specific questions about the types of stress they experienced due to their data breach (e.g., "I felt irritable and angry"; "I had waves of strong feelings about it"). The IES-R is a widely used self-report measure of event-specific stress with good psychometric properties.

Data breaches vary in terms of how personal/sensitive the stolen data are and whether there are actual or potential financial repercussions, and thus the nature of a data breach should be taken into account when trying to understand individual differences in participants' reactions (e.g., unauthorized access to sensitive digital photos would be expected to create more psychological stress than unauthorized access to a hotel membership account). To do so, we created a Data Breach Severity Index (DBSI) to quantify the severity of each participant's data breach based on their description of the incident. We expected that data breaches with higher DBSI scores would be associated with more psychological stress (higher IES-R scores). Controlling for data breach severity in the analyses assisted with identifying individual differences that moderated data-breach-induced stress independently of the stress attributable to the data breach itself.

We hypothesized that several individual differences would moderate the stress participants experienced due to their data breach. First, because previous studies have documented associations between data breach anxiety and a history of data breach victimization [1,17], we hypothesized that participants with higher levels of trait anxiety (as measured by the GAD-7) would report greater data-breach-induced stress (higher IES-R scores). Second, we hypothesized that data-breach-induced stress would positively correlate with negative emotionality, as measured by the Big Five Inventory for negative emotionality (BFI-2) [26]. Negative emotionality is a personality trait that reflects individual differences in the intensity and frequency of negative emotions and was expected to moderate the severity of stress experienced after a data breach incident. Third, we hypothesized that data-breach-induced stress would positively correlate with participants' propensity to worry, as measured by the Penn State Worry Questionnaire (PSWQ) [27], with stress responses being more severe for individuals who experience worry more frequently and intensely than others. Fourth, we hypothesized that participants' digital security expertise and practices would be associated with their stress responses, given the previous finding that individuals with higher levels of hacking anxiety are more likely to practice digital security behaviors [19]. Finally, with respect to demographic variables, we hypothesized that women would report higher levels of data-breach-induced stress than men given the documented gender differences in anxiety [28], negative emotionality [26,29], and propensity to worry [27], all of which are related to stress responses.

## 2. Materials and Methods

### 2.1. Participants

The study received ethics approval from an institutional research ethics review board prior to data collection (REB19-1927). A total of 914 participants consented to complete an online survey about their experiences with data breach incidents. Participants were recruited using the Amazon Mechanical Turk (MTurk) system, an online crowdsourcing marketplace with an option for survey participation, and from a research participation website for students administered by the Department of Psychology at the University of Calgary (Canada). Prospective participants were provided with a description of the study and procedure, and those who consented to participate then followed a link to the study website hosted on Qualtrics (www.qualtrics.com). MTurk participants received USD 3.00 as compensation. MTurk participants were "master workers"; those who have demonstrated a high level of accuracy and reliability in their past tasks on the platform. Almost all (99.4%) of the MTurk participants reported their country of residence as the United States. Student participants received bonus credit (1% of their final grade) that could be applied to a psychology course they were registered in.

### *2.2. Measures*

The online survey was divided into nine sections, which consisted of (1) demographic questions, (2) questions on the use of digital devices and online services, (3) questions on digital security expertise and practices, (4) self-reported experiences with anxiety and depression, (5) the Big Five Inventory for negative emotionality (BFI-2) [26], (6) the Generalized Anxiety Disorder seven-item inventory (GAD-7) [20], (7) the Penn State Worry Questionnaire (PSWQ) [27], (8) questions about personal experiences with data breaches and post-data breach behaviors, and (9) the Impact of Event Scale Revised (IES-R) [24,25], which was completed in reference to the most severe data breach incident described by the participant. Two attention checks were embedded in the survey ("Please select Strongly Agree"). The survey required 30–45 min to complete.

#### 2.2.1. Demographic Questions

Demographic information collected included country of residence, age, gender, cultural/ethnic background, student status, employment, marital status, education (certification pursuing, certifications obtained, total years of education), and number of drinks of alcohol consumed per day.

#### 2.2.2. Use of Digital Devices and Online Services

Participants' use of digital devices and online services was assessed with questions on how many hours per day they spent on smartphones, social media sites, and internet browsers. Participants were also asked about their use of online banking, online banking apps on a smartphone, alternative payment apps (e.g., Android Pay), the number of phone applications connected to their credit card (e.g., Uber, Skip the Dishes), and the number of recent online purchases made.

#### 2.2.3. Digital Security Ratings

An online protection behavior scale [19] was revised and used to query nine common digital security practices (e.g., password protection, two-factor authentication, encrypted email). The number of practices endorsed was summed to create a digital security practices score ranging from 0 to 9. Two additional self-ratings were collected: participants were asked to rate their digital security expertise ("How would you rate your digital security expertise?") using a scale from 1 ("very low") to 7 ("very high") and their digital threat awareness ("How would you rate your awareness about digital security threats; e.g., phishing, malware, Facebook scams, etc.?") using a scale from 1 ("not aware at all") to 5 ("very aware").

#### 2.2.4. Data Breach Experiences

Participants were asked to select the types of data breach incidents they had experienced from a list (e.g., email hacked, cloud storage hacked, sensitive photos posted by others) and then describe their most severe data breach incident (via text entry). They were also asked to estimate the recency of the incident ("within the past month", "1–3 months ago", "3–6 months ago", "6–12 months ago", "1–2 years ago", "more than 2 years ago"), if they continued using the breached application/service and, if so, for how long after the breach. Participants were asked about changes in their post-data breach security measures using five items (e.g., "I started changing my passwords more often after the data breach"; "I became more careful about my online security after the data breach"). Each item was rated on a scale from 0 ("strongly disagree") to 6 ("strongly agree"). A total score was created by summing the ratings for the five items, with higher scores reflecting greater changes in security measures following the data breach. Cronbach's alpha for this measure was 0.90.

### 2.2.5. Experiences with Anxiety and Depression

Participants were asked about their experiences with anxiety and depression, including diagnoses (e.g., "Have you ever been diagnosed with depression by a mental health professional?"), medication usage (e.g., "Are you currently taking prescription medication for anxiety?"), and experiences with therapy (e.g., "Are you currently taking part in therapy or counselling for depression?").

### 2.2.6. Negative Emotionality

Negative emotionality was assessed using the negative emotionality scale of the Big Five Inventory-2 [26]. The negative emotionality scale consists of 12 items (e.g., "I am someone who is temperamental, gets emotional easily"), each rated on a five-point scale from 1 ("disagree strongly") to 5 ("agree strongly"). Higher scores indicate stronger negative emotionality personality characteristics (i.e., a greater propensity to experience negative emotions). The negative emotionality scale has excellent psychometric properties [29]. Cronbach's alpha for the current sample was 0.94.

### 2.2.7. Generalized Anxiety Disorder-7

The Generalized Anxiety Disorder-7 scale (GAD-7) [20] was used to measure symptoms of anxiety. The GAD-7 inquires about anxiety symptoms experienced during the previous two weeks (e.g., "feeling nervous, anxious or on edge"), with each of the seven items rated on a four-point scale from 0 ("not at all") to 3 ("nearly every day"). Total scores can range from 0 to 21, with higher scores representing a greater severity of anxiety symptoms. Scores of 5, 10, and 15 represent cut-off points for mild, moderate, and severe anxiety, respectively [20]. The GAD-7 has excellent psychometric properties [28]. Cronbach's alpha for the current sample was 0.93. The GAD-7 is commonly used to identify generalized anxiety disorder [20]. Higher GAD-7 scores are associated with higher trait levels of anxiety.

### 2.2.8. Penn State Worry Questionnaire

The Penn State Worry Questionnaire (PSWQ) [27] was used to measure the propensity to worry. The PSWQ was developed as a trait measure for worry and measures the tendency, intensity, and uncontrollability of worry. The PSWQ is a 16-item scale, with each item (e.g., "My worries overwhelm me") rated from 1 ("not typical at all of me") to 5 ("very typical of me"). Higher scores represent a greater propensity to worry. The PSWQ has excellent internal consistency [30]. Cronbach's alpha for the current sample was 0.97.

### 2.2.9. Impact of Events Scale—Revised

The Impact of Events Scale—Revised [24,25] is a 22-item inventory used to assess event-specific subjective stress. Respondents are asked to identify a specific stressful life event and indicate how much they were distressed or bothered by each of the 22 difficulties listed (e.g., "Any reminder brought back feelings about it"; "I felt irritable and angry"; "I had waves of strong feelings about it"; "I tried not to think about it"). The 22 items correspond directly to 14 of the 17 symptoms of post-traumatic stress disorder (PTSD) in the Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) [31]. Participants were asked to think about their most serious data breach incident when responding to the items (a retrospective assessment). For each item, the rating scale choices were "not at all", "a little bit", "moderately", "quit a bit", and "extremely" (scored 0–4). The sum of all the items is used to create a total IES-R score, with total scores ranging from 0 to 88. The total IES-R score is designed to represent the total subjective stress experienced in response to a single event. Subscale scores can be calculated for intrusion (repeated thoughts about the incident), avoidance (effortful avoidance of situations that serve as reminders of the incident), and hyperarousal (hypervigilance, difficulty concentrating). Total scores greater than 24 are considered "high", and total scores greater than 32 suggest elevated PTSD symptoms that should be professionally assessed [24,25]. The IES-R has excellent psychometric properties [32,33]. Cronbach's alpha for the current sample was 0.92.

