

Knowledge-Action Gap and Optimism Bias in Digital Scam Prevention in the Royal University of Bhutan

Tandin Wangchuk^{1*}, Jeevan Gurung², Tad Gonsalves³

^{1,3}Department of Information and Communication Sciences, Faculty of Science and Technology, Sophia University, 7-1 Koicho, Chiyoda-ku, 102-8554, Tokyo, Japan

^{1,2}Computing Technologies Department, College of Science and Technology, Royal University of Technology

E-mail: tandin@eagle.sophia.ac.jp¹/tandinwangchuk.cst@rub.edu.bt^{1*}, jeewangurung.cst@rub.edu.bt², t-gonsal@sophia.ac.jp³

Received: 14 April 2026; Revised: 23 April 2026; Accepted: 12 July 2026; Published: 17 August 2026

Abstract

The ongoing digital transformation in Bhutan has led to an increase in the number of digital scams. Despite public awareness campaigns conducted regularly by the Royal Bhutan Police and Bhutan Cyber Incident Response Team, individuals still fall for digital scams. Understanding the link between optimism bias and digital scams is critical for mitigating digital security threats. In this study, we explore the knowledge-action gap regarding digital scams. Specifically, we investigated the prevalence of optimism bias, its associated behaviors, and its relationship with vulnerability to digital scams at the Royal University of Bhutan. Data were collected from 330 participants through a cross-sectional survey, along with two scam-simulation scenarios. In this study, we compared generational differences and associations between campaign recall, bias levels, and preventive behaviors. This study found that the sample demonstrated widespread optimism bias and consistently overrated the susceptibility of peers compared to themselves. Unlike some studies, a comparison of bias levels across generations using Welch's t-test showed no differences in optimism between youth and adults. Similarly, there was no association between general awareness of campaigns and high optimism bias, but the specific recall of campaign messages was connected to optimism bias. This study highlights the importance of targeted education to bolster self-efficacy among digital users. Unlike the prevalent assumptions, the two digital scam-simulation scenarios did not confirm that a high bias level was linked to increased vulnerability. However, our findings indicate that optimism bias is a proxy for self-efficacy in digital environments. This study provides a foundation for large-scale national surveys and may support concerned agencies in creating effective cybersecurity strategies.

Keywords: *Optimism bias, knowledge-action gap, cyber scams, digital self-efficacy, cybersecurity*

1. INTRODUCTION

As Bhutan is undergoing digital transformation, the number of digital scams has increased, as in other parts of the world (FBI 2025; Khiaonarong and Zheng 2026). Despite ongoing awareness efforts by the Bhutan Cyber Incident Response Team (BtCIRT) and the Royal Bhutan Police (RBP), falling victim to digital scams remains a major issue. Several media outlets (Bhutan Today, 2025; The Bhutanese, 2025; Kuensel, 2026) have reported an increase in scams in the country. A latest news report by The Bhutanese (2026) noted two new scam methods: email compromise and mobile phone 'bland out.' These methods led to reported losses of Nu 1.6 million that have not yet been recovered. Although new schemes continue to appear, existing scam methods still represent most cases.

There appears to be a gap between people's

awareness of digital scams and the actions they take to prevent them. Similarly, there is a lack of studies on cybersecurity in Bhutan, with a particular emphasis on scams. This dearth of literature shows that although digital scams are a growing concern, they are not well understood or studied. The limited studies (Wangchuk et al., 2024; Yangchen et al., 2025; Choejey et al., 2015; Tenzin et al., 2024) that exist mostly focus on general cybersecurity. In the broader field of cybersecurity, digital scams such as phishing, investment or crypto scams, lottery scams, mobile blackout scams, and other types of online fraud must be studied in Bhutan. This missing link underscores the need to bridge the gap between awareness and preventive measures.

On the other hand, cybersecurity and optimism bias are well-researched in the literature (Owen et al., 2024; Rhee et al., 2005, 2012; Lei, Hu, and Hsu, 2023; Fatoki, Shen, and

Mora-Monge, 2024). According to existing research, optimism bias (OB), the cognitive bias in which one is less likely to fall for scams than others, is linked to impulsive decision-making and is prone to falling victim to scams. There has been no research on optimism bias among Bhutanese digital users. Optimism bias increases the likelihood of impulsive choices and underestimates personal risk (Fatoki, Shen, and Mora-Monge 2024; Lei, Hu, and Hsu 2023). Not studying this issue among Bhutanese digital users means that the key factors contributing to scam vulnerability remain unclear. This highlights the need for targeted studies on optimism bias among Bhutanese digital users and its impact on vulnerability to scamming.

