CUSTOMERS' KNOWLEDGE OF ETHICAL HACKING PRACTICES AND ITS INFLUENCE ON BRAND IMAGE

(A Case of Machhapuchchhre Bank Limited)

A CIS Research Project Report

Course Code: COM 444

Submitted to:

Little Angels' College of Management

Kathmandu University School of Management

In partial fulfillment of requirements for the degree of

Bachelor of Business Information Systems (BBIS)

Submitted by:

Shleshma Shrestha

K.U. Registration No.: A030676-21

Under the supervision of:

Bibhav Adhikari

Research Coordinator, LACM

August 2025

Hattiban, Lalitpur

CUSTOMERS' KNOWLEDGE OF ETHICAL HACKING PRACTICES AND ITS INFLUENCE ON BRAND IMAGE

(A Case of Machhapuchchhre Bank Limited)

A CIS Research Project Report

Course Code: COM 444

Submitted to:

Little Angels' College of Management

Kathmandu University School of Management

In partial fulfillment of requirements for the degree of

Bachelor of Business Information Systems (BBIS)

Submitted by:

Shleshma Shrestha

K.U. Registration No.: A030676-21

Under the supervision of:

Bibhav Adhikari

Research Coordinator, LACM

August 2025

Hattiban, Lalitpur

RECOMMENDATION LETTER

ACKNOWLEDGEMENT

The researcher sincerely thanks Kathmandu University and Little Angels' College of Management for providing the opportunity to undertake this research project. Special gratitude goes to the Principal, Dr. Mitra Bandhu Poudel, who consistently encouraged and supported the researcher throughout this journey. The researcher also extends heartfelt appreciation to the supervisor and Research Coordinator, Bibhav Adhikari, whose unwavering support, insightful guidance, constructive feedback, and constant motivation played a crucial role in successfully completing the research.

The researcher deeply appreciates Machhapuchchhre Bank Limited for granting permission to conduct the research and for the support extended during the process. Gratitude is also expressed to all individuals who assisted throughout the project. The encouragement and help provided by friends and family significantly contributed to the successful completion of this report.

Finally, the researcher sincerely thanks all respondents who participated in the survey and made this research possible.

Sincerely,

Shleshma Shrestha

K.U. Registration No.: A030676-21

DECLARATION

I, Shleshma Shrestha, hereby declare this CIS Research Project titled “Customers' Knowledge of Ethical Hacking Practices and Its Influence on Brand Image (A Case of Machhapuchchhre Bank Limited)”, is submitted to Little Angels’ College of Management, affiliated with Kathmandu University, in partial fulfillment of the requirements for the Bachelor of Business Information Systems degree.

I affirm that the content of this report has not been submitted for any other degree, diploma, or academic qualification at any other institution. All sources of information used in the preparation of this report have been properly cited and acknowledged.

_____

Shleshma Shrestha

Batch 2021-2024

KU reg. no.: A030676-21

Little Angels’ College of Management

Kathmandu University

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CIS	Computer Information Systems
COM	Computer
IT	Information Technology
MBL	Machhapuchchhre Bank Limited
PMT	Protection Motivation Theory
SMEs	Small and Medium Enterprises
SPSS	Statistical Package for the Social Sciences
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior

EXECUTIVE SUMMARY

Ethical hacking is a growing cybersecurity practice used by organizations to test and strengthen their digital security systems. In the banking sector, where trust and data protection are vital, understanding customer awareness of such practices is important for building and maintaining a strong brand image. This research focuses on exploring the level of knowledge customers have about ethical hacking practices implemented by MBL and how this knowledge influences their perception of the bank's brand.

The general objective of this study is to examine the impact of ethical hacking knowledge on customers' perception of MBL's overall brand image. The research is quantitative and descriptive in nature, using survey-based data collection. A structured questionnaire with close-ended questions was developed using a five-point Likert scale. The questionnaire was distributed to a sample of 389 customers of MBL selected through simple random sampling.

The data collected was analyzed using SPSS, applying descriptive statistics and inferential techniques to interpret customer responses. The findings of this study aim to provide valuable insights for banking institutions on how cybersecurity communication strategies can influence customer perceptions and brand positioning.

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

In today's digital era, cybersecurity has become a critical priority for financial institutions as banking services increasingly shift towards digital platforms. The Nepal banking sector has witnessed rapid digitalization with the expansion of online banking, mobile banking, and digital payment systems. (Nepal Rastra Bank, 2023) This digital transformation, while offering convenience and accessibility, has also exposed banks to various cyber threats, making robust cybersecurity measures essential for maintaining customer trust and confidence.

Ethical hacking has emerged as a proactive cybersecurity approach where authorized security professionals attempt to identify vulnerabilities in banking systems before malicious hackers can exploit them. This practice has become an integral component of modern banking cybersecurity strategies, particularly for institutions like MBL that handle sensitive financial data and transactions. (Dongol & Chatterjee, 2019) By employing ethical hacking practices, banks can strengthen their security posture while demonstrating their commitment to protecting customer assets and information.

The relationship between cybersecurity practices and brand image has become increasingly significant in the banking sector. Research indicates that customer awareness and understanding of a bank's security measures, including ethical hacking practices, can substantially influence their perception of the institution's reliability and trustworthiness (Hammond, 2024). When customers are informed about their bank's proactive security measures, it enhances their confidence in the institution's ability to protect their financial interests.

Furthermore, studies suggest that effective communication about cybersecurity practices can enhance consumer confidence and mitigate negative perceptions, particularly in an industry where trust is paramount (Mirbahar, 2024). In the context of

Nepal's banking sector, where customer trust directly impacts brand loyalty and reputation, understanding how customers perceive ethical hacking practices becomes crucial for banks like MBL.

The significance of this relationship is further emphasized by research indicating that consumers are more likely to engage with financial institutions that prioritize and transparently communicate their cybersecurity measures (Sheik, 2023). For MBL, which serves a diverse customer base across Nepal, understanding customer knowledge and perceptions of ethical hacking practices can provide valuable insights into how these security measures influence the bank's brand image.

This study focuses specifically on MBL, one of Nepal's prominent commercial banks known for its innovative banking service. By examining customers' knowledge of ethical hacking practices and its influence on the bank's brand image, this research aims to contribute to the understanding of cybersecurity communication strategies in Nepal's banking sector.

1.2 Statement of Problem

Despite the increasing adoption of ethical hacking practices by financial institutions to safeguard digital assets, there remains a significant gap in customer awareness and understanding of these efforts. (Pant, 2020) In urban areas of Nepal, particularly Kathmandu and Lalitpur, many customers actively use digital banking platforms but lack basic knowledge of cybersecurity and ethical hacking practices. This limited awareness restricts their ability to appreciate the proactive security measures taken by banks and hinders the development of trust in the institution's digital infrastructure. (Dongol & Chatterjee, 2019)

This study addresses the limited awareness among customers regarding ethical hacking and its role in enhancing brand image. While organizations adopt ethical hacking to strengthen cybersecurity, a lack of customer knowledge hampers their ability to recognize these efforts. In Nepal, many individuals and businesses remain unaware of potential cyber threats and lack the knowledge to protect themselves effectively, creating opportunities for cybercriminals to exploit vulnerabilities (Yadav, 2024). The public has little-to-no cybersecurity education, which is a critical reason why

cybercrimes have proliferated rapidly in the country (Ghimire, 2024). This lack of awareness is particularly evident among individuals who frequently engage with digital platforms but lack the necessary knowledge to protect themselves from cyber threats. As a result, cybercriminals have been able to exploit these vulnerabilities, leading to a rapid increase in cybercrimes.