### 2.2.10. Data Breach Severity Index

Data breaches vary in terms of the quantity of information accessed, the sensitivity of that information, and the difficulty of recovering from the breach. From the perspective of an affected individual, the severity of a data breach can be evaluated by taking these three factors into account. For example, a breach of an infrequently used hotel rewards account would typically be considered less severe than a breach of a frequently used smartphone, given the differences in the amount of information at risk, the sensitivity of that information, and the difficulty of recovering from the breach. Any analysis of an individual's psychological response to a data breach should take into account the severity of the data breach, as more severe breaches can be expected to elicit more substantial psychological responses. We developed a Data Breach Severity Index (DBSI) for this purpose (Appendix A). The DBSI consists of three subscales, which we refer to as Breach Extent, Sensitivity, and Recovery. Each participant's written description of their most severe data breach incident was scored using these three subscales, and these scores were summed to create a DBSI score. The DBSI score was intended to quantify the invasiveness and consequences of a data breach from the victim's perspective so that this information could be incorporated into our multiple regression analyses. By controlling for data breach severity in the analyses, we could identify demographic and psychological variables that accounted for variance in IESR-R scores not attributable to the severity of the data breach.

The DBSI-Breach-Extent subscale captured the quantity of information accessed in a data breach. Each participant's data breach was assigned a score of low (1), medium (2), or high (3). For example, a breach that gained access to multiple accounts with many sources of personal information was assigned a score of 3 (e.g., a breach of multiple social media or email accounts, or of an entire phone or computer). A breach with limited access to information was assigned a score of 1 (e.g., breach of a single online shopping account, credit card, online gaming account), and intermediate cases were assigned a score of 2 (e.g., a breach of a single social media account).

The DBSI-Sensitivity subscale captured the sensitivity of the information breached. We used a four-point score for this subscale to reflect the range of sensitivity of information accessed and the higher potential for distress created by unauthorized access to sensitive personal information. Data breaches that involved access to sexually explicit content of a personal nature (e.g., the Ashley Madison breach) were assigned a score of 4 (very high), as were thefts of intimate photos and communications (emails/text messages). Breaches involving personal communications (e.g., text messages, social media communications, emails), private (not publicly accessible) photos, a social media account, bank accounts, or phone/computer access were assigned a score of 3 (high). Breaches that involved limited financial or personal information (e.g., the Equifax breach, a SIN/SSN, a driver's license) were assigned a score of 2 (medium). Breaches that involved unauthorized access to publicly available information or information of limited utility, such as access to online accounts that do not store sensitive personal or financial information (e.g., Netflix), were assigned a score of 1 (low).

The DBSI-Recovery subscale captured the degree of difficulty recovering from a data breach incident. A score of 1 (low) was assigned to situations where the victim could recover from the breach without much effort and with little or no loss of time or money (e.g., changing a password; contacting a bank to reverse charges; using an online account recovery process). A score of 2 (medium) was assigned to situations where a typical account recovery process would not work, where a dispute with a credit card company ensued when getting charges refunded and, in other instances, where more than minimal effort was required to rectify the problems caused by the breach. Situations where fraudulent messages were sent out from the victim's account were also assigned a score of 2. A score of 3 (high) was assigned when there was a permanent lockout of a social media or email account, theft of a computer or phone, permanent financial loss, and when private (not publicly accessible) photos were shared.

The minimum DBSI score was 3, and the maximum score was 10. For the 525 participants in the sample, the mean DBSI score was 4.92 (SD = 1.39). The median score was 4, and the 75th percentile was a score of 6. The range of scores was 3–10.

### *2.3. Data Preparation and Statistical Analyses*

Participants who did not correctly answer both attention check questions (including non-responses) were excluded from the analyses ($N = 63$). In addition, participants with a large percentage of missing data for the IES-R and/or the psychological measures (>20%) were excluded from all analyses ($N = 134$). Of the remaining 717 participants, 525 reported a genuine data breach experience and completed the IES-R (359 MTurk participants and 166 student participants).

All statistical analyses were carried out using the Statistical Package for the Social Sciences (SPSS, version 29, IBM Corp., Armonk, NY, USA, 2023). $t$-tests and chi-square tests were used to compare the demographic characteristics of men and women and student and community participants. Bivariate correlations (Pearson's $r$) were used to assess associations between IES-R scores, psychological measures (negative emotionality scores, GAD-7 scores, and PSWQ scores), and digital security ratings. Hierarchical linear regression was used to identify demographic, psychological, and digital security variables that accounted for unique variance in IES-R scores when controlling for DBSI scores and other variables.

## **3. Results**

### *3.1. Comparisons between Student and Community Participants*

Table 1 shows the demographic characteristics of the entire sample ($N = 525$) and comparisons between student ($n = 166$) and community (MTurk) participants ($n = 359$). Most participants reported their ethnicity as White (67.6%), although many identified as Asian (18.3%). As expected, the community participants were significantly older than the student participants, although they did not differ in years of education. A higher percentage of community participants reported their ethnicity as White (79.7% vs. 41.6% for student participants), whereas a higher percentage of student participants reported their ethnicity as Asian (42.8% vs. 7.0% for community participants). There were also differences in smartphone usage and social media usage, with student participants reporting greater daily use. With respect to the estimated recency of the data breach, a higher percentage of student participants estimated that their breach occurred within the past year (46.4% vs. 27.6% for community participants). Conversely, a higher percentage of community participants estimated that their breach occurred more than 2 years ago (47.6% vs. 33.1% for student participants). The IES-R scores were not correlated with recency estimates, $r(523) = -0.06$, $p = 0.166$).

Table 2 shows comparisons between student and community participants on the psychological measures. Student participants had significantly higher negative emotionality scores, PSWQ scores, and GAD-7 scores. They also had higher scores on the IES-R and each of its three subscales (intrusion, avoidance, and hyperarousal). The percentage of student and community participants with IES-R scores greater than 24 (scores considered to be high) did not differ significantly (25.9% vs. 19.2%), $\chi^2(1) = 3.02$, $p = 0.082$, $\Phi = 0.08$. With respect to the digital security variables, community participants had higher self-ratings for digital security expertise and digital security awareness than student participants, whereas they did not differ in their digital security practices or post-data breach security.

**Table 1.** Demographic characteristics of the sample and comparisons between student and community participants.

| | **Total Sample** | **Student** | **Community** | | | |
|---|---|---|---|---|---|---|
| | **Mean (SD)** | **Mean (SD)** | **Mean (SD)** | ***t*** | ***p*** | ***ES*** |
| **Age** | 35.2 (13.6) | 20.4 (3.9) | 41.9 (10.7) | 33.47 | <0.001 | 2.35 |
| **Education (years)** | 14.9 (2.2) | 14.1 (1.7) | 15.3 (2.3) | 6.55 | <0.001 | 0.56 |
| | *n* (%) | *n* (%) | *n* (%) | $\chi^2$ | *p* | *ES* |
| **Gender** | | | | 44.30 | <0.001 | 0.290 |
| Males | 190 (36.2) | 26 (15.7) | 164 (45.7) | | | |
| Females | 335 (63.8) | 140 (84.3) | 195 (54.3) | | | |
| **Ethnicity** | | | | 119.79 | <0.001 | 0.48 |
| White | 355 (67.6) | 69 (41.6) | 286 (79.7) | | | |
| Asian | 96 (18.3) | 71 (42.8) | 25 (7.0) | | | |
| Black or African American | 24 (4.6) | 2 (1.2) | 22 (6.1) | | | |
| Hispanic or Latin American | 21 (4.0) | 7 (4.2) | 14 (3.9) | | | |
| Other | 29 (5.5) | 17 (10.2) | 12 (3.3) | | | |
| **Smartphone use (per day)** | | | | 100.39 | <0.001 | 0.44 |
| 12+ h | 10 (1.9) | 5 (3.0) | 5 (1.4) | | | |
| 6–12 h | 67 (12.8) | 39 (23.5) | 28 (7.8) | | | |
| 3–6 h | 170 (32.4) | 85 (51.2) | 85 (23.7) | | | |
| 1–3 h | 200 (38.1) | 36 (21.7) | 164 (45.7) | | | |
| 0–1 h | 72 (13.7) | 1 (0.6) | 71 (19.8) | | | |
| No smartphone | 6 (1.1) | 0 (0.0) | 6 (1.7) | | | |
| **Social media use (per day)** | | | | 109.05 | <0.001 | 0.46 |
| 12+ h | 0 (0.0) | 0 (0.0) | 0 (0.0) | | | |
| 6–12 h | 13 (2.5) | 12 (7.2) | 1 (0.3) | | | |
| 3–6 h | 85 (16.2) | 58 (34.9) | 27 (7.5) | | | |
| 1–3 h | 264 (50.3) | 79 (47.6) | 185 (51.5) | | | |
| 0–1 h | 163 (31.0) | 17 (10.2) | 146 (40.7) | | | |
| **Browser use (per day)** | | | | 11.96 | 0.018 | 0.15 |
| 12+ h | 37 (7.0) | 9 (5.4) | 28 (7.8) | | | |
| 6–12 h | 162 (30.9) | 46 (27.7) | 116 (32.3) | | | |
| 3–6 h | 195 (37.1) | 73 (44.0) | 122 (34.0) | | | |
| 1–3 h | 113 (21.5) | 28 (16.9) | 85 (23.7) | | | |
| 0–1 h | 18 (3.4) | 10 (6.0) | 8 (2.2) | | | |

*ES* = effect size; Cohen's *d* for *t*-tests and Phi coefficient for chi-square.