To this end, our study examines how exposure to RBP/BtCIRT digital safety campaigns among digital users at the Royal University of Bhutan influences the gap between their theoretical knowledge of scams and their actual behavioral responses, and the extent to which optimism bias contributes to scam susceptibility. A cross-sectional survey combined with simulated scam scenarios was conducted using a mailing list. The study sought to fulfil the following research objectives:

- **RO1:** Assess the level of awareness and recall of RBP and BtCIRT digital safety campaigns among different age groups.
- **RO2:** Measure and compare "Optimism Bias" (the difference between perceived risks for others and for oneself) between Digital Residents (Youth) and Digital Visitors (Adults).
- **RO3:** Evaluate the knowledge-action gap by testing whether theoretical understandings of safety rules translate into protective behavior during simulated scam scenarios.

This case study is relevant because it serves as the baseline for similar studies, given the high literacy level in the sample. Future studies that incorporate the entire Bhutanese population will help determine the effectiveness of digital safety campaigns. Studies accounting for psychological factors, such as optimism bias, can reduce the knowledge-action gap and better protect Bhutanese digital users from real-world scams.

The remainder of the paper is divided into Section 2, explaining the common concepts and related work; Section 3 outlines the methodology used for the study; Section 4 presents the results and findings; Section 5 discusses the results; and Section 6 concludes the paper.

2. RELATED WORKS

Younger generations have been reported to be more susceptible to scams than older generations (Toomey, 2023) because of their comfort in online shopping, banking, and communication. Therefore, we classify youth in Bhutan as "Digital Residents," defined as people born after the introduction of the Internet (1999) and mobile services (2003). Those born before are grouped as "Digital Visitors," or adults. Prensky (2001) initially coined the terms "Digital Natives" and "Digital Immigrants" to address the growing divide in education at the time. He used the term "Digital Natives" to describe students born into the digital world who grew up with technology such as computers, video games, and the Internet. On the contrary, the term "Digital Immigrants" was used to describe those not born into the digital world who later had to adapt and became fascinated by it. These terms have received criticism and have evolved over the years. We used the modern terms proposed by White and Cornu (2011) for these two groups, along with our own definitions. The reason for using this grouping is not for an education study but is based on the degree of familiarity with technology. The distinction between Digital Residents and Digital Visitors is the main part of our study. This differentiation helps interpret the differences in scam susceptibility and digital behavior in Bhutan.

Despite regular advocacy programs, a gap appears to exist between scam awareness and individuals' actions taken to prevent falling victim. Several news outlets (Bhutan Today, 2025; The Bhutanese, 2025, 2026; Kuensel, 2026) have reported an increase in online scams. The news reports that people have suffered monetary losses. One of the objectives of our study was to examine the knowledge and action gap (i.e., the discrepancy between knowing what to do and doing it). Understanding this gap is critical for designing effective interventions and public awareness campaigns in Bhutan.

The fundamental focus of our study is optimism bias (OB). Existing research on OB provides a new perspective on the gap between knowledge and action. OB refers to the belief that others are likely to fall into a scam. This cognitive bias was first examined as "Unrealistic Optimism" by D. Weinstein (1980), who suggested that people consistently believe they are less likely than their peers to experience negative events. Cognitive bias serves as a

protective mechanism that enhances motivation and mental health. This can also lead to hazardous behavior. Therefore, optimism bias can cause individuals to underestimate their risk of deception. Consequently, their vulnerability increases, even if they believe that others are at a higher risk.

In addition to traditional psychology, several studies have addressed the link between optimism bias and the tendency to fall for scams or be caught in phishing attacks. Specifically, Lei et al. (2021, 2023) and Owen et al. (2024) reported that the presence of more pronounced levels of optimism bias is positively linked to dangerous phishing behaviors. Nonetheless, no similar research has been conducted in Bhutan that focuses on digital user behaviors concerning scams and the frequency of victimization. This serves as a foundation to study the impact of exposure to safety campaigns on the discrepancy between the theoretical understanding of scams and the behavioral practices of Bhutanese digital users and further explore the impact of optimism bias on vulnerability to digital scams.

