Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

ANALYZING CYBER ATTACKS AS A BASIS FOR PROACTIVE CYBERSECURITY AWARENESS PROGRAM

Mike Centenno M. Caban
Apayao State College
mikecentenno@gmail.com

Abstract
This study analyzed cyber-attacks as a basis for developing a proactive cybersecurity awareness program in the Province of Apayao. Specifically, it examined the types of cyber-attacks experienced by respondents, perceived causes and vulnerabilities, level of cybersecurity awareness, perceived impacts, and existing preventive measures. A descriptive-developmental research design was employed, utilizing a structured survey questionnaire complemented by qualitative interviews. Respondents included college students, employees, business owners, and individual internet users. Findings revealed that common cyber-attacks experienced include phishing, account hacking, and online scams. Weak passwords, clicking suspicious links, and lack of cybersecurity knowledge were identified as primary vulnerabilities. While respondents demonstrated a high level of cybersecurity awareness, particularly in basic practices such as password management and two-factor authentication, their participation in formal training programs was low. The perceived impacts of cyber-attacks were significant, including data loss, reduced trust in digital systems, and emotional stress. Preventive measures were moderately practiced, indicating a gap between knowledge and actual behavior. The study concludes that although respondents are digitally active and aware, there exists a new knowledge-practice gap and continued exposure to cyber threats due to limited structured training and behavioral reinforcement. It is therefore recommended that a proactive, localized cybersecurity awareness program be implemented, focusing on continuous training, policy enforcement, and behavior-based interventions to strengthen cyber resilience among internet users in Apayao

Keywords: *Cybersecurity awareness, cyber-attacks, vulnerability, preventive measures, knowledge-practice gap, awareness program, cyber resilience*

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Introduction

In the 21st century, cyberspace evolved into a critical infrastructure that underpins global economic growth, governance, education, communication and social interaction. The rapid expansion of digital technologies, cloud computing, e-commerce, and social media platforms has transformed how individuals and institutions operate. However, this increased connectivity has simultaneously expanded the global threat landscape. Cybersecurity attacks are now recognized as one of the most significant global risks, with impacts that extend beyond financial loss to include reputational damage, operational disruption, and erosion of public trust (World Economic Forum, 2024).

Globally, cyber-attacks have grown in both frequency and sophistication. Threat actors employ tactics such as ransomware, phishing, denial-of-service (DoS), malware infections, and identity theft to exploit system vulnerabilities and human error (Symantec, 2023). The 2022 Verizon Data Breach Investigation Report revealed 82% of breaches involved a human element, highlighting how social engineering and credential misuse remain primary attack vectors. Furthermore, IBM (2023) reported that the global average cost of a data breach reached USD 4.45 million, emphasizing the economic magnitude of cyber incidents. These trends demonstrate that cybersecurity is not merely a technical issue but a socio-technical challenge requiring awareness, behavioral change, and institutional preparedness.

The Asia-Pacific region has experienced a corresponding rise in cyber threats as digital transformation accelerates across developing and emerging economies. According to Interpol (2022), cybercrime activities including online fraud, phishing, and ransomware have significantly increased in the region. Similarly, the European Union Agency for Cybersecurity (ENISA 2024) noted that cyber-attacks increasingly target public institutions, educational systems, and small enterprises, sectors that often lack advanced cybersecurity defenses. As internet penetration expands, both urban and rural communities become potential targets.

In the Philippine context, digitalization has rapidly progressed through e-governance, online banking, digital payments, and virtual learning environments. While these innovations enhance efficiency and accessibility, they also increase exposure to cyber risks. The Department of Information and Communication technology (DICT, 2022) reported a surge in cybercrime cases nationwide, particularly online scams, phishing, and identity theft. The Philippine National Police Anti-Cybercrime Group (PNP-ACG, 2023) intensified its advocacy campaigns such as #CyberSafePH to promote digital safety awareness. Despite these efforts, implementation gaps persist, particularly in geographically isolated and disadvantaged areas where ICT infrastructure and cybersecurity training remain limited.

Within the Cordillera Administrative Region, province such as Apayao face unique challenges. Apayao is one of the country's geographically isolated and economically developing provinces. As internet connectivity expands and government transactions,

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

academic activities, and business operations shift online, local institutions and individuals increasingly rely on digital platforms. However, limited ICT infrastructure, scarce cybersecurity expertise, and insufficient awareness programs may heighten vulnerability to cyber threats. A DICT bulletin (2022) reported phishing emails targeting Local Government Units (LGUs) in Northern Luzon and Cordillera Administrative Region, underscoring the urgency of strengthening local cyber defenses.

Recent local experiences from 2022 to 2025 further highlight the vulnerability of the province. Employees of national line agencies, state colleges, and private institutions in Apayao have reported incidents of fraud, cyberbullying, phishing, and hacking. Several cases involved Facebook account compromises where attackers impersonated victims to solicit money from friends, send malicious QR codes and links, and issue threatening messages. These incidents demonstrate how cyber-attacks exploit both technological weaknesses and human trust.