**Table 2.** Comparisons between student and community participants on the self-report measures.

| | **Total Sample** | **Student** | **Community** | | | |
|---|---|---|---|---|---|---|
| | **Mean (SD)** | **Mean (SD)** | **Mean (SD)** | ***t*** | ***p*** | ***ES*** |
| **Impact of Events Scale—R** | | | | | | |
| Total score | 15.36 (13.28) | 17.84 (15.94) | 14.21 (11.69) | 2.63 | 0.009 | 0.28 |
| Intrusion | 4.40 (5.48) | 5.21 (6.56) | 4.02 (4.87) | 2.08 | 0.038 | 0.22 |
| Avoidance | 7.17 (5.68) | 8.18 (6.41) | 6.71 (5.25) | 2.59 | 0.010 | 0.26 |
| Hyperarousal | 3.79 (4.04) | 4.45 (4.92) | 3.48 (3.52) | 2.29 | 0.023 | 0.24 |
| **Psychological Measures** | | | | | | |
| Negative emotionality | 37.81 (3.62) | 38.68 (3.72) | 37.41 (3.50) | 3.79 | <0.001 | 0.36 |
| PSWQ | 46.81 (9.71) | 51.10 (7.81) | 44.82 (9.87) | 7.85 | <0.001 | 0.68 |
| GAD-7 | 13.26 (5.58) | 15.90 (5.61) | 12.04 (5.14) | 7.54 | <0.001 | 0.73 |
| **Digital Security Measures** | | | | | | |
| Digital security practices | 4.27 (1.48) | 4.10 (1.48) | 4.35 (1.48) | 1.79 | 0.073 | 0.17 |
| Digital security expertise | 4.28 (1.12) | 3.84 (1.19) | 4.49 (1.03) | 6.44 | <0.001 | 0.60 |

**Table 2.** *Cont.*

| | Total Sample | Student | Community | | | |
|---|---|---|---|---|---|---|
| | **Mean (SD)** | **Mean (SD)** | **Mean (SD)** | $t$ | $p$ | *ES* |
| Digital threat awareness | 4.03 (0.84) | 3.83 (0.90) | 4.12 (0.79) | 3.76 | <0.001 | 0.35 |
| Post-DB security | 22.03 (7.03) | 21.78 (7.02) | 22.14 (7.04) | 0.55 | 0.584 | 0.05 |

Negative emotionality = negative emotionality scale of the Big Five Inventory-2; PSWQ = Penn State Worry Questionnaire; GAD-7 = Generalized Anxiety Disorder-7; DB = data breach; *ES* = Cohen's *d*.

### *3.2. Comparisons between Men and Women*

Table 3 shows comparisons between the men ($n$ = 190) and women ($n$ = 335) in the sample. The men were slightly older than the women and had more years of education, but they did not differ in ethnicity. Women reported more daily smartphone use than men and more daily social media use. With respect to the psychological measures (Table 4), as expected, women had significantly higher PSWQ scores and GAD-7 scores, consistent with previous research [20,25–27]. As predicted, women had higher IES-R scores, as well as higher scores on the intrusion, avoidance, and hyperarousal subscales. A larger percentage of women had IES-R scores greater than 24 (25.4% vs. 14.2% for men), $\chi^2(1) = 9.00$, $p = 0.003$, $\Phi = 0.13$. Men had significantly higher self-ratings for digital security practices, digital security expertise, and digital threat awareness. Men and women did not differ in their post-data breach security.

**Table 3.** Demographic characteristics of the sample and comparisons between men and women.

| | Total Sample | Men | Women | | | |
|---|---|---|---|---|---|---|
| | **Mean (SD)** | **Mean (SD)** | **Mean (SD)** | $t$ | $p$ | *ES* |
| **Age** | 35.16 (13.61) | 37.61 (11.78) | 33.77 (14.38) | 3.31 | 0.001 | 0.29 |
| **Education (years)** | 14.94 (2.17) | 15.22 (2.17) | 14.79 (2.15) | 2.19 | 0.029 | 0.20 |
| | $n$ (%) | $n$ (%) | $n$ (%) | $\chi^2$ | $p$ | |
| **Ethnicity** | | | | 4.69 | 0.321 | 0.09 |
| White | 355 (67.6) | 137 (72.1) | 218 (65.1) | | | |
| Asian | 96 (18.3) | 29 (15.3) | 67 (20.0) | | | |
| Black or African American | 24 (4.6) | 8 (4.2) | 16 (4.8) | | | |
| Hispanic or Latin American | 21 (4.0) | 9 (4.7) | 12 (3.6) | | | |
| Other | 29 (5.5) | 7 (3.7) | 22 (6.6) | | | |
| **Smartphone use (per day)** | | | | 35.32 | <0.001 | 0.26 |
| 12+ h | 10 (1.9) | 1 (0.5) | 9 (2.7) | | | |
| 6–12 h | 67 (12.8) | 17 (8.9) | 50 (14.9) | | | |
| 3–6 h | 170 (32.4) | 43 (22.6) | 127 (37.9) | | | |
| 1–3 h | 200 (38.1) | 84 (44.2) | 116 (34.6) | | | |
| 0–1 h | 72 (13.7) | 43 (22.6) | 29 (8.7) | | | |
| No smartphone | 6 (1.1) | 2 (1.1) | 4 (1.2) | | | |
| **Social media use (per day)** | | | | 20.63 | <0.001 | 0.20 |
| 12+ h | 0 (0) | 0 (0) | 0 (0.0) | | | |
| 6–12 h | 13 (2.5) | 2 (1.1) | 11 (3.3) | | | |
| 3–6 h | 85 (16.2) | 15 (7.9) | 70 (20.9) | | | |
| 1–3 h | 264 (50.3) | 100 (52.6) | 164 (49.0) | | | |
| 0–1 h | 163 (31.0) | 73 (38.4) | 90 (26.9) | | | |
| **Browser use (per day)** | | | | 0.71 | 0.950 | 0.04 |
| 12+ h | 37 (7.0) | 15 (7.9) | 22 (6.6) | | | |
| 6–12 h | 162 (30.9) | 56 (29.5) | 106 (31.6) | | | |
| 3–6 h | 195 (37.1) | 73 (38.4) | 122 (36.4) | | | |
| 1–3 h | 113 (21.5) | 40 (21.1) | 73 (21.8) | | | |
| 0–1 h | 18 (3.4) | 6 (3.2) | 12 (3.6) | | | |

*ES* = effect size; Cohen's *d* for *t*-tests and Phi coefficient for chi-square.

**Table 4.** Comparisons between men and women on the self-report measures.

| | Total Sample | Men | Women | | | |
|---|---|---|---|---|---|---|
| | **Mean (SD)** | **Mean (SD)** | **Mean (SD)** | ***t*** | ***p*** | ***ES*** |
| **Impact of Events Scale—R** | | | | | | |
| Total score | 15.36 (13.28) | 12.30 (10.22) | 17.09 (14.46) | 4.42 | <0.001 | 0.37 |
| Intrusion | 4.40 (5.48) | 3.18 (4.26) | 5.09 (5.95) | 4.25 | <0.001 | 0.35 |
| Avoidance | 7.17 (5.68) | 6.37 (4.87) | 7.63 (6.04) | 2.61 | 0.009 | 0.22 |
| Hyperarousal | 3.79 (4.04) | 2.76 (2.93) | 4.37 (4.44) | 5.01 | <0.001 | 0.41 |
| **Psychological Measures** | | | | | | |
| Negative emotionality | 37.81 (3.62) | 37.41 (3.19) | 38.04 (3.83) | 1.93 | 0.055 | 0.18 |
| PSWQ | 46.81 (9.71) | 43.68 (9.45) | 48.60 (9.41) | 5.75 | <0.001 | 0.52 |
| GAD-7 | 13.26 (5.58) | 11.81 (4.92) | 14.09 (5.77) | 4.79 | <0.001 | 0.42 |
| **Digital Security Measures** | | | | | | |
| Digital security practices | 4.27 (1.48) | 4.60 (1.42) | 4.09 (1.48) | 3.87 | <0.001 | 0.35 |
| Digital security expertise | 4.28 (1.12) | 4.75 (1.02) | 4.02 (1.09) | 7.50 | <0.001 | 0.68 |
| Digital threat awareness | 4.03 (0.84) | 4.20 (0.74) | 3.93 (0.87) | 3.54 | <0.001 | 0.32 |
| Post-DB security | 22.03 (7.03) | 21.46 (7.01) | 22.36 (7.03) | 1.41 | 0.160 | 0.13 |

Negative emotionality = negative emotionality scale of the Big Five Inventory-2; PSWQ = Penn State Worry Questionnaire; GAD-7 = Generalized Anxiety Disorder-7; DB = data breach; *ES* = Cohen's *d*.