Furthermore, many small and medium enterprises (SMEs), which are vital to Nepal's economy, do not have sufficient resources or skilled staff to build robust cybersecurity systems against probable threats (Ghimire, 2024). Without addressing these gaps in awareness and infrastructure, the potential of ethical hacking to enhance brand image remains constrained.

1.3 Objective of the Study

The primary objective of this study is to examine the influence of customers' knowledge of ethical hacking practices on the brand image of MBL.

The specific objectives are:

1. To assess the level of knowledge among customers regarding ethical hacking practices at MBL.
2. To assess customers' overall perception of MBL's brand image.
3. To examine the relationship between knowledge of ethical hacking practices and MBL's overall brand image.
4. To identify whether a significant association exists between the level of ethical hacking knowledge and customers' brand image perception.

1.4 Significance of the Study

This examines how customers' knowledge of ethical hacking practices influences the brand image of MBL. Understanding this relationship helps the bank improve its communication and marketing strategies to build greater trust, loyalty, and credibility among customers. Additionally, the findings contribute to the limited research on cybersecurity awareness and its impact on customer perceptions in Nepal's banking sector. This study also provides valuable insights for policymakers, banking

professionals, and researchers interested in enhancing cybersecurity transparency and strengthening brand reputation in the financial industry.

1.5 Research Questions

1. What is the level of customer knowledge regarding ethical hacking practices MBL?
2. How do customers perceive the overall brand image of MBL?
3. Is there a significant relationship between customers' knowledge of ethical hacking practices and their perception of MBL's brand image?
4. Does the level of customer knowledge of ethical hacking practices significantly associate with the customers' brand image perception of MBL?

1.6 Delimitation of the Study

This study is delimited to customers of MBL and focuses specifically on their knowledge of ethical hacking practices and its influence on the bank's brand image. The research is limited to quantitative data collected through surveys and does not include qualitative methods such as interviews. It is also confined to customers within Nepal, so the findings may not be generalizable to other banks or countries. The study focuses only on key variables such as knowledge, trust, loyalty, credibility, and brand image, excluding other possible factors influencing brand perception.

CHAPTER 2

REVIEW OF LITERATURE

2.1 Introduction

This chapter presents a comprehensive review of existing literature related to customers' knowledge of ethical hacking practices and their influence on brand image in the banking sector. The theoretical review establishes the conceptual foundation by examining key theories related to brand image, customer knowledge, and cybersecurity practices. The empirical review analyzes relevant studies that have investigated similar relationships in various contexts. Finally, the research gap section identifies the limitations in existing literature that this study aims to address.

The review focuses on understanding how customer awareness and knowledge of cybersecurity practices, particularly ethical hacking, influences their perception of organizational brand image. Given the increasing importance of cybersecurity in the digital banking era, this literature review provides insights into the relationship between security practices and customer perceptions in financial institutions.

2.2 Theoretical Review

2.2.1 Brand Image Theory

Brand image is widely regarded as a multidimensional construct in marketing literature, encompassing various psychological and emotional associations that consumers hold toward a brand. According to Keller (2020), brand image reflects consumers' perceptions based on the brand's associations in their memory, including aspects such as trust, credibility, and loyalty. Aaker (1991) also emphasizes that brand equity is built upon brand associations, perceived quality, loyalty, and brand awareness, all of which contribute to a brand's image. Loyalty, both behavioral and attitudinal, further strengthens the brand image by reflecting a customer's commitment and preference for the brand (Aaker, 1991). Collectively, these studies provide a theoretical foundation for viewing brand image as a composite of trust, loyalty, and credibility, which are essential for forming a positive and strong brand perception.

2.2.2 Theory of Planned Behavior (TPB)

According to the Theory of Planned Behavior (Ajzen, 1991), individual behaviors are guided by three key factors: attitudes, subjective norms, and perceived behavioral control. In the context of this study, TPB is applied to understand how customers' attitudes toward ethical hacking, shaped by their awareness, beliefs, and social influence, impact their brand-related behaviors, such as trust, loyalty, and preference. For instance, customers who hold a positive attitude toward the use of ethical hacking in banking, and perceive social approval for such practices, are more likely to support and remain loyal to brands that prioritize cybersecurity. Prior research supports this, showing that favorable attitudes toward cybersecurity initiatives, including ethical hacking, significantly influence customer trust and loyalty (Singh & Lien, 2023). Thus, TPB provides a useful lens to examine how knowledge and perceptions of ethical hacking translate into brand image formation and customer behavior.

2.2.3 Signaling Theory

Signaling Theory, developed by Spence (1973), suggests that organizations communicate information about their quality and capabilities through various signals to reduce information asymmetry with stakeholders. In the banking sector, ethical hacking practices can serve as quality signals, indicating the bank's commitment to cybersecurity and customer protection. Customers who understand these signals are likely to develop more positive perceptions of the bank's reliability and competence.

2.2.4 Protection Motivation Theory (PMT)

According to Protection Motivation Theory (PMT), individuals are motivated to protect themselves against threats based on two cognitive processes: threat appraisal and coping appraisal (Rogers, 1975). In the context of ethical hacking, customers who are aware of potential cybersecurity threats may perceive brands that employ ethical hacking as more proactive and trustworthy. PMT suggests that when customers understand how ethical hacking helps safeguard their personal and financial data, they are more likely to feel secure and develop greater trust in the brand. This increased sense of security can positively influence their perception of the brand's image (Chen & Jai, 2019).

2.2.5 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) explains how users come to accept and use technology based on their perceptions of its usefulness and ease of use (Davis, 1989). In the context of this study, TAM provides a framework to assess how the perceived usefulness and transparency of ethical hacking practices influence customer trust. For example, when customers believe that ethical hacking effectively protects their data, they are more likely to trust the bank's technological capabilities and security infrastructure. Research has shown that the perceived usefulness of cybersecurity measures directly impacts customer trust and brand loyalty (Johri, 2023). This trust contributes to a stronger and more positive brand image, particularly in sectors such as banking where data protection is a key customer concern.

2.3 Empirical Review

Hammond (2024) conducted a study examining the relationship between cybersecurity communication and consumer trust in digital platforms. The study involved 450 respondents from various industries and found that effective communication about cybersecurity practices significantly enhances consumer trust. The research revealed that consumers who were informed about organizational security measures demonstrated 34% higher trust levels compared to those who lacked such knowledge. The study concluded that transparency in cybersecurity communication serves as a critical factor in building and maintaining consumer trust.

Mirbahar (2024) investigated the impact of ethical hacking awareness on brand perception among 320 banking customers across three countries. The study employed a mixed-methods approach and found that customers with higher awareness of ethical hacking practices showed significantly more positive brand perceptions. The research identified that 67% of informed customers expressed higher confidence in their bank's security capabilities. The study emphasized that customer education about ethical hacking practices could serve as a strategic tool for enhancing brand image.

The study "Ethical Hacking and Its Role in Cybersecurity" (Choudhary & Kaushik, 2023) explores the integral role of ethical hacking in mitigating cybersecurity threats and enhancing organizational resilience. It examines fundamental concepts,

methodologies, and techniques employed by ethical hackers, such as penetration testing and vulnerability assessment, to safeguard digital infrastructure. The paper also addresses legal and ethical considerations. Real-world applications and case studies illustrate how ethical hacking identifies vulnerabilities and strengthens security defenses. Additionally, the study highlights the contribution of ethical hacking to fostering a security-aware culture and proactive risk management. This research is particularly relevant as it provides insights into how ethical hacking practices can enhance organizational cybersecurity, align with legal frameworks, and build a positive brand image.