College students, employees, business owners, and private individual internet users represent particularly vulnerable sectors within the province. College students frequently use social media and online platforms for academic research and communication, often without comprehensive cybersecurity knowledge. A study by Dela Cruz (2021) in Northern Luzon found that although social media usage among students was high, only 45% demonstrated adequate knowledge of safe online practices such as two-factor authentication. Employees increasingly rely on digital communication tools for official transactions, while business owners use online banking and digital payment systems to manage financial operations. Each group faces distinct exposure risks that require targeted intervention.

Awareness is widely regarded as the first line of defense against cyber threats. The SANS Institute (2022) reported that organizations implementing structured cybersecurity awareness programs significantly reduced successful phishing attempts. Preventive strategies such as multi-factor authentication, regular software updates, strong password management, and critical evaluation of suspicious links are effective only when users understand and consistently apply them. Thus, cybersecurity resilience depends not only on technical safeguards but also on informed and vigilant users.

Given the global escalation of cyber threats, the increasing digitalization of Philippine society, and the emerging local incidents within Apayao, there is a pressing need to examine the province's cybersecurity landscape. While national policies and campaigns provide a broad framework, localized research is essential to understand the specific patterns, vulnerabilities, and awareness gaps affecting Apayao's students, employees, business owners, and individual internet users.

Therefore, this study seeks to analyze the nature and prevalence of cyber-attacks experienced in the Province of Apayao and to use these findings as a foundation for developing a proactive cybersecurity awareness program tailored to the local context. By

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

situating global and national cybersecurity concerns within the realities of Apayao, this research aims to contribute to a more resilient, informed, and secure digital environment in the province.

Statement of the Problem

This study seeks to analyze cyber-attacks to severe as the basis for a proactive cyber security awareness program. Specifically, it seeks to answer the following questions:

1. What are the cyber-attacks experienced by the respondents?
2. What are the perceived causes or vulnerabilities leading to cyber-attacks?
3. What is the level of awareness of respondents regarding cyber security practices and preventive measures?
4. What is the perceived impact of cyber-attacks on productivity, security, and trust in digital systems?
5. What measures are currently being implemented to prevent or respond to cyber-attacks?
6. What proactive cyber security awareness program can be based on the findings of the study?

THEORETICAL FRAMEWORK

This study is anchored on three interrelated theories that explain cyber-attacks, user vulnerability, and the adoption of cybersecurity practices: the Routine Activity Theory, the Protection Motivation Theory, and the Technology Acceptance Model.

First, the Routine Activity Theory (Cohen & Felson, 1979) explain that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship. In the context of cybersecurity, motivated offenders include hackers and cybercriminals, suitable targets include individuals and organizations with weak security practices, and the absence of capable guardians refers to lack of cybersecurity awareness, weak passwords, and inadequate system protection.

Second, the Protection Motivation Theory (Rogers 1975; 1983) explains how individuals are motivated to adopt protective behaviors based on their perception of threat severity, vulnerability, response effectiveness, and self-efficacy. In cybersecurity, individuals are more likely to implement protective measures when they understand the risks and believe they can effectively prevent cyber-attacks.

Third, the Technology Acceptance Model (Davis, 1989) explains that individuals are more likely to adopt new technologies or practices when they perceive them as useful and easy to use. In the context of cybersecurity awareness programs, users will adopt safe practices such as multi-factor authentication, secure password management, and phishing detection if they perceive these practices as beneficial and manageable.

Together, these theories provide a comprehensive framework for understanding cyber-attacks and cybersecurity behavior. and support the development of a proactive

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindunaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

cybersecurity awareness program tailored to the needs of internet users in the Province of Apayao.

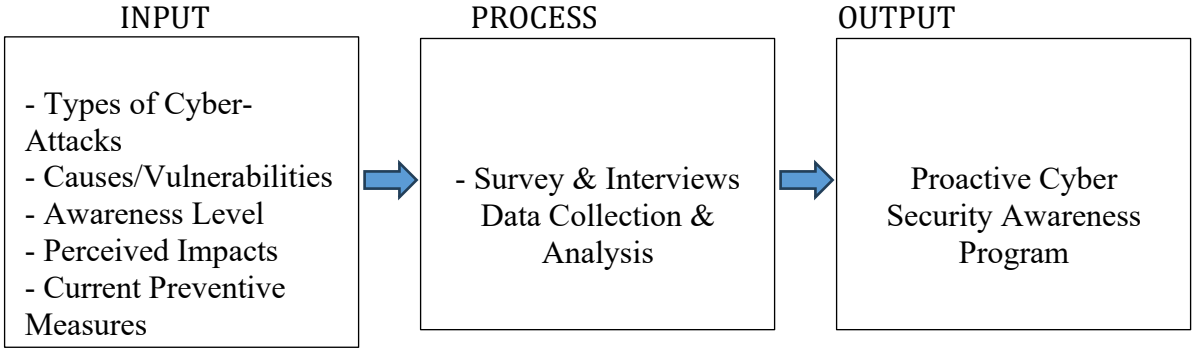

Figure 1: Research Paradigm

The study adopts the Input-Process-Output (IPO) research paradigm as a systematic framework for analyzing cyber threats and developing a proactive cybersecurity awareness program. The input component consists of key variables describing the respondents' cybersecurity condition including experienced cyber-attacks, perceived causes and vulnerability, level of cybersecurity awareness, impacts on productivity and trust in digital system, and existing preventive practices. The process involves the collection and analysis of data through surveys and interviews to identify prevalent threats, awareness gaps, and behavioral patterns. The output is the development of a context-specific cybersecurity awareness program designed to address identified vulnerabilities, enhance knowledge, and promote safe online practices among diverse user groups. Overall, the IPO framework ensures a logical progression from empirical data to evidence-based intervention, resulting in a localized and practical program responsive to the cybersecurity needs of Apayao.