### 3.3. Types of Data Breach Incidents

Table 5 shows the frequencies of the types of data breaches reported as the "most severe" incidents experienced. Credit card fraud was the most frequently reported, followed by social media account and email breaches. Instant messaging and GPS tracking data breaches were much less common in the sample.

**Table 5.** Frequencies of data breach incidents ($N$ = 525).

| Data Breach Type | *N* | % |
|---|---|---|
| Instant messages intercepted | 31 | 5.9 |
| Email hacked | 168 | 32.0 |
| Social media account hacked | 175 | 33.3 |
| Theft of personal information | 157 | 29.9 |
| Theft of personal photos | 23 | 6.2 |
| Password compromised | 151 | 28.8 |
| Debit card breach | 37 | 9.3 |
| Credit card breach | 119 | 29.8 |
| 3rd party account linked to credit card (e.g., Amazon) | 21 | 5.3 |
| Computer/phone accessed | 18 | 4.5 |
| Cloud storage hacked | 12 | 2.3 |
| GPS tracking | 1 | 0.3 |
| Gaming account breach | 15 | 3.8 |

### 3.4. Correlational Analyses

As expected, the IES-R scores were positively correlated with the DBSI scores, $r(523) = 0.24$, $p < 0.001$, as more invasive and consequential data breaches were associated with higher stress. There were similar correlations between the DBSI scores and each of the IES-R subscales (for the intrusion subscale, $r = 0.22$, $p < 0.001$; for the avoidance subscale, $r = 0.22$, $p < 0.001$; for the hypervigilance subscale, $r = 0.19$, $p < 0.001$). There was no reason to expect that DBSI scores would be correlated with the psychological measures (negative emotionality scores, GAD-7 scores, and PSWQ scores), as the severity of a participant's data breach incident should be unrelated to their trait levels of negative emotionality, anxiety, and propensity to worry. Consistent with this expectation, none of these correlations were statistically significant ($r$ = 0.04, 0.08, and 0.03, respectively; all $p > 0.05$).

Table 6 shows the correlations between the IES-R scores and the psychological measures. As expected, there were positive correlations between the IES-R scores and negative emotionality scores ($r$ = 0.12), PSWQ scores ($r$ = 0.28), and GAD-7 scores ($r$ = 0.32), which indicated that participants with higher scores on these measures tended to have higher IES-R scores. Table 7 shows the correlations between IES-R scores and the digital security ratings. Digital security expertise was negatively correlated with IES-R scores, but the magnitude of the correlation ($r$ = −0.13) reflected only a weak association. Post-data breach security was positively correlated with IES-R scores ($r$ = 0.18), with higher IES-R scores associated with greater post-data breach security.

**Table 6.** Correlations among psychological measures and IES-R scores.

| | 1. | 2. | 3. | 4. | 5. | 6. | 7. |
|---|---|---|---|---|---|---|---|
| 1. IES-R total score | — | | | | | | |
| 2. IES-R intrusion | 0.92 ** | — | | | | | |
| 3. IES-R avoidance | 0.82 ** | 0.56 ** | — | | | | |
| 4. IES-R hyperarousal | 0.89 ** | 0.86 ** | 0.54 ** | — | | | |
| 5. Negative emotionality | 0.12 * | 0.08 | 0.11 | 0.11 | — | | |
| 6. PSWQ | 0.28 ** | 0.29 ** | 0.15 ** | 0.31 ** | 0.15 ** | — | |
| 7. GAD-7 | 0.32 ** | 0.32 ** | 0.21 ** | 0.33 ** | 0.11 * | 0.77 ** | — |

IES-R = Impact of Events Scale—Revised. PSWQ = Penn State Worry Questionnaire; GAD-7 = Generalized Anxiety Disorder-7. * $p < 0.01$. ** $p < 0.001$.

**Table 7.** Correlations among digital security measures and IES-R scores.

| | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. |
|---|---|---|---|---|---|---|---|---|
| 1. IES-R total score | — | | | | | | | |
| 2. IES-R intrusion | 0.92 ** | — | | | | | | |
| 3. IES-R avoidance | 0.82 ** | 0.56 ** | — | | | | | |
| 4. IES-R hyperarousal | 0.89 ** | 0.86 ** | 0.54 ** | — | | | | |
| 5. Digital security practices | −0.06 | −0.06 | −0.04 | −0.07 | — | | | |
| 6. Digital security expertise | −0.13 * | −0.11 | −0.11 * | −0.11 * | 0.38 ** | — | | |
| 7. Digital threat awareness | −0.09 | −0.08 | −0.09 | −0.04 | 0.29 ** | 0.50 ** | — | |
| 8. Post-data breach security | 0.18 ** | 0.18 ** | 0.12 * | 0.18 ** | 0.27 ** | 0.22 ** | 0.14 ** | — |

IES-R = Impact of Events Scale—Revised. * $p < 0.01$. ** $p < 0.001$.

### 3.5. Hierarchical Multiple Regression Predicting IES-R Scores

A hierarchical multiple regression analysis was used to identify demographic characteristics and psychological measures predictive of IES-R scores. Digital security practices and digital threat awareness were not included in the analysis because they were not significantly correlated with the IES-R scores (Table 7). All variance inflation factors (VIFs) were below 2.8, which indicated that there was no problematic multicollinearity between the predictors (a VIF greater than 4.0 is generally considered to reflect a multicollinearity issue).

A summary of the regression analysis is shown in Table 8, and the full results are shown in Table 9. The DBSI scores were entered first (Model 1) to control for the severity of the data breach in subsequent steps of the analysis, thereby ensuring that the analysis identified demographic and psychological variables that accounted for variance in the IESR-R scores not attributable to the severity of the data breach incident. As expected, the DBSI scores accounted for a significant percentage of the variance in the IES-R scores, $\Delta R^2$ = 5.7%, $F(1, 521) = 31.78$, $p < 0.001$, as more severe data breaches were associated with higher IES-R scores, β = 0.240, $t(521) = 5.64$, $p < 0.001$. Demographic variables were added in Model 2, which included gender, sample (student or community), age, and years of education. Together, these variables accounted for a significant percentage of the variance in the IES-R scores above and beyond that accounted for by the DBSI scores, $\Delta R^2$ = 2.4%, $F(4, 517) = 3.31$, $p = 0.011$. As can be seen in Table 9, however, gender was the only demographic variable that was statistically significant, β = 0.135, $t(517) = 3.04$, $p = 0.002$, with women having higher IES-R scores than men after controlling for DBSI scores and the other demographic variables. For Model 3, negative emotionality, PSWQ, and GAD-7 scores were added to the analysis, and together these accounted for a significant percentage of variance, $\Delta R^2$ = 9.3%, $F(3, 514) = 19.26$, $p < 0.001$. However, of these three measures, only the GAD-7 scores were a significant predictor, β = 0.250, $t(514) = 3.91$, $p < 0.001$, with higher trait anxiety associated with higher IES-R scores. Notably, gender remained a significant predictor in Model 3, β = 0.088, $t(514) = 2.05$, $p = 0.041$, which indicated that women had higher IES-R scores than men even after accounting for their higher GAD-7 scores (as shown in Table 4). For Model 4, the addition of smartphone use, social media use, and browser use did not increase the percentage of variance explained, $\Delta R^2$ = 0.8%, $F(3, 511) = 1.75$, $p = 0.157$. Finally, for Model 5, which added digital security expertise and post-data breach security, the percentage of variance explained increased significantly, $\Delta R^2$ = 1.9%, $F(2, 509) = 6.01$, $p = 0.003$, with post-data breach security being a significant predictor, β = 0.145, $t(509) = 3.44$, $p < 0.001$. Higher scores on the post-data breach security measure were associated with higher IES-R scores after controlling for the other predictors. The total percentage of variance accounted for by Model 5 was 20.1% (adjusted $R^2$ = 18.1%), $F(13, 509) = 9.86$, $p < 0.001$, and the significant predictors were DBSI scores, GAD-7 scores, and post-data breach security. Higher scores on each of these measures were uniquely associated with higher IES-R scores. The same predictors were statistically significant when using robust standard errors to correct for possible heteroscedasticity. Excluding the DBSI score predictor from the regression analysis reduced the total $R^2$ to 16.7%, $F(12, 510) = 8.50$, $p < 0.001$. GAD-7 scores and scores on post-data breach security remained statistically significant predictors (*p*s < 0.001). In addition, digital security expertise was significant, β = −0.10, $t(510) = 2.06$, $p = 0.040$.

