sustainability

Article

Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping

Artur Strzelecki * **and Mariia Rizun**

Department of Informatics, University of Economics in Katowice, 40-287 Katowice, Poland; mariia.rizun@ue.katowice.pl
* Correspondence: artur.strzelecki@ue.katowice.pl

Abstract: This research is dedicated to one of the significant problems connected with purchasing online: consumers' personal data security. The purpose of the paper is to present the results of a study of an incident of a personal data breach from the Morele.net online store that occurred in Poland. The current gap in the literature is the lack of research done among consumers who suffered from a data breach. Data from 826 people affected by this incident were collected and used for drawing conclusions regarding the changes that took place after the incident. The data obtained are both qualitative and quantitative. The data set was analyzed using the IBM SPSS software package. The evolution in consumers' trust towards the store was studied and results reveal that it has strongly decreased, although this did not influence consumers' attitudes towards online shopping in general. The main finding of the research is that one out of three affected consumers will discontinue online shopping on Morele.net; however, they will not tend to change their online shopping behavior in general—they will just purchase in other online stores. Moreover, even though consumers were disappointed, and many were considering no longer purchasing from this site, the store still had significant opportunities to regain consumers' trust and save its competitiveness in the market. The results suggest several improvements that should help online stores stay secure and trustworthy for their consumers. It was revealed that consumers had not previously been greatly concerned about their data being protected by the store; this incident, however, had changed this fact, and now consumers had become much more conscious about providing any of their data to any website.

Keywords: data breach; data leakage; e-commerce; online shopping; trust; security

check for updates

Citation: Strzelecki, A.; Rizun, M. Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability* **2022**, *14*, 5866. https://doi.org/10.3390/su14105866

Academic Editor: Arkadiusz Kawa

Received: 26 March 2022
Accepted: 9 May 2022
Published: 12 May 2022

1. Introduction

E-commerce, or online shopping, is considered in this paper as any business-to-consumer (B2C) sale of products or services, fully or partly conducted by distance communication technology. The objective of this paper is to describe consumers' change in trust in the online store, as well as their awareness of its security, before and after the incident of a data breach. Some consumers were directly affected by the data breach and suffered from the results of personal data theft. In this paper, the intent is to report the exact consequences for consumers and their future anxieties after the incident. The paper is also organized to reveal how consumers evaluate the obligations of an organization to report such an incident within the framework of the General Data Protection Regulation (GDPR).

Therefore, this paper focuses on the consequences of a personal data breach that took place in an online store. The research is based on a case study of the Morele.net online store, which had faced such a breach incident and, as a result, a significant financial loss [1]. The contribution of this study to general research on online shopping consists in obtaining the opinions of consumers who have used this online store, have lost their personal data, and have faced the consequences of the data breach. The state-of-the-art of the research is that it contains a complex study of changes in consumers' opinions: their trust towards this online store; their attitude to online shopping in general; and their awareness of the security of their personal data that they provide to online stores. The data were gathered through a survey of the online store's consumers.

This paper focuses on consumers' trust and security, yet they are not the only important issues related to online shopping. For instance, service quality, usability, and website design are, in fact, valuable components of consumers' overall attitude towards online stores. Trust of consumers towards online stores is based on an aggregation of factors. Among them, there are: consumers' attitudes [2], other consumers' attitudes [3], the reaction of online stores to reviews [4], quality factor [5], set of guarantees such as product warranty policies and product return policies [6], the quality of an online store's website [7], brand reputation or awareness, and product diversity [8].

Security is the feeling consumers using online stores experience when they know that their personal data, provided for a store, are protected and will not be obtained by third parties. Online stores can (and do) guarantee this, for example, by displaying privacy policy agreements and cookies policy information. However, these measures alone may not ensure the safety of consumers' data.

The motivation to study consumers' change in trust and security comes from risks associated with online shopping. Much survey research has been conducted that has further become the basis for models describing attitudes towards online purchase intention [7,9–18]. These studies were conducted among consumers selected by various criteria; however, they were not those who suffered because of the data breach and further consequences of such incidents. Participants in these earlier studies reported their opinions rather than their actual experiences with a data breach or other online phenomena that affected them personally.

In May 2018, in the European Union (EU), Regulation 2016/679, known as GDPR, came into force [19]. Under this rule, reporting a data breach is one of the obligations for all organizations. A data breach occurs when the data for which the organization is responsible suffer a security incident resulting in a breach of confidentiality, availability, or integrity. If that occurs, and it is likely that the breach poses a risk to an individual's rights and freedoms, the organization has to notify the supervisory authority without undue delay and at the latest, within 72 h after having become aware of the breach [20].

The EU implemented the GDPR to make sure online stores take proper care of consumer security [21]. To comply with the GDPR, a website must clearly notify consumers of several important aspects, including pre- and post-contractual information, withdrawal period, usage of cookies, and data protection. To gather consumer information (via registration forms, contact forms, or in the ordering process), online stores must notify consumers that their personal data are being recorded (and why). Additionally, consumers need to be aware of the tools they may use to access their data and modify or delete data if needed.

2. Theoretical Background

Significant for this research is a literature review dedicated to two aspects of e-commerce: data breaches and consumers' trust towards online purchase intention. Detailed exploration of data breaches and consumers' trust towards online purchase intention will help clarify the data breach phenomenon and reveal the gap in consumer trust research. This, in turn, will lead to obtaining thorough answers to the four research questions set out further in the paper.

2.1. Data Breach in Online Shopping

A data breach is a confirmed incident in which sensitive, confidential, or otherwise protected data have been accessed and/or disclosed by any unauthorized party. Data breaches may involve personal health information, personally identifiable information, trade secrets, or intellectual property [22]. Data leakage is the unauthorized transmission of data to another person or entity. Data leakage is not necessarily caused by an intended action. There is no precise definition in the literature. Some researchers use data breach and data leakage as synonyms [23]. Others define this as identity theft [24] or data loss [25]. Identity theft on the Internet is any kind of fraud that results in the loss of personal data, such as passwords, usernames, banking information, or credit card numbers [26]. However, identity theft is caused by data breaches [27]. For some, "leakage" is a situation in which online stores forward data about consumers and purchases to external organizations such as payment systems [28].

Modern cybercriminals are more interested in gathering valuable information about users or platforms themselves than simply in taking down websites [29]. Data leakage is not peculiar to online stores or any other websites but also occurs through mobile applications [30]. In one study, consumers reported more trust in online stores that, as they were told, had never been breached. However, in response to data breaches, the participants did not create more complex passwords or indicate more attention to security of websites [23]. Most internet users consider online stores, not their consumers, to be responsible for online data protection and elimination of consequences of a data breach. The companies that experienced a data breach and took responsibility for its effects were rated high for three trust components—honesty, benevolence, and competence [31]. In this paper, the word "data breach" is used to describe a deliberate action taken by a hacker.

2.2. Trust in Online Shopping

At the beginning of online shopping's development, the topic of trust was well researched. Different models based on the technology acceptance model and different theories based on the theory of reasoned action and the theory of planned behavior affecting trust towards online purchase intention were introduced [32,33]. It was found that in the early days of online shopping development, consumers did not want to provide any of their personal data [5,34].