RESEARCH DESIGN & METHODOLOGY

This study used a descriptive developmental research design to analyze cyber-attacks experienced by internet users in the Province of Apayao and to develop a proactive cybersecurity awareness program based on the findings. The descriptive component focused on identifying and examining the types of cyber-attacks experienced by respondents, their perceived vulnerabilities, level of cybersecurity awareness, perceived impacts of cyber incidents, and existing preventive measures. This phase provided a comprehensive understanding of the cybersecurity situation within the province. The developmental component utilized the analyzed data to design a proactive cybersecurity awareness program tailored to the needs of college students, employees, business owners, and individual internet users in Apayao. The proposed program is evidence-based and grounded on the results of both quantitative and qualitive data. The study primarily used a quantitative

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

approach through a structured survey questionnaire, supported by qualitative interviews to gather deeper insights that strengthened the program development phase.

The study was conducted in the Province of Apayao, located in the Cordillera Administrative Region of the Philippines. Apayao is a geographically isolated and developing province where digital technologies are increasingly used in education, business, government services, and communication. With the growing reliance on internet connectivity, the province has become more exposed to cyber threats, making it an appropriate locale for examining cyber-attacks and cybersecurity awareness among internet users.

The respondents of the study consisted of active internet users in the Province of Apayao, including college students, employees from national line agencies, local government units, and private institutions, business owners, and individual internet users. These respondents were selected because they regularly use the internet for academic, professional, business, and personal purpose, making them vulnerable to cyber-attacks. To qualify for inclusion in the study, respondents were required to be at least 18 years old, residing, studying, or working in Apayao, and actively using internet or social media. These criteria ensured that participants had relevant experiences and knowledge related to cybersecurity.

Convenience sampling was used as a method of selecting respondents who are readily available at a given place and time, making data collection faster and easier for the researcher. In the context of this study conducted in the Province of Apayao, this approach involves gathering data from participants who are easily accessible, such as students within the school, employees in the nearby offices, business owners within the locality, and private individuals who can be conveniently contacted. To ensure more meaningful and relevant results, the study specifically included respondents who have experienced cyber threats. These participants were identified through snowball sampling, wherein initial respondents referred other individuals who had similar experiences with cyber-attacks. This combined approach allowed the researcher to efficiently collect data while ensuring that the participants possessed firsthand knowledge and experiences necessary for a deeper analysis of cybersecurity issues.

In effect there were one hundred twenty-two (122) respondents involved in the study which involved professionals, students, business owners and private individuals.

The primary instrument used in this study is a structured survey questionnaire developed by the researcher based on related literature and cybersecurity frameworks. The questionnaire consisted of six parts. The first part gathered the demographic profile of the respondents. The second part identified the types of cyber-attacks experienced. The third part examined the causes and vulnerabilities associated with cyber-attacks. The fourth part measured the respondents' level of cybersecurity awareness. The fifth part assessed the perceived impacts of cyber-attacks. The sixth part identified the preventive measures

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindunaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

practiced by the respondents. A four-point Likert scale was used to measure awareness, vulnerabilities, and impacts. The instrument was validated by experts in cybersecurity such as the personnel of Department of Information and Communication Technology (DICT) in Cordillera Region. The members of the thesis panel were also involved in the content validity.

To ensure the reliability of the research instrument, a Cronbach's Alpha test was conducted across all variables included in the study. This statistical measure assesses the internal consistency of the items within each scale, determining how closely related they are as a group. The instrument consists of four subscales Causes or Vulnerabilities Leading to Cyber Attacks, Level of Cyber Security Awareness, Perceived Impacts of Cyber Attacks, and Existing Preventive Measures each containing 10 items, with a total of 40 items for the overall scale.

The results revealed that all subscales obtained Cronbach's Alpha values ranging from 0.90 to 0.94, which are interpreted as **excellent** levels of internal consistency. Specifically, the "Causes or Vulnerabilities Leading to Cyber Attacks" achieved the highest reliability (α = 0.94), followed by "Perceived Impacts of Cyber Attacks" (α = 0.93), "Level of Cyber Security Awareness" (α = 0.91), and "Existing Preventive Measures" (α = 0.90). The overall scale also demonstrated excellent reliability (α = 0.90), indicating that the entire instrument is highly consistent and dependable.

These findings suggested that the items within each variable are well-correlated and effectively measure their intended constructs, making the instrument suitable for data collection and further analysis.

