THE JOURNAL OF RESEARCH REVIEW

P-ISSN: 3006-2632	E-ISSN: 3006-2640
Vol. 3. No. 01 (Jan-Mar) 2026	Page 355-376

https://doi.org/10.5281/zenodo.20290538

Users' Response to Data Breach Notifications: A Survey-Based Study

Maheen Asghar Khan	*BSCyS, Air University Multan Campus, Islamabad.* maheenasghar3122@gmail.com
Sheraz Hussain	*BSCyS, Air University Multan Campus, Islamabad.* sheraztabish749@gmail.com
Muhammad Jameel	*BSCyS, Air University Multan Campus, Islamabad.* pak101135512@gmail.com
Faheem Shahid	*BSCyS, Air University Multan Campus, Islamabad* faheemshahid8017@gmail.com
Dr. Muhammad Arfan Lodhi **(Corresponding Author)**	Higher Education Department, Punjab samaritan_as@hotmail.com

Abstract: *Data breaches have become an increasingly persistent challenge in the digital era, making user response a critical component of effective cyber security. Organizations commonly rely on data breach notifications (DBNs) to inform affected individuals and encourage protective action; however, user reactions often vary considerably. This study examines how users perceive and respond to breach notifications by focusing on five key dimensions: awareness, threat detection capability, emotional response, trust in organizational communication, and protective behavioral intentions. Using a structured survey distributed among undergraduate students through a stratified sampling approach, the study explores the relationship between users' understanding of data breaches and their actual security-related behavior. The findings reveal that while participants generally demonstrate strong awareness of cyber security risks and are capable of identifying suspicious activities, this awareness does not consistently translate into proactive protective behavior. A noticeable gap exists between recognizing security threats and taking effective action in response to them. The results further indicate that users' emotional reactions are closely linked to how severe they perceive a breach to be, with stronger emotional responses often motivating greater behavioral engagement. In addition, the clarity, transparency, and credibility of breach notifications emerged as influential factors shaping user trust and willingness to respond appropriately. The study highlights that awareness alone is insufficient to ensure secure user behavior. Instead, the effectiveness of breach notifications largely depends on how information is communicated. Clear, transparent, and user-centered notifications can strengthen trust, encourage timely action, and ultimately reduce the negative impact of cybersecurity incidents on individuals and organizations alike.*

Keywords: Data Breach Notifications (DBNs), Cyber security Awareness, Detection Ability, Protective Behavior, Emotional Response, Information Security, Risk Communication.

1. Introduction

The pervasive integration of digital systems into modern society has fundamentally restructured how we interact, learn, commerce, and manage daily life. Today, online platforms are no longer merely convenient tools; they are the core infrastructure supporting human communication, academic instruction, financial transactions, and civic engagement. However, this total reliance on digital ecosystems has created an unprecedented expansion of the collective attack surface, leaving individuals more exposed than ever to sophisticated cybersecurity threats. Foremost among these dangers is the data breach as an incident where private, sensitive, or protected information is accessed by unauthorized actors. As organizations aggressively collect and store vast repositories of user data to power their services, the stakes of data security have grown exponentially. When a security failure occurs, the blast radius is rarely contained; instead, it tends to be widespread, impacting millions of individuals simultaneously and exposing highly sensitive assets like financial records, cryptographic credentials, and personally identifiable information (PII). In response to this escalating threat landscape, regulatory frameworks and corporate protocols have standardized the use of Data Breach Notifications (DBNs). These alerts are dispatched to affected users with the dual objective of establishing operational transparency and prompting immediate, defensive behaviors such as rotating passwords, monitoring credit reports, or enabling multi-factor authentication. Despite the critical importance of these notifications, cybersecurity professionals face a persistent and frustrating challenge: DBNs frequently fail to elicit the necessary protective actions from the users who receive them. Instead of acting immediately, many users ignore the warnings, delay their response, or dismiss the threat entirely. This systemic failure in risk communication highlights a significant disconnect between a technical alert and human psychology. Consequently, understanding the behavioral economics, cognitive biases, and psychological barriers that dictate how individuals actually read, interpret, and react to breach notifications has become one of the most critical frontiers in modern cybersecurity. Investigating these human-centric factors is essential for designing communication strategies that move beyond mere legal compliance and instead effectively drive proactive, real-world defense.

1.1 Background of the Study

A data breach occurs whenever unauthorized individuals gain access to sensitive, confidential, or protected information that they were never intended to see. These incidents are highly diverse in their origins and generally manifest in one of three ways: external attacks, internal vulnerabilities, or accidental exposures. External threats involve sophisticated cybercriminal tactics such as hacking, spear-phishing, or the deployment of malicious software. Conversely, internal breaches are precipitated from within an organization, often driven by employee negligence or, in rarer cases, malicious insiders. Accidental exposures represent purely operational or administrative lapses, such as misconfigured cloud databases or files shared inadvertently by staff. Regardless of the root cause, the fallout of these events typically involves the compromise of high-value assets, including cryptographic credentials, financial records, and personally identifiable information (PII).

To mitigate the subsequent risks of identity theft and financial fraud, global regulatory frameworks increasingly mandate that organizations issue data breach notifications (DBNs) to affected individuals. The core objective of these notifications is operational transparency: they are designed to alert users to the compromise, quantify the potential risk to their personal data, and prescribe immediate remedial actions, such as rotating passwords or activating multi-factor authentication. However, empirical studies reveal that user compliance with these alerts remains highly inconsistent. This behavioral friction is largely driven by complex psychological phenomena and communication failures, most notably warning fatigue and the phishing paradox.

Warning fatigue manifests as a form of cognitive desensitization born from an over-connected digital ecosystem. Because modern users are continuously bombarded with security prompts, cookie consent

banners, and system alerts, they begin to tune out these signals. When a critical data breach notification finally arrives, it is often dismissed reflexively because the user has subconsciously rationalized that the risk is either exaggerated or irrelevant. This apathy is further compounded by the phishing paradox, a structural irony in cybersecurity communication. Because users are continuously trained to spot and distrust unsolicited emails that demand urgent security action, authentic breach notifications frequently mimic the exact visual and linguistic cues of the social engineering attacks they warn against. Fearful of falling victim to a scam, users routinely delete legitimate alerts, thereby delaying vital protective actions.

Ultimately, research demonstrates that a user's behavioral response to a data breach notification is governed by how they perceive the severity of the breach, the clarity of the message, and the honesty of the organization. If the notification uses alienating technical jargon or if the company appears defensive and evasive, user trust erodes, directly undermining the credibility of the remediation advice. University students represent an especially critical demographic for studying these behavioral dynamics. As digital natives whose personal, academic, and financial lives are deeply integrated with online platforms, their expansive digital footprint leaves them highly exposed to systemic risks. While this population is widely assumed to possess the digital literacy and technical competence necessary to protect them, empirical evidence highlights a stark knowledge-behavior gap. Students regularly demonstrate a sophisticated awareness of cybersecurity threats, yet they consistently fail to implement basic protective behaviors due to convenience or optimism bias. Investigating how this demographic reads and reacts to breach notifications is essential for designing psychologically optimized communication strategies that can effectively bridge the gap between risk awareness and proactive defense.

1.2 Statement of the Problem

Even with breach notification laws now in place across many regions, there's still a stubborn gap between users being told something happened and users actually doing something about it. Companies invest in technical defenses like encryption and multi-factor authentication, but none of that matters if people simply ignore the alerts or wait too long to act. The notifications themselves vary so much in tone, design, and detail that they often fall flat. Most existing research zooms in on what the organization does after a breach the apologies, the credit monitoring offers, the public statements but not enough has been said about how breach details (like who's really to blame and whether it could have been prevented) or the way the message is delivered shape individual responses. Then there's the "phishing paradox," which still hasn't gotten the attention it deserves: the more security alerts people see, the more they start treating real ones as scams. We also don't know nearly enough about how specific groups, like university students, interpret breach severity or assign blame. Things like the type of data leaked, how many records were involved, and how openly the company communicates probably all matter, but exactly how they combine to drive behavior isn't well understood. That makes it hard for organizations to design notifications that actually work. This study sets out to fill some of those gaps by examining how users react to breach notifications and what really moves the needle on their emotions, trust, and protective behavior. The goal is to feed into better communication practices that get people to respond and lower their risk after a breach.

1.3 Research Questions

To meet the research objectives, this study works through the following questions:

1. How do breach-related attributes, such as the sensitivity of compromised data and the perceived severity of the incident, influence users' perception of risk and their likelihood of taking protective actions?
2. To what extent do communication factors, including the clarity of the notification and the source of disclosure (organization vs. third party), affect users' trust and emotional response to

data breach notifications?