The study “Ethical Hacking as a Risk Management Tool in Organizations” (Singh & Lien, 2023) underscores the importance of ethical hacking as a key risk management tool. The research highlights that organizations implementing ethical hacking practices not only strengthen their cybersecurity framework but also project a brand image of responsibility and trustworthiness. Empirical evidence gathered from interviews and case studies demonstrates that companies actively involved in ethical hacking are viewed more positively by customers, resulting in increased loyalty and trust. This aligns with the focus of this research by illustrating how ethical hacking practices can influence brand perception and promote customer trust.

The study "Trust Fall: Data Breach Perceptions from Loyalty and Non-Loyalty Customers" (Chen & Jai, 2019) investigates how customer loyalty influences perceptions of data breaches, particularly in the hotel industry. Both loyalty and non-loyalty customers recognize the severity of data breaches, but loyalty program customers experience a more significant loss of trust in the organization following such incidents. This suggests that loyal customers have higher expectations for data protection, making them more vulnerable to trust erosion when breaches occur. The study emphasizes the importance of effective crisis management in rebuilding trust and safeguarding brand reputation. These findings are relevant to understanding how ethical hacking can positively impact on a company's image. By adopting proactive cybersecurity practices such as ethical hacking, organizations can mitigate trust concerns, particularly among loyal customers, and enhance their brand's resilience in the event of a data breach.

A study conducted by a researcher (Johri, 2023) in Saudi Arabia examines customer awareness and satisfaction regarding cybersecurity in the context of banking's digital transformation. The study reveals that customer awareness of threats like cyberattacks, phishing, and hacking significantly impacts satisfaction with digital services. It emphasizes the need for organizations to educate customers on cybersecurity and improve technical support to build trust. Organizations that prioritize security measures, including ethical hacking, are better positioned to meet customer expectations and achieve long-term sustainability. This study is relevant to understanding how customer awareness about cybersecurity, including ethical hacking, contributes to their perception of a brand's reliability and commitment to security.

The article "Importance of Cybersecurity Awareness Training for Employees in Business" (Tolossa, 2023) highlights the critical role that employee training plays in fortifying organizational defenses against cyber threats. The study reveals that training employees to identify and address threats such as phishing and social engineering not only reduces security incidents but also fosters a culture of cybersecurity awareness. It suggests that organizations with a proactive approach to cybersecurity, including ethical hacking, can enhance brand reputation and customer confidence. By communicating these efforts to customers, organizations can build a stronger image of commitment to data security.

The study "Security Threats and Legalities with Digitalization in Nepal" (Acharya & Dahal, 2021) highlights the vulnerabilities arising from Nepal's growing dependence on digital technologies, exacerbated by inadequate legal frameworks. Key incidents, like the hacking of over 45 websites during geopolitical tensions in 2020, underscore the need for stronger cybersecurity measures. The study emphasizes the importance of awareness programs and ethical hacking practices to identify and mitigate cyber threats, which are crucial for enhancing cybersecurity and fostering trust in Nepal's digital landscape. This regional context adds value to understanding how ethical hacking can shape brand image in Nepal, where cybersecurity awareness is still developing.

2.4 Research Gap

Although existing literature has explored cybersecurity and brand perception, notable gaps remain. Most studies are concentrated in developed countries, with limited research in developing regions like South Asia, where banking digitalization is rapidly growing. Moreover, few studies focus specifically on ethical hacking as a distinct cybersecurity practice. Research in this area is also sparse within the banking sector, despite its critical need for strong cybersecurity and customer trust. Additionally, most studies use broad industry samples or continuous variables for knowledge, overlooking case-specific analyses and categorized knowledge levels. This study addresses these gaps by examining the impact of ethical hacking knowledge on the multidimensional brand image of MBL in Nepal.

2.5 Conceptual Framework

The representation of the relationship of the variables that we want to study based on the literature review of similar studies related to our topic is known as Conceptual framework (Swaen & George, 2022).

This study is based on a conceptual framework that explores the relationship between customers' knowledge of ethical hacking practices and the overall brand image of MBL. The core idea is that as customers become more informed about ethical hacking, particularly how it is used by banks to protect digital banking systems, their perception of the bank's security may improve, thereby enhancing the overall brand image of the institution.

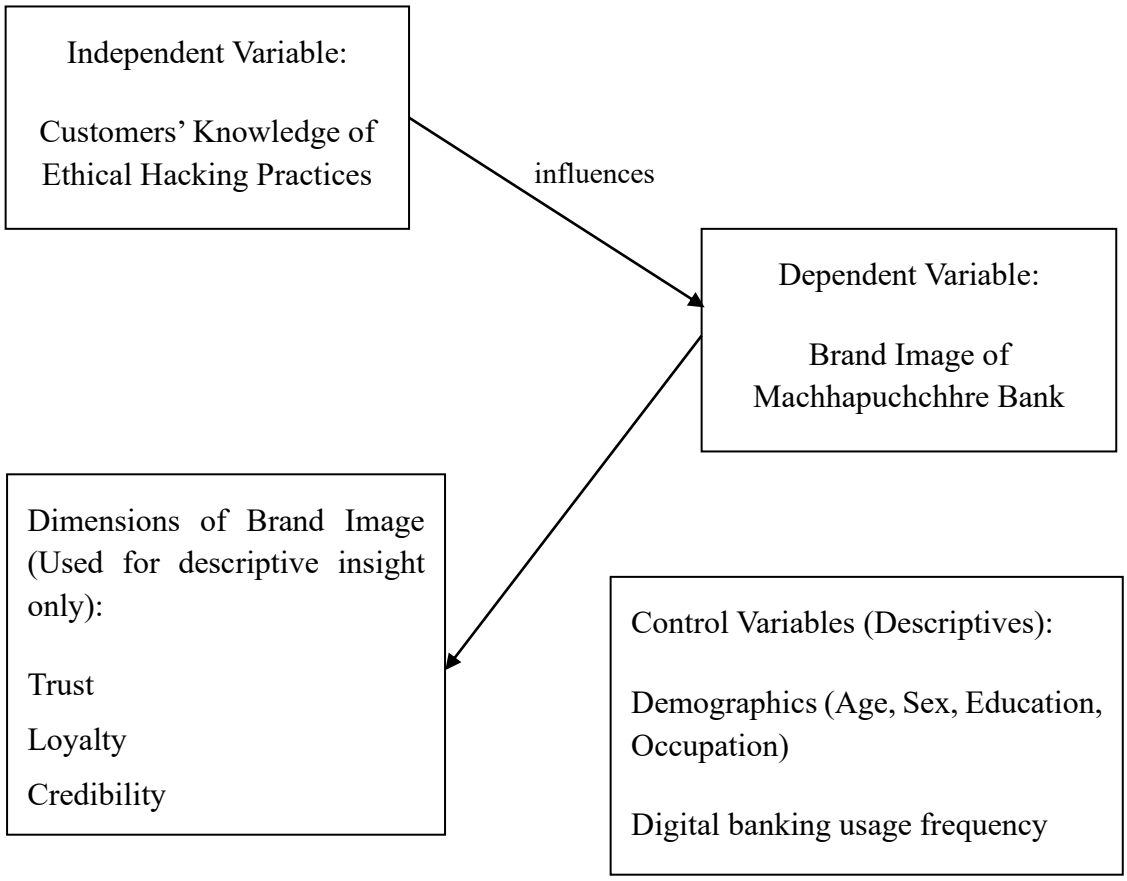

Figure 1: Conceptual Framework

Source: Author, 2025

In this framework, the independent variable is the customers' knowledge of ethical hacking practices. This refers to how much customers know about the ethical hacking practices followed by MBL, including their objectives, ethical nature, and how they contribute to enhancing digital banking security. The dependent variable is the overall brand image of MBL, which represents customers' overall perception of the bank's reputation and credibility.