Variable/Scale	Number of Items	Cronbach's Alpha	Interpretation/ Internal Consistency
Causes or Vulnerabilities Leading to Cyber Attacks	10	0.94	Excellent
Level of Cyber Security Awareness	10	0.91	Excellent
Perceived Impacts of Cyber Attacks	10	0.93	Excellent
Existing Preventive Measures	10	0.90	Excellent
Overall Scale	**40**	**0.90**	**Excellent**

Reliability Test Results Using Cronbach's Alpha

In addition to the survey questionnaire, a semi-structured interview was used to gather deeper insights from selected respondents. The interview questions focused on respondents' personal experiences with cyber-attacks, perceived vulnerabilities, behavioral

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

responses, institutional support, cybersecurity training needs, and recommendations for the development of the cybersecurity awareness program.

Before conducting the study, the researcher secured permission from relevant institutions, offices, and authorities in the Province of Apayao. Ethical clearance was obtained from the appropriate ethics committee. The researcher distributed the survey questionnaires personally and through secure online platforms. The respondents were provided with informed consent forms explaining the purpose of the study, the voluntary nature of participation, and their rights as participants. After collecting the survey responses, selected respondents were invited to participate in interviews to provide deeper insights. The interviews were conducted face-to-face and through online communication platforms, depending on availability and convenience. With the respondents' permission, interview responses were recorded and transcribed for analysis.

Frequency and percentage were used to identify the types of cyber-attacks experienced by respondents and the preventive measures they practiced. Weighted mean was used to determine the level of cybersecurity awareness, perceived vulnerabilities, and perceived impacts of cyber-attacks. Standard deviation was used to measure the variability of the responses. Ranking was used to identify the most common cyber-attacks and vulnerabilities. For the qualitative data, thematic analysis was used to identify common themes, patterns, and insights that contributed to the development of the proactive cybersecurity awareness program.

To interpret the results, the following scale and verbal descriptions was used:
For Causes, Impact, and Preventive Measures:
3.26 – 4.00= Strongly Agree/ Always
2.51 – 3.25= Agree / Often
1.76 – 2.50= Disagree / Rarely
1.00 – 1.75= Strongly Disagree / Never

For Level of Awareness:
3.26 – 4.00= Very High Awareness
2.51 – 3.25= High Awareness
1.76 – 2.50= Low Awareness
1.00 – 1.75= Very Low Awareness

Ethical Considerations

This study adhered to ethical standards in conducting research involving human participants. Respondents were provided with informed consent forms explaining the purpose of the study, and their participation will be voluntary. Confidentiality and

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

anonymity were strictly maintained, and no personal identifying information was disclosed. Codes were used instead of names to protect respondents' identities. The study complied with the Data Privacy Act of 2012 (Republic Act 10173), and all collected data was securely stored and accessible only to the researcher. Respondents were informed of their right to withdraw from the study at any time without penalty. The researcher ensure that the study does not cause harm or discomfort to participants. Permission from relevant institutions and ethical clearance from appropriate authorities will be obtained prior to data collection.

RESULTS AND DISCUSSION

This portion discusses the findings based on the collected data. The tables are arranged sequentially to address the questions outlined in the problem statement.

Table 1. Types of Cyber Attacks Experienced by the respondents

Cyber Attacks Experienced	Frequency	Rank
Online Fraud/Scams	30	1
Malware Attack	24	2
Cyberbullying	19	3
Social Media Hacking	18	4
Phishing	6	5
Data Breach	5	6
Website Defacement	4	7
Ransomware	3	8
Denial of Service Attack	2	9.5
Social Engineering	2	9.5
Insider Threat	1	11.5
Verbal Bullying	1	11.5

Table 1 reflects the types of cyber-attacks experienced by the respondents. The most frequently reported are online fraud/scams, malware attacks, cyberbullying, and social media hacking. Lower-ranked threats include ransomware, denial-of-service attacks, and insider threats.

According to the Verizon Data Breach Investigations Report (2024), the majority of cyber incidents are financially motivated, with approximately 90% of breaches driven by financial gain, highlighting the prevalence of scams and fraud-related attacks . This supports the result that online fraud and scams are among the most dominant threats experienced by respondents.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Moreover, phishing and social engineering attacks often used in scams and account hacking remain among the most widespread cyber threats. Studies show that social engineering techniques, including phishing and pretexting, account for a significant portion of cyber incidents, with phishing being a primary method for stealing credentials and gaining unauthorized access This explains the high occurrence of social media hacking and scam-related incidents.

In addition, malware continues to be a major cybersecurity concern worldwide. Reports indicate that malware and ransomware are consistently among the top threats affecting individuals and organizations, often used for financial extortion or data theft.

The presence of cyberbullying in the findings also reflects the growing social dimension of cyber risks, particularly among younger and highly connected populations. Cyber threats are no longer purely technical but also involve social interactions and online behavior, making users vulnerable to harassment and exploitation in digital platforms.

On the other hand, the lower occurrence of highly technical attacks such as denial-of-service (DoS) and insider threats is also supported by literature. These types of attacks are typically more complex and often target organizations or critical infrastructures rather than individual users, making them less commonly experienced by the general population.