3. How does user awareness and detectionability influence their actual behavioral response to data breach notifications, particularly in terms of actions such as password changes and adoption of additional security measures?
4. Is there a gap between awareness and behavior, and what factors contribute to users failing to take appropriate protective actions despite understanding the risks associated with data breaches?

1.4 Significance of the Study

This study matters on three levels theoretical, practical, and policy for anyone trying to make sense of how users react to data breach notifications. On the theory side, it brings Situational Crisis Communication Theory (SCCT) and the Social-Mediated Crisis Communication (SMCC) model into the world of digital security incidents, where most research has focused on the technical side and not so much on the people involved. It offers empirical evidence on how things like perceived breach severity, notification clarity, and organizational transparency shape user emotions, trust, and the actions they take afterward. The study also calls out the gap between knowing about data breaches and actually doing something about them, especially among university students who spend plenty of time online but don't always follow through on basic security practices. On the practical side, the findings give organizations and security teams something concrete to work with when designing notifications that actually do their job. By calling out problems like warning fatigue, vague wording, and inconsistent formats, it opens the door to building user-centered communication strategies that nudge users to take action quickly. The takeaway here is that companies need to drop the cookie-cutter notification approach and switch to messaging that's clearer, better organized, and honest enough to actually keep users on board. The study points to clear directions for both institutions and regulators trying to tighten up data protection.

1.5 Hypotheses

- **H1:** Higher perceived severity of a data breach is positively associated with stronger emotional responses.
- **$H0_1$:** Perceived breach severity has no significant relationship with emotional responses.
- **H2:** Stronger emotional responses are positively associated with protective behavioral intentions.
- **$H0_2$:** Emotional responses have no significant effect on protective behavioral intentions.

2. Literature Review

2.1 Conceptual Background

A data breach is basically a security incident where sensitive or protected information ends up exposed, stolen, or seen by someone who shouldn't have access to it. They can happen in a few different ways outside attackers using hacking or malware, employees misusing access from the inside, or simple slip-ups like a database left open by mistake. Since companies now lean on digital systems for almost everything, breaches have grown both more common and more damaging, which is why they've turned into such a big worry for users and organizations alike.

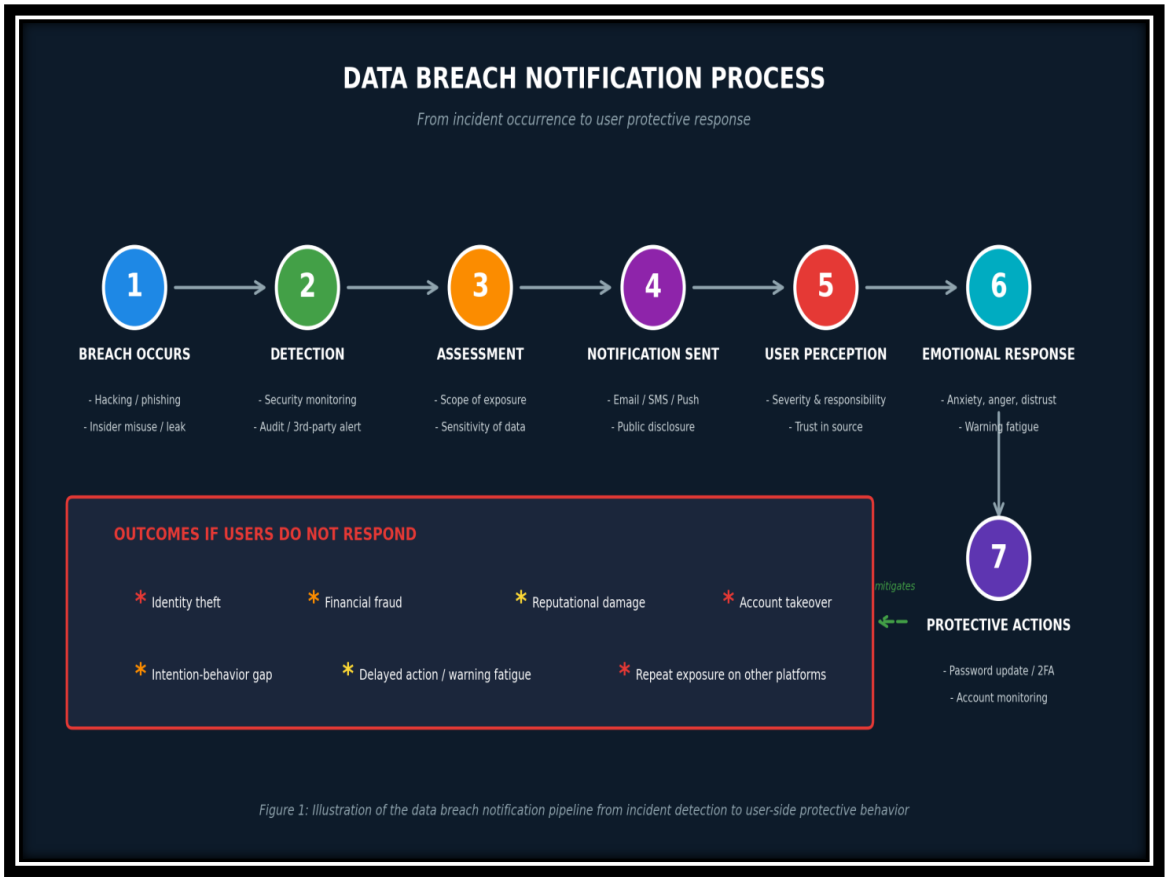

Figure 1: Conceptual diagram of key factors influencing user responses to data breach notifications

When a breach happens, companies usually respond by sending out data breach notifications (DBNs) to let affected users know what happened, what kind of data was caught up in it, and what they should do to limit the damage. The whole point is to push users toward protective steps like updating passwords, keeping an eye on their accounts, or turning on extra security. The catch is that whether those notifications actually work depends almost entirely on how users read and react to them. How users respond isn't just about the technical side of the breach. A lot of it comes down to human factors how people perceive what happened, whether they trust the source, and how it makes them feel. Things like perceived severity of the breach, clarity of the notification message, and transparency of the organization all play a big part in shaping how users behave. When a notification is vague, hard to follow, or missing important detail, people often just ignore it or don't bother taking the right steps. Research has shown that being aware of breaches doesn't automatically push users to act on them. That gap between knowing and doing is exactly why breach notifications need to be studied from both a technical and a behavioral angle. So in this study we look not just at what data breaches are, but also at how users actually read and respond to notifications, with a focus on how the design of the message and the way people perceive it can improve the bigger cyber security picture.

2.2 Review of Empirical Studies

Existing literature on user responses to data breach notifications highlights a broad range of interconnected issues, including usability challenges, gaps in cybersecurity awareness, emotional and psychological reactions, trust in organizations, and the effectiveness of protective behavioral responses. Collectively, these studies demonstrate that while breach notifications are intended to encourage timely and informed action, users' actual responses are often inconsistent, delayed, or ineffective. A recurring theme throughout the literature is the persistent disconnect between awareness and meaningful behavioral change.

A significant body of research has focused on the usability and readability of breach notifications themselves. For instance, Zou et al. conducted a content analysis of data breach notifications and identified major readability and usability concerns. Their findings revealed that many notifications are written at a complexity level that exceeds the comprehension ability of the average user. In addition, the use of vague or hedging language often obscures the seriousness of the breach, making it difficult for users to accurately assess risk and determine appropriate actions. Building on this issue, Mayer et al. observed that although a large proportion of users had previously experienced data breaches, many remained unaware of numerous incidents affecting them. This finding exposed a clear intention–behavior gap, where users express concern and an intention to act but fail to translate those intentions into practical cybersecurity measures.

Similarly, Hassanzadeh et al. examined how users mentally conceptualize data breaches and found that while most individuals possess a general understanding of what a breach entails, they often struggle to comprehend underlying system vulnerabilities and the specific actions required after receiving a notification. This lack of technical understanding weakens users' ability to respond effectively. In a related context, Turjeman and Feinberg reported that users initially demonstrate increased caution following breach announcements by reducing online activity or deleting sensitive information; however, these protective behaviors tend to diminish over time as users gradually revert to previous habits. This suggests that the behavioral impact of breach notifications is frequently temporary rather than sustained.