3. METHODOLOGY

This section outlines the study's design, participant demographics, and statistical methodologies used to investigate the gap between individuals' knowledge and actions and the influence of optimism bias on digital users.

3.1 Research Design

This study used cross-sectional quantitative methods to evaluate optimism bias and response patterns to digital scams. A structured survey was employed to gather information regarding perceived risk, exposure to cybersecurity awareness campaigns, and the probability of participants falling for simulated scams, as constrained by time and resources. The possibility of floating the survey online via social media to voluntary responses was deemed impossible because only a few people responded.

3.2 Sampling and Data Collection

This study employed a non-probability and convenience sampling strategy. Surveys, with the help of a questionnaire and mock scenarios, were administered through KoboToolbox for two weeks, that is, from January 22 to March 3, 2026. A shortened version of the survey link, along with QR codes, was provided for convenient access to a broader group of individuals.

In the first instance, an effort was made to find participants by engaging people through the popular social media platform, Facebook. As this did not yield significant responses, the surveys were later disseminated using group mailing lists of the Royal University of Bhutan (RUB). This use of convenience and the purposive sampling strategy made it easier to recruit both Digital Residents (youth) and Digital Visitors (adults) at the academic level. However, this method resulted in a high response rate at the cost of having a self-selected sample owing to the direct reach of the participants. Eventually, 330 responses were obtained, of which 136 were defined as Digital Residents (youth) and 174 as Digital Visitors (adults). The vast majority of Digital Residents and Digital Visitors belong to academic institutions.

3.3 Instrumentation

The survey was divided into six sections comprising 20 questions, some of which were part of a separate study. The collected data included demographic information (age, location, and occupation), perceived risk assessment, awareness and recall of cybersecurity campaigns, and responses to simulated scam scenarios. For the perceived risk assessment, participants rated the risk of falling for scams about themselves (self-risk) and their average peers in Bhutan (other-risk) on a 10-point scale. This was used to calculate the OB score. Under awareness and recall, we assessed the general awareness of the Bhutan Cybersecurity Response Team (BtCIRT) and Royal Bhutan Police (RBP) campaigns as well as the ability to recall specific safety messages. For the simulated scam scenarios, the participants were provided with two simulated digital threats: highway and AUD exchange scams. In the highway scam, participants were given three courses of action to choose from if they received an urgent message on Facebook Messenger from a friend stranded on an Indian highway between Phuentsholing and Samdrup Jongkhar. Similarly, in the AUD exchange scam, participants were asked to choose among three options when exchanging dollars in a Facebook group. Responses were categorized as "Pass" (safe behavior) or "Fail" (victim behavior).

3.4 Data Analysis and Hypotheses

Data were analyzed using Microsoft Excel and t-tests to evaluate the five primary hypotheses (Table 1).

Table 1: Hypotheses and statistical tests used.

Hypothesis	Statistical Test	Variable Comparison
Universal Bias	Paired Two-Sample T-Test	Others-Risk vs. Self-Risk
Generational Bias	Two-Sample T-Test (Unequal Variances)	Youth OB vs. Adult OB
Susceptibility	Two-Sample T-Test (Unequal Variances)	OB of “Failed” vs. OB of “Passed” groups
Campaign Awareness	Two-Sample T-Test (Unequal Variances)	OB of “Aware” vs. OB of “Unaware” groups
Campaign Recall	Two-Sample T-Test (Unequal Variances)	OB of those “Remembered” vs. OB of those “Forgot” group