Furthermore, studies emphasize that human factors play a critical role in cyber incidents, with about 68% of breaches involving human error or social engineering. This explains why common, user-targeted attacks such as scams, phishing, and social media hacking are more prevalent than technical attacks.

Causes Leading to Cyber Attacks

Table 2. Perceived causes leading to Cyber Attacks

Statement	Mean	Description
1. Weak or reused passwords increase vulnerability to attacks.	3.40	Strongly Agree
2. Lack of knowledge about online safety contributes to risks.	3.33	Strongly Agree
3. Outdated software and devices expose users to threats.	3.03	Agree
4. Clicking unknown links or attachments makes users prone to malware.	3.35	Strongly Agree
5. Ignoring software or system updates causes vulnerabilities.	3.03	Agree
6. Using unsecured Wi-Fi networks increases exposure to hackers.	3.03	Agree
7. Weak security policies in offices/schools make systems at risk.	3.08	Agree

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

8. Limited awareness of social engineering tactics makes people victims.	3.26	Strongly Agree
9. Oversharing personal data on social media increases risks.	3.30	Strongly Agree
10. Lack of training on cyber threats makes users vulnerable.	3.31	Strongly Agree
OVERALL MEAN	**3.21**	**Agree**

Table 2 presents the causes leading to cyber-attacks. The overall mean of 3.21 revealed that participants generally agree that multiple behavioral and technical factors contribute to cyber vulnerability. The highest-rated causes include weak passwords (3.40), clicking suspicious links (3.35), and lack of online safety knowledge (3.33).

These findings emphasize that human error and poor digital habits are the primary drivers of cyber risk. Technical issues such as outdated systems are also recognized but are slightly less emphasized, indicating that improving user behavior and awareness could significantly reduce vulnerability.

These results align with existing research that emphasizes the significant role of human behavior in cybersecurity risk. Hadlington (2017), highlight that psychological and behavioral trait, such as impulsivity and poor security attitudes, significantly predict risky cybersecurity behaviors, including falling for phishing attacks and unsafe online actions. Similarly, Tan (2025), notes that human factors, such as cognitive biases and susceptibility to social engineering, are critical contributors to cyber incidents alongside technical weaknesses. Weak passwords and poor credential management remain among the most persistent vulnerabilities, with compromised credentials frequently exploited by attackers (MKS Uddin, FZ Rozony, M.Kamruzzaman, 2024).

Furthermore, behavioral studies on phishing and social engineering underscore that lack of awareness and inadequate training increase susceptibility to clicking malicious links and other risky behaviors (Pujari ,2024). While technical factors such as outdated systems and misconfigurations also contribute to cyber risk, research suggests that improving user behavior, awareness, and security practices can substantially reduce vulnerability (MKS Uddin, FZ Rozony, M.Kamruzzaman, 2024).

Collectively, these studies support the view that addressing human factors through education, training, and improved digital hygiene is a crucial strategy for mitigating cyber-attacks.

Table 3. Level of Cyber Security Awareness on cyber security practices and preventive measures

Awareness of Cyber Security Practices	Mean	Description
1. Creating strong and unique passwords	3.56	Very High Awareness

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindumaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

2. Using two-factor authentication	3.48	Very High Awareness
3. Identifying phishing emails and suspicious links	3.37	Very High Awareness
4. Regularly updating software and applications	3.36	Very High Awareness
5. Backing up important files and data	3.48	Very High Awareness
6. Using antivirus and firewall protection	3.43	Very High Awareness
7. Setting social media privacy and security controls	3.56	Very High Awareness
8. Recognizing online scams and fraudulent sites	3.42	Very High Awareness
9. Reporting cybercrime to proper authorities	3.32	Very High Awareness
10. Attending or participating in cyber security awareness programs	3.20	High Awareness
OVERALL MEAN	**3.60**	**Very High Awareness**

The high overall mean of 3.60 for cybersecurity awareness indicates that participants generally have a strong understanding of basic cybersecurity practices, such as password security, privacy settings, and two-factor authentication. This aligns with research conducted by Alqahtani, 2022 and Nasrullah, 2025, which stated that frequent internet users often develop practical cybersecurity knowledge through regular online interactions that contributes to higher awareness levels. Studies have also highlighted that awareness of protective measures, including strong passwords and privacy controls, is a critical component of overall cybersecurity competency (Nasrullah, 2025 & Taherdoost, 2025). However, the relatively lower engagement in formal cybersecurity awareness programs with a mean of 3.20 reflects a common challenge: while individuals may acquire knowledge informally, structured training is often underutilized despite its importance in reinforcing secure behaviors and addressing knowledge gaps (Taherdoost, 2025 ; Nasir , 2023). These findings suggest that while participants are knowledgeable about basic cybersecurity practices, institutionalized training programs remain essential to ensure comprehensive and consistent cybersecurity awareness (Charalambous,2025; Shillair,2022; Armas, 2025; Abrahams,2024; Ussher-Eke D,2024).