**Table 8.** Summary of hierarchical linear regression analysis predicting IES-R scores.

| | $R$ | $R^2$ | $\Delta R^2$ | $\Delta F$ | $p$ |
|---|---|---|---|---|---|
| Model 1 (with DBSI) | 0.240 | 0.057 | 0.057 | 31.78 | <0.001 |
| Model 2 (with gender, sample, age, years of education) | 0.285 | 0.081 | 0.024 | 3.31 | 0.011 |
| Model 3 (with NE, PSWQ, GAD-7 scores) | 0.417 | 0.174 | 0.093 | 19.26 | <0.001 |
| Model 4 (with smartphone use, social media use, browser use) | 0.423 | 0.182 | 0.008 | 1.75 | 0.157 |
| Model 5 (with digital security expertise, post-data breach security) | 0.448 | 0.201 | 0.019 | 6.01 | 0.003 |

$R$ and $R^2$ are the values for each model. $\Delta R^2$ is the increase in variance due to the addition of a set of predictors; the associated $F$ statistic and *p*-value are a test of whether the increase in variance explained by the predictors is statistically significant (greater than zero). For Model 1, the predictor was DBSI scores. For Model 2, the additional predictors were gender, sample, age, and years of education. For Model 3, the additional predictors were negative emotionality (NE), PSWQ, and GAD-7 scores. For Model 4, the additional predictors were smartphone use (hours per day), social media use (hours per day), and browser use (hours per day). For Model 5, the additional predictors were digital security expertise and post-data breach security.

An additional exploratory regression analysis was carried out for the participants with high IES-R scores (>24, according to the IES-R criteria). This analysis identified predictors of IES-R scores among the participants who had experienced higher levels of data-breach-induced stress ($N$ = 112). The predictors were entered in the same order as they were in the analysis of the full sample. A summary of this analysis is shown in Table 10, and the full results are shown in Table 11. As expected, DBSI scores accounted for a significant percentage of the variance in IES-R scores, $\Delta R^2$ = 14.1%, $F(1, 109) = 17.85$, $p < 0.001$, with more severe data breaches associated with higher IES-R scores, β = 0.375, $t(109) = 4.23$, $p < 0.001$. Demographic variables were added in Model 2, which included gender, sample (student or community), age, and years of education. Together these variables accounted for a significant percentage of the variance in IES-R scores above and beyond that accounted for DBSI scores, $\Delta R^2$ = 8.6%, $F(4, 105) = 2.92$, $p = 0.025$, although none of the individual demographic predictors were statistically significant. For Model 3, negative emotionality, PSWQ, and GAD-7 scores were added, which did not increase $R^2$ significantly, $\Delta R^2$ = 4.0%,

$F(3, 102) = 1.88$, $p = 0.138$. For Model 4, the addition of smartphone use, social media use, and browser use resulted in a significant increase in $R^2$, $\Delta R^2 = 7.4\%$, $F(3, 99) = 3.70$, $p = 0.014$. Social media use was a significant predictor, with greater daily social media use associated with higher IES-R scores, $\beta = 0.266$, $t(99) = 2.57$, $p = 0.012$. For Model 5, which added digital security expertise and post-data breach security, the percentage of variance explained increased significantly, $\Delta R^2 = 6.1\%$, $F(2, 97) = 4.97$, $p = 0.009$. Digital security expertise was a significant predictor, with higher expertise associated with lower IES-R scores, $\beta = -0.212$, $t(97) = 2.36$, $p = 0.020$. The total percentage of variance accounted for by Model 5 was 40.2% (adjusted $R^2 = 32.2\%$), $F(13, 97) = 5.02$, $p < 0.001$, and the significant predictors were DBSI scores, social media use, and digital security expertise (note that for PSWQ scores, $p = 0.051$). The same predictors were statistically significant when using robust standard errors to correct for possible heteroscedasticity. Excluding the DBSI score predictor from the regression analysis reduced the total $\mathrm{R}^2$ to 32.0%, $F(12, 98) = 3.85$, $p < 0.001$. Social media use and digital security expertise remained significant predictors ($p < 0.01$)).

**Table 9.** Hierarchical multiple regression predicting IES-R scores.

| | *B* | *SE* | *Beta* | *t* | *p* |
|---|---|---|---|---|---|
| **Model 1** | | | | | |
| DBSI | 2.286 | 0.406 | 0.240 | 5.64 | <0.001 |
| **Model 2** | | | | | |
| DBSI | 2.076 | 0.424 | 0.218 | 4.90 | <0.001 |
| Gender | 3.732 | 1.227 | 0.135 | 3.04 | 0.002 |
| Sample | 2.038 | 1.902 | 0.071 | 1.07 | 0.285 |
| Age | 0.069 | 0.062 | 0.070 | 1.11 | 0.267 |
| Years of education | −0.018 | 0.268 | −0.003 | 0.07 | 0.948 |
| **Model 3** | | | | | |
| DBSI | 2.218 | 0.404 | 0.233 | 5.49 | <0.001 |
| Gender | 2.429 | 1.187 | 0.088 | 2.05 | 0.041 |
| Sample | −0.238 | 1.839 | −0.008 | 0.13 | 0.897 |
| Age | 0.100 | 0.059 | 0.103 | 1.70 | 0.089 |
| Years of education | 0.035 | 0.256 | 0.006 | 0.14 | 0.890 |
| Negative emotionality | 0.254 | 0.150 | 0.069 | 1.69 | 0.092 |
| PSWQ score | 0.106 | 0.088 | 0.077 | 1.20 | 0.230 |
| GAD-7 score | 0.594 | 0.152 | 0.250 | 3.91 | <0.001 |
| **Model 4** | | | | | |
| DBSI | 2.169 | 0.406 | 0.227 | 5.34 | <0.001 |
| Gender | 2.131 | 1.197 | 0.077 | 1.78 | 0.076 |
| Sample | −1.069 | 1.881 | −0.037 | 0.57 | 0.570 |
| Age | 0.120 | 0.060 | 0.123 | 2.00 | 0.046 |
| Years of education | 0.018 | 0.256 | 0.003 | 0.07 | 0.944 |
| Negative emotionality | 0.232 | 0.150 | 0.063 | 1.54 | 0.124 |
| PSWQ score | 0.105 | 0.088 | 0.077 | 1.19 | 0.235 |
| GAD-7 score | 0.564 | 0.152 | 0.237 | 3.70 | <0.001 |
| Smartphone use | 0.721 | 0.670 | 0.053 | 1.08 | 0.282 |
| Social media use | 1.257 | 0.883 | 0.071 | 1.42 | 0.155 |
| Browser use | −0.013 | 0.573 | −0.001 | 0.02 | 0.982 |
| **Model 5** | | | | | |
| DBSI | 1.923 | 0.411 | 0.202 | 4.68 | <0.001 |
| Gender | 1.587 | 1.220 | 0.057 | 1.30 | 0.194 |
| Sample | −1.359 | 1.906 | −0.048 | 0.71 | 0.476 |
| Age | 0.090 | 0.061 | 0.093 | 1.49 | 0.137 |
| Years of education | 0.100 | 0.255 | 0.016 | 0.39 | 0.696 |
| Negative emotionality | 0.248 | 0.149 | 0.067 | 1.66 | 0.098 |
| PSWQ score | 0.100 | 0.087 | 0.073 | 1.14 | 0.255 |
| GAD-7 score | 0.541 | 0.151 | 0.228 | 3.58 | <0.001 |
| Smartphone use | 0.585 | 0.665 | 0.043 | 0.88 | 0.379 |
| Social media use | 1.222 | 0.876 | 0.069 | 1.40 | 0.164 |
| Browser use | −0.004 | 0.574 | 0.000 | 0.01 | 0.994 |
| Digital security expertise | −0.727 | 0.545 | −0.061 | 1.33 | 0.183 |
| Post-data breach security | 0.274 | 0.080 | 0.145 | 3.44 | <0.001 |

**Table 10.** Summary of hierarchical linear regression analysis for participants with high IES-R scores (>24).

| | *R* | $R^2$ | $\Delta R^2$ | $\Delta F$ | *p* |
|---|---|---|---|---|---|
| Model 1 (with DBSI scores) | 0.375 | 0.141 | 0.141 | 17.85 | <0.001 |
| Model 2 (with gender, sample, age, years of education) | 0.476 | 0.227 | 0.086 | 2.92 | 0.025 |
| Model 3 (with NE, PSWQ, GAD-7 scores) | 0.517 | 0.267 | 0.040 | 1.88 | 0.138 |
| Model 4 (with smartphone use, social media use, browser use) | 0.584 | 0.341 | 0.074 | 3.70 | 0.014 |
| Model 5 (with digital security expertise and post-data breach security) | 0.634 | 0.402 | 0.061 | 4.97 | 0.009 |

*R* and $R^2$ are the values for each model. $\Delta R^2$ is the increase in variance due to the addition of a set of predictors; the associated *F* statistic and *p*-value are a test of whether the increase in variance explained by the predictors is statistically significant (greater than zero). For Model 1, the predictor was DBSI scores. For Model 2, the additional predictors were gender, sample, age, and years of education. For Model 3, the additional predictors were negative emotionality (NE), PSWQ, and GAD-7 scores. For Model 4, the additional predictors were smartphone use (hours per day), social media use (hours per day), and browser use (hours per day). For Model 5, the additional predictors were digital security expertise and post-data breach security.