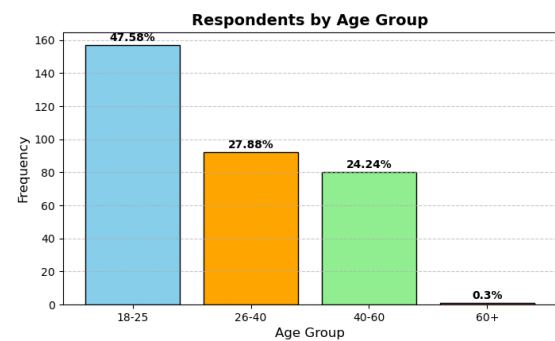
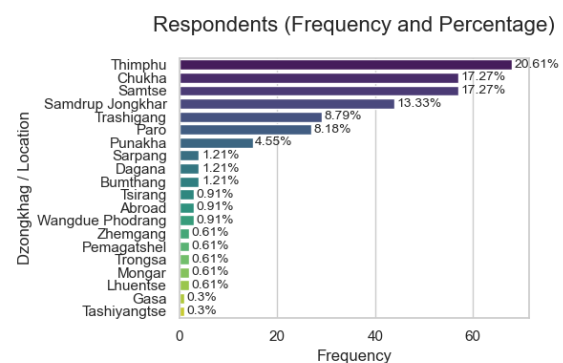
To measure optimism bias, this study employed the direct comparison method (Klein and Weinstein, 1997). Participants rated their own risk of falling for a scam and that of an average peer on a 1–10 scale. Following the subtraction logic of Shepperd et al. (2013), the individual OB score was calculated as follows: score = (RiskOthers – RiskSelf). To compare the means of Digital Natives and Digital Migrants, a Welch’s t-test was conducted (Delacre et al., 2017), as it provides a more reliable analysis when sample sizes are unequal.

3.5 Ethical Considerations

Participation was voluntary and anonymous. No personally identifiable information was gathered through KoboToolBox, and the participants were informed that their data would be used exclusively for academic research. Any identifiable information was removed from the data during the analysis.

4. RESULTS

A total of 330 individuals participated in this survey. Respondents’ ages were divided into four groups: A (18-25), B (26-40), C (40-60), and D (60+), as shown in Fig. 1. According to the figure, 47.58 per cent of respondents belong to group A, 27.88 per cent to group B, 24.4 per cent to group C, and only 0.3 per cent to group D. Fig. 2 shows respondents from different dzongkhags. The majority (20.61 per cent) were from Thimphu, followed by Chukha and Samtse (17.27 per cent each), Samdrup Jongkhar (13.33 per cent), Trashigang (8.79 per cent), Paro (8.18 per cent), and others.

**Fig. 1:** Number of respondents in each group**Fig. 2:** Dzongkhag-wise respondents

We initially tested whether optimism bias applies to RUB academics in the Bhutanese context. For this test, we assumed that others' risks would be rated higher than their own risk of being scammed. Consequently, the following null and alternative hypotheses were derived:

$$H_0: M_{OR} - M_{SR} \leq 0$$

$$H_1: M_{OR} - M_{SR} > 0$$

Where M_{OR} represents the average risk rating for others, and M_{SR} is the average risk rating for oneself. Using a 95% confidence level and an alpha of 0.05, a paired two-sample t-test was conducted using Microsoft Excel. Table 2 displays the results of the t-tests.

Table 2. T-test for others' risk rating vs. self-risk rating.

	Others-Risk	Self-Risk
Mean	6.11650	2.95793
Variance	3.88898	4.77419
Observations	309	309
Pearson Correlation	0.22945	
Hypothesized Mean Difference	0	
df	308	
t Stat	21.47304	
P(T<=t) one-tail	1.83E-63	
t Critical one-tail	1.64982	

P(T<=t) two-tail	3.66E-63
t Critical two-tail	1.96770

As expected, the average risk for others was rated higher than self-risk. The t-stat value was 21.47, which exceeded the t-critical one-tailed value of 1.65, and the p-value of 1.83083E-63 was lower than the alpha value of 0.05. The effect size (Cohen's d value) was 1.22, indicating a large effect. Consequently, there is significant statistical evidence to reject the null hypothesis H_0 and support the alternative hypothesis H_1 .

In the second test, we investigated whether there was a difference in optimism bias between generational groups (youth vs. elders). As most studies (Habicht et al., 2022; Toomey, 2023) have shown, younger generations display greater optimism bias than older generations. Therefore, the following hypotheses were proposed:

$$H_0: Y_{OB} \leq E_{OB}$$

$$H_1: Y_{OB} > E_{OB}$$

Where Y_{OB} represents the mean optimistic bias score of the younger generation (Youth), and E_{OB} indicates the mean optimistic bias of older generations (Adults). The OB score was calculated as the difference between the risk ratings of others and their own. Welch's t-test for two samples with unequal variances was performed at an alpha level of 0.05. The test results are presented in Table 3.