Several attitudes that have an impact on trust towards online purchase intention have been tested. The identified attitudes positively affecting online purchase intention are: perceived ease-of-use [16]; trust in an offline store [17]; perceived benefits and web quality [7]; relative advantage and perceived website image [35]; quality, awareness, and associations of an online store [9]; efficiency, privacy, and consumer service [36]; convenience and enjoyment [11]; information security; and website performance [14,37]. The attitude that is most often identified as negatively influencing online purchase intention is perceived risk [11,16,38,39]. Studies testing different attitudes affecting online purchase intention have been supported by the answers given in surveys. Participants for these surveys usually were recruited among university students or through Amazon Mechanical. Nevertheless, it has been revealed that consumers are mostly aware of some threats in online shopping.

Other studies of trust have been based on identifying technical factors influencing trust. The trust factor can be strengthened by online consumers' reviews displayed in online stores [3]; web security, availability, and experiences [40]; and the summary review of star rating of the product in online shopping [41]. It has also been found that consumers' trust in online retailers is positively influenced by the level of sophistication of a website when they first see it [42].

Adoption of e-commerce shows that consumers are using mobile websites on mobile devices more and more [43,44]. Security, design, and content factors influence consumers' trust in mobile commerce websites. Trusted websites can provide mobile commerce with powerful competitive advantages [45]. Consumers can easily minimize the possibility of suffering identity theft if they choose safe connections, remember to log out, and use complex passwords [46]. Changes in the European environment that can ensure safe online shopping for consumers are also stressed: terms of service adjusted to the GDPR; usage of well-known payment methods; presence in local price comparison engines; and SSL certificates [47,48]. However, it appears that trust in an online store is more generally determined first by the pleasure features of online use, then by the perceived security features, and rarely by security statements given at a website [23].

Studies on trust towards online shopping intention have been primarily conducted using survey samples to assess opinions about online consumption. They have not been based on actual firsthand experiences of a personal data breach. The participants provided hypothetical responses about online phenomena.

This short review of related works supports claiming that there is still a rather significant gap in the literature regarding the study of post-security breach/data leakage situations in terms of changing trust towards online stores. These situations do not happen very often, nor are they often reported, unless some other factors influence an online store to inform the public that data have been stolen. Usually, online stores do not want to confirm a data breach and maintain that nothing has happened. However, in Europe (since May 2018), the GDPR has been applied, and data administrators are obliged to inform national data protection authorities within 72 h after identifying the incident. Furthermore, consumers who are victims of a data breach can publish or share proof that an incident has taken place [49].

The current gap in the literature exists due to a lack of studies conducted among consumers who suffered from a data breach. Referenced studies are performed among consumers who were aware of some incidents happening but were not directly affected. This work aims at contributing to filling this gap by providing a study on consumers who suffered from a data breach in online shopping [50]. Personal data, including names, addresses, emails, passwords, phone numbers, identity cards, and credit worthiness of around 2.2 M Polish consumers, were stolen [51]. Passwords of 350 K victims were decoded and were used together with email addresses to cause further damages [52]. Considering these facts, this study was prepared to be conducted among the victims of this particular data breach, with the purpose of filling the current gap in the literature. Performing this study is justified by a unique opportunity to conduct research on a large group of people who had suffered from a data leak.

Based on the debates around this topic, the following research questions related to consumers were formulated:

RQ1. Can a personal data breach incident influence consumers' future trust in online shopping in general?

A personal data breach changes consumers' experiences of online shopping. It is necessary to determine the direction of this change: is it a general change or only specific towards a particular online store?

RQ2. Do consumers lose trust in an online store where they have experienced a personal data breach?

A decrease in consumers' trust after losing personal data should be fairly noticeable. However, it is not taken for granted. It is reasonable to investigate how trust has changed by asking about the level of trust before and after the incident. At the same time, it is necessary to determine whether the decrease in trust is correlated with the following research question concerning the fulfillment of the obligations set by the GDPR.

RQ3. How do consumers evaluate the efficacy of the GDPR obligations after a personal data breach?

Current GDPR legislation requires organizations to notify the supervisory authority within 72 h after the organization becomes aware of a data breach. Regardless of how the organization actually fulfilled this obligation, it is necessary to reveal how consumers perceive fulfillment of this obligation by the online store.

RQ4. What actions do consumers take after a personal data breach incident?

After learning that their personal data have been stolen and can be used by hackers, consumers take some actions. Such actions taken by consumers to minimize the consequences of this data breach and avoid future similar incidents are of interest. It is also interesting to find out what consequences the victims of a personal data breach in the selected online store have faced.

The paper is organized as follows. Section 3 includes the concept of the survey and describes its development, while Section 4 presents its qualitative and quantitative results. In Section 5, the contribution of the research is highlighted, its limitations are discussed, conclusions are drawn about the results, and possible future research avenues are proposed.

3. Materials and Methods

In this section, we present the research methodology. We introduce the study subjects, and then we describe our measurement method, which is a questionnaire form followed by the survey procedure.

3.1. Study Subjects

Participants in this survey are customers of the Polish online store Morele.net (hereafter, Morele). Morele provides consumers primarily with electronic goods. It has been operating in the Polish market since 2004 and has around 1.5 million visitors monthly. In November–December 2018, the store had all its consumers' personal data stolen by hackers. Therefore, all consumers who had used Morele during that period became victims of the personal data breach incident (hereafter, "incident"). For this reason, this study is directed at examining consumers' reactions to this incident. It is necessary to add that the victims started facing the first consequences of the data breach (such as email spam, false invoices, and even phone calls) only by the end of December 2018. The survey presented in this paper took place at the beginning of January 2019. Therefore, the feedback of the respondents is considered to be still relevant for the research since their emotions from the data breach were still fresh.

3.2. Measurement Development

The questionnaire contained 14 questions, divided into four sections. Table 1 presents the survey items and their description (what results each question brings for the research). Four of the fourteen questions required answers on a 1–5 Likert-type scale [53], which allowed quantitative data to be obtained (questions 2, 3, 5, and 6). The options for the Likert scale ranged from Lack of—1, e.g., Lack of security feeling, Lack of trust feeling; to Full—5, e.g., Full security feeling. Options 2,3,4 were not named, as they were options to choose between 1 and 5. The remaining questions were close-ended multiple-choice; one open-ended question, which allowed qualitative data to be obtained, was included as well.

Table 1. Questionnaire items.

	Item	Description	Sources
		Introduction	
1	Were you a client of Morele before November 2018?	The questionnaire is directed only at victims of the data breach at Morele. All other users were excluded here.	Own
		The incident	
2	Determine the perceived level of security when transferring data to Morele before the incident.	By security, the "green padlock," privacy policy awareness, logotypes of SSL certificates, cookies policy, etc., are understood. Assessment of the actions taken by Morele to make the consumers feel secure.	[21,54]
3	Determine the trust level when conducting transactions at Morele before the incident.	Trust is consumers' certainty that the entire commercial transaction will proceed correctly, i.e., the parcel will be received on time and without complications, etc. Assessment of the service quality at Morele.	[2,12]
4	How did you find out about the data breach at Morele?	Did Morele succeed in informing all the consumers about the incident quickly enough? Assessment of Morele information campaign.	[55]
5	Determine the level of trust in Morele after the incident.	The attitude of consumers towards Morele after the incident. Most likely based on emotions rather than on the actual security policy of the store.	[2,12,56]
6	Do you think that Morele has fulfilled its GDPR obligations after the incident?	Opinions of consumers on this issue may be subjective, yet they will allow additional assessment of consumers' trust in Morele after the incident.	[19,21]

Table 1. *Cont.*

	Item	Description	Sources
		Post-incident actions	
7	Did you change your password at other online stores after the incident at Morele?	Assessment of changes in consumers' security awareness after the incident.	[21,54]
8	Do you intend to use more complex passwords at online stores after the incident at Morele?		
9	Has the incident at Morele had consequences for you (receiving suspicious emails, false transactions, etc.)?	Assessment of the scale of the incident—its influence on consumers' overall activity on the Internet.	[55,57]
10	Do you intend to continue buying at Morele after the incident?	Assessment of changes in consumers' trust in Morele and online shopping in general after the incident.	[2,56]
11	Do you intend to buy at any other online store after the incident at Morele?		
12	What kinds of goods did/do you mostly buy at Morele?	Answering the only open-ended question in the survey, a respondent shows his/her thoughtful approach to the survey and reliability.	[58,59]
		Metrics	
13	Gender	Demographic characteristics of the sample of respondents (see Table 2).	[60,61]
14	Age		

Source: Own, adapted from [15].