**Table 11.** Hierarchical multiple regression predicting IES-R scores > 24.

| | *B* | *SE* | β | *t* | *p* |
|---|---|---|---|---|---|
| **Model 1** | | | | | |
| DBSI | 2.633 | 0.623 | 0.375 | 4.23 | <0.001 |
| **Model 2** | | | | | |
| DBSI | 2.254 | 0.632 | 0.321 | 3.57 | <0.001 |
| Gender | 4.362 | 2.336 | 0.176 | 1.87 | 0.065 |
| Sample | 3.797 | 3.243 | 0.174 | 1.17 | 0.244 |
| Age | −0.033 | 0.103 | −0.043 | 0.32 | 0.751 |
| Years of education | 0.623 | 0.410 | 0.139 | 1.52 | 0.132 |
| **Model 3** | | | | | |
| DBSI | 2.479 | 0.632 | 0.353 | 3.92 | <0.001 |
| Gender | 3.973 | 2.320 | 0.160 | 1.71 | 0.090 |
| Sample | 3.158 | 3.252 | 0.145 | 0.97 | 0.334 |
| Age | −0.022 | 0.103 | −0.029 | 0.21 | 0.834 |
| Years of education | 0.616 | 0.406 | 0.137 | 1.52 | 0.132 |
| Negative emotionality | 0.145 | 0.227 | 0.057 | 0.64 | 0.523 |
| PSWQ score | 0.124 | 0.193 | 0.083 | 0.64 | 0.522 |
| GAD-7 score | 0.263 | 0.255 | 0.129 | 1.03 | 0.306 |
| **Model 4** | | | | | |
| DBSI | 2.428 | 0.610 | 0.346 | 3.98 | <0.001 |
| Gender | 4.142 | 2.280 | 0.167 | 1.82 | 0.072 |
| Sample | 0.443 | 3.261 | 0.020 | 0.14 | 0.892 |
| Age | −0.002 | 0.100 | −0.003 | 0.02 | 0.982 |
| Years of education | 0.537 | 0.396 | 0.120 | 1.36 | 0.178 |
| Negative emotionality | 0.047 | 0.222 | 0.019 | 0.21 | 0.832 |
| PSWQ score | 0.295 | 0.193 | 0.196 | 1.53 | 0.129 |
| GAD-7 score | 0.086 | 0.254 | 0.042 | 0.34 | 0.735 |
| Smartphone use | 1.016 | 1.211 | 0.086 | 0.84 | 0.403 |
| Social media use | 3.900 | 1.517 | 0.266 | 2.57 | 0.012 |
| Browser use | −0.967 | 1.044 | −0.081 | 0.93 | 0.357 |
| **Model 5** | | | | | |
| DBSI | 2.185 | 0.598 | 0.311 | 3.65 | <0.001 |
| Gender | 3.065 | 2.250 | 0.123 | 1.36 | 0.176 |
| Sample | 0.329 | 3.149 | 0.015 | 0.11 | 0.917 |
| Age | 0.012 | 0.098 | 0.016 | 0.12 | 0.905 |
| Years of education | 0.522 | 0.382 | 0.116 | 1.37 | 0.175 |
| Negative emotionality | 0.007 | 0.214 | 0.003 | 0.03 | 0.975 |
| PSWQ score | 0.371 | 0.188 | 0.246 | 1.97 | 0.051 |
| GAD-7 score | 0.031 | 0.246 | 0.015 | 0.13 | 0.900 |
| Smartphone use | 1.009 | 1.168 | 0.085 | 0.86 | 0.390 |
| Social media use | 4.225 | 1.464 | 0.288 | 2.89 | 0.005 |
| Browser use | −0.740 | 1.009 | −0.062 | 0.73 | 0.465 |
| Digital security expertise | −2.108 | 0.892 | −0.212 | 2.36 | 0.020 |
| Post-data breach security | −0.150 | 0.142 | −0.091 | 1.05 | 0.295 |

To summarize, the analysis of the participants with high (>24) IES-R scores revealed several notable differences from the analysis of the full sample, namely, (1) the GAD-7 scores were a significant predictor in the full sample but not in the high IES-R sample, (2) post-data breach security was a significant predictor in the full sample but not in the high IES-R sample, (3) social media use was a significant predictor in the high IES-R sample but not in the full sample, and (4) digital security expertise was a significant predictor in the high IES-R sample but not in the full sample. Also notable is the fact that the percentage of variance accounted for in the high IES-R sample (40.2%) was much larger than that accounted for in the full sample (20.1%). These differences must be interpreted with caution, however, given that the high IES-R sample size was not large (*N* = 112).

## 4. Discussion

As internet use has become ubiquitous, psychologists have focused their research on the mental-health-related issues of internet-enabled technology, such as the risks and harms of social media use, smartphone addiction, cyberbullying, and online gambling addiction. The psychological impact of data breach incidents has received far less attention, and few studies have investigated the psychological reactions of data breach victims. This was the first study to examine the psychological stress experienced after a personal experience with a data breach incident and individual differences in demographic and psychological variables that could moderate that stress.

We found some evidence that women are more likely to experience greater data-breach-induced stress than men. More specifically, in the regression analysis of the full sample, after controlling for data breach severity, and when negative emotionality, trait anxiety, and propensity to worry were also controlled (which took into account women's higher scores on these measures), women had higher IES-R scores than men. This gender difference was eliminated when additional predictors were added to the regression analysis, but these additional predictors likely accounted for variation that could also be explained by gender (e.g., social media use). The gender difference that we observed is consistent with some of the previous data breach research [1,17] and with the larger literature on gender differences in emotional reactivity [34–36]. It is also consistent with documented gender differences in anxiety [28], negative emotionality [26], and propensity to worry [27], all of which are related to stress responses. Nevertheless, researchers have very little data available to generalize from, so future studies should also test for gender differences in psychological responses to data breach incidents to determine whether there are genuine differences in data-breach-induced stress and related adverse consequences.

We also found evidence that trait anxiety (as measured by the GAD-7) is associated with higher levels of data-breach-induced stress. Participants with higher GAD-7 scores had higher IES-R scores even after accounting for numerous individual differences in demographic and psychological variables (e.g., age, gender, negative emotionality, propensity to worry), as well as the severity of the data breach incident. Of course, this association makes sense, given that higher levels of trait anxiety likely exacerbate the stress created by a data breach incident. It is possible that greater anxiety leads to greater rumination about these incidents, which creates higher levels of chronic stress. The impact of trait anxiety on data-breach-induced stress is also consistent with the literature that shows that higher trait anxiety often results in heightened negative emotional responses to adverse events [37,38]. Taken as a whole, our findings suggest that higher levels of trait anxiety can predispose individuals or increase one's vulnerability to stronger negative reactions following a data breach victimization. Future studies should confirm this finding and examine the possibility that this association is moderated by individual differences in rumination, cognitive control, or attentional control [39–41].

On this note, it is somewhat surprising that the predicted associations between IES-R scores and negative emotionality and propensity to worry were not observed. Although both measures were correlated with IES-R scores, they were not unique predictors of IES-R scores in any of the regression analyses. Previous research has shown that negative emotionality is associated with anxiety, depression, and greater emotional volatility [26], and thus one would expect that individuals high in negative emotionality would experience greater data-breach-induced stress. On the other hand, it is possible that the negative emotionality scale we used [26] is too broad a measure and does not target with enough specificity the tendency to overreact to stressors and perceived threats. With respect to propensity to worry, it was expected that those with a higher propensity to worry would experience more data-breach-induced stress and, as a consequence, would have higher IES-R scores. However, GAD-7 scores and PSWQ scores were highly correlated ($r = 0.77$), and this association may have masked any unique influence of trait levels of worrying. Studies with different measures and significantly larger samples ($N > 1000$) should be able to clarify whether negative emotionality and propensity to worry are individual differences that influence psychological reactions to data breach incidents.

An exploratory analysis of participants with high (>24) IES-R scores revealed that much more of the variance in the IES-R scores could be accounted for and that both social media use and digital security expertise were significant predictors (which was not true for the full sample). Notably, higher digital security expertise was associated with lower data-breach-induced stress, which was the only protective factor identified in the analyses. Of course, given the much smaller sample size for this analysis ($N = 112$) relative to the full sample ($N = 525$), caution is necessary when interpreting this finding. In addition, digital security expertise was assessed using a single self-rating, and thus there was no way to carry out a detailed examination of the specific components of digital security expertise that might contribute to resilience. Future studies should attempt to replicate this finding by using more comprehensive measures to understand the mechanisms through which digital literacy and awareness potentially alleviate the psychological repercussions of data breach incidents. Ultimately, individuals who experience significant data-breach-induced stress may be more relevant for understanding and ameliorating serious psychological reactions to these incidents, and thus it will be advantageous for researchers to recruit samples that include a higher proportion of such individuals when the goal is to identify the factors that contribute to personal resilience [21].