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindumaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Table 4. Perceived Impacts of Cyber Attacks on productivity, security, and trust in digital systems

Statement	Mean	Description
1. Cyber-attacks reduce productivity in work or studies.	3.35	Strongly Agree
2. Cyber-attacks cause financial loss to individuals or organizations.	3.47	Strongly Agree
3. Cyber-attacks damage trust in digital systems and transactions.	3.54	Strongly Agree
4. Cyber-attacks result in emotional stress or anxiety.	3.52	Strongly Agree
5. Cyber-attacks disrupt government services.	3.33	Strongly Agree
6. Cyber-attacks interrupt business operations.	3.38	Strongly Agree
7. Cyber-attacks harm the reputation of institutions.	3.48	Strongly Agree
8. Cyber-attacks create fear of using digital platforms.	3.41	Strongly Agree
9. Cyber-attacks lead to loss of important data.	3.66	Strongly Agree
10. Cyber-attacks affect community trust in online services.	3.65	Strongly Agree
OVERALL MEAN	**3.50**	**Strongly Agree**

Table 4 shows the perceived impact of cyber-attacks. The strong agreement among participants regarding the negative consequences of cyber-attacks (overall mean = 3.50), particularly for data loss (3.66), reduced trust in digital systems (3.54), and emotional stress (3.52), aligns with extensive research documenting the multidimensional impacts of cyber incidents. Academic literature categorizes cyber-attack consequences into technological, economic, reputational, and psychological domains, noting that cyber incidents often result in significant data compromise, operational disruption, and financial harm (Agrafiotis, 2018; Adekoya,2025). For example, systematic reviews of cyber security impacts highlight that data loss and erosion of trust are common outcomes following breaches, contributing to reputational damage and diminished stakeholder confidence in digital platforms (Agrafiotis, 2018; Perera 2022). Beyond measurable technical and financial effects, cyber-attacks also produce emotional and psychological consequences for victims, with research showing that individuals report emotional reactions such as frustration, anxiety, and distress in the aftermath of cybersecurity breaches (Budimir, Fontaine Huijts , Haans, Loukas, Roesch, 2021; , Moskwa, 2024). Psychological studies further indicate that cyber-attacks can lead to ongoing worry, negative feelings, and reduced trust in technology, underscoring the broad psychosocial toll of these events (Budimir, 2021; Bada, Nurse, 2020). These findings demonstrate that participants' serious perception of risk and awareness of cyber-attack impacts reflects broader scholarly evidence that cyber incidents have far-reaching effects on data integrity, trust, operational continuity, and emotional well-being.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindumaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Table 5. Preventive Measures to prevent cyber-attacks

Preventive Measure	Mean	Description
1. Using strong and unique passwords	3.69	Always
2. Installing and updating antivirus/firewall	3.35	Always
3. Attending seminars or training on cyber security	2.83	Always
4. Conducting regular data backups	3.24	Often
5. Avoiding suspicious links or attachments	3.60	Always
6. Reporting cyber incidents to proper authorities	3.06	Often
7. Using two-factor authentication	3.53	Always
8. Educating others (family/colleagues) about cyber safety	3.48	Always
9. Using licensed and updated software	3.36	Always
10. Monitoring devices and accounts for unusual activities	3.51	Always
OVERALL MEAN	**3.50**	**Always**

Table 5 shows the preventive measures to prevent cyber-attacks. The overall mean of 3.50 signified that participants often practice cybersecurity measures, particularly using strong passwords (3.69), avoiding suspicious links (3.60), and enabling two-factor authentication (3.53). However, the low engagement in formal cybersecurity training programs (mean = 2.83) reflects a persistent issue highlighted in prior research: while users may possess awareness, structured training participation remains limited (3,4).

The findings suggest that preventive cybersecurity behaviors are largely individual and experienced based rather than guided by structured programs. This aligns with existing literature indicating that users often develop security practices informally through repeated digital exposure rather than formal training interventions (Nugraha, 2024). While participants demonstrate awareness and apply basic protection, limited engagement in structured training programs may restrict their ability to respond effectively to complex and evolving cyber threats. Research shows that cybersecurity awareness programs frequently encounter challenges such as low participation and limited institutional support, which reduces their effectiveness in influencing behavior (Haney et, al., 2022) . Furthermore, the observed pattern of high awareness but only moderated practice reflects the widely documented knowledge-practice gap in cybersecurity. Empirical studies confirm that although knowledge influences behavior, it does not always translate into consistent secure practices (Setiawan et al., 2026). This gap is further supported by research emphasizing that cybersecurity is not only a knowledge issue but also a behavioral one that requires continuous reinforcement (Akter et al., 2022). Additionally, structured and theory-based cybersecurity training programs have been shown to significantly improve both knowledge

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

and behavioral intentions, highlighting their importance in strengthening cyber resilience (Ifinedo, 2012)

The following program may be proposed as a proactive cybersecurity awareness program as a result of the findings of the study:

Proactive Cybersecurity Awareness Program for the Province of Apayao

I. Program Overview

The program aims to enhance cybersecurity awareness, reduce vulnerabilities, and promote safe online behaviors among internet users in Apayao, including college students, government employees, business owners, and individual users.

II. Program Objectives

1. Increase awareness of common cyber threats and preventive measures.
2. Improve adoption of protective cybersecurity practices.
3. Bridge the knowledge-practice gap through structured training and behavioral interventions.
4. Strengthen community and institutional cybersecurity culture.