Table 2. Demographic characteristics of sample (n = 826).

Characteristic	Count	Percentage
	Gender	
Male	795	96.24
Female	31	3.76
	Age (years)	
<18	18	2.18
18–24	354	42.86
25–34	307	37.17
35–44	117	14.16
45–54	23	2.78
55–64	4	0.48
65+	0	0
Not given	3	0.36

3.3. Survey Procedure

In order to conduct an effective survey and obtain valid results, it was necessary to have a questionnaire that would be clear for respondents and would contain all the relevant questions. Therefore, a small pre-test was conducted (with a sample of 25 respondents) to find out whether: the order of questions was logical; the questions were clear; the suggested answers (those of multiple choice) were all mutually exclusive; and the questionnaire covered all the issues important for respondents (as victims of the incident). The questionnaire was sent to the people who agreed to take part in the test, attached to a cover letter explaining the purpose of the test and the research itself. Not all respondents of the test sample were affected by the incident, although all the feedback obtained in the test was valuable for the questionnaire improvement. The recommendations on questionnaire refinement were received as direct emails. On the basis of the suggestions, the following amendments to the questionnaire were made: (1) questions 2 and 3 (Table 1, section "Incident") were added to find out how consumers of Morele.net felt about the level of security the store offered before the incident, and also if they generally paid attention to this issue; (2) questions 10 and 11 (Table 1, section "Post-incident actions") were reformulated to be more precise to reveal whether the data breach situation had changed consumers' plans on further using online stores (others than Morele) and whether they still plan to trust Morele when shopping online; (3) answer options to question 11 (Table 1, section "Post-incident actions") were expanded to make sure the consumer can state whether they plan to find a new online store/stay with the one(s) previously used/stop shopping online for a while/never return to shopping online; (4) the answer option "Other" was added to each question to allow the respondents to express an opinion that was not foreseen in the questionnaire; (5) for question 4 (Table 1, section "Incident"), the radio buttons were changed to check boxes to enable the respondents to choose more than one option.

The final version of the questionnaire was shared with potential respondents on 17 January 2019, using such internet channels as: several interest groups on Facebook; personal accounts on LinkedIn; a post on the website Ithardware.pl; and emails to friends and colleagues. The questionnaire was published a month after the official announcement of the data breach and was open for respondents for seven days. We did not measure the individual time of filling; however, we consider question no. 12 to be, to a certain extent, a question to control answers' consistency. The title of the questionnaire was "Morele.net and the incident of a personal data breach." The description of the questionnaire explained that the objective of the survey was to examine the opinions of Morele's consumers who had been affected by the incident. This information, together with the title, was supposed to narrow the target audience to those people who had used Morele. However, to ensure that answers were provided by Morele clients only, question 1 was added (see Table 1) to exclude respondents who did not fit this criterion. Within one week, 1038 questionnaires had been completed, of which 212 contained the answer "No" to the question, "Were you a client of Morele before November 2018?" Therefore, the final sample (*n*) contained 826 respondents—clients of Morele store. Table 2 presents the demographic characteristics of this sample.

4. Results

Based on the collected data, we performed several statistical tests. We present descriptive statistics, followed by the one-way ANOVA test, and then we introduce a hierarchical regression analysis. Finally, we present a summary of qualitative results. The data set was analyzed using the IBM SPSS Software package.

4.1. Descriptive Statistics

The survey contained four questions (2, 3, 5, and 6) with a 1–5 Likert-type scale, from which quantitative data for analysis were obtained. Table 3 presents the data with six indicators. NS (sample size for statistics) is the number of answers obtained for each question. All four questions were answered by all respondents (n = 826). We have achieved statistical reliability for these questions: Split-Half (odd–even) Correlation (0.565), and Split-Half with Spearman–Brown Adjustment (0.722).

Table 3. Descriptive statistics.

	NS	Mean	Median	SD	S. Err	Variance	Security	Original Trust	Changed Trust	GDPR
Security	826	3.3717	4	1.5851	0.0552	2.5126	1			
Original trust	826	4.0218	4	1.0477	0.0365	1.0977	0.394 * (0.417 **)	1		
Changed trust	826	1.7446	1	1.0555	0.0367	1.1140	0.164 * (0.165 **)	0.253 * (0.259 **)	1	
GDPR	826	2.0835	2	1.2569	0.0437	1.5796	0.152 * (0.153 **)	0.202 * (0.205 **)	0.629 * (0.74 **)	1

* p-value < 0.001; ** Fisher's r-to-Z transformation.

The items defined in questions 2, 3, 5, and 6 are security, original trust, changed trust, and GDPR. The Pearson correlation coefficient calculated between these items is given in Table 3. The correlation between security and original trust is moderate (r = 0.394). It reflects the consumers' attitude to perceived security and trust in the online store before the incident. The correlation between changed trust and GDPR is strong (r = 0.629). These two items represent consumers' attitude to the online store after the incident. Items measuring attitude before the incident (security and original trust) have low to very low correlation to items measuring attitude after the incident (changed trust and GDPR): from r = 0.152 to r = 0.253.

The correlation data obtained in this section show that we observe the strongest connection between the variables "GDPR" and "changed trust", i.e., the respondents who stated that Morele had fulfilled its obligation set by the GDPR also expressed higher change in trust of the store after the incident. At the same time, those who stated that Morele had not fulfilled (or weakly fulfilled) GDPR obligations also expressed very low change in trust to this store.

4.2. One-Way ANOVA Test

In Table 4, the one-way ANOVA test is presented. We analyzed four groups: security, original trust, change in trust, and GDPR. Since p-value < α, H_0 is rejected. Some of the groups' averages are considered to not be equal. The difference between the averages of some groups is large enough to be statistically significant. p-value equals 4.44089×10^{-16}. This means that the chance of type1 error (rejecting a correct H_0) is small: 4.441×10^{-16}. The test statistic F equals 602.1535, which is not in the 95% critical value accepted range: $[-\infty: 2.6076]$. The overall observed effect size f is large (0.74). That indicates that the magnitude of the difference between the averages is large. The effect size for the between-group η^2 equals 0.354. It means that the group explains 35.4% of the variance from the average, and the effect is large.

Table 4. One-way ANOVA for four groups: security, original trust, change in trust, and GDPR.

Source	SS	DF	MS	F-Stat	*p*-Value	F-Test
Groups (between groups)	2847.02	3	949.00	602.15	4.44089×10^{-16}	2.60
Error (within groups)	5200.87	3300	1.57			
Total:	8047.90	3303				

SS—Sum of Squares; DF—Degrees of Freedom; MS—Mean Square.