However, the test results showed the opposite. The optimism bias of the youth was lower than that of the older generations. The t-stat value was below the t-critical one-tailed value of 1.65, and the p-value (0.062) exceeded the alpha level of 0.05. Cohen's d value is 0.18, indicating a small effect. There was no statistically significant evidence to reject the null hypothesis.

Table 3: T-test for optimism bias among youth and adults.

	Youth	Adults
Mean	2.90441	3.35838
Variance	6.42783	6.83593
Observations	136	173
Hypothesized Mean Difference	0	
df	294	
t Stat	-1.54107	
P(T<=t) one-tail	0.06219	
t Critical one-tail	1.65005	
P(T<=t) two-tail	0.12437	
t Critical two-tail	1.96807	

Third, we tested the susceptibility to falling for scams among individuals with high and low optimism bias, with the literature indicating that those with high OB are more likely to do so. Of the 156 participants who rated high-risk for others and low risk for oneself, 134 passed both scam scenarios, and only 22 failed either or both scams. The hypotheses for the test are as follows:

$$H_0: M_{\text{pass}} \geq M_{\text{fail}}$$

$$H_1: M_{\text{pass}} < M_{\text{fail}}$$

We presented the respondents with a highway Scam scenario and offered them three options. For the test, respondents were divided into those who could not steer through the simulated scam (M_{fail}) and those who could (M_{pass}). The results of Welch's t-test are shown in Table 4.

Again, the test results showed the opposite. Those who passed through the scam had slightly higher OB scores than those who failed, although the difference was not statistically significant ($t = 0.94$, $p = 0.177$, $d = 0.2$). This finding is supported by another scenario presented to the respondents of the AUD Exchange scam (Table 5). The results were similar, although this test involved only a small number of participants who failed the scam scenario.

Table 4: T-test for those who passed and failed to steer through the highway scam scenario.

	Passed	Failed
Mean	3.36196	2.83333
Variance	7.42990	6.49275
Observations	163	24
Hypothesized Mean Difference	0	
df	31	
t Stat	0.94022	
P(T<=t) one-tail	0.17719	
t Critical one-tail	1.69552	
P(T<=t) two-tail	0.35437	
t Critical two-tail	2.03951	

Table 5: T-test for those who passed and failed to steer through the AUD Exchange scam.

	Passed	Failed
Mean	3.33708	2.44444
Variance	6.91398	16.02778
Observations	178	9
Hypothesized Mean Difference	0	
df	8	

t Stat	0.66172
P(T<=t) one-tail	0.26337
t Critical one-tail	1.85955
P(T<=t) two-tail	0.52675
t Critical two-tail	2.30600

One of the survey questions asked whether the respondents were aware of the cybersecurity campaigns conducted by BtCIRT and RBP. Among the respondents, 56.7% reported being aware of these campaigns. Welch's t-test was performed to determine whether OB Scores were higher among those aware of the campaigns.

Table 6: T-test between those who were aware and unaware of the campaigns.

	Aware	Unaware
Mean	3.29412	3.02797
Variance	7.30550	5.61893
Observations	187	143
Hypothesized Mean Difference	0	
df	322	
t Stat	0.95076	
P(T<=t) one-tail	0.17122	
t Critical one-tail	1.64960	
P(T<=t) two-tail	0.34244	
t Critical two-tail	1.96736	

From Table 6, although the mean OB scores of those aware of the campaigns were slightly higher than those of those not aware, there was no statistically significant difference ($t = 0.95 < \text{critical value} = 1.65$, $p = 0.17 > \alpha = 0.05$, $d = 0.1$) to support the hypothesis.

We also examined whether individuals who could recall the recent RBP awareness message had higher OB scores. The mean OB scores of those who could recall the message were significantly higher than those of those who could not ($t = 3.44 > \text{critical value} = 1.77$; $p = 0.0022 < \alpha = 0.05$, $d = 0.77$). The test results are presented in Table 7.