Research has also explored the effectiveness of notifications in motivating concrete security actions. Bhagavatula et al. investigated password-related behaviors following breaches and found that only a limited proportion of users updated their passwords after receiving notifications. Many continued using weak or reused credentials, indicating that notifications often fail to produce the intended security outcomes. Reinforcing this argument, Zou and Schaub identified a substantial disconnect between users' stated concern and their actual behavior. Their study revealed that confusing terminology, unclear instructions, and poorly structured communication frequently caused users to dismiss or ignore breach notifications altogether.

Beyond individual behavior, several studies have examined the organizational and societal implications of data breaches. Song demonstrated that data breaches significantly increase both financial and reputational risks for organizations. Nevertheless, transparent communication and regulatory compliance were found to mitigate some of the long-term negative consequences. Supporting this perspective, De-Yolande et al. emphasized the importance of mandatory breach notification policies, arguing that timely and transparent disclosure enables users to adopt protective measures earlier while simultaneously fostering organizational trust. Likewise, Janakiraman et al. found that organizations often experience declines in customer spending following breaches; however, many customers do not entirely sever ties with the affected organization, instead shifting toward alternative channels within the same company.

The relationship between breaches and consumer trust has also been extensively explored. Strzelecki and Rizun reported a noticeable erosion of consumer trust following breach incidents. While some users abandoned affected platforms completely, others remained engaged but adopted more cautious behaviors, such as updating passwords more frequently and limiting the amount of personal information shared online. Expanding on the emotional dimension of breach experiences, Labrecque et al. examined the psychological effects associated with breaches and found that such incidents elevate stress, anxiety, and perceptions of organizational responsibility. These emotional reactions significantly influence both users' attitudes toward organizations and their subsequent protective actions.

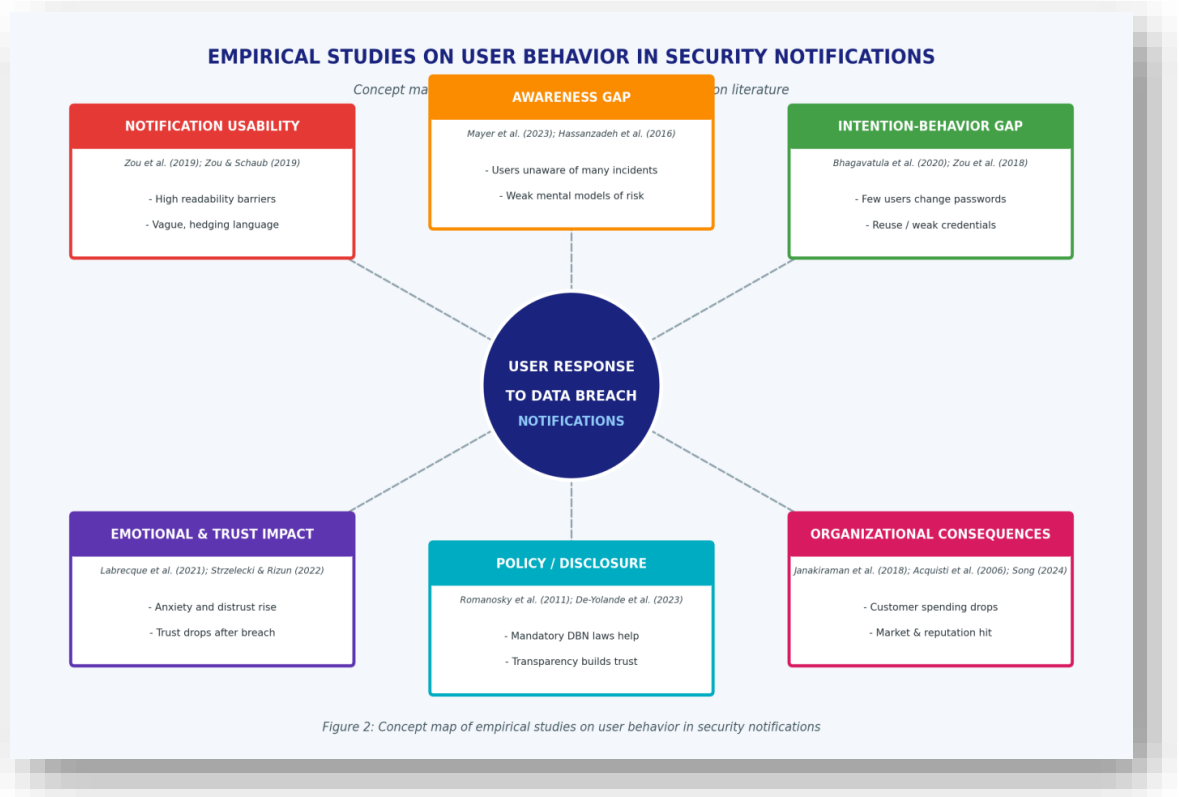

Figure 2: Concept map of empirical studies on user behavior in security notifications

In addition, Zou et al. observed that despite expressing substantial concern about cybersecurity threats, many users still engage in limited or delayed protective behavior. Factors such as perceived inconvenience, optimism bias, and dependence on external guidance often discourage immediate action. This pattern further reinforces the recurring gap between awareness and behavioral response identified throughout the literature. From a broader policy and economic perspective, Acquisti et al. demonstrated that public disclosure of data breaches frequently triggers negative market reactions, reflecting reputational damage and reduced stakeholder confidence. At the same time, Romanosky et al. found that breach notification laws can reduce certain forms of identity theft, particularly when notifications are delivered promptly and communicated clearly. Complementing these findings, Gordon et al. showed that organizations investing more heavily in information security infrastructure tend to experience less severe consequences during breach incidents, underscoring the importance of proactive rather than reactive cybersecurity strategies. Concluding, the literature consistently demonstrates that although data breaches increase awareness and concern among users, awareness alone rarely guarantees effective protective behavior. User responses are strongly influenced by factors such as notification clarity, perceived severity of the breach, emotional interpretation, organizational transparency, and trust in the communicating entity. The persistent gap between knowledge and action identified across these studies highlights the urgent need for more effective, user-centered breach notification strategies capable of promoting sustained and meaningful cybersecurity behavior.

2.3 Conceptual Framework

This study adopts a behavioral-response framework to examine how users interpret and respond to data breach notifications, with particular emphasis on the ways in which breach characteristics and communication strategies influence emotional reactions, trust, and subsequent protective behavior. The framework is grounded in the assumption that the effectiveness of a breach notification extends beyond the mere act of disclosure. Instead, user response is shaped by how clearly the risk is communicated, how severe the incident is perceived to be, and the extent to which responsibility for the breach is

attributed to the organization involved.

To provide a theoretical foundation for understanding these processes, the framework integrates principles from Situational Crisis Communication Theory and the Social-Mediated Crisis Communication Model. These theories collectively explain how individuals evaluate organizational crises, assign blame, interpret communicated information, and decide whether protective action is necessary. Within this framework, users assess a data breach through three interrelated dimensions: responsibility attributes, severity attributes, and communication attributes. Responsibility attributes refer to users' perceptions regarding the extent to which the organization caused or could have prevented the breach. Severity attributes relate to the perceived seriousness of the incident, including factors such as the sensitivity of the compromised data and the scale of exposure. Communication attributes focus on the credibility, clarity, source, and delivery method of the notification itself. Together, these dimensions shape users' perceptions of risk and influence the degree of trust placed in the organization's response.

The framework further proposes that these perceptions directly affect key psychological and behavioral outcomes. Emotional responses, such as anxiety, fear, frustration, or distrust, may emerge following notification exposure and influence users' willingness to engage in protective actions. Trust in the organization's communication also plays a central role in determining whether users perceive the notification as credible and actionable. These factors ultimately contribute to behavioral intentions, including actions such as updating passwords, enabling two-factor authentication, monitoring accounts for suspicious activity, or reducing engagement with the affected platform. Overall, the framework emphasizes that user behavior in the context of data breaches is not determined solely by technological factors. Rather, it reflects a complex interaction between perceived risk, communication quality, organizational accountability, and emotional interpretation. The primary constructs of the framework including responsibility, severity, communication quality, emotional response, trust, and behavioral intentions, are operationalized through Likert-scale measurement items designed to capture users' perceptions and intended responses to breach notifications.