The one-way ANOVA is used to determine whether there are any statistically significant differences between the means of three or more independent groups. There was a statistically significant difference between groups as determined by one-way ANOVA (F (33,300) = 602.15, $p = 4.441 \times 10^{-16}$).

In Table 5, the effect sizes for security, original trust, changed trust, and GDPR are presented.

Table 5. Effect size f for one-way ANOVA summary.

	Security	Original Trust	Changed Trust
Original trust	0.1831		
Changed trust	0.4582	0.6413	
GDPR	0.3628	0.5459	0.0954

4.3. Hierarchical Regression Analysis

Hierarchical regression analysis is a framework for model comparison. In this framework, we build several regression models by adding variables to a previous model at each step; later models include smaller models from previous steps. Our interest is to determine whether newly added variables show a significant improvement in R^2. We used hierarchical regression analysis with security as the dependent variable and original and changed trust plus GDPR as the independent variables. It shows the relative power of the breach and the influence of knowledge about GDPR.

Model 3 does not explain security better than Model 2. The difference of R^2 between Model 2 and 3 is not statistically significant. The increased R^2 0.002 (0.161 − 0.159 = 0.002) is not statistically significant. We can say that the GDPR does not explain an additional 0.2% of the variance in security and it is not statistically significant (Table 6).

Table 6. Hierarchical regression analysis model summary.

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	0.394 [a]	0.155	0.154	1.458	0.155	151.077	1	824	0.000
2	0.399 [b]	0.159	0.157	1.455	0.004	4.358	1	823	0.037
3	0.401 [c]	0.161	0.158	1.454	0.002	1.700	1	822	0.193

[a]. Predictors: (Constant), Original trust. [b]. Predictors: (Constant), Original trust, Changed trust. [c]. Predictors: (Constant), Original trust, Changed trust, GDPR.

The general conclusion from the hierarchical regression analysis would be that, with this particular type of analysis conducted, it is not possible to state with certainty that any of the three predictors (original trust, changed trust, and GDPR fulfillment) has a significantly stronger influence on consumers' feeling of security than the other two.

4.4. Qualitative Results

The other part of the survey (questions 4 and 7–12) allowed collecting qualitative data. Here, the respondents reported what actions they took after being informed about the data breach and whether they had faced any consequences (if yes, which exactly) of this incident. Each question had several possible answers, but the respondents, if they wanted, could also give custom answers. Such responses to each question enriched the obtained data and allowed studying this incident more deeply. Table 7 contains a summary of the answers given to questions 7–11 of the survey.

Table 7. Questions 7 to 11—summary.

Question	Answer Options				
Did you change your password at other online stores after the incident at Morele? (more than one answer possible)	All passwords (29.5%)	Only Morele password (26.8%)	Online shops I'm using (20%)	No changes (16.7%)	Custom answers (7%)
Do you intend to use more complex passwords at online stores after the incident at Morele?	Yes (26.4%)	Only important websites (33.9%)	No (25.1%)	Don't know (7.7%)	Custom answers (6.9%)
Has the incident at Morele had consequences for you (receiving suspicious emails, false transactions, etc.)?	Yes (27.6%)	No (72.4%)			
Do you intend to continue buying at Morele after the incident?	Never (35.5%)	No in any time soon (30.8%)	Yes, I do (22.8%)	Don't know (6.5%)	Custom answers (4.4%)
Do you intend to buy at any other online stores after the incident at Morele?	Yes, I already did (85%)	Yes, in the near future (9.3%)	No (2.8%)	Don't know (2.5%)	Custom answers (0.4%)

Both questions 10 and 11 (as well as all the closed-ended questions) contain the option "Other" (in Table 7, it is the column "Custom answers"), where the respondents could express their opinions in addition to the suggested answers. A few respondents claimed that they would consider buying at Morele only if the store offers better prices than its competitors, stressing that only a significant price difference will be considered. Several respondents also mentioned that they would continue using online stores but pay more attention to the security policy agreements these stores offer. Although such feedback was left by a minority of survey respondents (around 2%), these opinions are considered valuable for the overall research.

Respondents also had an open question (12), where they could provide details of the products they usually bought from Morele. The answers included, among many others, electronics, computer components, software, games and consoles, and small home appliances.

5. Discussion

The data from the questionnaire survey show the online store Morele.net, after the incident of data breach took place, did indeed take the first essential steps defined by the GDPR [62]. The store was obliged to inform the consumers that they had become victims of the data theft. Morele did send an email to all its consumers, but its importance was not that obvious for them [63]. Many recipients ignored it, thinking that this was just another privacy policy update. The subject of the email message, which is supposed to make the objective of the message clear for the recipient, was: "Information from Morele.net group about security". The absence of information about the data breach incident, leak, or personal data theft made the letter seem to be of no value to consumers. Some consumers received the message in their Gmail accounts, and the system sent it to the "Promotions" folder, while Gmail users tend to read only the messages from the main mailbox. Even though Morele tried to fulfill its obligations and sent messages to every consumer, the method of delivering such an important piece of information resulted in only 45% of consumers actually reading it. At the same time, 87.8% of respondents first found information about the incident in online resources such as blogs and portals, 14.8% at Morele.net website, and 12.2% were informed about the incident by their friends. Such a result was obtained from question 4 of the survey used in the research. Answering Research Question 3, it was revealed that the mean value of consumers' opinions on GDPR fulfillment is 2.10 on a scale of 1 to 5, which is relatively low. This confirms that data breach notifications should be improved, as previously noticed by Zou and Schaub [64].

The statistics given in Tables 3–6 lead to the conclusion that Morele lost the trust of its consumers after the data breach. The loss was quite significant and resulted in 35.5% of consumers deciding not to purchase at Morele ever again. Here, Research Question 2 was answered. However, the figures do not reveal a complete loss of consumers' trust. With a proper privacy policy that makes consumers feel secure (and, of course, by not decreasing the quality of goods) [65], Morele still can be trusted by its current consumers and gain new ones in the future [66]. This confirms findings from the theoretical model of post-breach online shopping [13]: the impact of perceived online shopping risk on post-breach online shopping differs significantly from that perceived before this breach. In current literature, respondents in the research studies are often presented with a hypothetical scenario in which a retailer had abused their data through a data breach [67]. This study uses real-life data from a data breach incident.

As the answer to Research Question 1, it was found that a data breach incident at one online store cannot significantly change consumers' attitude towards online shopping in general and make them give it up completely. As seen in Table 7, only 35.5% of the respondents stated that they do not intend to buy at Morele ever again. Similar conclusions after a data breach were reported by Zou et al. [68]. However, some changes in attitude are inevitable. Morele's consumers are now much more aware of the importance of their personal data being secure. That is why many will be using more complex passwords at online stores (and probably at other websites as well). A total of 26.4% stated they will create more complex passwords for every store they use, and 33.9% planned to change passwords only at some most important (perhaps the most frequently used) websites (Table 7). They will also choose online stores more carefully and consciously, paying attention not only to the goods offered but also to the security policies that these stores have [69]. Such a conclusion is drawn from the "other" option, where the respondents could express their opinion in addition to the standard answers. Thus, it can be claimed that Research Question 4 is answered as well.