Table 7: T-test between those who could recall and those who could not recall campaign messages

	Yes	No
Mean	3.41477	1.36364
Variance	7.31841	3.45455
Observations	176	11
Hypothesized Mean Difference	0	
df	13	

t Stat	3.43949
P(T<=t) one-tail	0.00220
t Critical one-tail	1.77093
P(T<=t) two-tail	0.00440
t Critical two-tail	2.16037

5. DISCUSSION

In this study, we examined the gap in the digital space of RUB with reference to 'what people know versus what they actually do online' regarding scams. We identified how optimism bias influences behavior towards cybersecurity measures. There was considerable optimism bias among the samples. Most participants reported that they were considerably less likely than others to fall into scams of this kind, as evidenced by the t-test results ($t = -21.47$, $p = 0.001$). Participants' average rating for the chance of others being scammed ($M = 6.12$) was higher than their likelihood of being scammed ($M = 2.96$). To be precise, many appear to throw a 'mental shield' around themselves to convince themselves that the worst is far more likely to happen to other people than themselves. This leaves many, if not all, vulnerable to online threats. Thus, within the RUB framework of online activities, this attitude could weaken their online security, whereby they are perfectly aware of scams' prevalence and severe nature but would be unwilling to take very basic security measures like creating strong passwords and being alert about clicking on any suspicious links due to the simple fact that 'scam will not happen to me.'

It was originally hypothesized that the Digital Resident group would be the most overly confident. Nevertheless, within the samples, the adult group, Digital Visitors, showed greater optimism bias than the youth group. Although the sample largely came from an academic context, the adult sample had a higher optimism bias score ($M = 3.36$) than the youth sample ($M = 2.90$, $p = 0.062$). This finding suggests that even though Digital Residents spent more time online, they would be more wary and knowledgeable of their vulnerabilities as opposed to adults, who may not understand as much regarding modern social engineering and therefore feel a false sense of security. Therefore, educational efforts must address not only youthful Digital Residents but also older Digital Visitors.

Perhaps the most striking finding was a "confidence paradox": as optimism bias increases, security behavior improves, instead of

becoming riskier. Of the 156 participants who reported high optimism bias for other-risk and low optimism bias for own-risk, only 22 fell for either or both scams. During the highway scam simulation, those who avoided the scam scored higher in optimism bias ($M=3.36$) than those who did not avoid the scam ($M=2.83$, $p=0.051$). Similarly, in the AUD Exchange Scam, participants who averted the scam exhibited a higher optimism bias ($M=3.34$) than those who fell for the scam ($M=2.44$). Therefore, a high optimism bias may not inherently signify foolish recklessness. In this context, increased optimism bias was associated with digital self-efficacy (even if not specifically tested in this study), that is, confidence in one's own ability to detect and tackle online security issues. However, this could simply be because young students and academics did not lack digital confidence and had genuine faith in their ability to detect and tackle the threat when it arises. Therefore, their greater confidence would not represent naïve optimism but a belief in one's ability to deal with threats in the environment.

The findings would also partially explain why broad awareness campaigns, if at all, appear to have minimal effects. Having mere exposure to campaigns did not increase security behaviors. The study did not find any significant relationship between knowledge of RBP and BtCIRT initiatives and increased security behavior or lower bias ($p=0.171$). However, awareness of specific message recall was highly significant ($p=0.002$), and individuals remembering messages had significantly higher levels of optimism bias ($M=3.41$), which served as a proxy for self-efficacy. This suggests that it is not exposure but retention that makes us feel safe online.

For RUB, awareness campaigns must focus on message retention rather than campaign visibility. By and large, security campaigns could encourage memorability and digital self-efficacy, which could indirectly promote behavioral changes in digital users. Therefore, rather than just broadcasting a wide array of awareness messages and encouraging general vigilance in RUB, we suggest that authorities target people directly and try to implement debiasing messages tailored to challenge the "not me" syndrome. Rather than simply propagating the fear of consequences (such as fines), efforts should focus on bolstering people's confidence in their ability to avoid scams. Such campaigns should involve scenario-based training and simulations

to allow users to make decisions in a controlled environment. With proper interventions that highlight both the risks and methods of mitigation, we can strengthen digital self-efficacy among users and foster more cautious and informed online behavior in RUB.