III. Key Components

1. Awareness Campaigns

- Develop educational content addressing common local cyber-attacks such as phishing, malware, social media hacking, and online scams.
- Use videos, infographics, flyers, and storytelling incorporating local experiences.
- Employ social media platforms, local radio, community events, schools, and government offices for message delivery.
- Special messaging streams customized for students, employees, entrepreneurs, and individual residents.

2. Structured Training and Workshops

A. Regular Interactive Sessions: Conduct quarterly cybersecurity workshops focusing on:

- Password management and multi-factor authentication.
- Identifying phishing and fraudulent websites.
- Safe use of social media and privacy controls.
- Updating software and utilizing antivirus/firewall protections.

B. Sector-Specific Modules: Develop specialized modules for:

- Academic institutions.
- Local government staff.
- Small and medium enterprises.

C. Delivery Modes: In-person and online.

3. Behavioral Change Initiatives

a. Promote Safe Habits

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

- Campaigns on best practices such as verifying links before clicking, reporting suspicious activities, and regular system updates.

b. Peer Lead Program
- Train select respondents as *Cybersecurity Advocates* to spread awareness in their communities and networks.

c. Incentive Mechanisms
- Recognize individuals and groups demonstrating exemplary cybersecurity practices to motivate continued engagement.

4. Institutional Partnerships and Policy Support

a. Collaborate with LGUs and Institutions
- Integrate cybersecurity awareness into local government programs, school curricula, and workplace policies.

b. Incident Reporting and Response
- Facilitate clear and accessible reporting channels linking users to the Philippine National Police Anti-Cybercrime Group and DICT for immediate assistance.

c. Policy Development
- Support local institutions in formulating and enforcing cybersecurity protocols and guidelines.

5. Resource Development and Support

a. Cybersecurity Toolkit: Provide easy-to-use guides, checklists, and FAQs in local dialects.
b. Helpdesk and Support Services: Establish a local cybersecurity helpdesk for technical assistance, available via hotlines and online platforms.
c. Continuous Learning Portal: Develop an online portal with resources, updates on emerging threats, and self-paced training materials.

6. Monitoring and Evaluation

- Regular Assessments: Conduct periodic surveys and focus group discussions to evaluate program effectiveness and identify emerging needs.
- Feedback Integration: Utilize data-driven insights to refine content, delivery strategies, and intervention focus.
- Reporting: Publish summary reports to stakeholders to encourage transparency and ongoing support.

IV. Implementation Timeline

Phase	Activities	Timeframe
Phase 1: Preparation	Curriculum development, partnerships, resource creation	Months 1–3
Phase 2: Launch	Awareness campaigns & initial training sessions	Months 4-5

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Phase	Activities	Timeframe
Phase 3: Expansion	Additional workshops, behavioral initiatives, toolkit distribution	Months 6-8
Phase 4: Review & Improve	Monitoring, data collection, program adjustments	Months 9-10
Phase 5: Sustainability	Institutionalizing program within local structures	Month 11-12

V. Expected Outcomes

a. Elevated cybersecurity awareness scores among participants.
b. Increased adoption of multi-factor authentication, strong passwords, and safe internet practices.
c. Reduced incidence of successful phishing and social engineering attacks reported locally.
d. Active community participation in cybersecurity education and prompt incident reporting.
e. Strengthened cybersecurity policies and culture within local institutions.

Summary of Findings

This study analyzed the nature, causes, and impacts of cyber-attacks experienced by internet users in the Province of Apayao to develop a proactive cybersecurity awareness program tailored to the local context. Findings revealed that the most common cyber threats faced by respondents include online fraud/scams, malware attacks, cyberbullying, and social media hacking, with financial gain as a primary motivator. Human factors such as weak or reused passwords, clicking unknown links, and lack of cybersecurity knowledge were identified as major vulnerabilities. While respondents demonstrated a generally high level of cybersecurity awareness, gaps remained in formal training and consistent application of protective measures. The impacts of cyber-attacks were found to be significant, affecting productivity, financial security, emotional wellbeing, and trust in digital systems. These results highlight the critical need for localized, structured, and behavioral-focused cybersecurity education and interventions to strengthen resilience among students, employees, business owners, and individual users in Apayao.

Conclusions

Based on the findings of the study, the following conclusions are drawn:

The respondents predominantly experienced online fraud/scams, malware attacks, cyberbullying, social media hacking, and phishing. These prevalent cyber-attacks highlight the significant and varied digital threats faced by students, employees, business owners, and individual users.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

The main vulnerabilities contributing to cyber-attacks include lack of cybersecurity knowledge and awareness, weak password practices, susceptibility to social engineering tactics, and limited ICT infrastructure and local cybersecurity expertise. Human factors, especially inadequate understanding of safe online behaviors, remain critical weak points.

The overall level of cybersecurity awareness among respondents is moderate, with many recognizing basic protective measures but inconsistent application in real life. This gap between knowledge and practice underscores the need for more focused awareness and training programs to enhance protective behaviors.