To provide additional descriptive insight into how customers perceive the brand, the study considers three key dimensions of brand image: trust, loyalty, and credibility. These dimensions are not treated as separate dependent variables or part of the main hypothesis testing; rather, they are used solely for descriptive analysis to offer a more detailed understanding of brand perception. Trust reflects how secure and dependable customers believe the bank to be, loyalty captures their intention to continue using the

bank's services, and credibility refers to how honest and transparent the bank is perceived to be.

Furthermore, several control variables are incorporated for descriptive purposes to better understand the respondent profile and their potential influence on perceptions. These include demographic factors such as age, sex, education level, and occupation, as well as the frequency of digital banking usage. These variables are not used to test relationships but rather to provide context and control for background characteristics during data analysis.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methods used to investigate how customers' knowledge of ethical hacking practices influences MBL's brand image. It includes research design, population, sampling techniques, data collection tools, and analysis methods.

3.2 Research Design

Initially, the research title was "Knowledge of Ethical Hacking and Its Influence on Brand Image", but it was later revised to "Customers' Knowledge of Ethical Hacking and Its Influence on Brand Image (A Case of Machhapuchchhre Bank Limited)" to better reflect the study's scope and context. The researcher adopted a quantitative research design using descriptive and explanatory approaches. This design enabled the description of customers' knowledge of ethical hacking practices and the explanation of its influence on brand image. The study relied on structured questionnaires to collect data. For the analysis, the Chi-square test was primarily used to assess associations between variables. In cases where the expected cell counts were less than five, Fisher's Exact Test was applied to ensure the accuracy and reliability of the p-values.

3.3 Study Population

The study focused on customers of MBL. This population included individuals using MBL's banking services who held varying levels of knowledge regarding ethical hacking practices.

3.4 Sample Size

The sample size was calculated using Cochran's formula for an infinite population, as the exact number of MBL customers was not accessible. This approach ensured statistical validity and allowed for generalization within a large population context.

$$n_0 = \frac{Z^2 pq}{e^2} \quad \text{(Cochran, 1977)}$$

Where:

n_0 = initial sample size

Z = Z-score for the confidence level

p = estimated proportion of the population that has knowledge of ethical hacking

q= (1-p)

e = margin of error

Assuming a confidence level of 95% (Z=1.96), and a margin of error of 5% (e=0.05), the sample size is calculated as follows:

$$n_0 = \frac{1.96^2 \times 0.5 \times (1 - 0.5)}{0.05^2}$$

$$\therefore n_0 = 384.16$$

According to Cochran's formula, a sample size of approximately 384 respondents was recommended for a large population, assuming a 95% confidence level and a 5% margin of error. However, the study analyzed a total of 389 valid responses, which exceeds the minimum requirement and enhances the reliability of the findings.

3.5 Sampling Technique

Due to the unavailability of a complete customer list, the researcher used snowball sampling to collect data. The questionnaire was initially sent to known customers of MBL, who were then asked to share it with other MBL users. Additionally, with the bank's permission, an employee helped distribute the questionnaire personally to further reach potential respondents. This approach allowed the researcher to access a broader group of customers despite professional restrictions on direct contact.

3.6 Data Collection Procedure

The researcher distributed structured questionnaires online through Google Forms. Participants received an explanation of the study's purpose, and their involvement remained voluntary throughout the process. The data collection avoided the use of any personally identifiable information.

3.7 Data Collection Tools

The primary tool for data collection was a structured questionnaire employing a five-point Likert scale. The questionnaire included multiple items measuring the customers' knowledge of ethical hacking practices, trust in the bank, customer loyalty, perceived credibility of the bank, and the overall brand image of MBL.

3.8 Data Analysis Procedure

The researcher used SPSS software to analyze the data. The analysis included:

1. Descriptive statistics to summarize participant responses.
2. Reliability testing using Cronbach's Alpha.
3. Correlation analysis to identify relationships between customers' knowledge of ethical hacking and MBL's brand image.
4. Chi-square test to examine the association between customers' knowledge of ethical hacking and MBL's brand image.

3.9 Reliability and Validity

The reliability of the questionnaire scales was assessed using Cronbach's Alpha. All variables showed excellent reliability, with values above the acceptable threshold of 0.70, as summarized below:

Table 1

Reliability Test

n = 389

Reliability Statistics		
	Cronbach's Alpha	N of Items
Knowledge	0.924	5
Trust	0.948	5
Loyalty	0.912	5
Credibility	0.953	5
Brand Image	0.925	5

Source: Questionnaire, 2025

3.10 Ethical Consideration

The researcher prioritized ethical considerations to ensure the integrity of the study and protect participants' rights. Participants were fully informed about the study's purpose, the voluntary nature of their participation, and the confidentiality of their responses. Informed consent was obtained through a consent form attached to the survey, which outlined the study's objectives, explained how the data would be used, and confirmed that no personally identifiable information would be collected.

To uphold privacy and confidentiality, no personal identifiers were gathered, and data were securely stored in password-protected systems accessible only to the researcher, preventing unauthorized access throughout the study. Reliability and validity were ensured by designing a well-structured questionnaire, which was pre-tested with a small sample group.

The data collected was used solely for research purposes and was not shared with any third parties. By adhering to these ethical guidelines, the research will safeguard participants' rights and maintain the integrity of the study's findings.

CHAPTER 4

RESULTS

4.1 Basic Information of the Respondents

Table 2

Information of Respondents Based on Age, Sex, and Education

n = 389

	N	Percent
Age (Binned)		
<= 30	199	51.20
31+	190	48.80
Md (Q1, Q3)	30(27,33.5)	
Sex		
Male	242	62.2
Female	144	37
Prefer not to say	3	0.8
Education Level		
Bachelor's Degree	265	68.10
High School	17	4.40
Master's Degree and above	107	27.50

Source: Field Survey, 2025

Out of the total 389 respondents, 242 (62.2%) were male and 144 (37%) were female, while 3 respondents (0.8%) preferred not to disclose their gender. In terms of age, 199 respondents (51.2%) were 30 years old or younger, while 190 respondents (48.8%) were above 30. The median age was 30, with an interquartile range from 27 to 33.5 years, indicating a relatively young and balanced sample.

In terms of sex, most respondents identified as male (62.2%), followed by female (37.0%), while a small proportion (0.8%) chose not to disclose their gender.

Regarding education, most participants (265 or 68.1%) held a bachelor's degree, followed by 107 (27.5%) who had completed a master's degree or above, and 17 respondents (4.4%) with only a high school education.

Table 3

Information of Respondents Based on Occupation and Usage Frequency

n = 389

	N	Percent
Occupation		
Banking/Finance	69	17.70
Corporation	1	0.30
Education	68	17.50
Government	25	6.40
Healthcare	1	0.30
IT/Cybersecurity	108	27.80
Retail	16	4.10
Retired	1	0.30
Service	1	0.30
Student	98	25.20
Videographer	1	0.30
Usage Frequency		
Rarely (less than once a month)	40	10.30
Occasionally (1–3 times per month)	72	18.50
Frequently (1–6 times per week)	117	30.10
Daily (at least once per day)	160	41.10

Source: Field Study, 2025

Respondents came from various occupational backgrounds. The largest group was from the IT and cybersecurity sector, representing 108 respondents (27.8%), followed by students (98 or 25.2%), and individuals in banking and finance (69 or 17.7%). Other sectors included education (68 or 17.5%), government (25 or 6.4%), retail (16 or 4.1%), and a few individuals from fields such as healthcare, corporate, media, and service-related jobs.