5.1. Findings

In recent years, online e-commerce transactions have become an essential part of the e-market and have shown great potential. Unfortunately, consumers sometimes experience unexpected consequences when sharing their personal data [70]. When a data breach incident happens, online stores can show that they recognize its significance and treat consumers who have suffered from such incidents efficiently and fairly. This study empirically explores the relationship between an online store and its perception by consumers who have suffered from a personal data breach from this store.

This research has nine major findings. First, consumers tend to evaluate online stores' security factors incompletely, without much awareness. Usually, they seek only the presence of SSL certificates, well-known payment systems, and well-known delivery services [71]. Second, after an incident, consumers dramatically lose their trust in the affected online store. Online stores work to develop their brand and recognition for many years, but they can be irreversibly damaged by one major incident [69]. Third, since May 2018, all online stores in Europe have complied with the GDPR. Consumers are supposed to be well informed that their data needs to be protected, and any organization that processes these data should do so according to the GDPR. However, it seems that organizations are only in the early stages of the complete adaptation of the GDPR. In the event of a data breach, retailers require guidance for mitigating the damage and repairing their relationship with consumers [72]. In our research, we provide such directions based on real-life occurrence. Fourth, emails informing consumers about data breaches should do so in a precise and clear manner. Unfortunately, due to many other incoming emails, consumers do not always pay attention to every email concerning security [64].

Fifth, most users apply the same passwords for all (or many) websites they use. Three out of four consumers stated that they had to change their password after the incident. This implies that they do not use different passwords for different services or do not use any software to manage passwords [73]. Sixth, most of the users do not use complex passwords. More than half of the respondents aimed to increase the complexity of their passwords after the incident. This shows that not only the variety of passwords is significant, but also their complexity [74]. Seventh, not every victim of a data breach faced further consequences [75]. Nearly three out of four consumers did not face any consequences, while some experienced an increase in spam emails in their inbox. However, there is no proof that this spam was caused by this particular data breach incident. Eighth, after the incident of a data breach, most consumers refused to use the online store, which represents a significant loss in the store's expected turnover. Such an incident had a severe negative impact on the store's income [76]. In addition to a natural loss of turnover caused by a decrease in the number of consumers [77], in September 2019, the President of the Personal Data Protection Office (Polish—"UODO") imposed a fine on Morele.net in the amount of 2,830,410 PLN (approximately 660,000 EUR) for the leakage of 2.2 million records as a result of a hacking attack. Finally, consumers became more likely to buy from several online stores rather than just one (even if it was a large store with many different goods). If they stop using one store (or use it less), they will always have other stores where they can continue purchasing online [78]. A data breach's potential costs also include hidden costs such as those resulting from a loss in consumer trust in the online store [79].

5.2. Theoretical Contribution

This research can contribute to the literature on e-commerce behavior from the following perspectives. First, it contributes from a consumer-security perspective. Referring to RQ4, it is important to know what actions the consumers take after a personal data breach incident occurs in an online store they use. Some consumers explicitly use different passwords for different web services. Some consumers use random complex passwords that are stored in password management software such as KeePass or LastPass. More experienced consumers use two-factor authentication. Other consumers, after knowing that data have been leaked, immediately delete their online store account. Using unique passwords for each new account is the best way to protect consumers' data from the possible consequences of the password being stolen. However, some consumers noted that using complex passwords could be useless if there is no proper encryption on the server side. The assumption is that no one should have access to passwords unless they are encrypted in a very strong way. This contribution is new to what was stated previously. A recent study showed that the presence or absence of a previous breach had a minimal impact on consumers' behavioral intentions to be personally more secure [23]. The study presented in this paper evidences that this impact among the affected consumers of the online store is strong. At the same time, the study proves the existence of the "privacy paradox" once again by showing that, on the one hand, the respondents are aware of the significance of the data breach, but on the other hand, they will continue buying at the store (especially if it provides them with good offers).

Second, the paper contributes from a consumer-trust perspective. Referring to RQ2, it is reasonable to find out how consumers change (if they do) their attitude and, in particular, trust towards an online store that has faced a data breach incident [66]. Some consumers experienced a massive loss of access to their accounts in different services. For example, hackers logged in and stole email accounts (e.g., Gmail), social network accounts (e.g., Facebook and Endomondo), gaming accounts (e.g., Steam), accounts for music services (e.g., Spotify), and accounts for TV platforms (e.g., Netflix). Wherever there was the same email address and decrypted password, users' accounts were stolen. Other consumers noticed phone calls from foreign countries and received text messages on mobile phones inviting them to use some premium services. Some consumers were blackmailed regarding having their private data revealed or having false information sent to Facebook friends about viewing pornographic material unless they paid a ransom. Others received false invoices on their email accounts. A recent study showed that consumers are not afraid of identity theft in online shopping and identity theft is insignificant in online shopping [80]. The study in this paper shows that after the identity is stolen, it becomes significant for consumers.

Third, the paper contributes from the perspective of the price of goods. Some consumers stated that they would continue buying at Morele because the store offers the best prices. However, if there was only a slight difference in prices compared to Morele, they would choose another online store.

Fourth, the paper contributes from the perspective of personal data sharing. Some consumers stated that they did not want to give as much personal data as they used to provide before. For instance, they would rather choose a collection point to collect a parcel than provide address details and wait at home for delivery by a courier company. They would also give fewer personal data when they used online stores. They noticed the difference compared to buying at brick-and-mortar stores: usually, there is no need to provide any personal data to purchase there. This contribution stays in line with the previous study's findings that organizations should only collect and hold on to data if needed, and only so long as is required, to limit potential damages if a company is hacked [81].

5.3. Practical Implications

This research is believed to have several practical implications for the online shopping industry. First, from the perspective of consumer-security awareness, it is suggested that online stores make improvements to their website interfaces so that all the necessary information about security and personal data protection is either located and highlighted on the home page or is located on another page, a link to which is highlighted on the home page. This will help decrease the risk of potential data breach incidents. Additionally, showing consumers that online stores care about their personal data will help these stores win (and increase) consumers' trust.

Secondly, the complexity of consumers' passwords is of great importance. The minimum that should be done is for online stores to keep reminding their users about using complex passwords when they register and each time they log into the system. Another important measure for the stores is to make sure the database of passwords provided by the consumers is strongly protected [82].

Another implication suggested concerns consumers' preferences in shopping [76]. They will undoubtedly be much more demanding than they were before the incident. That is why one of the solutions for online stores would be to alter their offers so that they become attractive to consumers, by decreasing prices, creating/improving the discount system, creating more promotions (e.g., buy two, get one free), etc. In the beginning, such a policy might be a little unprofitable for these stores, but when the number of consumers grows significantly, the profit should increase as well.

5.4. Limitations

The study has a few limitations. First, it is limited by the sample size. The number of 826 consumers is not enough to represent the whole population of consumers who have had their personal data stolen from Morele. To draw more valuable conclusions, a survey of a much larger scale would be required.

Second, the timing of the conducted survey might be a certain limitation. The victims of the data breach received the questionnaire almost one month after the incident took place. Although the consequences of the data breach (e.g., spam emails, SMS, etc.) were occurring rather long after the day the data were stolen, it is possible that some of the respondents did not face serious problems and, thus, their emotions as to the incident were not as fresh as they were right after the incident. Moreover, this study represents only a particular slice of time and does not show how consumers' trust may change over time. We encourage future studies to employ a longitudinal design, as it would show the changes, if any, in consumers' trust toward using online shopping over time.