Table 1: Conceptual Framework Components

Component	**Definition**	**Measurement**
Responsibility Attributes	User perception of who is responsible for the breach (internal vs. external, controllability)	Likert scale items (perception-based)
Severity Attributes	Perceived seriousness of breach based on data sensitivity and volume	Likert scale items
Communication Attributes	Clarity, transparency, and source of notification	Likert scale items
Emotional Response	User feelings such as anxiety, fear, distrust	Likert scale items
Behavioral Intentions	Protective actions (password change, 2FA, reduced usage)	Likert scale items

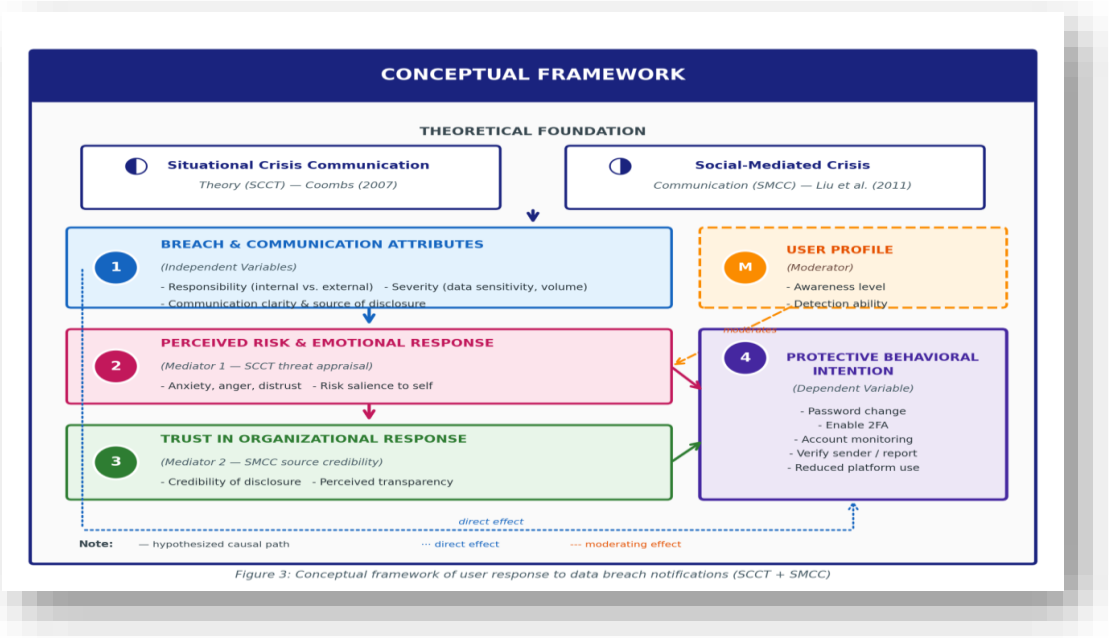

Figure 3: Conceptual framework of user response to data breach notifications

3. Research Methodology

3.1 Research Design

We went with a quantitative, descriptive-correlational survey design to figure out how users respond to data breach notifications. It's a cross-sectional study, meaning we collected data at one point in time to describe what was happening and see how the variables connect. The independent variables are perceived breach severity, notification clarity, and organizational transparency. The main dependent variables are emotional responses (anxiety, distrust, anger) and behavioral intentions (the protective steps users say they take). Trust in how an organization responds sits in between, acting as a mediator. A correlational approach made sense here since it lets us study these variables as they naturally occur, without staging experiments something that would be tough to do ethically when it comes to simulating real breach notifications anyway.

3.2 Population and Sampling

Our target group was university students in Pakistan, mostly those in BS programs, since they spend a lot of time online and are pretty likely to come across breach incidents. We went with stratified sampling so each academic year would be represented equally. The total sample came to 300 respondents, with 75 students from each year (1st through 4th). That balance helped us pick up on differences in digital exposure and academic background. We only included students who were actively enrolled and willing to participate, and any incomplete responses got tossed out before analysis.

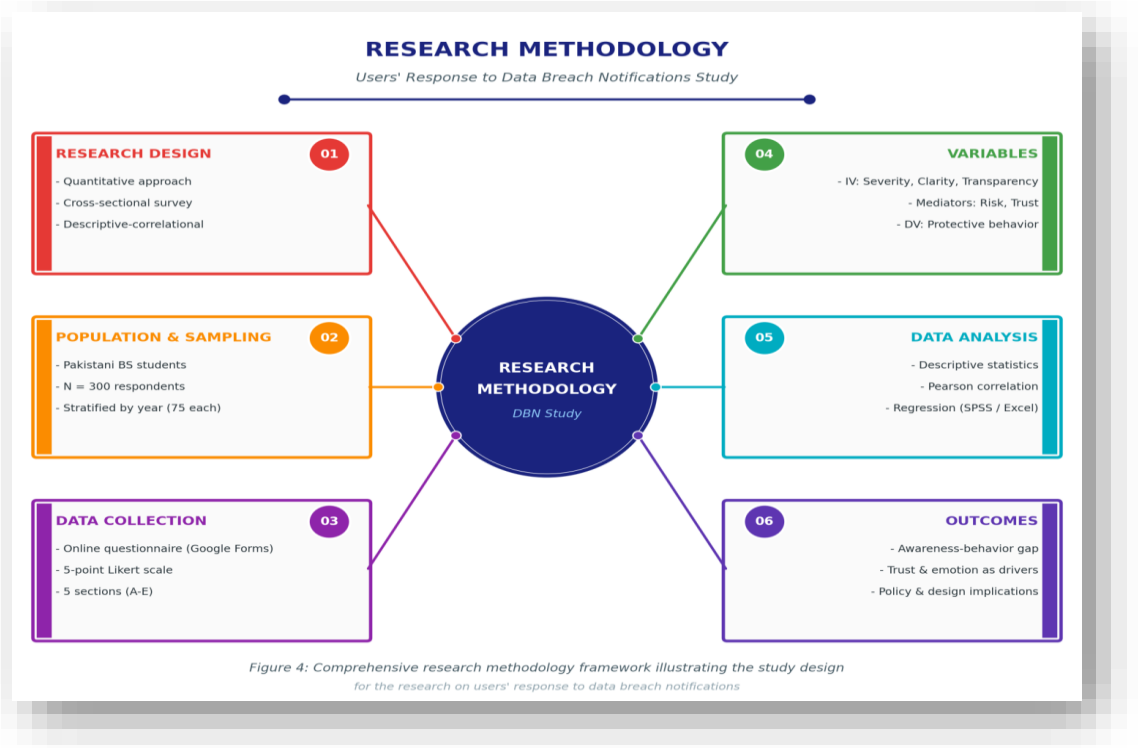

Figure 4: Research Methodology of user response to data breach notifications

Table 2: Sampling Distribution by Campus and Academic Year

University	Program	Year	No. of Students
University Students	BS	1st Year	75
University Students	BS	2nd Year	75
University Students	BS	3rd Year	75
University Students	BS	4th Year	75
Total			**300**

3.3 Data Collection Instruments

A structured questionnaire served as our main tool for collecting data, and we built it around what existing research already says about breaches and user behavior. We split it into five sections. Section A looked at how aware students are of data breaches and whether they recognize the basics what a breach is and what kinds of data tend to get exposed. Section B dealt with how users actually react when a notification lands in their inbox do they read it, change passwords, keep an eye on their accounts? Section C rated the clarity and quality of notifications whether they're easy to follow, complete, and actually useful. Section D measured emotional reactions and trust things like anxiety, fear, or how much confidence users have in the way companies communicate. Section E looked at protective behavior in practice turning on two-factor authentication, updating passwords, checking account settings, and so on. Every item used a five-point Likert scale running from 1 (Strongly Disagree /Never) to 5 (Strongly Agree /Always), which kept our measurements steady across the board.

3.4 Data Collection Procedure

We gathered the data using an online survey distributed through Google Forms, which made it easy for students to take part. We circulated the link through the usual university channels WhatsApp groups and academic networks over about two to three weeks. Before students started the survey, they got a short introduction explaining what the study was about, that taking part was voluntary, and that their responses would stay confidential. Everyone gave informed consent before answering anything. Responses were saved automatically and later moved into Excel and SPSS so we could clean and analyze them.

3.5 Data Analysis Technique

For the analysis, we used IBM SPSS and Microsoft Excel. Descriptive stats including frequencies, percentages, mean scores, and standard deviationshelped us summarize what people said in each section. For every construct, we averaged the related items to get a composite mean. We used the usual cut-offs to interpret those scores: 1.00–2.49 was Low, 2.50–3.49 Moderate, 3.50–4.49 High, and 4.50–5.00 Very High. We laid the results out in tables alongside short explanations so the patterns are easy to follow.