### *Limitations and Directions for Future Research*

Recruiting a student sample and an MTurk sample was both a strength and a limitation of this study. Given that a great deal of psychological research is based on undergraduate student samples, which limits generalizability, the recruitment of an older and more demographically diverse MTurk sample undoubtedly increased the generalizability of our findings. Nevertheless, our student and community samples might not fully represent the population of individuals affected by data breaches, and the reactions of our participants might not reflect the typical experiences and reactions of individuals across various age groups, professions, and socioeconomic backgrounds. Researchers have noted that MTurk samples vary and may not be representative of the general population [42,43]. Although recent reviews have found that MTurk samples recruited for personality studies [44], addiction research [45], and psychopathology studies [46] are comparable to those recruited by traditional methods, it would be unsurprising if MTurk participants differed in other ways that could be relevant to this research. For example, by virtue of being recruited via the MTurk website, MTurk samples may be more frequent and/or more sophisticated users of online services. They may also have higher levels of digital security expertise and digital threat awareness than the general population, which could influence their data-breach-induced stress (recall that MTurk participants had higher scores than student participants on both measures). One possible consequence is that MTurk users may be desensitized in their reactions to data breach incidents relative to less sophisticated internet users. Consistent with this possibility, the MTurk sample had a lower mean IES-R score than the student sample (Table 2). Relative to less sophisticated internet users, MTurk users may possess a different and perhaps more accurate understanding of the risks associated with various types of data breaches and may not experience the same degree of data-breach-induced stress in response to the same incidents.

Complicating the situation is the fact that the MTurk sample had significantly lower levels of negative emotionality, propensity to worry, and trait anxiety relative to the student sample, which could also influence stress responses. Ultimately, the regression analyses did not indicate that the level of data-breach-induced stress reported by MTurk participants was different when demographic and psychological variables were controlled, but future studies should nevertheless focus on recruiting samples more representative of adults living and working in advanced economies. To do so, researchers could employ different recruitment strategies, such as reaching out to community organizations, workplaces, and online forums frequented by individuals of varying demographics. Collaborations with institutions and organizations that have access to a large and diverse membership could also enhance the generalizability of findings. Ideally, longitudinal designs would be used, collecting baseline psychological measures and then tracking individuals' responses to a personal data breach incident over time, thereby providing deeper insights into long-term psychological effects and coping mechanisms.

Although the DBSI proved to be a useful tool for quantifying the severity of a data breach for the purposes of the regression analyses, the measure has several limitations and could no doubt be improved and refined. For one, given that the scoring of the DBSI is based on a participant's written description of their data breach, it is vulnerable to omissions and misunderstandings of respondents (i.e., quality and accuracy issues with the raw data used to create the total score). Assuming that data are collected online, one possible solution is to ask participants a series of specific questions about their data breach incident and use these responses to create a DBSI score (e.g., "Which of the following types of accounts were compromised?"; "Did you lose money due to the data breach?"; "Did someone use your Facebook account to deceive others?"). Of course, from a participant's perspective, this approach is likely to be much more taxing and tedious relative to simply describing their experience via free-form text entry. A combination of these two methods might be ideal, but extensive pilot testing would be necessary to identify the optimal strategy. Another possibility is to recruit a sample of individuals who have experienced the same data breach, the full details of which are known to the investigators (e.g., the Equifax breach). In these situations, a study could focus on the diversity of psychological reactions to a data breach of a known severity (in terms of the breach extent, sensitivity, and ease of recovery). Of course, the possible disadvantages would be that the findings may be generalizable only to the larger population of individuals affected by the same data breach and/or only to data breaches of identical severity. Ultimately, given the current state of this literature and the methodological challenges of this research, investigators will need to pursue a variety of strategies to further our understanding of the psychology of data breach experiences.

## 5. Conclusions

Data breach incidents have affected millions of people worldwide, but the psychological aspects of these experiences are only beginning to be examined. This study focused on the psychological stress associated with a personal experience with a data breach and several individual differences hypothesized to modulate such stress (age, gender, trait anxiety, negative emotionality, and propensity to worry). The findings indicate that there are individual differences linked to the degree of data-breach-induced stress experienced, independent of data breach severity, including gender, trait anxiety, social media use, digital security expertise, and post-data breach security. Future research can build and expand on this study by considering these findings and the study's methodological strengths and limitations.

**Author Contributions:** Conceptualization, C.R.S. and D.R.C.; methodology, C.R.S. and D.R.C.; formal analysis, D.R.C. and C.R.S.; investigation, D.R.C.; resources, C.R.S.; writing—original draft preparation, D.R.C. and C.R.S.; writing—review and editing, C.R.S. and D.R.C.; supervision, C.R.S.; project administration, C.R.S.; funding acquisition, C.R.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Faculty of Arts, University of Calgary, grant number 10018065.

**Institutional Review Board Statement:** The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board of the University of Calgary (REB19-1927, 21 June 2024).

**Informed Consent Statement:** Informed consent was obtained from all subjects involved in the study.

**Data Availability Statement:** Participants in this study did not agree for their data to be shared publicly, so supporting data are not publicly available. Data are available from the corresponding author for researchers who meet the criteria for access to confidential data.

**Acknowledgments:** We thank Emma Cherry for her assistance with the DBSI scoring. We also thank three anonymous reviewers for their excellent feedback and suggestions.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Appendix A. Data Breach Severity Index (DBSI)

| Score | Breach Extent | Sensitivity | Recovery |
|---|---|---|---|
| 1 | **Low**: credit card or debit card number; password(s) exposed in a leaked list; Netflix, gaming, or online shopping account. | **Low**: publicly available information; personal information of limited utility; Netflix or Spotify access; gaming account; email address. | **Low**: no financial loss; contact credit card company to remove charges and cancel card; typical account recovery process; change passwords; remove credit card from online shopping account or delete the account; minimal or no effort. |
| 2 | **Medium**: access to accounts with a multitude of information (e.g., email, Facebook or other social media, Equifax, health insurance provider breach); personal pictures; driver's license; GPS tracking. [a] | **Medium**: financial information; credit rating; driver's license; SIN/SSN; medical information. | **Medium**: small financial costs; requires more than minimal effort to recover (e.g., undo edits to social media account after retrieval; request new SSN/SIN); typical account recovery does not work (e.g., cannot recover SM account using recovery email); dispute with bank about fraudulent charges to credit or debit account. |
| 3 | **High**: breach of multiple accounts (email, social media, financial, etc.); multiple sources of personal information stolen; audio or video recordings; access to entire phone or computer. | **High**: personal communications (email, social media messaging, IMs, DMs, etc.); social media account access; phone access; personal/sensitive photos. | **High**: permanent loss; cannot return to "normal"; significant financial loss; financial audit, safeguarding financial assets; unable to recover or delete social media account; must contact websites to remove material (photos, etc.); sexually explicit photos no longer private. |
| 4 | | **Very High**: sexually explicit material (nude photos, audio, or video recordings, etc.); GPS tracking data. | |

[a] An email account breach would be scored as "medium" because an email account may contain a great deal of information and because an email address is commonly used to recover passwords for other accounts. However, if the email is explicitly described as being tied to an "old" or "unused" account then it would be scored as "low". GPS tracking is scored as "medium" because it involves location data and because that data can be used to infer other information (travel, personal visits, etc.).

## References

1. Elhai, J.D.; Chai, S.; Amialchuck, A.; Hall, B.J. Cross-cultural and gender associations with anxiety about electronic data hacking. *Comput. Hum. Behav.* **2017**, *70*, 161–167. [CrossRef]
2. Identity Theft Resource Center. 2022 Data Breach Report. Available online: https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/ (accessed on 14 July 2024).
3. Schumacher, S.; Kent, N. 8 Charts on Internet Use around the World as Countries Grapple with COVID-19. Pew Research Report. 2020. Available online: https://www.pewresearch.org/short-reads/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/ (accessed on 1 August 2024).