In terms of usage frequency of banking services, 160 respondents (41.1%) reported daily usage, 117 (30.1%) used banking services frequently (1–6 times per week), 72 (18.5%) occasionally (1–3 times per month), and only 40 (10.3%) used them rarely (less than once a month). This suggests that a significant portion of the sample actively engages with banking platforms, which is highly relevant to the research context.

4.2 Descriptive Frequencies of Variables

Table 4

Knowledge of Ethical Hacking Practices Among Customers of MBL

n = 389

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware that MBL invests in ethical hacking to test its digital security systems.	7(1.8)	3(0.8)	100(25.7)	177(45.5)	102(26.2)
I know that ethical hackers at MBL help identify and fix potential security flaws.	4(1.0)	10(2.6)	103(26.5)	166(42.7)	106(27.2)
I have seen or heard that MBL publicly communicates its use of ethical hacking.	8(2.1)	51(13.1)	135(34.7)	140(36.0)	55(14.1)
I understand how ethical hacking helps MBL protect customer data.	4(1.0)	2(0.5)	79(20.3)	152(39.1)	152(39.1)
I am aware of specific cybersecurity initiatives taken by MBL.	5(1.3)	11(2.8)	136(35.0)	148(38.0)	89(22.9)

Source: Field Study, 2025

The findings indicate that customers of MBL generally possess a good level of knowledge regarding the bank's ethical hacking practices. Most respondents (45.5% agreed and 26.2% strongly agreed) reported being aware that MBL invests in ethical hacking to test its digital security systems. Similarly, 42.7% agreed and 27.2% strongly agreed that they know ethical hackers at the bank help identify and fix security flaws, reflecting a strong understanding of their role. When asked whether the bank publicly communicates its use of ethical hacking, responses were more varied, with 36.0% agreeing and 14.1% strongly agreeing, while a notable 34.7% remained neutral and 13.1% disagreed. This indicates that some customers may not be fully aware of the bank's communication efforts regarding cybersecurity. Furthermore, a combined 78.2% of respondents agreed or strongly agreed that they understand how ethical hacking helps MBL protect customer data, suggesting a solid conceptual understanding among most participants. In terms of awareness of specific cybersecurity initiatives taken by the bank, 38.0% agreed and 22.9% strongly agreed, although 35.0% remained neutral, implying that while general awareness is high, more detailed knowledge of specific initiatives may still be limited.

Overall, the results reflect a positive level of knowledge among customers, though enhanced communication from the bank could further strengthen customer knowledge and engagement with its cybersecurity practices.

Table 5

Trust in MBL

n = 389

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I trust MBL to protect my sensitive financial information.	1(0.3)	49(12.6)	32(8.2)	196(50.4)	111(28.5)
I trust MBL to act in my best interests.	0(0.0)	19(4.9)	45(11.6)	268(68.9)	57(14.7)
I trust MBL to provide secure banking services.	0(0.0)	17(4.4)	34(8.7)	203(52.2)	135(34.7)
I feel confident using MBL's banking services.	0(0.0)	16(4.1)	79(20.3)	221(56.8)	73(18.8)
I have confidence in MBL's ability to manage my financial needs.	0(0.0)	16(4.1)	72(18.5)	222(56.8)	78(20.1)

Source: Field Study, 2025

The results indicate that customers generally have a high level of trust in MBL. Over three-fourths of the respondents (50.4% agreed and 28.5% strongly agreed) trust MBL to protect their sensitive financial information, while only 0.3% strongly disagreed and 12.6% disagreed, suggesting a small portion of skepticism. When asked if the bank acts in their best interests, a significant 68.9% agreed and 14.7% strongly agreed, with no respondents strongly disagreeing, further highlighting the bank's positive perception. Similarly, 52.2% agreed and 34.7% strongly agreed that MBL provides secure banking services, reinforcing confidence in its digital security. Confidence in using MBL's

services was also strong, with 56.8% agreeing and 18.8% strongly agreeing, although 20.3% remained neutral. Lastly, a combined 76.9% of customers expressed confidence in the bank's ability to manage their financial needs.

Overall, these findings demonstrate that MBL enjoys a high level of trust among its customers, particularly in terms of security, service quality, and ethical conduct.

Table 6

Loyalty to MBL

n = 389

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am likely to continue using MBL.	2(0.5)	3(0.8)	72(18.5)	236(60.7)	76(19.5)
I prefer MBL over other banks.	8(2.1)	65(16.7)	172(44.2)	91(23.4)	53(13.6)
I recommend MBL to others.	4(1.0)	14(3.6)	114(29.3)	205(52.7)	52(13.4)
I would choose MBL even if other banks offer similar services.	21(5.4)	63(16.2)	225(57.8)	35(9.0)	45(11.6)
I feel more committed to MBL.	10(2.6)	62(15.9)	83(21.3)	180(46.3)	54(13.9)

Source: Field Study, 2025

The data suggests a generally favorable level of customer loyalty toward MBL, though responses reflect varying degrees of commitment. A strong majority of respondents (60.7% agreed and 19.5% strongly agreed) indicated they are likely to continue using MBL, with only 1.3% expressing disagreement. When asked if they prefer MBL over other banks, responses were more divided, while 23.4% agreed and 13.6% strongly agreed, a substantial portion (44.2%) remained neutral and 18.8% expressed disagreement. Regarding customer advocacy, more than half (52.7%) agreed they

would recommend MBL to others, and 13.4% strongly agreed, showing a high level of satisfaction and trust in sharing the brand with peers. However, loyalty was more mixed when participants were asked if they would still choose MBL if other banks offered similar services, only 20.6% agreed or strongly agreed, while 21.6% disagreed and a majority of 57.8% stayed neutral, indicating that competitive offerings may influence their decisions. Lastly, 60.2% of respondents (46.3% agree and 13.9% strongly agree) felt a personal commitment to MBL, although a notable portion (21.3% neutral and 18.5% disagree) may be less emotionally attached. These findings reflect a generally loyal customer base, especially in terms of continued use and willingness to recommend, though competitive sensitivity may affect their long-term loyalty.

Table 7

Credibility of MBL

n = 389

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I believe MBL is a professional organization.	2(0.5)	0(0.0)	68(17.5)	174(44.7)	145(37.3)
MBL is a competent institution.	0(0.0)	3(0.8)	83(21.3)	176(45.2)	127(32.6)
I trust MBL to deliver high-quality services.	0(0.0)	17(4.4)	90(23.1)	212(54.5)	70(18.0)
I view MBL as a reliable organization.	0(0.0)	3(0.8)	71(18.3)	171(44.0)	144(37.0)
MBL demonstrates expertise in banking services.	1(0.3)	46(11.8)	43(11.1)	169(43.4)	130(33.4)

Source: Field Study, 2025

The findings indicate a strong perception of MBL as a credible institution among its customers. Most respondents viewed the bank as professional, with 44.7% agreeing and 37.3% strongly agreeing that MBL maintains professionalism, while only a small fraction (0.5%) disagreed. Similarly, perceptions of the bank's competence were positive, as 45.2% agreed and 32.6% strongly agreed that MBL is a competent institution, with just 0.8% disagreement. Many participants (54.5% agree and 18.0% strongly agree) expressed trust in the bank's ability to deliver high-quality services, though a small minority (4.4%) disagreed. Regarding reliability, 44.0% agreed and 37.0% strongly agreed that MBL is reliable, with minimal disagreement (0.8%). Finally, the bank's expertise in banking services was also well regarded, with 43.4% agreeing and 33.4% strongly agreeing, despite 11.8% disagreeing. Overall, these results suggest that customers generally perceive MBL as a credible and trustworthy institution, which is likely to contribute positively to its brand image.