3.6 Limitations of the Study

A few things are worth keeping in mind when reading these results. For one, while 300 respondents is enough statistically, sticking to university students means we can't really generalize to everyone. The questionnaire also leans on self-reported data, so people might give answers they think sound good rather than what they actually do day to day. Because it's cross-sectional, we're only catching one moment in time and not whether their habits change later on. Also worth noting: distributing the survey online probably skewed our sample toward people who are already pretty comfortable in digital spaces. Even so, the study still gives a useful look at how users respond to breach notifications and where the communication and engagement gaps really lie.

4. Data Analysis

This section walks through the full analysis of the data we collected from 300 student respondents. Each sub-section pairs a table with a short write-up covering the main themes of the study awareness of data breaches, behavioral response to notifications, notification clarity, emotional response, and protective behavior**.**

4.1 Demographic Profile of Respondents

Our sample is made up of undergraduate students spread evenly across all four years, with a slightly higher number of male respondents which lines up with what we usually see in computing programs in Pakistan. Most of the students are studying Computer Science or IT, so they already come in with at least some familiarity with digital tools and cybersecurity. A lot of them also reported spending several hours online every day, meaning they're heavily engaged digitally and more likely to be exposed to risks like breaches. That makes them a particularly good fit for this kind of study because they're the ones most likely to face these issues in real life, which gives weight to the patterns we're seeing in awareness, perception, and behavior.

Table 3: Gender Distribution of Respondents

Category	Frequency	Percentage (%)	Cumulative %
Male	174	58.0	58.0
Female	126	42.0	42.0
Total	**300**	**100.0**	**100.0**

By academic year, the split was even 150 students (50%) from years one and two, and another 150 (50%) from years three and four. That gave us a balanced mix across different levels of academic exposure to cybersecurity.

4.2 Section B: Awareness of Data Breach Notifications

Table 4: Awareness of Data Breach Notifications

Item	Statement	Mean	Interpretation
B1	I am familiar with data breach incidents	3.58	Moderate-High
B2	I understand that breaches can occur on online platforms	4.21	High
B3	I can recognize risks related to compromised data	3.89	High
B4	I understand the risks of sharing personal information online	4.24	High
B5	I am aware of data breach notification practices	3.46	Moderate
Composite Awareness Mean		**3.88**	**High**

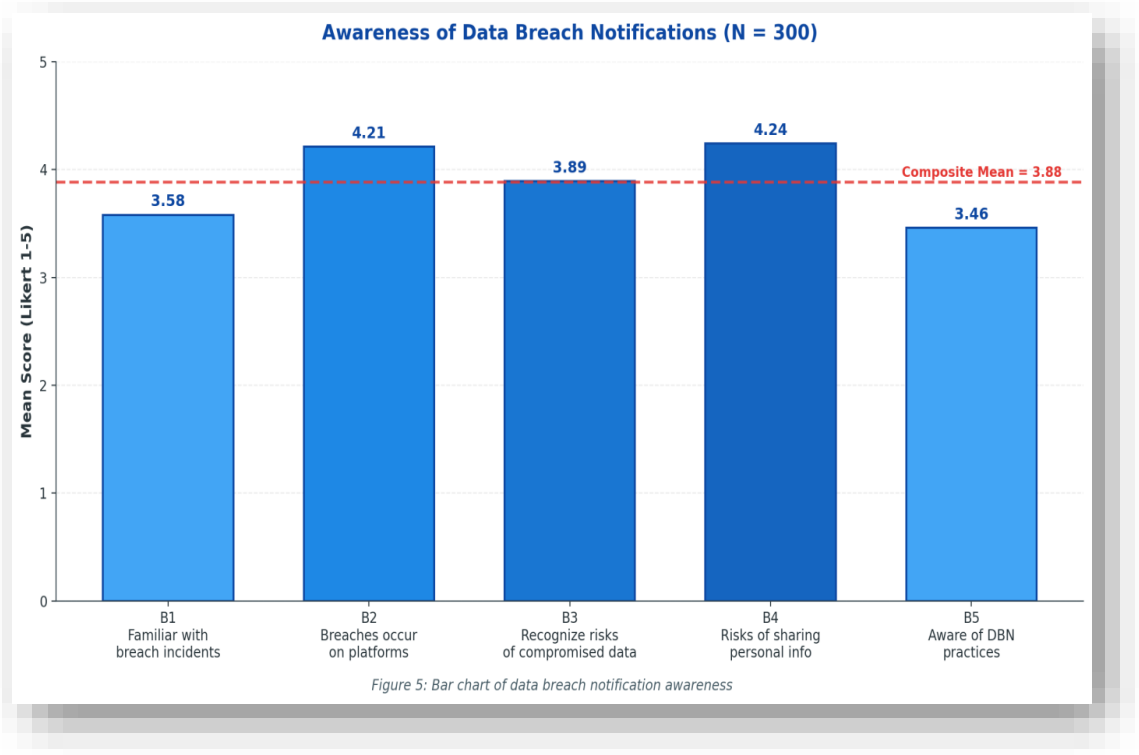

Figure 5: Bar Chart of data breach notifications awareness.

Overall, the sample sits in the high awareness category, scoring a composite mean of 3.88, which means students have a fairly strong grasp of what breaches are and the risks that come with them. The top scorers were B4 (M = 4.24) and B2 (M = 4.21), showing that students get the dangers of sharing personal info online and know breaches happen on digital platforms a lot. That kind of awareness has clearly sunk in probably because they spend so much time online and have come across plenty of security messaging along the way. That said, B1 (M = 3.58) and B5 (M = 3.46) come out a bit lower, which suggests that while students know breaches exist, they don't really know much about how breach notifications work or what the deeper concepts behind them are. There's a clear split here between general awareness and more specific knowledge people get the consequences but miss the details on how to read and respond to a notification. The bottom line is that awareness exists at a surface level,

but it doesn't always carry through to the practical or technical side, which is exactly why we need clearer messaging and better user education around breach notifications.

4.3 Section D: Detection Ability of Data Breach Risks

Table 5: Detection Ability of Data Breach Risks

Item	Statement	Mean	Interpretation
D1	I can identify fake or suspicious login pages	3.74	High
D2	I check links or URLs carefully before clicking	3.54	High
D3	I can detect suspicious or phishing-like messages	3.61	High
D4	I can identify fake or impersonator profiles	3.89	High
D5	I avoid clicking links from unknown sources	4.09	High
Composite Detection Mean		**3.77**	**High**

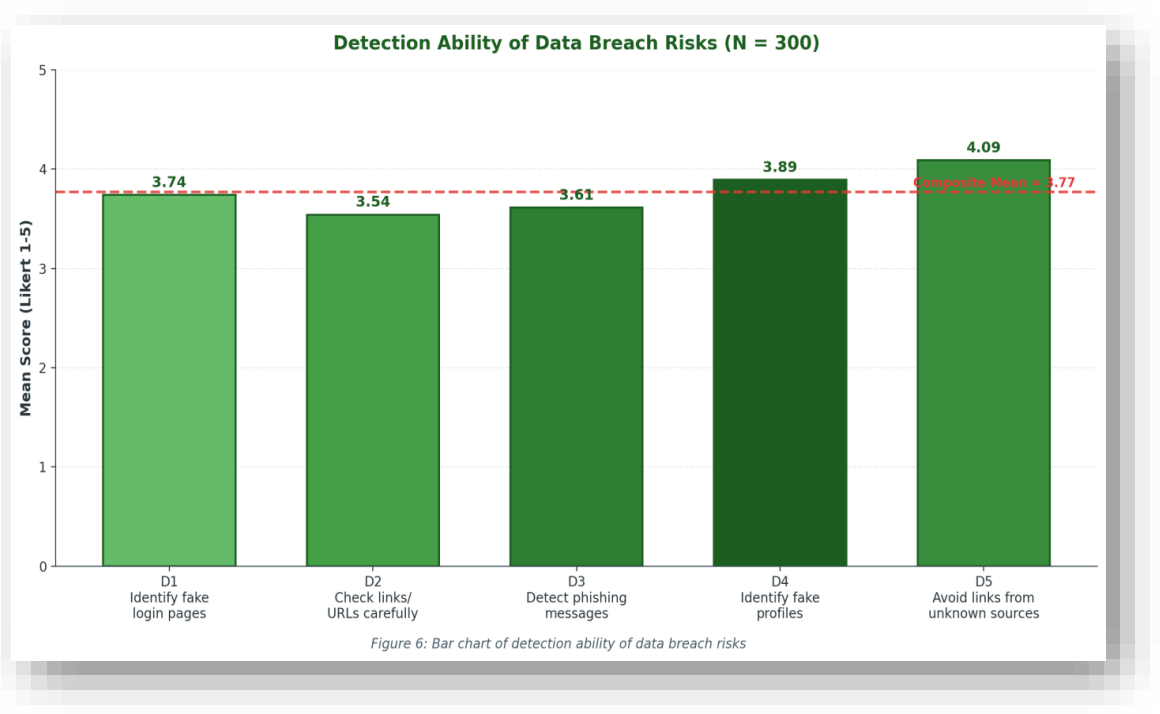

Figure 6: Bar Chart - Detection Ability of Data Breach Risks.