This study had several significant limitations. The researchers did not use any of the standard measurement instruments for self-efficacy; therefore, optimism bias could have served as a substitute measure for self-efficacy in the academic sample. As most of the sample was recruited from a single institution, the results cannot be generalized to the Bhutanese population. Owing to time constraints and a low response rate to our online survey disseminated on social media, data collection mostly involved using an institutional e-mail list to reach potential participants in the sample, which consisted of students and staff members from the same university. As all participants had similar educational backgrounds, access to digital technology, and socioeconomic status, the present sample did not reflect the public. Furthermore, selecting participants from a single institution also introduced sampling bias; for example, a wider range of ages, occupations, geographical locations, and levels of digital familiarity were excluded from this study. Therefore, the generalizability of these findings to the general Bhutanese population remains unclear. Nevertheless, given the highly educated sample, this study can provide a valuable baseline for future large-scale surveys. Future research should include diverse respondents (varying in geographical regions, age groups, levels of education, occupations, etc.) so that the data can become a reliable basis for informing policies on digital inclusion and cybersecurity. They must also investigate self-efficacy measures to make it easier for researchers to design targeted educational messages and campaigns that suit people's needs and challenges when surfing online.

6. CONCLUSION

The current study aimed to understand how RBP and BtCIRT digital safety campaigns impact the perception-behavior discrepancy about scams in RUB digital users, as well as how optimism bias influences susceptibility to scams. One strong finding emerged: an overwhelming and widespread global optimism bias regarding the likelihood of falling victim to scams. Such

optimism bias has the potential to undermine the effectiveness of cybersecurity measures by encouraging complacency towards defensive behaviors.

Another finding contradictory to the assumption was that Digital Residents, that is, youths, did not have higher levels of optimism bias. The results show that Digital Visitors (that is, adults with higher educational levels) have a higher level of optimism bias. This means while youth are the most 'active' online, they also have the most pessimistic outlook, and possibly the most knowledge about their vulnerability to risks. In contrast, those who are new to social engineering tactics might believe that they have high levels of competence, simply because their learning curves are steep. This can lead to overconfidence and negligence. Regarding the general pattern of optimism bias among individual digital users, a focused program must cater to differences in perceived risk, prior experience, exposure levels, and other generational differences. The results also show that this contradicts the notion that the higher the optimistic bias, the more careless users are. A higher optimistic bias was related to digital self-efficacy in our study population (academics), indicating that optimism among safe digital users in RUB may reflect true self-confidence rather than inflated perceptions of capability. The study also showed that this higher optimism bias can provide some level of confidence that makes users remain calm in suspicious situations, think carefully about situations, and respond without succumbing to fear or impulsive behavior. However, we should remember that this may not be the case for all Bhutanese people. These findings also address why massive online security awareness initiatives have often been unsuccessful.

The way forward is for agencies to tailor effective cybersecurity campaigns in RUB towards enhancing people's ability to recall campaign messages, instead of merely making campaigns visible. Agencies can use targeted approaches, such as microsimulations and story-based content shared on social media platforms, to promote narrative engagement, aid message recall, and develop culturally relevant mnemonic messages. These programs will help promote more confident and less panicked responses to online threats.

The main limitation of this study is its primary focus on sampling from a single institution, which limits its generalizability to the

broader Bhutanese population. Further research should include a broader range of participants of different ages, educational levels, working areas, and geographical locations across Bhutan.

7. ACKNOWLEDGEMENT

The authors acknowledge the support provided for the paper presentation by Sophia University and the JDS Scholarship.

8. REFERENCES

- Bhutan Today. (2025, n.d.). Police Warn of Rising Sophisticated Scams as Victims Surge Across Bhutan. Retrieved March 29, 2026, from <https://www.bhutantoday.bt/Police-Warn-of-Risi/>
- Choeje, P., Chun Che Fung, Kok Wai Wong, Murray, D., & Sonam, D. (2015). Cybersecurity challenges for Bhutan. 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications, and Information Technology (ECTI-CON), 1–5. <https://doi.org/10.1109/ECTICon.2015.7206975>
- Delacre, M., Lakens, D., & Leys, C. (2017). Why psychologists should by default use Welch's t-test instead of Student's t-test. *International Review of Social Psychology*, 30(1), 92–101. <https://doi.org/10.5334/irsp.82>
- Dema, T. (2026). RBP records new scam methods: Email compromise and mobile 'bland out.' The Bhutanese. <https://thebhutanese.bt/rbp-records-new-scam-methods-email-compromise-and-mobile-bland-out/>
- Fatoki, Jimoh G., Zixing Shen, and Carlo A. Mora-Monge. 2024. "Optimism amid Risk: How Non-IT Employees' Beliefs Affect Cybersecurity Behavior." *Computers & Security* 141:103812. doi: 10.1016/j.cose.2024.103812.
- Federal Bureau of Investigation. 2025. Internet Crime Report 2025. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- Habicht, J., Bowler, A., Moses-Payne, M. E., & Hauser, T. U. (2022). Children are full of optimism, but those rose-tinted glasses are fading—Reduced learning from negative outcomes drives hyperoptimism in children. *Journal of Experimental Psychology: General*, 151(8), 1843–1853. <https://doi.org/10.1037/xge0001138>
- Khiaonarong, T., and Zheng, S. 2026. The Rise of Cyber Events and Digital Fraud in the Financial Sector. Working paper. 2026/062. IMF Working Papers. International Monetary Fund. <https://EconPapers.repec.org/RePEc:imf:imfwpa:2026/062>
- Klein, W. M., & Weinstein, N. D. (1997). Social comparison and unrealistic optimism about