Cyber-attacks adversely affect respondents by causing financial losses, emotional distress, disruption of academic and work activities, and erosion of trust in digital platforms and online services. These impacts highlight the socio-technical consequences cyber threats impose on individuals and institutions in Apayao.

Current preventive efforts include basic personal safeguards such as password usage and occasional software updates. However, there is limited formal cybersecurity training, inadequate institutional policies, and insufficient community-wide awareness initiatives, resulting in persistent vulnerabilities.

A multifaceted proactive cybersecurity awareness program is recommended featuring awareness campaigns tailored to local threats, structured training/workshops, behavioral change initiatives, institutional partnerships, resource development, and continual monitoring and evaluation. This program aims to bridge knowledge gaps, enhance protective practices, and foster a resilient cybersecurity culture among Apayao's internet users.

Recommendations

1. The Local Government Units (LGUs) should take the lead in institutionalizing cybersecurity awareness by incorporating awareness programs into local government policies and workplace regulations. This includes formalizing cybersecurity protocols and establishing clear incident reporting and response channels linking to national agencies like PNP-ACG and DICT.
2. Higher Education Institution (HEIs) and Basic Education Schools (BES) should develop and deliver regular, sector-specific cybersecurity training and workshops targeting students, faculty, and staff. These sessions should focus on practical skills such as password management, phishing identification, social media safety, and software updates.
3. Business owners and entrepreneurs must actively participate in cybersecurity awareness initiatives, adopt recommended protective practices, and collaborate with LGUs and institutions to strengthen digital security within the local economy.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

4. The DICT Provincial office should identify and train motivated individuals as Cybersecurity Advocates who will serve as peer educators within their communities, spreading awareness and reinforcing safe online behaviors through peer-led programs.
5. The DICT Provincial office should create accessible resources such as cybersecurity toolkits in local dialects, helpdesks, and online learning portals that provide technical assistance and continuous education to empower users across all sectors.
6. The DICT Provincial office should strengthen collaboration with the Philippine National Police Anti-Cybercrime Group and the Department of Information and Communications Technology for incident handling, expertise sharing, and enforcement of cybersecurity measures.
7. Conduct regular assessments through surveys and focus groups to evaluate program effectiveness, integrate feedback, and adjust strategies accordingly to sustain and enhance cybersecurity culture in Apayao.

References

African Cyberthreat Assessment Report 2022. Lyon: INTERPOL; 2022.

Akter, S., Uddin, M.R., Sajib,S.,Lee,W.J.T..,& Michael, K.(2022).Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research.https://doi.org/10.1007/s10479-022-04844-8.

Alqahtani MA. Factors Affecting Cybersecurity Awareness among University Students. Appl Sci. 2022;12(5):2589.

Cohen LE, Felson M. Social change and crime rate trends: A routine activity approach. *Am Sociol Rev*. 1979;44(4):588–608.

Cost of a Data Breach Report 2023. Armonk (NY): IBM Corporation; 2023.

Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q*. 1989;13(3):319–40.

De la Cruz LM, Burdeos JA, Dela Cruz EN, Parreño MN, Verdadero MF, Dacles PJ. *Use of self-deprecating humor in social media and its relationship with academic stress among BS Psychology students in a private higher education institution* (Doctoral dissertation, Central Philippine University).

Department of Information and Communications Technology. *National Cybersecurity Plan 2022*. Manila: DICT; 2022.

European Union Agency for Cybersecurity. *ENISA Threat Landscape 2024*. Athens: ENISA; 2024.

Haney, J., Jacobs, J., & Furman, S. M. (2022). *Federal cybersecurity awareness programs: A mixed methods research study*. National Institute of Standards and Technology (NIST).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Internet Security Threat Report 2023. Mountain View (CA): Symantec; 2023.

Nasir S. Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions. InProceedings of the Cyber Secure Nigeria Conference 2023 Jul (Vol. 1, pp. 9-22).

Nasrullah NF. Systematic Analysis of Cyber Security Awareness Among Internet Users: Behavior, Risks, and Prevention Efforts. 2025.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindduraresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026

Nugraha, V. P. (2024). *Cybersecurity awareness through training: A systematic literature review based on the KAB model*. Quanta Research.

Philippine National Police Anti-Cybercrime Group. *Annual Cybercrime Report 2023*. Camp Crame, Quezon City: PNP-ACG; 2023.

Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: Cacioppo JT, Petty RE, editors. *Social psychophysiology*. New York: Guilford Press; 1983. p. 153–76.

Security Awareness Report 2022. Bethesda (MD): SANS Institute; 2022.

Setiawan, Y., Abdullah, A. G., & Salam, H. (2026). *Bridging the knowledge–behavior gap: A PLS-SEM analysis of cybersecurity awareness*.

Taherdoost H. Towards an innovative model for cybersecurity awareness training. Information. 2024 Aug 23;15(9):512.

World Economic Forum. Global Risks Report 2024. 19th ed. Geneva: World Economic Forum; 2024.

Journal of Social Transformation, Governance and Public Administration (JSTGPA)
Volume 2 Issue 2-2026
e-ISSN 3116-2916
https://jstgc.mindumaresearch.com/journal/index
Submitted 3-1-2026: | Accepted: 5-5-2026 | Published 6-30-2026