The detection mean of 3.77 tells us students feel pretty confident about spotting breach risks and suspicious activity online, with every item landing in the high range. D5 came in highest (M = 4.09), so most users say they avoid clicking links from unknown sources a solid basic habit. D4 (M = 3.89) and D1 (M = 3.74) point to a similar story for spotting fake profiles and shady login pages. D2 (M = 3.54) was the weakest, which means actually checking URLs before clicking isn't something everyone does and that's a real worry since dodgy links are one of the most common ways attacks happen. So while students are confident and detect threats reasonably well, the gaps across items suggest that some hands-on skills, especially the careful-verification kind, still need work.

4.4 Section E: Behavioral Protection Practices

Table 6: Behavioral Protection Practices

Item	Statement	Mean	Interpretation
E1	I click links in messages without checking them first	2.28	Low
E2	I share personal information online freely	2.43	Low
E3	I accept friend requests from unknown people	2.61	Moderate
E4	I always verify the sender identity before responding	3.28	Moderate
E5	I use security features such as 2FA	3.59	High
Composite Behavioral Mean		**2.84**	**Moderate**

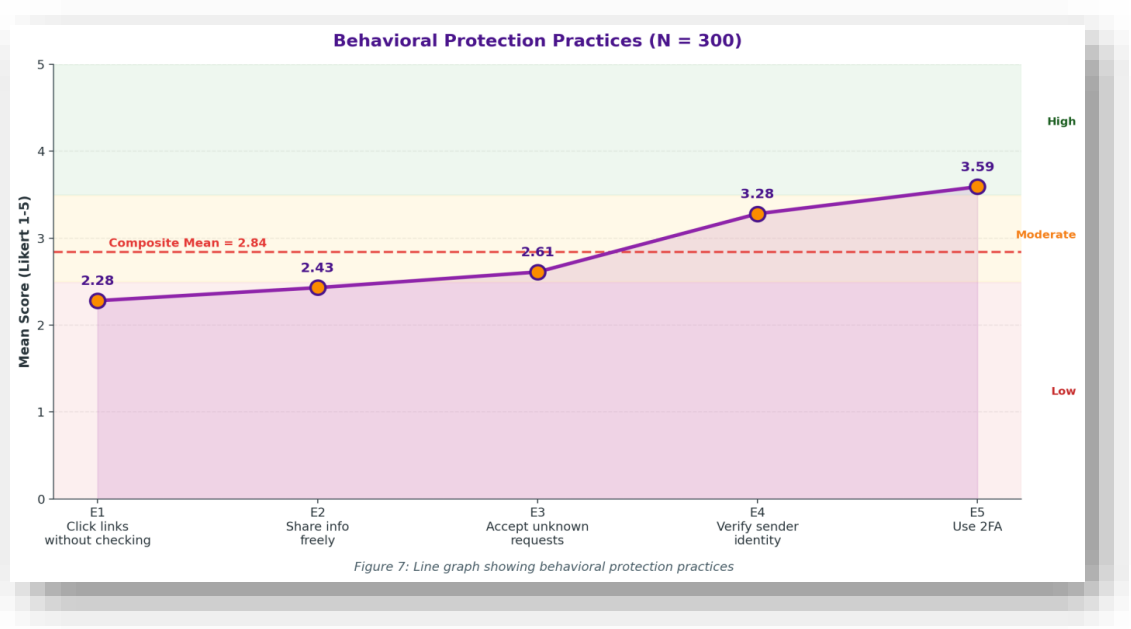

Figure 7: Line Graph Behavioral Protection Practices

When it comes to actual behavior, the results are a mixed bag some habits are safe, others not much with the composite mean landing at 2.84, putting students in the moderate range. The lower scores on E1 (M = 2.28) and E2 (M = 2.43) suggest most students steer clear of obviously risky moves like clicking unknown links or oversharing personal info, which shows at least basic security sense. E3 (M = 2.61) sat in the moderate zone, hinting that a fair number still do iffy things like accepting requests from strangers, which puts them at risk. On the brighter side, E4 (M = 3.28) and E5 (M = 3.59) show moderate to strong protective behavior, especially around checking who's sending what and using things like two-factor authentication. Even with those positives, that overall 2.84 makes it clear that security practices don't always carry across different situations. The lower scores on routine stuff like regular password updates also tell us users skip basic upkeep more often than they should. It all points back to the central finding: people know the risks, but knowing doesn't always turn into consistent, all-around protective behavior in real life.

4.5 Construct-Level Composite Mean Comparison

Table 7: Construct-Level Composite Mean Comparison

Construct	Composite Mean	Std. Dev.	Level
Awareness (B1–B5)	3.84	0.51	High
Detection Ability (D1–D5)	3.77	0.48	High
Behavioral Practices (E1–E5)	2.84	0.55	Moderate

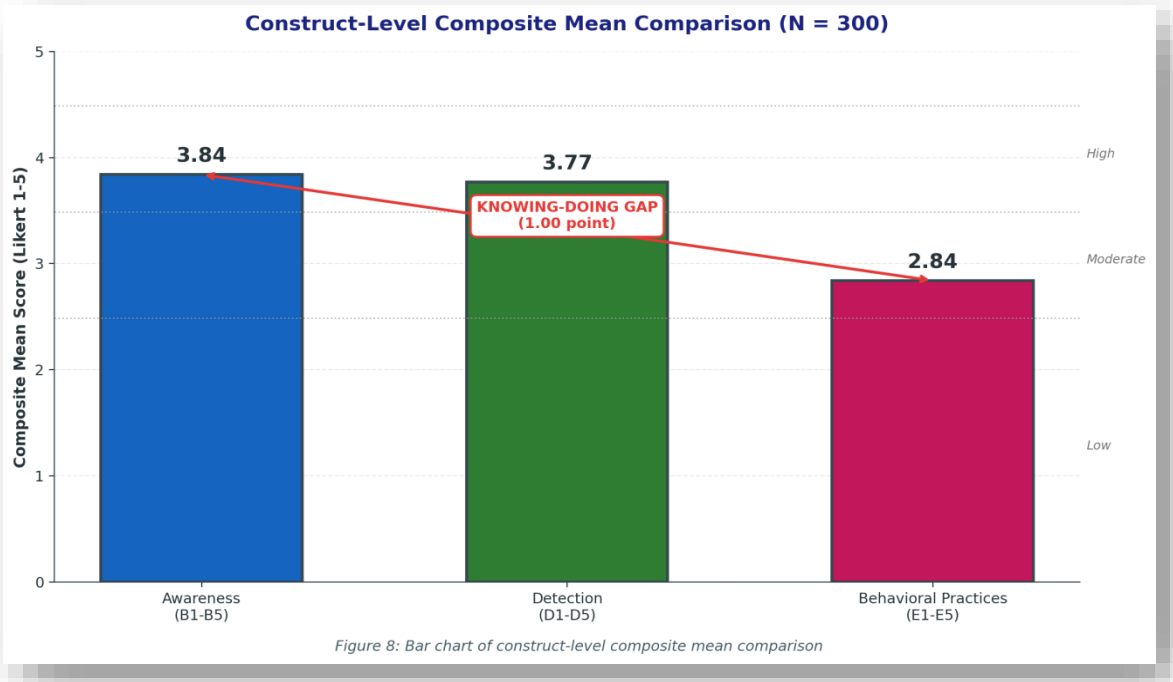

Figure 8: Bar chart of construct-level composite mean comparison

Figure 8: Bar Chart - Construct-Level Composite Mean Comparison

One of the biggest takeaways from this analysis is the obvious split between what people know and what they actually do. Awareness (M = 3.84) and detection (M = 3.77) both score high, which says students get the risks and can usually spot threats. But behavior comes in at a moderate 2.84, meaning that knowledge doesn't always turn into secure habits when it counts. Put simply, users know what they should do they just don't always do it. To close that gap, we need more action-focused approaches: clearer notifications, simpler guidance, and security practices that actually become habits over time.