- personal risk. In *Health, coping, and well-being: Perspectives from social comparison theory* (pp. 25–61). Lawrence Erlbaum Associates Publishers.
- Kuensel. (2026, March 9). *Email scams, a new trend in Bhutan's online fraud cases*. Retrieved March 29, 2026, from <https://asianews.network/email-scams-a-new-trend-in-bhutans-online-fraud-cases/>
- Lei, W., Hu, S., & Hsu, C. (2021). Understanding Optimism Bias in Phishing: A Health Belief Model Perspective. PACIS 2021 Proceedings. <https://aisel.aisnet.org/pacis2021/169>
- Lei, W., Hu, S., & Hsu, C. (2023). Unveiling the process of phishing precautions taking: The moderating role of optimism bias. *Computers & Security*, 129, 103249. <https://doi.org/10.1016/j.cose.2023.103249>
- Owen, M., Flowerday, S. V., & van der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information and Computer Security*, 32(5), 656–675. <https://doi.org/10.1108/ICS-02-2023-0023>
- Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon: The International Journal of Learning Futures*, 9(5), 1–6. <https://doi.org/10.1108/10748120110424816>
- Rhee, H.-S., Ryu, Y., & Kim, C.-T. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *Proceedings of the International Conference on Information Systems*, ICIS 2005, December 11–14. International Conference on Information Systems 2005, Las Vegas, NV, USA.
- Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221–232. <https://doi.org/10.1016/j.cose.2011.12.001>
- Shepperd, J. A., Klein, W. M. P., Waters, E. A., & Weinstein, N. D. (2013). Taking Stock of Unrealistic Optimism. *Perspectives on Psychological Science: A Journal of the Association for Psychological Science*, 8(4), 395–411. <https://doi.org/10.1177/1745691613485247>
- Tenzin, S., McGill, T., & Dixon, M. (2024). An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan. *Journal of Global Information Technology Management*, 27(1), 37–62. Scopus. <https://doi.org/10.1080/1097198X.2023.2297634>
- The Bhutanese. (2025, October 18). *Surge in online scams and gambling*. *The Bhutanese*. Retrieved March 29, 2026, from <https://thebhutanese.bt/surge-in-online-scams-and-gambling/>
- Toomey, J. (2023). *The Age of Fraud*. Elisabeth Haub School of Law Faculty Publications. <https://digitalcommons.pace.edu/lawfaculty/1247>
- Wangchuk, T., Tshering, Y., & Pradhan, P. (2024). Navigating Cyber Perils in Bhutan: Challenges and Opportunities. *Journal of Applied Engineering, Technology and Management*, 4(1), 23–30. <https://doi.org/10.54417/jaetm.v4i1.132>
- Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820. <https://doi.org/10.1037/0022-3514.39.5.806>
- White, D. S., & Cornu, A. L. (2011). Visitors and Residents: A new typology for online engagement. *First Monday*. <https://doi.org/10.5210/fm.v16i9.3171>
- Yangchen, T. (2025). Strengthening Digital Defenses: Evaluating the Impact of Cybersecurity Awareness Workshops Among First-Year Engineering Students in Bhutan. *Bhutan Journal of Research and Development*, 14(3). <https://doi.org/10.17102/bjrd.rub.14.3.008>