4. Identity Theft Resource Center. 2023 Data Breach Report. Available online: https://www.idtheftcenter.org/publication/2023-data-breach-report/ (accessed on 14 July 2024).
5. Office of the Privacy Commissioner of Canada, 2019. A Full Year of Mandatory Data Breach Reporting: What We've Learned and What Businesses Need to Know. Available online: https://www.priv.gc.ca/en/blog/20191031/ (accessed on 17 August 2024).
6. Malhotra, A.; Malhotra, C.K. Evaluating customer information breaches as service failures: An event study approach. *J. Serv. Res.* **2010**, *14*, 44–59. [CrossRef]
7. Schatz, D.; Bashroush, R. The impact of repeated data breach events on organisations' market value. *Inf. Comput. Secur.* **2016**, *24*, 73–92. [CrossRef]
8. Rosati, P.; Deeney, P.; Cummins, M.; van der Werff, L.; Lynn, T. Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Res. Int. Bus. Financ.* **2019**, *47*, 458–469. [CrossRef]
9. Aivazpour, Z.; Valecha, R.; Chakraborty, R. The impact of data breach severity on post-breach online shopping intention. *ICIS 2018 Proc.* **2018**, *13*. Available online: https://aisel.aisnet.org/icis2018/security/Presentations/13 (accessed on 1 July 2024).
10. Janakiraman, R.; Joon, H.L.; Rishika, R. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *J. Mark.* **2018**, *82*, 85–105. [CrossRef]
11. Martin, K.D.; Borah, A.; Palmatier, R.W. Data privacy: Effects on customer and firm performance. *J. Mark.* **2018**, *81*, 36–58. [CrossRef]
12. Zetter, K. Hackers Finally Post Stolen Ashley Madison Data. 2015. Available online: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (accessed on 12 June 2024).
13. Doffman, Z. Ashley Madison Hack Returns to 'Haunt' Its Victims: 32 Million Users Now Watch and Wait. 2020. Available online: https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/?sh=6f776c375677 (accessed on 27 July 2024).
14. Schager, N. 'The Ashley Madison Affair' Puts Cheaters on Blast. 2023. Available online: https://www.thedailybeast.com/the-ashley-madison-affair-review-putting-cheaters-on-blast (accessed on 12 June 2024).
15. BBC Ashley Madison Hack Victims Receive Blackmail Letters. BBC News: Technology. 2015. Available online: http://www.bbc.com/news/technology-35101662 (accessed on 13 September 2023).
16. Cross, C.; Parker, M.; Sansom, D. Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *Int. Rev. Vict.* **2019**, *25*, 53–69. [CrossRef]
17. Chai, S.; Bagchi-Sen, S.; Morrell, C.; Rao, H.R.; Upadhyaya, S.J. Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Trans. Prof. Commun.* **2009**, *52*, 167–182. [CrossRef]
18. Elhai, J.D.; Hall, B.J. Anxiety about internet hacking: Results from a community sample. *Comput. Hum. Behav.* **2016**, *54*, 180–185. [CrossRef]
19. Elhai, J.D.; Levine, J.C.; Hall, B.J. Anxiety about electronic internet hacking: Predictors and relations with digital privacy protection behavior. *Internet Res.* **2017**, *27*, 631–649. [CrossRef]
20. Spitzer, R.L.; Kroenke, K.; Williams, J.B.; Lowe, B. A brief measure for assessing generalized anxiety disorder: The GAD-7. *Arch. Intern. Med.* **2006**, *166*, 1092–1097. [CrossRef]
21. Joinson, A.D.; Dixon, M.; Coventry, L.; Briggs, P. Development of a new 'human cyber-resilience scale'. *J. Cybersecur.* **2023**, *9*, tyad007. [CrossRef]
22. Schneiderman, N.; Ironson, G.; Siegel, S.D. Stress and health: Psychological, behavioral, and biological determinants. *Annu. Rev. Clin. Psychol.* **2005**, *1*, 607–628. [CrossRef] [PubMed]
23. Slavich, G.M.; Irwin, M.R. From stress to inflammation and major depressive disorder: A social signal transduction theory of depression. *Psychol. Bull.* **2014**, *140*, 774–814. [CrossRef] [PubMed]
24. Weiss, D.S.; Marmar, C.R. The Impact of Event Scale—Revised. In *Assessing Psychological Trauma and PTSD*; Wilson, J.P., Keane, T.M., Eds.; Guilford Press: New York, NY, USA, 1997.
25. Weiss, D.S. The Impact of Event Scale: Revised. In *Cross-Cultural Assessment of Psychological Trauma and PTSD*; Wilson, J.P., Tang, C.S., Eds.; International and Cultural Psychology Series; Springer: Boston, MA, USA, 2007.
26. Soto, C.J.; John, O.P. The Next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. *J. Personal. Soc. Psychol.* **2017**, *113*, 117–143. [CrossRef] [PubMed]
27. Topper, M.; Emmelkamp, P.M.G.; Watkins, E.; Ehring, T. Development and assessment of brief versions of the Penn State Worry Questionnaire and the Ruminative Response Scale. *Br. J. Clin. Psychol.* **2014**, *53*, 402–421. [CrossRef]
28. McLean, C.P.; Asnaani, A.; Litz, B.T.; Hofmann, S.G. Gender differences in anxiety disorders: Prevalence, course of illness, comorbidity, and burden of illness. *J. Psychiatr. Res.* **2011**, *45*, 1027–1035. [CrossRef] [PubMed]
29. Shchebetenko, S.; Kalugin, A.Y.; Mishkevich, A.M.; Soto, C.J.; John, O.P. Measurement invariance and sex and age differences of the Big Five Inventory-2: Evidence from the Russian version. *Assessment* **2020**, *27*, 472–486. [CrossRef]
30. Dear, B.F.; Titov, N.; Sunderland, M.; McMillan, D.; Anderson, T.; Lorian, C.; Robinson, E. Psychometric comparison of the Generalized Anxiety Disorder Scale-7 and the Penn State Worry Questionnaire for measuring response during treatment of Generalised Anxiety Disorder. *Cogn. Behav. Ther.* **2011**, *40*, 216–227. [CrossRef] [PubMed]
31. American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders*, 4th ed.; text rev.; American Psychiatric Association: Washington, DC, USA, 2000.

32. Creamer, M.; Bell, R.; Failla, S. Psychometric properties of the Impact of Event Scale-Revised. *Behav. Res. Ther.* **2003**, *41*, 1489–1496. [CrossRef] [PubMed]
33. Beck, J.G.; Grant, D.M.; Read, J.P.; Clapp, J.D.; Coffey, S.F.; Miller, L.M.; Palyo, S.A. The Impact of Event Scale-Revised: Psychometric properties in a sample of motor vehicle accident survivors. *J. Anxiety Disord.* **2008**, *22*, 187–198. [CrossRef] [PubMed]
34. Gard, M.G.; Kring, A.M. Sex differences in the time course of emotion. *Emotion* **2007**, *7*, 429–437. [CrossRef] [PubMed]
35. Kret, M.E.; De Gelder, B. A review on sex differences in processing emotional signals. *Neuropsychologia* **2012**, *50*, 1211–1221. [CrossRef] [PubMed]
36. Matud, M.P. Gender differences in stress and coping styles. *Personal. Individ. Differ.* **2004**, *37*, 1401–1415. [CrossRef]
37. Endler, N.S.; Kocovski, N.L. State and trait anxiety revisited. *J. Anxiety Disord.* **2001**, *15*, 231–245. [CrossRef] [PubMed]
38. Rapee, R.M. The development of generalized anxiety. In *The Developmental Psychopathology of Anxiety*; Vasey, M.W., Dadds, M.R., Eds.; Oxford University Press: Oxford, UK, 2001; pp. 481–503.
39. Beckwé, M.; Deroost, N.; Koster, E.H.; De Lissnyder, E.; De Raedt, R. Worrying and rumination are both associated with reduced cognitive control. *Psychol. Res.* **2014**, *78*, 651–660. [CrossRef] [PubMed]
40. Zareian, B.; Wilson, J.; LeMoult, J. Cognitive control and ruminative responses to stress: Understanding the different facets of cognitive control. *Front. Psychol.* **2021**, *12*, 660062. [CrossRef] [PubMed]
41. Wright, C.A.; Dobson, K.S.; Sears, C.R. Does a high working memory capacity attenuate the negative impact of trait anxiety on attentional control? Evidence from the antisaccade task. *J. Cogn. Psychol.* **2014**, *26*, 400–412. [CrossRef]
42. Hauser, D.J.; Paolacci, G.; Chandler, J. Common concerns with MTurk as a participant pool: Evidence solutions. In *Handbook of Research Methods in Consumer Psychology*; Kardes, F.R., Herr, P.M., Schwarz, N., Eds.; Routledge: London, UK, 2019; pp. 319–337.
43. Paolacci, G.; Chandler, J. Inside the Turk: Understanding Mechanical Turk as a participant pool. *Curr. Dir. Psychol. Sci.* **2014**, *23*, 184–188. [CrossRef]
44. Miller, J.D.; Crowe, M.; Weiss, B.; Maples-Keller, J.L.; Lynam, D.R. Using online, crowdsourcing platforms for data collection in personality disorder research: The example of Amazon's Mechanical Turk. *Personal. Disord. Theory Res. Treat.* **2017**, *8*, 26–34. [CrossRef] [PubMed]
45. Kim, H.S.; Hodgins, D.C. Reliability and validity of data obtained from alcohol, cannabis, and gambling populations on Amazon's Mechanical Turk. *Psychol. Addict. Behav.* **2017**, *31*, 85–94. [CrossRef] [PubMed]
46. Shapiro, D.N.; Chandler, J.; Mueller, P.A. Using Mechanical Turk to study clinical populations. *Clin. Psychol. Sci.* **2013**, *1*, 213–220. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.