4.6 Section E: Behavioral Practices and Security Habits

Table 8: Behavioral Practices and Security Habits

Variable	Category	Frequency (n)	Percentage (%)
Avoid Clicking Unverified Links	Yes	216	72.0%
	No	84	28.0%
Avoid Sharing Personal Information Freely	Yes	229	76.3%
	No	71	23.7%
Avoid Accepting Unknown Requests	Yes	198	66.0%
	No	102	34.0%

Verify Sender Identity Before Responding	Yes	164	54.7%
	No	136	45.3%
Use Security Features (2FA)	Yes	189	63.0%
	No	111	37.0%

Section E paints a clear picture of how students actually act online. Most of them said they steer clear of obviously risky things like clicking unverified links (72.0%) or sharing personal info freely (76.3%), so the basic security instincts are there. But once you get to behaviors that take a bit more thought, the numbers slip only 66.0% say they avoid accepting requests from people they don't know, and just 54.7% consistently check who's sending a message before replying. Two-factor authentication use also sits at 63.0%, which means it's catching on but isn't universal yet. Put together, students know the obvious risks but their habits get shaky in situations that need careful judgment. It echoes what we've been seeing throughout the study: awareness alone doesn't guarantee consistent protection, and what we really need is more hands-on training and habit-building around security.

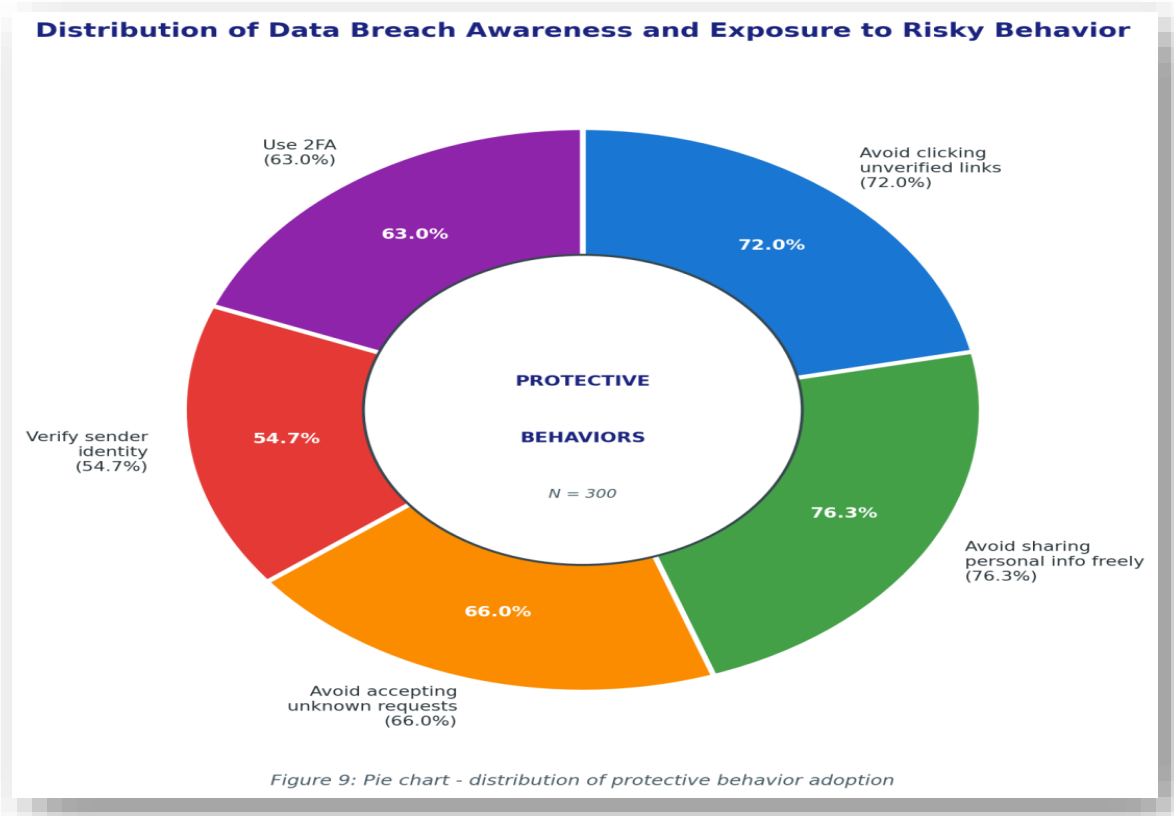

Figure 8: Pie Chart -Distribution of data breach awareness and exposure to risky behavior

5. Implications of the Study

This study explicates that there is a real gap between knowing about breaches and actually doing something about them. Users get that breaches are serious, but their responses tend to be uneven or slow. On the theory side, the findings build on Situational Crisis Communication Theory (SCCT) and similar attribution-based ideas, by showing how things like locus of causality, controllability, and perceived severity shape how users place blame and react, while the type of attack itself doesn't actually influence perception all that much. What users mainly key in on is the sensitivity of compromised data and the clarity of communication**,** a reminder that cybersecurity research has to think about the people on the receiving end. On the practical side, the study gives organizations and security teams something

to work with: there's a real need for clear, transparent, and well-structured data breach notifications that get the risk across and push users to act updating passwords, turning on extra security, and so on. Cleaner language, consistent formatting, and direct guidance go a long way in keeping users engaged and cutting down on the "I'll deal with it later" reaction. From a policy angle, the study backs the case for mandatory data breach notification regulations and highlights the need for standardized reporting frameworks so breach communication stays consistent, complete, and honest. It also makes the case for regulators and institutions to push data breach awareness and response training, so users actually understand the risks and know how to react. Bottom line: handling breaches well isn't just about tech defenses. It also takes good communication and policies that put users front and center if we want cybersecurity to really hold up.

6. Conclusion

The primary objective of this study was to examine how users respond to data breach notifications and to determine whether awareness of such breaches translates into safer security behavior. Data was collected through a structured survey that explored several dimensions, including users' level of awareness, perceived severity of breaches, emotional reactions, trust in organizational communication, and intended behavioral responses. Rather than focusing solely on what users know about data breaches, the study aimed to understand how individuals actually behave once they receive a breach notification. The findings reveal a significant gap between awareness and actionable security behavior. Although most students demonstrated moderate to high awareness regarding the importance of breach notifications, this awareness did not consistently lead to proactive protective measures. Essential security practices such as updating passwords, enabling additional authentication mechanisms, or limiting platform usage were adopted inconsistently. While many respondents reported feelings of anxiety, concern, or distrust following a breach notification, these emotional responses alone were often insufficient to motivate timely or effective action. The results therefore suggest that awareness, in isolation, does not necessarily foster secure user behavior.

The study further highlights the critical role of breach characteristics and communication quality in shaping user responses. Factors such as the sensitivity of the compromised data, the degree of responsibility attributed to the organization, and the clarity and transparency of the notification significantly influenced users' trust and decision-making processes. Notifications that were detailed, transparent, and easy to understand were far more likely to encourage users to take protective action. In contrast, vague or incomplete notifications frequently resulted in confusion, delayed responses, or complete inaction. Overall, the study emphasizes the need to move beyond a purely procedural or "check-the-box" approach to breach notifications and adopt communication strategies that are clear, transparent, and user-centered. By presenting breach information in a manner that users can readily understand and act upon, organizations can encourage faster responses, maintain user engagement, and reduce the potential harm caused by security incidents. In an increasingly digital environment where reliance on data continues to grow alongside cybersecurity threats, fostering effective user responses to breach notifications remains a critical component of overall digital security.

7. Recommendations

1. The findings of this study suggest that organizations should prioritize the development of data breach notifications that are clear, concise, and actionable, enabling users to quickly understand the nature of the incident and the steps required to protect themselves. Technical jargon and overly complex explanations should be avoided in favor of straightforward language that clearly communicates what data was compromised, why the breach is significant, and what actions users should take immediately. Incorporating risk-based messaging—such as emphasizing the potential consequences of delayed action—may further encourage faster and more proactive user responses. In addition, adopting standardized notification formats that consistently outline the timeline of the breach, the type of data affected, and recommended next

steps can reduce confusion and strengthen user trust. Since a large proportion of users access such notifications through mobile devices, messages should also be optimized for mobile readability through the use of concise sentences, clear headings, and a well-structured layout.

2. Beyond improving communication design, organizations should actively encourage stronger cybersecurity practices by guiding users toward practical protective measures, such as enabling Two-Factor Authentication (2FA), rather than relying solely on routine password changes. Providing step-by-step instructions can make recommended actions more accessible and easier to follow, particularly for less technically experienced users. Elements that enhance credibility—such as verified sender information, official branding, and authentic communication channels—can also increase users' confidence in the legitimacy of the notification. Furthermore, offering notifications in multiple or local languages would improve accessibility and ensure that critical information reaches a broader and more diverse audience effectively.