Third, the sample comprised mostly of men (96.24%), and 94% fell between the age of 18 and 44. This is conditioned by the fact that the leading group of goods at Morele includes computer electronics, hardware, and software. It is commonly believed that these products are more frequently bought by men, as well as being more often used by men [83]. However, with a larger sample, more responses from women would be obtained, and they would probably alter the results significantly. Our research participants were the consumers of one particular online shop, and they may not be representative of all consumers who have ever experienced a data breach. Further research is needed to generalize our findings. The questionnaire was sent, among other places, to a large Polish internet portal (ithardware.pl) dedicated to the topics of software and hardware. It can be assumed that men read such portals (and this one in particular) more often than women. This might condition the predominance of male respondents in the questionnaire. However, for now, this is only the authors' assumption, and it would need to be proved by thorough research.

The fourth limitation is derived from the geographical context of the current study: it was conducted in Poland. Although the findings are believed to apply to other European countries that share similar characteristics with Poland and provide their consumers with similar experiences of e-commerce in general and online shopping in particular, these findings are not necessarily applicable to other European countries that lagged behind or moved beyond Poland in terms of e-commerce and online shopping. Therefore, further studies in different countries would most likely strengthen and validate the findings of this study. Our study gives a picture of how consumers react to data breach incidents, but there is no guarantee that consumers' reactions (emotional and those dictated by legislation) in other countries globally (or even within the EU) would be the same. International research would allow data to be gathered that could be processed into general and universal recommendations for behavior during and following such data breach incidents.

Fifth, both questions about trust were asked after the incident. Asking consumers about the level of trust before the incident happened could result in different scores for questions where consumers evaluated the level of trust. As the findings show, the incident influenced trust level, but the initial level was actually set after the incident. The focus of this study was on assessing consumers' intentions rather than their actual behavior.

We believe that it would be worthwhile to investigate real e-commerce behavior towards Morele in future research. This study mainly focused on the effect of trust. There are other factors that might also affect consumers' willingness to use the online store where they lost their data. These factors may include loyalty [66], awareness [71], risk [68], and so on.

Sixth, it is necessary to stress that the situation with Morele was very much discussed in the media. This is not surprising, judging by the scale of the incident (2.2 million consumers). Consumers' discontent and anxiety may have been intensified by all the information (and, possibly, rumors) about the incident. However, this study examines only one case in point, which is Morele, and thus findings cannot be generalized to other online shopping websites. It is highly encouraged that future research examine the trust of consumers toward other online shopping web sites in Poland and discuss any discrepancies or differences in terms of results.

Finally, it is important to mention that the design of the conducted survey may be a certain limitation. In particular, the 1–5 Likert-type scale, although quite widely used, is not a universal tool for surveys and might not give results that would be consistent enough. For further research in this area, it would be reasonable to design a survey with better confirmatory factor analysis. Moreover, it is considered that except for a pilot survey with a small sample of respondents, a pre-test with a few experts might be reasonable for survey improvement. In this study, we measured concepts with a single item in a survey. This is a limitation, because real-world concepts are often complex and therefore require measurement that reflects this complexity. Typically, concepts are measured by multiple items in a questionnaire.

5.5. Future Research

This study has inspired several directions for further research. First, it would be reasonable to study the data breach more from the perspective of online stores to find out how (and if) their policy (for consumers' data protection, server security, GDPR fulfillment, etc.) changes after they have a data breach incident. To get a broader picture of the situation, such research would require information from more than one online store and, probably, more than one country. From this idea comes another direction of research: conducting a comparative analysis of several of the most well-known data breach incidents that have occurred in the online shopping industry. Such a study would enable researchers to see if, and to what extent, the scale and consequences of an incident depend on the region, the population, or, probably, customers' mentality. This would also represent a contribution from the point of view of experience, as the steps taken by online stores that have had data breach incidents would help create valuable guidelines for other online stores that may become victims of hackers.

It is necessary to note that the above-mentioned research avenues are limited to online shopping. There are, however, many more websites that require personal data from their users and, as a result, may become potential targets for hackers. That is why to expand the field of research, it can be suggested to proceed with studying data breach incidents in the other spheres of internet usage (e.g., forums and portals for gaming, music, or TV). A comparison of these incidents in online shopping would also make an interesting contribution to the research on electronic commerce.

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

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved by the Faculty of Informatics and Communication of the University of Economics in Katowice (WIIK-180102019: 18 January 2019).

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

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

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

References

1. Gabriel, B.S.; Silviu, G.A. Trends regarding fines and sanctions in competition law, labor law and data protection law. *Law Rev.* **2019**, *10*, 17–25.
2. Chen, Y.; Chou, T. Exploring the continuance intentions of consumers for B2C online shopping. *Online Inf. Rev.* **2012**, *36*, 104–125. [CrossRef]
3. Lee, J.; Park, D.H.; Han, I. The different effects of online consumer reviews on consumers' purchase intentions depending on trust in online shopping malls: An advertising perspective. *Internet Res.* **2011**, *21*, 187–206. [CrossRef]
4. Matzat, U.; Snijders, C. Rebuilding Trust in Online Shops on Consumer Review Sites: Sellers' Responses to User-Generated Complaints. *J. Comput. Commun.* **2012**, *18*, 62–79. [CrossRef]
5. Grabner-Kraeuter, S. The role of consumers' trust in online-shopping. *J. Bus. Ethics* **2002**, *39*, 43–50. [CrossRef]
6. Stouthuysen, K.; Teunis, I.; Reusen, E.; Slabbinck, H. Initial trust and intentions to buy: The effect of vendor-specific guarantees, customer reviews and the role of online shopping experience. *Electron. Commer. Res. Appl.* **2018**, *27*, 23–38. [CrossRef]
7. Al-Debei, M.M.; Akroush, M.N.; Ashouri, M.I. Consumer attitudes towards online shopping: The effects of trust, perceived benefits, and perceived web quality. *Internet Res.* **2015**, *25*, 707–733. [CrossRef]
8. Kim, S.S. Purchase Intention in the Online Open Market: Do Concerns for E-Commerce Really Matter? *Sustainability* **2020**, *12*, 773. [CrossRef]
9. Das, G. Antecedents and consequences of trust: An e-tail branding perspective. *Int. J. Retail Distrib. Manag.* **2016**, *44*, 713–730. [CrossRef]
10. Sreeram, A.; Kesharwani, A.; Desai, S. Factors affecting satisfaction and loyalty in online grocery shopping: An integrated model. *J. Indian Bus. Res.* **2017**, *9*, 107–132. [CrossRef]
11. Akram, M.S. Drivers and Barriers to Online Shopping in a Newly Digitalized Society. *TEM J.* **2018**, *7*, 118–127. [CrossRef]
12. Yi, Y.; Gong, T. The effects of customer justice perception and affect on customer citizenship behavior and customer dysfunctional behavior. *Ind. Mark. Manag.* **2008**, *37*, 767–783. [CrossRef]
13. Chakraborty, R.; Lee, J.; Bagchi-Sen, S.; Upadhyaya, S.; Raghav Rao, H. Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decis. Support Syst.* **2016**, *83*, 47–56. [CrossRef]
14. Shafiee, M.M.; Bazargan, N.A. Behavioral Customer Loyalty in Online Shopping: The Role of E-Service Quality and E-Recovery. *J. Theor. Appl. Electron. Commer. Res.* **2018**, *13*, 26–38. [CrossRef]
15. Lin, A.J.; Li, E.Y.; Lee, S.-Y. Dysfunctional customer behavior in cross-border e-commerce: A Justice-affect-behavior model. *J. Electron. Commer. Res.* **2018**, *19*, 36–54.
16. van der Heijden, H.; Verhagen, T.; Creemers, M. Understanding online purchase intentions: Contributions from technology and trust perspectives. *Eur. J. Inf. Syst.* **2003**, *12*, 41–48. [CrossRef]
17. Hahn, K.H.; Kim, J. The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context. *Int. J. Retail Distrib. Manag.* **2009**, *37*, 126–141. [CrossRef]
18. Lim, W.M. Antecedents and consequences of e-shopping: An integrated model. *Internet Res.* **2015**, *25*, 184–217. [CrossRef]
19. European Parliament Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (accessed on 27 January 2019).
20. Mohan, J.; Wasserman, M.; Chidambaram, V. Analyzing GDPR Compliance Through the Lens of Privacy Policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*; Springer: Cham, Switzerland, 2019; pp. 82–95.
21. Presthus, W.; Sørum, H. Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Procedia Comput. Sci.* **2018**, *138*, 603–611. [CrossRef]
22. Chatterjee, S.; Gao, X.; Sarkar, S.; Uzmanoglu, C. Reacting to the scope of a data breach: The differential role of fear and anger. *J. Bus. Res.* **2019**, *101*, 183–193. [CrossRef]
23. Curtis, S.R.; Carre, J.R.; Jones, D.N. Consumer security behaviors and trust following a data breach. *Manag. Audit. J.* **2018**, *33*, 425–435. [CrossRef]
24. Maitlo, A.; Ameen, N.; Peikari, H.R.; Shah, M. Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. *Inf. Technol. People* **2019**, *32*, 1184–1214. [CrossRef]
25. Valecha, R.; Bachura, E.; Chen, R.; Raghav Rao, H. An Exploration of Public Reaction to the OPM Data Breach Notifications. In *Internetworked World*; Lecture Notes in Business Information Processing; Fan, M., Heikkilä, J., Li, H., Shaw, M.J., Zhang, H., Eds.; Springer: Cham, Switzerland, 2017; Volume 296, pp. 185–191, ISBN 978-3-319-69643-0.
26. Van Schaik, P.; Jeske, D.; Onibokun, J.; Coventry, L.; Jansen, J.; Kusev, P. Risk perceptions of cyber-security and precautionary behaviour. *Comput. Human Behav.* **2017**, *75*, 547–559. [CrossRef]