Table 8

Brand Image of MBL

n = 389

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have a positive overall image of MBL.	2(0.5)	6(1.5)	118(30.3)	201(51.7)	62(15.9)
I view MBL as an innovative organization.	3(0.8)	68(17.5)	133(34.2)	133(34.2)	52(13.4)
MBL stands out among other banks in Nepal.	8(2.1)	62(15.9)	166(42.7)	88(22.6)	65(16.7)
I believe MBL is a leader in the banking industry.	19(4.9)	91(23.4)	207(53.2)	23(5.9)	49(12.6)
MBL has a strong reputation.	0(0.0)	5(1.3)	111(28.5)	192(49.4)	81(20.8)

Source: Field Study, 2025

The overall brand image of MBL is generally positive among customers. Over half of the respondents (51.7%) agreed and 15.9% strongly agreed that they hold a positive overall image of the bank, with very few expressing disagreement. When considering innovation, perceptions were mixed; 34.2% agreed and 13.4% strongly agreed that MBL is innovative, though 17.5% disagreed and a significant portion remained neutral (34.2%). Regarding distinctiveness, fewer customers believed the bank stands out among other banks in Nepal, with only 22.6% agreeing and 16.7% strongly agreeing, while 15.9% disagreed and 42.7% were neutral. The perception of MBL as a leader in the banking industry was less strong, as over half (53.2%) remained neutral, and only 18.5% agreed or strongly agreed, while 28.3% disagreed. However, the bank's reputation was rated positively, with nearly 70% agreeing or strongly agreeing that MBL has a strong reputation and very few expressing disagreement. Overall, the results suggest that while customers view MBL positively and respect its reputation, perceptions about its innovation and leadership position in the industry are less definitive and could be areas for further development.

4.3 Distribution by Knowledge Level and Brand Perception

Table 9

Distribution of Respondents by Knowledge Level of Ethical Hacking Practices at MBL

n = 389

	N	Percent
Low	8	2.10
Moderate	132	33.90
High	249	64.00

Source: Field Study, 2025

The data indicates that a significant majority of respondents (64%) possess a high level of knowledge regarding ethical hacking, suggesting that most customers are aware of how such practices contribute to digital security. Meanwhile, 33.9% of respondents reported a moderate level of knowledge, reflecting partial awareness. Only 2.1% demonstrated low knowledge, highlighting that very few customers are unfamiliar with

ethical hacking concepts. This suggests a generally well-informed customer base, which may influence their trust and perception of the bank's security initiative.

Table 10

Distribution of Respondents by Perception of Brand Image of MBL

n = 389

	N	Percent
Negative	99	25.40
Neutral	30	7.70
Positive	260	66.80

Source: Field Study, 2025

The results show that a large majority of respondents (66.8%) hold a positive perception of MBL's brand image. This indicates strong approval of the bank's reputation and overall customer experience. Additionally, 7.7% of the respondents remained neutral, suggesting indifference or uncertainty toward the brand. On the other hand, 25.4% of the participants expressed a negative perception, pointing to areas where the bank may need to improve its image or services. Overall, the findings reflect a generally favorable brand image among customers.

4.4 Correlation Between Key Variables

Table 11

Correlation Between Knowledge of Ethical Hacking and Brand Image

n = 389

	Brand Image	
	r	p-value
Knowledge Score	0.737	<0.01
Brand Image Score	0.737	<0.01

Source: Field Study, 2025

The analysis revealed a strong positive correlation between customers' knowledge of ethical hacking practices and the overall brand image of MBL, with a correlation coefficient (r) of 0.737. This relationship is statistically significant at the 0.01 level (p

< 0.01), indicating that higher knowledge of ethical hacking among customers is associated with a more favorable perception of the bank's brand image.

4.5 Association Between Key Variables

Table 12

Association Between Knowledge Level and Perception of MBL's Brand Image

n = 389

		Perception of Brand Image			
		Negative	Neutral and Positive	Chi-Square Value	p-value
Knowledge Level	Low and Moderate	84(84.8)	108(37.2)	66.92	<0.001
	High	15(15.2)	182(62.8)		

Source: Field Study, 2025

**Fisher's Exact Test was used when expected cell counts were less than 5 to ensure accuracy of the p-value.*

The analysis examined the association between customers' knowledge level about ethical hacking and their perception of MBL's brand image. Results show that among those with low or moderate knowledge, 84.8% held a negative perception of the brand image, while only 37.2% viewed it neutrally or positively. In contrast, among those with high knowledge, just 15.2% reported a negative perception, whereas 62.8% perceived the brand image neutrally or positively. The Chi-square test indicated a statistically significant association between knowledge level and brand image perception ($\chi^2 = 66.92$, $p < 0.001$), suggesting that higher knowledge of ethical hacking is linked to more favorable perceptions of the bank's brand image.

CHAPTER 5

SUMMARY, DISCUSSION, IMPLICATIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter summarizes the entire study and highlights its key findings. It is organized into six sections. The first section provides a general introduction to the chapter. The second section summarizes the conclusions drawn from the analysis of the results. The third section discusses the findings in relation to existing literature. The fourth section outlines the implications of the study's results. The fifth section offers recommendations for future research in related areas. Finally, the sixth section concludes the study.

5.2 Summary

This study aimed to examine the level of customers' knowledge regarding ethical hacking practices at MBL and how this knowledge influences their perception of the bank's brand image. Data collected from 389 customers revealed that a majority (64%) possess high knowledge of ethical hacking, while 33.9% have moderate knowledge and only 2.1% have low knowledge. Correspondingly, 66.8% of respondents hold a positive brand image of MBL, with 25.4% negative and 7.7% neutral perceptions.

Statistical analysis showed a significant positive correlation between knowledge of ethical hacking and brand image perception. The chi-square test confirmed a strong association between knowledge categories and brand image, supported by a moderate to strong effect size. These findings indicate that higher awareness of ethical hacking practices is linked to a more favorable view of the bank.

5.3 Discussion

In this section, the findings of this study are compared with existing literature in the same field. The similarities, differences, and distinct aspects of each study are highlighted.

The findings of this study align with Hammond (2024), who demonstrated that effective communication of cybersecurity practices significantly enhances consumer trust across various industries. Similarly, this research confirms that knowledge of ethical hacking positively influences trust in MBL. However, while Hammond's study took a broader industry perspective on digital platforms, this study specifically focuses on the banking sector in Nepal, providing localized insights into the role of ethical hacking awareness in shaping brand image.

Mirbahar's (2024) investigation into ethical hacking awareness and brand perception across multiple countries also supports the positive correlation found in this study between higher awareness and favorable brand perceptions. Both studies emphasize that educating customers about ethical hacking builds confidence in security measures. Nonetheless, Mirbahar's mixed-methods approach contrasts with this study's quantitative survey design, and this research contributes unique data on the Nepalese banking context, enriching the global understanding of the topic.

The work by Choudhary and Kaushik (2023) explores the technical and legal aspects of ethical hacking as a cybersecurity tool, highlighting its role in vulnerability assessment and organizational resilience. While their study offers a theoretical and methodological foundation, this study adds a customer-focused perspective by empirically linking ethical hacking knowledge to brand trust, loyalty, and credibility, thus bridging technical practices with consumer perceptions.