3. At a broader institutional level, policymakers and regulatory authorities should consider establishing standardized guidelines for breach communication to ensure consistency, transparency, and user-centered practices across organizations. Public awareness initiatives should also be strengthened to educate users not only about the existence of data breaches but also about the appropriate actions to take in response to them. Ultimately, improving the clarity, accessibility, and usability of breach notifications has the potential to significantly enhance user response behavior and reduce the overall impact of cybersecurity incidents.

References

Cranor, L. F. (2005). Giving notice: Why privacy policies and security breach notifications aren't enough. *IEEE Communications Magazine*. https://doi.org/10.1109/MCOM.2005.1497545

Ge, Y. (2025). Investigation into the causes of user data breaches based on improved discriminant coefficient and gray correlation analysis. In *Proceedings of the International Conference on Smart Energy and Communication Systems (SCECS)*. https://doi.org/10.1109/SCECS65243.2025.11065588

Holm, E., & Mackenzie, G. (2014). The importance of mandatory data breach notification to identity crime. In *Proceedings of the International Conference on Cyber Security (CyberSec)*. https://doi.org/10.1109/CyberSec.2014.6913963

Karyda, M., & Mitrou, L. (2016). Data breach notification: Issues and challenges for security management. In *Proceedings of the Mediterranean Conference on Information Systems (MCIS 2016)* (Article 60).

Kolevski, D., Abbas, R., Michael, K., & Freeman, M. (2021). Cloud computing data breaches: A review of U.S. regulation and data breach notification literature. In *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*. https://doi.org/10.1109/ISTAS52410.2021.9629173

Kuznetsov, M., Novikova, E., & Kotenko, I. (2022). An approach to formal description of user notification scenarios in privacy policies. In *Proceedings of the International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. https://doi.org/10.1109/PDP55904.2022.00049

Nayak, D. (2024). Data breach notifications and their completeness. In *Proceedings of the International Conference on Computing and Communication (ICOCO)*. https://doi.org/10.1109/ICOCO62848.2024.10928177

Nikkhah, H. R., & Grover, V. (2024). Strategizing responses to data breaches: A multi-method study

of organizational responsibility and effective communication with stakeholders. *Journal of Management Information Systems, 41*(4), 1042–1077.

Song, Q., Deng, X., Li, Y., Dong, Z., Zhu, X., & Li, H. (2024). CAREFUL: A secure and privacy-preserving deletion notification distribution protocol. In *Proceedings of the IEEE International Conference on High Performance Computing and Communications (HPCC)*. https://doi.org/10.1109/HPCC64274.2024.00140

Tamanna, M., Anwar, M., & Stephens, J. D. W. (2025). Security implications of user non-compliance behavior to software updates: A risk assessment study. *Journal of Information Security and Applications, 93*, 104152. https://doi.org/10.1016/j.jisa.2025.104152

Tomaszewski, J. P. (2006). Are you sure you had a privacy incident? *IEEE Security & Privacy*. https://doi.org/10.1109/MSP.2006.143

Wei, T., Wang, D., Li, Y., & Wang, Y. (2025). "Who is trying to access my account?" Exploring user perceptions and reactions to risk-based authentication notifications. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2025)*.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256–286. https://doi.org/10.1002/pam.20567

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In Proceedings of the International Conference on Information Systems (ICIS). https://doi.org/10.2139/ssrn.556510

Markos, E., Peña, P., Labrecque, L. I., & Swani, K. (2023). Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs*. https://doi.org/10.1111/joca.12554

Janakiraman, R., Lim, J., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Curtis, S. R., Carré, J. R., & Jones, D. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal, 33*(4/5), 425–435. https://doi.org/10.1108/MAJ-11-2017-1692

Questionnaire

Rate each statement by selecting one option per item. Please answer all 30 parts.

PART A — Awareness and Recognition of Data Breach Notifications

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Q1. I am aware that organizations are legally obligated to notify users in the event of a data breach.	☐	☐	☐	☐	☐
Q2. I can clearly distinguish a legitimate data breach notification from a phishing email or scam message.	☐	☐	☐	☐	☐
Q3. I understand what a data breach means and the potential consequences it may have for my personal data.	☐	☐	☐	☐	☐
Q4. I am familiar with the types of personal information (e.g., passwords, financial details) commonly compromised in breaches.	☐	☐	☐	☐	☐
Q5. I am aware of regulatory frameworks (e.g., GDPR, PDPA) that govern how organizations report data breaches to affected users.	☐	☐	☐	☐	☐
Q6. I believe most individuals in my social or professional circle are adequately informed about data breach notification practices.	☐	☐	☐	☐	☐

PART B — Frequency and Behavioral Response to Notifications

Scale: 1= Never | 2 = Rarely | 3 = Sometimes | 4 = Often | 5 = Always

Statement	1. Never	2. Rarely	3. Sometimes	4. Often	5. Always
Q7. When I receive a data breach notification, I read it in full before taking any action.	☐	☐	☐	☐	☐
Q8. I change my password immediately upon receiving a notification that my account credentials have been compromised.	☐	☐	☐	☐	☐
Q9. I report suspicious breach-related communications to the relevant platform, authority, or IT department.	☐	☐	☐	☐	☐
Q10. I check whether my other linked online accounts may also be at risk when notified of a breach on one platform.	☐	☐	☐	☐	☐
Q11. I monitor my financial statements or credit report in the period following a data breach notification.	☐	☐	☐	☐	☐
Q12. I follow the specific remediation steps recommended	☐	☐	☐	☐	☐

Statement	1. Never	2. Rarely	3. Sometimes	4. Often	5. Always
in the breach notification rather than ignoring them.					

PART C — Clarity, Quality, and Usability of Notification Content

Scale: 1 = Very Poor | 2 = Poor | 3 = Average | 4 = Good | 5 = Excellent

Statement	1. Very Poor	2. Poor	3. Average	4. Good	5. Excellent
Q13. The language and terminology used in data breach notifications I have received are clear and easy to comprehend.	☐	☐	☐	☐	☐
Q14. Breach notifications I have encountered adequately explain the nature and full scope of the compromised personal data.	☐	☐	☐	☐	☐
Q15. The recommended protective actions provided in data breach notifications are practical and straightforward to implement.	☐	☐	☐	☐	☐
Q16. Data breach notifications are delivered through appropriate and trusted communication channels (e.g., verified email, SMS).	☐	☐	☐	☐	☐
Q17. The overall structure and design of breach notifications make it easy to identify the most critical information at a glance.	☐	☐	☐	☐	☐
Q18. The timeliness of data breach notifications allows me to take adequate protective action before significant harm occurs.	☐	☐	☐	☐	☐

PART D — Emotional Impact and Trust Implications

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Q19. Receiving a data breach notification causes me significant anxiety or emotional distress regarding my data security.	☐	☐	☐	☐	☐
Q20. I feel that my personal information is fundamentally unsafe after learning that a service I use has been breached.	☐	☐	☐	☐	☐
Q21. A data breach notification significantly erodes my trust in the organization responsible for the security failure.	☐	☐	☐	☐	☐
Q22. I am more likely to permanently discontinue using a service or platform following receipt of a breach notification.	☐	☐	☐	☐	☐
Q23. Breach notifications that include a transparent explanation and sincere apology help to partially restore my confidence in the organization.	☐	☐	☐	☐	☐

Statement	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Q24. I believe organizations genuinely priorities user safety when they proactively disclose a breach rather than concealing it.	☐	☐	☐	☐	☐

PART E — Protective Action and Post-Notification Security Behavior

Scale: 1 = Never | 2 = Rarely | 3 = Sometimes | 4 = Often | 5 = Always

Statement	1. Never	2. Rarely	3. Sometimes	4. Often	5. Always
Q25. After receiving a data breach notification, I enable two-factor authentication (2FA) on affected accounts.	☐	☐	☐	☐	☐
Q26. I review and tighten the privacy settings on affected platforms in the aftermath of a breach notification.	☐	☐	☐	☐	☐
Q27. I use or begin using a password manager to generate and store strong, unique passwords following a breach incident.	☐	☐	☐	☐	☐
Q28. I inform family members or colleagues about a confirmed data breach when I believe they may also be at risk.	☐	☐	☐	☐	☐
Q29. I conduct a personal audit of my linked online accounts and services in the aftermath of a breach notification.	☐	☐	☐	☐	☐
Q30. I adopt long-term protective measures (e.g., identity theft protection, credit monitoring) following a major data breach.	☐	☐	☐	☐	☐