27. Pelteret, M.; Ophoff, J. A review of information privacy and its importance to consumers and organizations. *Inf. Sci.* **2016**, *19*, 277–301. [CrossRef]
28. Preibusch, S.; Peetz, T.; Acar, G.; Berendt, B. Shopping for privacy: Purchase details leaked to PayPal. *Electron. Commer. Res. Appl.* **2016**, *15*, 52–64. [CrossRef]
29. Molok, N.N.A.; Chang, S.; Ahmad, A. Information leakage through online social networking: Opening the doorway for advanced persistence threats. In Proceedings of the 8th Australian Information Security Management Conference, Perth, Australia, 30 November–2 December 2010; pp. 70–80.
30. Yang, Z.; Yang, M.; Zhang, Y.; Gu, G.; Ning, P.; Wang, X.S. AppIntent: Analyzing sensitive data transmission in android for privacy leakage detection. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security—CCS '13, Berlin, Germany, 4–8 November 2013; ACM: New York, NY, USA, 2013; pp. 1043–1054.
31. Carre, J.R.; Curtis, S.R.; Jones, D.N. Ascribing responsibility for online security and data breaches. *Manag. Audit. J.* **2018**, *33*, 436–446. [CrossRef]
32. Gefen, D.; Karahanna, E.; Straub, D.W. Trust and TAM in online shopping: An integrated model. *MIS Q.* **2003**, *27*, 51–90. [CrossRef]
33. Lankton, N.K.; McKnight, D.H.; Thatcher, J.B. The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website. *IEEE Trans. Eng. Manag.* **2012**, *59*, 654–665. [CrossRef]
34. Hoffman, D.L.; Novak, T.P.; Peralta, M. Building consumer trust online. *Commun. ACM* **1999**, *42*, 80–85. [CrossRef]
35. Akroush, M.N.; Al-Debei, M.M. An integrated model of factors affecting consumer attitudes towards online shopping. *Bus. Process Manag. J.* **2015**, *21*, 1353–1376. [CrossRef]
36. Al-dweeri, R.M.; Obeidat, Z.M.; Al-dwiry, M.A.; Alshurideh, M.T.; Alhorani, A.M. The impact of e-service quality and e-loyalty on online shopping: Moderating effect of e-satisfaction and e-trust. *Int. J. Mark. Stud.* **2017**, *9*, 92–103. [CrossRef]
37. Akram, U.; Hui, P.; Kaleem Khan, M.; Tanveer, Y.; Mehmood, K.; Ahmad, W. How website quality affects online impulse buying. *Asia Pac. J. Mark. Logist.* **2017**, *30*, 235–256. [CrossRef]
38. Pappas, N. Marketing strategies, perceived risks, and consumer trust in online buying behaviour. *J. Retail. Consum. Serv.* **2016**, *29*, 92–103. [CrossRef]
39. Harrison McKnight, D.; Choudhury, V.; Kacmar, C. The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *J. Strateg. Inf. Syst.* **2002**, *11*, 297–323. [CrossRef]
40. Köksal, Y.; Penez, S. An investigation of the important factors influence web trust in online shopping. *J. Mark. Manag.* **2015**, *6*, 28–40.
41. Tamimi, N.; Sebastianelli, R. The relative importance of e-tailer website attributes on the likelihood of online purchase. *Internet Res.* **2015**, *25*, 169–183. [CrossRef]
42. Mohr, H.; Walter, Z. Formation of Consumers' Perceived Information Security: Examining the Transfer of Trust in Online Retailers. *Inf. Syst. Front.* **2019**, *21*, 1231–1250. [CrossRef]
43. Liébana-Cabanillas, F.; Marinković, V.; Kalinić, Z. A SEM-neural network approach for predicting antecedents of m-commerce acceptance. *Int. J. Inf. Manag.* **2017**, *37*, 14–24. [CrossRef]
44. Gupta, A.; Arora, N. Understanding determinants and barriers of mobile shopping adoption using behavioral reasoning theory. *J. Retail. Consum. Serv.* **2017**, *36*, 1–7. [CrossRef]
45. Nilashi, M.; Ibrahim, O.; Reza Mirabi, V.; Ebrahimi, L.; Zare, M. The role of security, design and content factors on customer trust in mobile commerce. *J. Retail. Consum. Serv.* **2015**, *26*, 57–69. [CrossRef]
46. Van Bavel, R.; Rodríguez-Priego, N.; Vila, J.; Briggs, P. Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud.* **2019**, *123*, 29–39. [CrossRef]
47. Strzelecki, A. Key Features of E-Tailer Shops in Adaptation to Cross-Border E-Commerce in the EU. *Sustainability* **2019**, *11*, 1589. [CrossRef]
48. Kalinić, Z.; Ranković, V.; Kalinić, L. Challenges in Cross-border E-commerce in the European Union. *Zesz. Nauk. Uniw. Ekon. Krakowie* **2018**, *5*, 159–170. [CrossRef]
49. Strzelecki, A.; Rizun, M. Consumers' security and trust for online shopping after GDPR: Examples from Poland and Ukraine. *Digit. Policy Regul. Gov.* **2020**, *22*, 289–305. [CrossRef]
50. Kosior, K. Economic, Ethical and Legal Aspects of Digitalization in the Agri-Food Sector. *Probl. Agric. Econ.* **2020**, *263*, 53–72. [CrossRef]
51. Wojtkowski, Ł.; Brodzińska-Mirowska, B.; Seklecka, A. Polish Privacy Media Discourse: Privacy as Imposed Policies. *Media Commun.* **2020**, *8*, 302–313. [CrossRef]
52. Zaburko, J.; Szulżyk-Cieplak, J. Information security risk assessment using the AHP method. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *710*, 12036. [CrossRef]
53. Likert, R. A technique for the measurement of attitudes. *Arch. Psychol.* **1932**, *22*, 55.
54. Vladlena, B.; Saridakis, G.; Tennakoon, H.; Ezingeard, J.N. The role of security notices and online consumer behaviour: An empirical study of social networking users. *Int. J. Hum. Comput. Stud.* **2015**, *80*, 36–44. [CrossRef]
55. Adjerid, I.; Acquisti, A.; Brandimarte, L.; Loewenstein, G. Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proceedings of the Ninth Symposium on Usable Privacy and Security—SOUPS '13, Newcastle, UK, 24–26 July 2013; ACM: New York, NY, USA, 2013; pp. 9:1–9:17.