Singh and Lien (2023) also underscore ethical hacking as a risk management tool that enhances brand responsibility and trustworthiness. Their qualitative research through interviews and case studies complements the present study's quantitative findings, which statistically confirm the significant relationship between ethical hacking knowledge and positive brand image among bank customers.

Chen and Jai (2019) examine trust erosion following data breaches in the hotel industry, noting that loyal customers suffer greater trust loss due to higher expectations. This contrasts with the proactive approach of the current study, which focuses on how ethical hacking awareness can build trust and prevent such erosion, highlighting the importance of preemptive cybersecurity measures in fostering resilient brand images.

Johri's (2023) study in Saudi Arabia similarly finds that customer awareness of cybersecurity threats improves satisfaction with digital banking services. Both studies agree on the importance of educating customers about cybersecurity, but while Johri covers a broad spectrum of threats, this research zooms in on ethical hacking knowledge and its specific influence on brand image within Nepal's banking industry.

Tolossa (2023) emphasizes the critical role of employee cybersecurity training in strengthening organizational defenses and fostering a security-aware culture. Although Tolossa's focus is on internal organizational factors, this study extends the concept by investigating the impact of external customer awareness on brand reputation, showing that communicating ethical hacking efforts to customers can enhance confidence and brand loyalty.

Finally, Acharya and Dahal (2021) highlight the cybersecurity challenges and legal vulnerabilities in Nepal, stressing the need for awareness programs and ethical hacking to improve trust in the country's digital environment. This study complements their findings by providing empirical evidence that customer knowledge of ethical hacking plays a crucial role in shaping positive brand perceptions in Nepal's banking sector, underlining the regional relevance of cybersecurity education.

5.4 Implications

The study underscores the critical role that ethical hacking knowledge plays in shaping customers' brand perception in the banking sector. For MBL and other banks, investing in clear communication and educational initiatives about cybersecurity can strengthen brand trust, loyalty, and credibility. Enhancing customers' understanding of ethical hacking may also provide a competitive advantage by differentiating the bank as a secure and customer-focused institution.

From a broader perspective, the findings contribute to the field of banking and cybersecurity marketing, suggesting that ethical hacking is not only a technical measure but also a strategic branding tool.

5.5 Recommendations

Based on the findings, the following recommendations are proposed for MBL:

i. Increase Public Awareness: Launch targeted campaigns to inform customers about the bank's ethical hacking initiatives and how these efforts protect their data and financial assets.
ii. Transparent Communication: Regularly publish cybersecurity updates and success stories to reinforce the bank's commitment to digital security.
iii. Customer Education Programs: Provide workshops, webinars, or digital content to enhance customers' cybersecurity literacy, focusing on ethical hacking's role.
iv. Feedback Mechanisms: Establish channels for customers to ask questions or report concerns about cybersecurity, fostering trust and engagement.
v. Leverage Brand Image: Incorporate cybersecurity credentials as a key element in branding and marketing strategies to highlight the bank's secure and innovative image.

5.6 Conclusion

This study aimed to examine the relationship between customers' knowledge of ethical hacking and their perception of brand image, with a focus on MBL. The findings revealed a significant positive relationship, indicating that higher awareness of ethical hacking among customers is associated with greater trust, loyalty, credibility, and an overall positive brand image. Statistical analyses, including Chi-square tests and correlation analysis, confirmed that ethical hacking knowledge plays a vital role in shaping brand perceptions.

Furthermore, the study established that most customers had a high level of awareness regarding ethical hacking, and those with greater awareness tended to associate MBL with a more positive brand image. These results align with prior studies that emphasize the importance of cybersecurity transparency and customer education in enhancing trust and brand credibility.

In conclusion, ethical hacking knowledge is not only a technical aspect of cybersecurity but also a strategic tool for improving brand perception. Banks and other organizations can benefit by actively educating customers about their cybersecurity measures,

including ethical hacking practices, strengthen brand trust and foster long-term customer relationships.

REFERENCES

Aaker, D. A. (1991). *Managing Brand Equity: Capitalizing on Brand Loyalty.* New York: Free Press.

Acharya, S., & Dahal, S. (2021). Security threats and legalities with digitalization in Nepal. *Research Nepal Journal of Development Studies*, 1-15.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 179-211. doi:https://doi.org/10.1016/0749-5978(91)90020-T

Chen, H. S., & Jai, T.-M. (. (2019). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, 947-963. doi:https://doi.org/10.1080/02642069.2019.1603296

Choudhary, D., & Kaushik, H. (2023). Ethical hacking and it's role in cyber security. *Journal of Nonlinear Analysis and Optimization*. Retrieved from https://jnao-nu.com/Vol.%2014,%20Issue.%2001,%20January-June%20:%202023/7.1.pdf

Cochran, W. (1977). *Sampling Techniques* (Third ed.). New York: John Wiley & Sons.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design* (Fifth ed.). California: SAGE Publications, Inc.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*, 297–334. doi:https://doi.org/10.1007/BF02310555

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. doi:https://doi.org/10.2307/249008

Dongol, R., & Chatterjee, J. M. (2019). Robust Security Framework for Mitigating Cyber Threats in Banking Payment System: A Study of Nepal. *LBEF Research Journal of Science, Technology and Management*, 1-21.

Ghimire, R. (2024, September 12). *The growing threat of cybercrime in Nepal: How prepared are we?* Retrieved from onlinekhabar: https://english.onlinekhabar.com/the-growing-threat-of-cybercrime-in-nepal-how-prepared-are-we.html

Hammond, A. (2024, July 3). *Six must-know ethical hacking facts and stats for businesses*. Retrieved from intigriti: https://www.intigriti.com/blog/business-insights/six-must-know-ethical-hacking-facts-and-stats-for-businesses

IBM Corp. (2020). *IBM SPSS Statistics*. Retrieved from IBM: https://www.ibm.com/products/spss-statistics

Johri, A. (2023). *Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation.* Retrieved from https://onlinelibrary.wiley.com/doi/10.1155/2023/2103442

Keller, K. L. (2020). *Strategic Brand Management.* London: Pearson Education Limited.

Khandoker, Z. (2024). How ethical hacking can improve digital marketing security: A case study approach. *American Journal of Business*. Retrieved from https://www.researchgate.net/publication/384092546_How_Ethical_Hacking_Can_Improve_Digital_Marketing_Security_A_Case_Study_Approach

Maurushat, A. (2019). *Ethical Hacking.* Ottawa: University of Ottawa Press. Retrieved from https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/87998/9780776627922.pdf?sequence=1&isAllowed=y

Mayer, R. C., James H. Davis, F., & Schoorman, D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 709–734. doi:https://doi.org/10.2307/258792

Mirbahar, A. (2024). *Analysing the impact of Cybercrime on customer Perception: Perspective of Pakistan.* Pakistan: ResearchGate. Retrieved from

https://www.researchgate.net/publication/377729653_Analysing_the_impact_of_Cybercrime_on_customer_Perception_Perspective_of_Pakistan

Nepal Rastra Bank. (2023). *Annual report 2022-23.* Nepal Rastra Bank. Retrieved from https://www.nrb.org.np/contents/uploads/2024/03/Annual-Report-2022-23-English.pdf

Pant. (2020, March 3). *What you need to know about ethical hackers in Nepal*. Retrieved from The Kathmandu Post: https://kathmandupost.com/science-technology/2020/03/03/what-you-need-to-know-about-ethical-hackers-in-nepal

Prime, D. R. (2024, September 11). *Positivism Philosophy in Research and Its Role in Research Paradigms.* Retrieved from Best Dissertation Writers: https://bestdissertationwriter.com/positivism-philosophy-in-research/

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 93-114. doi:https://doi.org/10.1080/00223980.1975.9915803

Sheik, A. T. (2023). *Customers' Perception of Cybersecurity Risks in E-commerce Websites.* Venice, Italy: ResearchGate.