56. Ba, S. Establishing online trust through a community responsibility system. *Decis. Support Syst.* **2001**, *31*, 323–336. [CrossRef]
57. Choi, K. Computer crime victimization and integrated theory: An empirical assessment. *Int. J. Cyber Criminol.* **2008**, *2*, 308–333.
58. Alreck, P.; Settle, R.B. Gender effects on Internet, catalogue and store shopping. *J. Database Mark. Cust. Strateg. Manag.* **2002**, *9*, 150–162. [CrossRef]
59. Hernández, B.; Jiménez, J.; José Martín, M. Age, gender and income: Do they really moderate online shopping behaviour? *Online Inf. Rev.* **2011**, *35*, 113–133. [CrossRef]
60. Babin, B.J.; Griffin, M. A closer look at the influence of age on consumer ethics. In *Advances in Consumer Research*; Association for Consumer Research: Duluth, MN, USA, 1995; Volume 22, pp. 668–673, ISBN 0098-9258r0-915552-34-5.
61. Couper, M.P. Review: Web Surveys: A Review of Issues and Approaches. *Public Opin. Q.* **2000**, *64*, 464–494. [CrossRef]
62. Renaud, K.; Shepherd, L.A. How to Make Privacy Policies both GDPR-Compliant and Usable. In Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, 11–12 June 2018; pp. 1–8.
63. Zou, Y.; Danino, S.; Sun, K.; Schaub, F. You "Might" Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In Proceedings of the CHI Conference on Human Factors in Computing Systems—CHI '19, Glasgow, UK, 4–9 May 2019; ACM Press: New York, NY, USA, 2019; pp. 1–14.
64. Zou, Y.; Schaub, F. Beyond Mandatory: Making Data Breach Notifications Useful for Consumers. *IEEE Secur. Priv.* **2019**, *17*, 67–72. [CrossRef]
65. Syed, R. Enterprise reputation threats on social media: A case of data breach framing. *J. Strateg. Inf. Syst.* **2019**, *28*, 257–274. [CrossRef]
66. Chen, H.S.; Jai, T.-M. Trust fall: Data breach perceptions from loyalty and non-loyalty customers. *Serv. Ind. J.* **2021**, *41*, 947–963. [CrossRef]
67. Pallant, J.I.; Pallant, J.L.; Sands, S.J.; Ferraro, C.R.; Afifi, E. When and how consumers are willing to exchange data with retailers: An exploratory segmentation. *J. Retail. Consum. Serv.* **2022**, *64*, 102774. [CrossRef]
68. Zou, Y.; Mhaidli, A.H.; McCall, A.; Schaub, F. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018), Baltimore, MD, USA, 12–14 August 2018; {USENIX} Association: Baltimore, MD, USA, 2018; pp. 197–216.
69. Janakiraman, R.; Lim, J.H.; Rishika, R. The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *J. Mark.* **2018**, *82*, 85–105. [CrossRef]
70. Hao, J.; Dai, H. Social media content and sentiment analysis on consumer security breaches. *J. Financ. Crime* **2016**, *23*, 855–869. [CrossRef]
71. Nield, J.; Scanlan, J.; Roehrer, E. Exploring Consumer Information-Security Awareness and Preparedness of Data-Breach Events. *Libr. Trends* **2020**, *68*, 611–635. [CrossRef]
72. Martin, K.D.; Kim, J.J.; Palmatier, R.W.; Steinhoff, L.; Stewart, D.W.; Walker, B.A.; Wang, Y.; Weaven, S.K. Data Privacy in Retail. *J. Retail.* **2020**, *96*, 474–489. [CrossRef]
73. Ion, I.; Reeder, R.; Consolvo, S. "...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In Proceedings of the Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015), Ottawa, ON, Canada, 22–24 July 2015; {USENIX} Association: Ottawa, Canada, 2015; pp. 327–346.
74. Thomas, K.; Pullman, J.; Yeo, K.; Raghunathan, A.; Kelley, P.G.; Invernizzi, L.; Benko, B.; Pietraszek, T.; Patel, S.; Boneh, D.; et al. Protecting accounts from credential stuffing with password breach alerting. In Proceedings of the 28th {USENIX} Security Symposium ({USENIX} Security 19), Santa Clara, CA, USA, 14–16 August 2019; Association: Santa Clara, CA, USA, 2019; pp. 1556–1571.
75. Alazab, M.; Hong, S.-H.; Ng, J. Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Futur. Gener. Comput. Syst.* **2021**, *116*, 22–29. [CrossRef]
76. Goode, S.; Hoehle, H.; Venkatesh, V.; Brown, S.A. User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach. *MIS Q.* **2017**, *41*, 703–727. [CrossRef]
77. Gwebu, K.L.; Wang, J.; Wang, L. The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *J. Manag. Inf. Syst.* **2018**, *35*, 683–714. [CrossRef]
78. Choi, B.C.F.; Kim, S.S.; Jiang, Z. (Jack) Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *J. Manag. Inf. Syst.* **2016**, *33*, 904–933. [CrossRef]
79. Schneider, M.J.; Jagpal, S.; Gupta, S.; Li, S.; Yu, Y. A Flexible Method for Protecting Marketing Data: An Application to Point-of-Sale Data. *Mark. Sci.* **2018**, *37*, 153–171. [CrossRef]
80. Yu, S. Does fear of victimization deter online shopping? *J. Financ. Crime* **2018**, *25*, 770–783. [CrossRef]
81. Manworren, N.; Letwat, J.; Daily, O. Why you should care about the Target data breach. *Bus. Horiz.* **2016**, *59*, 257–266. [CrossRef]
82. Wei, W.; Zhang, L.; Hua, N. Error management in service security breaches. *J. Serv. Mark.* **2019**, *33*, 783–797. [CrossRef]
83. Morahan-Martin, J. The gender gap in internet use: Why men use the internet more than women—A literature review. *CyberPsychology Behav.* **1998**, *1*, 3–10. [CrossRef]