Singh , N., & Lien, L. (2023). *Ethical Hacking as a Risk Management Tool in Organizations.* Nord University. Retrieved from https://nordopen.nord.no/nord-xmlui/bitstream/handle/11250/3093522/SinghLien.pdf?sequence=1&isAllowed=y

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, 355-374. doi:https://doi.org/10.2307/1882010

Swaen, B., & George, T. (2022). *What Is a Conceptual Framework? | Tips & Examples.* Scribbr

Tolossa, D. N. (2023). Importance of cybersecurity awareness training for employees in business. *Vidya- A Journal of Gujarat University*, 104-107. doi:http://dx.doi.org/10.47413/vidya.v2i2.206

Yadav, P. K. (2024, March 18). *Safeguarding cyberspace: Nepal's journey in addressing cybersecurity challenges*. Retrieved from The Annapurna Express: https://theannapurnaexpress.com/story/47977/

ANNEX-1 QUESTIONNAIRE

CUSTOMERS' KNOWLEDGE ON ETHICAL HACKING PRACTICES AND ITS INFLUENCE ON BRAND IMAGE (A Case of Machhapuchchhre Bank Limited)

Researcher:

Shleshma Shrestha
Bachelor of Business Information Systems (BBIS)
Little Angels' College of Management, Kathmandu University

Purpose of the Study:

This study aims to assess customers' knowledge of ethical hacking practices and how it influences their trust, loyalty, and perception of Machhapuchchhre Bank's brand image.

Participation Information:

- Your participation is voluntary.
- You may choose to withdraw at any time without any penalty.
- The survey will take about 5–7 minutes to complete.
- Your responses will be kept confidential and used solely for academic research purposes.
- No personal identifiers will be collected.

By ticking the box below, you confirm that:

1. You have read and understood the purpose of this study.
2. You voluntarily agree to take part in the survey.
3. You are at least 18 years of age.

☐ I agree to participate in this survey.

Basic Information

1. Age: _____
2. Gender:
   ☐ Male
   ☐ Female
   ☐ Other
   ☐ Prefer not to say
3. Education Level:
   ☐ High School
   ☐ Bachelor's Degree
   ☐ Master's Degree and above
4. Occupation/Industry:
   ☐ Student
   ☐ Banking/Finance
   ☐ IT/Cybersecurity
   ☐ Healthcare
   ☐ Education
   ☐ Government
   ☐ Retail
   ☐ Other
5. How often do you use Machhapuchhre Bank's digital/online banking services?
   ☐ Rarely (less than once a month)
   ☐ Occasionally (1–3 times per month)
   ☐ Frequently (1–6 times per week)
   ☐ Daily (at least once per day)

Customers' Knowledge of Ethical Hacking Practices in Machhapuchchhre Bank

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware that Machhapuchchhre Bank invests in ethical hacking to test its digital security systems.					
I know that ethical hackers at Machhapuchchhre Bank help identify and fix potential security flaws.					
I have seen or heard that Machhapuchchhre Bank publicly communicates its use of ethical hacking.					
I understand how ethical hacking helps Machhapuchchhre Bank protect customer data.					
I am aware of specific cybersecurity initiatives taken by Machhapuchchhre Bank.					

Trust in Machhapuchchhre Bank

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I trust Machhapuchchhre Bank to protect my sensitive financial information.					
I trust Machhapuchchhre Bank to act in my best interests.					
I trust Machhapuchchhre Bank to provide secure banking services.					
I feel confident using Machhapuchchhre Bank's banking services.					
I have confidence in Machhapuchchhre Bank's ability to manage my financial needs.					

Loyalty to Machhapuchchhre Bank

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am likely to continue using Machhapuchchhre Bank.					
I prefer Machhapuchchhre Bank over other banks.					
I recommend Machhapuchchhre Bank to others.					
I would choose Machhapuchchhre Bank even if other banks offer similar services.					
I feel more committed to Machhapuchchhre Bank.					

Credibility of Machhapuchchhre Bank

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I believe Machhapuchchhre Bank is a professional organization.					
Machhapuchchhre Bank is a competent institution.					
I trust Machhapuchchhre Bank to deliver high-quality services.					
I view Machhapuchchhre Bank as a reliable organization.					
Machhapuchchhre Bank demonstrates expertise in banking services.					

Brand Image of Machhapuchchhre Bank

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have a positive overall image of Machhapuchchhre Bank.					
I view Machhapuchchhre Bank as an innovative organization.					
Machhapuchchhre Bank stands out among other banks in Nepal.					
I believe Machhapuchchhre Bank is a leader in the banking industry.					
Machhapuchchhre Bank has a strong reputation.					

ANNEX-2 WORKPLAN

Research Activities	Dec 2024	Jan 2025	Feb 2025	Mar 2025	Apr 2025	May 2025	Jun 2025	Jul 2025	Aug 2025
Topic finalization, literature review									
Conceptual framework									
Research proposal, supervisor feedback									
Questionnaire, pilot test									
Data collection									
Data cleaning, preliminary analysis									
Main data analysis									
Results interpretation									
Final proofreading, submission									

APPROVAL LETTER

ANNEX-3 LOG BOOK

Little Angels College of Management

Affiliated to Kathmandu University

CIS Research/Project Log Book

Name: Shleshma Shrestha

Stream: BBIS Year: 4th Year

Reg. No: A030676-21

Title of the Project: Customers' Knowledge of Ethical Hacking Practices and Its Influence on Brand Image

Supervisor: Bibhav Adhikari

Detail

S.N.	Date	Contact Person	Purpose	Feedback	Signature	Duration (Hours)
1	05-12-2024	Bibhav Adhikari	Topic finalization and literature review discussion	Suggested refining research title and focusing on ethical hacking awareness among customers		3
2	15-01-2025	Bibhav Adhikari	Discussion on conceptual framework	Recommended removing mediating variables, keeping it simple		3
3	05-02-2025	Bibhav Adhikari	Review of alignment with objectives	Approved framework with minor adjustments		4

4	15-02-2025	Bibhav Adhikari	Research proposal review	Suggested to restructure objectives and improve research questions		3
5	05-03-2025	Bibhav Adhikari	Final research proposal checks before submission	Approved proposal after addressing feedback		3
6	10-03-2025	Namita Subedi	Questionnaire validation (content validity)	Suggested keeping the questions apt and understandable.		4
7	12-03-2025	Kumar Lohala	Questionnaire validation (technical terms and measurement)	Confirmed scale reliability; suggested adding one question for brand image		3
8	15-03-2025	Ishan Datta Mishra	Questionnaire validation (content and relevance)	Suggested minor rewording for better respondent understanding		3
9	05-04-2025	Bibhav Adhikari	Pilot test feedback discussion	Approved after good reliability indication		4
10	10-05-2025	Bibhav Adhikari	Mid-data collection progress meeting	Advised to increase outreach for higher response rate		4
11	15-06-2025	Bibhav Adhikari	Data cleaning and preliminary analysis review	Suggested handling missing data before analysis		3
12	05-07-2025	Bibhav Adhikari	Main data analysis guidance	Provided steps for data analysis using SPSS		5

13	20-07-2025	Bibhav Adhikari	Results interpretation discussion	Suggested linking findings back to literature and research objectives		3
14	05-08-2025	Bibhav Adhikari	Final proofreading and submission preparation	Approved final document after formatting corrections		3

Approved by: Bibhav Adhikari, Research Coordinator

Signature: