ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

CYBER HYGIENE PRACTICES OF GOVERNMENT EMPLOYEES IN IFUGAO

Sean Rey Zuñega Bongayon
Philippine College of Criminology, Manila, Philippines

Article DOI: https://doi.org/10.36713/epra24727
DOI No: 10.36713/epra24727

ABSTRACT

In the era of rapid digitalization, government agencies are increasingly vulnerable to cyber threats that compromise institutional integrity and public trust. This study examined the cyber hygiene practices of government employees in Ifugao, Philippines, focusing on their knowledge, practices, challenges, and support needs. Employing an explanatory sequential mixed-methods design, quantitative data were collected from 150 respondents across provincial and national agencies using structured questionnaires, followed by qualitative interviews to deepen the interpretation of trends. Findings revealed a discrepancy between knowledge and practice: while employees demonstrated awareness of cyber hygiene measures such as password security, software updates, email safety, and data backup, their actual implementation was inconsistent. National agency employees generally exhibited higher compliance compared to provincial counterparts. Qualitative insights highlighted recurring barriers, including inadequate training, limited resources, and weak institutional support. Respondents expressed the need for structured awareness campaigns, regular training, and policy reinforcement to sustain cyber hygiene practices. The study concludes that although government employees possess fundamental knowledge of cybersecurity, gaps in behavior and organizational readiness persist, undermining resilience against cyber threats. The integration of both quantitative and qualitative results underscores the necessity of capacity-building, institutionalized support systems, and context-specific interventions. These findings contribute to the national discourse on grassroots-level cyber resilience and align with the objectives of the Philippine National Cybersecurity Plan 2023–2028 to strengthen secure and digitally competent governance.

KEYWORDS: *Cyber Hygiene, Cybersecurity, Knowledge-practice Gap, Government Employees, Cyber Resilience*

INTRODUCTION

Cyber hygiene practices have become increasingly important in the digital age where technology underpins government operations and public service delivery. As organizations rely on digital systems to store and manage sensitive information, vulnerabilities to threats such as hacking, phishing, and data breaches have significantly increased. The Philippine National Cybersecurity Plan 2022 defines cybersecurity as the "collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies" that protect the cyber environment and organizational assets. This highlights the importance of cultivating safe digital habits among individuals, especially government employees who manage and access critical information systems. In the Philippines, efforts toward digital transformation are guided by national frameworks such as the Philippine National Cybersecurity Plan and the Philippine National Security Policy 2023–2028. These initiatives emphasize building a resilient and secure digital government. However, implementation at the local government level remains uneven. The Commission on Audit (COA) and the Department of Information and Communications Technology (DICT) have reported that many local government units (LGUs) still lack cybersecurity programs, trained personnel, and structured policies. Consequently, cyber hygiene practices among government employees are often informal and inconsistent, exposing offices to potential data breaches and cyberattacks. Locally, the province of Ifugao has also faced cybersecurity concerns. A notable case involved the hacking of the official Facebook page of Ifugao State University (IFSU), which led to reputational damage and highlighted weaknesses in password management and digital security protocols. Many government offices in the province lack dedicated IT personnel, standardized response mechanisms, and regular cybersecurity awareness training. These conditions make the local government particularly vulnerable to cyber threats. Given these challenges, this study - aims to assess the level of cyber hygiene among local government employees, identify areas for improvement, and recommend strategies to enhance cybersecurity readiness. By focusing on employee behavior and awareness, the study contributes to strengthening the overall cybersecurity posture of the local government. Ultimately, the research seeks to support national and global goals of building a cyber-resilient government from the grassroots level.

LITERATURE REVIEW

Cyber hygiene is recognized internationally as a critical component of organizational cybersecurity. According to Gaurav et al. (2022), cyber hygiene encompasses practices such as password management, regular software updates, and employee training on security protocols. Karayel and Akbıyık (2024) also emphasized that organizations adopting strong cyber hygiene practices are better prepared to defend against sophisticated cyber attacks. Regarding specific cyber hygiene practices, Nyachiro et al. (2024) highlighted that effective email practices significantly

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

reduce vulnerability to phishing attacks, while Mtukushe et al. (2023) found that timely reporting of suspicious email activity is crucial for mitigating cyberattacks. Frischmann and Johnson (2023) pointed out that weak password policies are systemic issues requiring both individual awareness and organizational support. Pfleeger et al. (2015) demonstrated that establishing clear reporting lines reduces breach escalation. Human factors, organizational culture, and cognitive abilities also influence cyber hygiene. Howell et al. (2024) explained that individuals with higher reflective decision-making skills are more likely to follow cybersecurity recommendations. Alkhaledi and Hawamdeh (2023) observed that financial and time constraints, lack of managerial support, and cultural barriers limit adoption of cybersecurity measures in healthcare. Malatji (2022) indicated that weak passwords, inadequate access controls, and insufficient updates present significant obstacles for operational technology networks. In the Philippines, cyber hygiene and cybersecurity remain reactive. Castillo (2023) noted that the "I Love You" virus incident revealed the consequences of delayed legislation. Bautista (2023) reported that the "Comeleak" data breach showed vulnerabilities in government websites and databases. Averia et al. (2022) highlighted that a general lack of investment in cybersecurity increases exposure to cyber risks.

However, studies on cyber hygiene practices show gaps between knowledge and implementation. Amante and Cacho (2020) found that 78% of university employees were aware of basic cybersecurity concepts, but only 45% implemented them regularly. Marcelo et al. (2022) reported that teaching staff were knowledgeable about cyber threats but lacked formal cybersecurity training, with only 32% attending workshops. Reyes and Garcia (2021) observed that 67% of users did not regularly update their mobile devices, 45% used public Wi-Fi without protection, and only 23% had mobile security applications installed.

Compliance with national policies also varies. Tan and Lopez (2022) found gaps in local government unit implementation of the National Cybersecurity Plan 2022, while Mendoza et al. (2022) reported that large corporations had high compliance with the Data Privacy Act (85%), but small and medium enterprises showed only 40% compliance. International research also indicates that organizational interventions enhance cyber hygiene. Sulaiman et al. (2022) emphasized that training can improve device security, while Dimitrov (2024) recommended institutionalizing reporting drills to reinforce compliance. Oliveira et al. (2023) found that cybersecurity knowledge varies by context, with Polish students showing higher knowledge than Portuguese counterparts. Tran et al. (2024) demonstrated that government social media projects and organizational policy compliance indirectly increased defensive cybersecurity actions among public servants in Vietnam. These studies indicate that while awareness of cyber hygiene is growing both internationally and locally, challenges remain in consistent implementation, enforcement, and organizational readiness. This highlights the need for structured policies, regular training, and technological support to strengthen cybersecurity practices among government employees and other stakeholders.

Theoretical/Conceptual Framework/Paradigm of the Study

The study is anchored in the Knowledge, Attitude, and Practice Model, which examines cyber hygiene among government employees by looking at three interconnected aspects. Knowledge refers to employees' understanding of cyber threats and relevant policies. Attitude concerns their perceptions, motivation, and willingness to follow security measures. Practice focuses on how they implement these measures, such as using secure passwords and updating software regularly. This framework helps identify the gap between awareness and consistent secure behavior, allowing the development of targeted interventions to improve compliance. The study aligns this model with Philippine legal and strategic mandates, including the 1987 Constitution, the National Cybersecurity Plan 2023-2028, Republic Act No. 10173 or the Data Privacy Act, and Republic Act No. 10175 or the Cybercrime Prevention Act. By linking employee behavior to these laws and policies, the research provides a foundation for developing effective programs that enhance national cyber resilience and ensure government institutions protect citizen data and secure information systems.

SIGNIFICANCE OF THE STUDY

The study holds significant importance to its key stakeholders, ultimately contributing to a more resilient and secure digital government environment. Government Employees are the primary beneficiaries, gaining deeper knowledge and empowerment through the study's findings, which will lead to more targeted, interactive training programs that better equip them to defend themselves and their agencies against cyber threats. For Policy and Decision Makers, the research provides essential empirical data to inform and influence the establishment of sound cybersecurity policies, allowing them to efficiently manage resources, prioritize security activities, and cultivate a strong security-conscious culture within government institutions. Government and Regulatory Bodies can also utilize the findings to build upon or improve existing cybersecurity legislation and standards, enabling them to develop regulations that address the specific, localized challenges uncovered by the research, thereby creating a more secure national digital environment. Lastly, the research contributes to the academic community by adding to the body of knowledge for Researchers, focusing on cybersecurity, human factors, and organizational behavior, serving as a foundational reference for further academic exploration into the behavioral effects of cybersecurity practices.

OBJECTIVES OF THE STUDY

The study generally aims to evaluate the overall cybersecurity posture within the government sector of Ifugao by investigating the respondents' level of cyber hygiene practices, attitudes towards cyber hygiene, knowledge regarding methods of operation related to various cybercrimes, and the incident response level concerning different cyber threats. It specifically aims:

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

- To determine the level of cyber hygiene knowledge among government employees in terms of Email Safety, Password Security, Software and System updates, Data Backup, Safe Internet Usage, Device Security, and Reporting of Suspicious Activities.
- To compare the level of cyber hygiene knowledge among government employees in terms of the identified variables according to provincial LGU and national agencies.
- To determine the level of cyber hygiene practices being implemented by government employees in terms of Email Safety, Password Security, Software and System updates, Data Backup, Safe Internet Usage, Device Security, and Reporting of Suspicious Activities.
- To differentiate the level of cyber hygiene practices being implemented by government employees according to their agency type.
- To investigate the challenges that influence the consistent practice of cyber hygiene.
- To determine the support or resources that would help government employees maintain consistent cyber hygiene practices.
- To propose an evidence-based program to enhance cyber hygiene awareness and practices among government employees.

METHODOLOGY

This presents the methods and procedures done throughout the study including the research design, participants, data collection, analysis, and ethical considerations.

Research Design

The researcher utilized the explanatory sequential mixed methods design to holistically capture the depth and breadth of the research problem. This design involves first collecting and analyzing quantitative data to identify general patterns, followed by qualitative data collection and analysis to further explain and elaborate on the quantitative findings. Through this approach, the researcher aims to gain a comprehensive understanding of the phenomena under investigation by integrating numerical trends with rich, contextual insights. During the initial phase, quantitative data will be collected and evaluated to discern patterns, trends, and linkages pertinent to the study issue. This preliminary research will offer a comprehensive overview of the topic and inform the identification of critical areas necessitating further investigation. During the second phase, qualitative data will be gathered to elucidate and refine the quantitative findings. This phase will entail collecting comprehensive insights from participants to comprehend the rationale behind the observed trends and statistical results. By organizing the study sequentially, the researcher seeks to augment the interpretation of quantitative results with qualitative insights, fostering a more thorough and nuanced comprehension of the research issue.

Research Method

The researcher used the mixed-method research design, a comprehensive approach that integrates both qualitative and quantitative research methods within a single study. This approach is designed to provide a thorough and comprehensive understanding of the research problem. It allows for the collection, analysis, and interpretation of numerical data and textual or narrative information, thereby offering a more holistic view of the phenomenon under investigation. By combining these two methodologies, the study can leverage the strengths of both approaches while minimizing their respective limitations. The quantitative aspect will provide measurable and statistically analyzable data, ensuring objectivity and generalizability. However, it's the qualitative component that truly enriches the research, allowing for an in-depth exploration of participants' experiences, perceptions, and insights, and adding a layer of depth and context to the numerical findings.

Population of the Study

The participants of the study were one hundred fifty (150) government employees of the Province of Ifugao who are the main workforce for their respective offices. The inclusion criteria require that the government employees must be directly engaged in the main functioning of their respective provincial government unit, department, or agency. This refers to their active involvement in the essential operations, programs, and services that fulfill the mandate of their office such as planning, implementation, decision-making, supervision, policy execution, and delivery of frontline services rather than purely administrative or auxiliary support roles. Seventy five (75) participants were taken from the Provincial Government of Ifugao and another seventy-five (75) participants from the various National Department/Agencies located at the Province.

Data Gathering Tools

The researcher used a self-administered survey questionnaire along with semi-structured interview guides, both developed and validated by experts for clarity, relevance, comprehensiveness, and alignment with the study objectives. The questionnaire was based on Supreme Court Order No. 150-2023, which provides guidelines for improving cybersecurity, protecting sensitive data, and reducing cyber risks. To ensure reliability, the questionnaire was pilot-tested with 30 respondents similar to the study participants, yielding a Cronbach's Alpha of 0.938 which indicated an excellent internal consistency as described by George and Mallery (2019). The instrument had three parts: first is an introduction with privacy assurance and permission letter, second is the survey items assessing knowledge, attitudes, and practices in cyber hygiene, and third is a semi-structured interview guide to collect qualitative insights on challenges and support needed for maintaining consistent cyber hygiene practices.

Data Gathering Procedures

The data gathering procedures followed a strict process after all necessary permissions were secured. First, the research instrument was submitted to the research adviser for content approval, and then to a panel of experts for validation to ensure its relevance and accuracy. Once approved, the researcher secured

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

official permission letters from the Governor of the Provincial Local Government of Ifugao and the heads of all relevant National Departments and Agencies in the province. With institutional permissions granted, and after receiving Ethics Review Committee approval, the researcher coordinated with the government employees to schedule the instrument administration. Before participation, all respondents received a letter of informed consent clearly explaining their rights, emphasizing voluntary participation, confidentiality, and anonymity. The data was then collected sequentially, beginning with administering the survey questionnaire followed by the conduct of semi-structured interviews. After which all responses were collected, tallied, and analyzed using appropriate statistical methods.

Treatment of Data

The researcher used both quantitative and qualitative methods to analyze the data. To determine the level of cyber hygiene knowledge and practices, descriptive statistics such as weighted means, frequencies, and percentages were used to interpret the results. Additionally, to compare their cyber hygiene knowledge and practices, the Mann-Whitney U test was applied, identifying statistically significant differences. Qualitative data from semi-structured interviews were analyzed using thematic analysis to uncover challenges affecting consistent cyber hygiene, as well as the support or resources needed to maintain these practices.

Ethical Considerations

The researcher adhered to strict ethical standards throughout the study. The participants experienced no damage of any kind as a result of their participation in this study. Prior to the study, complete consent was secured from both the subjects and the various government bodies involved. The voluntary participation of respondents in the research has been highly valued. Furthermore, respondents had the option to withdraw from the study at any point. The data was handled with a sufficient level of confidentiality. Misleading information and biased depiction of main data findings was avoided. And, maintaining the greatest level of objectivity in debate and analysis throughout the research is also taken into account. Furthermore, any relationships, funding sources, and potential conflicts of interest were disclosed. Finally, all communication with this dissertation was done with honesty and transparency.

RESULTS AND DISCUSSION

This details the findings of the study corresponding to the research objectives. The discussion integrates the quantitative results, supported by statistical analysis with the qualitative data gathered through interviews and focus group discussions.

Level of Cyber Hygiene Knowledge among Government Employees

Table 1 reveals the cyber hygiene knowledge among government employees from R-LGU and R-NA across seven key domains: Email Safety, Password Security, Software and System Updates, Data Backup, Safe Internet Usage, Device Security, and Reporting of Suspicious Activities. The data reveals a consistent knowledge gap between the two groups. Respondents from National Agencies (R-NA) rated themselves as "Knowledgeable" in all areas except Device Security, where they were only "Slightly Knowledgeable". On the other hand, R-LGU respondents consistently rated themselves as "Slightly Knowledgeable" across all categories, including Device Security. This finding suggests a significant difference in training where National Agency (R-NA) employees generally receive more robust and structured cybersecurity awareness training, possibly due to better resource allocation, stricter compliance protocols, or centralized IT governance. In contrast, the uniformly low scores of R-LGU respondents indicate limited exposure to or participation in formal cyber hygiene education, leaving them more vulnerable to common threats such as phishing, weak password practices, and unsafe browsing.

According to the Asia Pacific Cybersecurity Dashboard by the World Bank and Global Cybersecurity Index by ITU, decentralization without adequate local capacity building is a significant risk factor in national cybersecurity. Furthermore, literature by Schneider (2025) emphasizes that improving cyber hygiene knowledge across all levels of government is essential for creating a resilient digital ecosystem, particularly as threats become more sophisticated and pervasive.

Table 1. Summary of the Level of Cyber Hygiene Knowledge among Government Employees

Indicators	R-LGU	R-NA	Overall
Email Safety	2 – SK	3 – K	2.5 – K
Password Security	2 – SK	3 – K	2.5 – K
Software and System Updates	2 – SK	3 – K	2.5 – K
Data Backup	2 – SK	3 – K	2.5 – K
Safe Internet Usage	2 – SK	3 – K	2.5 – K
Device Security	2 – SK	2 – SK	2 – SK
Reporting of Suspicious Activities	2 – SK	3 – K	2.5 – K
Overall	**2 – SK**	**3 – K**	**2.5 – K**

Difference in the Level of Cyber Hygiene Knowledge among Government Employees Between the Two Groups of Respondents

Table 2 presents the results of the Mann-Whitney U test examining the differences in cyber hygiene knowledge between R-LGU and R-NA across seven key domains. In all indicators, email safety, password security, software and system updates, data backup, safe internet usage, device security, and reporting of suspicious activities. The differences were found to be statistically significant. The qualitative data support these gaps as

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

many LGU respondents expressed complacency, saying, "I'm not that important to be hacked, kaya di ko masyado iniisip" (R112) and "Cyber is not real life, so parang wala namang effect sa totoong buhay" (R034). Others admitted difficulty applying basic practices, such as "Kung walang notification, hindi ako nag-a-update" (R018). These statements reflect low risk perception, forgetfulness, and reliance on external prompts, which align with the consistently lower knowledge scores of LGU employees. This indicates a consistent and substantial gap in cyber hygiene knowledge between the two groups, with National Agency employees demonstrating significantly higher levels of knowledge than their LGU counterparts. The smallest coefficient with Email Safety having 297 and other low values such as Software Updates with 228, and Reporting with 354 suggest particularly pronounced gaps in those areas, implying that local employees are at greater risk of falling for phishing scams, failing to update systems, or mismanaging cybersecurity incidents. These findings echo concerns from Abrahams et al. (2024), who emphasize that awareness and education are the cornerstones of effective cybersecurity. When gaps persist across institutional levels, the overall resilience of government infrastructure is compromised. The World Bank's 2021 report on digital government transformation further highlights the risk of digital inequality in public service capacity where national agencies are often prioritized in digital skills training, leaving LGUs behind. The particularly large difference in password security with 1659 and device security with 1992 reinforces the idea that basic cybersecurity practices are underdeveloped at the local level. These findings are concerning given the increasing decentralization of data management and frontline digital services in local governance.

Table 2. Difference in the Level of Cyber Hygiene Knowledge among Government Employees Between the Two Groups of Respondents

Indicators	Coefficient	p-value	Decision	Remarks
Email Safety	297	<0.001	Reject H_0	Significant
Password Security	1659	<0.001	Reject H_0	Significant
Software and System Updates	228	<0.001	Reject H_0	Significant
Data Backup	362	<0.001	Reject H_0	Significant
Safe Internet Usage	424	<0.001	Reject H_0	Significant
Device Security	1992	<0.001	Reject H_0	Significant
Reporting of Suspicious Activities	354	<0.001	Reject H_0	Significant

Level of Cyber Hygiene Practices being Implemented by Government Employees

Table 3 presents the comparative summary of cyber hygiene practices implemented by government employees from R-LGU and R-NA across key cybersecurity dimensions. The overall median rating between the groups shows a significant difference. R-NA respondents practice cyber hygiene "Often", whereas R-LGU respondents do so only "Sometimes" which indicates a critical gap in implementation. In particular, R-LGU employees consistently report lower frequencies of safe practices in email safety, password security, system updates, data backup, and incident reporting. This trend aligns with prior findings in cybersecurity literature which suggest that limited training, inadequate infrastructure, and lack of institutional support are prevalent challenges in decentralized or local institutions (Atisa et al., 2021). Notably, the only area where both groups report similar behavior is device security, with a median of 3 and described as Often. This leads to a shared awareness of protecting physical and digital access to devices. These findings emphasize the need for targeted interventions in LGUs, including regular capacity-building programs, policy reinforcement, and practical simulations to improve day-to-day cybersecurity behaviors. As supported by studies of Mersinas et al., (2023) and Reittinger et al. (2025), habitual cybersecurity practices are most effectively reinforced through continuous learning, behavioral nudges, and leadership support.

Table 3. Summary of the Level of Cyber Hygiene Practices being Implemented by Government Employees

Indicators	R-LGU	R-NA	Overall
Email Safety	2 – S	3 – O	2.5 – O
Password Security	2 – S	3 – O	2.5 – O
Software and System Updates	2 – S	3 – O	2.5 – O
Data Backup	2 – S	3 – O	2.5 – O
Safe Internet Usage	2 – S	3 – O	2.5 – O
Device Security	3 – O	3 – O	3 – O
Reporting of Suspicious Activities	2 – S	3 – O	2.5 – O
Overall	**2 – S**	**3 – O**	**2.5 – O**

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Difference in the Level of Cyber Hygiene Practices being Implemented by Government Employees Between the Two Groups of Respondents

Table 4 presents the results on the difference in the level of cyber hygiene practices between government employees from R-LGU and those from R-NA. The results show statistically significant differences in most domains such as email safety, software and system updates, data backup, safe internet usage, and reporting of suspicious activities, all favoring R-NA employees. These findings suggest that national agency employees consistently engage in more frequent and proactive cybersecurity practices than their LGU counterparts. This is consistent with research by Ajayi et al. (2025), which highlights that centrally governed institutions often have stronger cybersecurity protocols, more structured training, and better access to digital infrastructure. Interestingly, password security ($p = 0.062$) was not statistically significant at the 0.05 level, implying a shared gap across both groups in implementing strong password practices. This could reflect a broader systemic issue in user behavior, where password hygiene is commonly overlooked or misunderstood as mentioned by Frischmann and Johnson (2023). Device security yielded a significant result ($p = 0.023$), though with a weaker level of significance compared to other categories. This indicates that while there is some difference in how device security practices are implemented, the gap is narrower because device locking and antivirus usage are more ingrained and easier to adopt across all levels of government. These results suggest an uneven implementation of cyber hygiene across government levels, with LGUs requiring targeted interventions and capacity-building efforts. Key recommendations include localized training programs, mandatory policy rollouts, and improved access to cybersecurity tools. The findings also support a growing consensus in cybersecurity literature that training alone is insufficient without supportive infrastructure and clear institutional enforcement mechanisms (Friday et al., 2022; Varma, 2020). Therefore, the statistical differences emphasize the need for policy harmonization and resource allocation to ensure that all government employees, regardless of agency level, maintain robust and consistent cyber hygiene practices.

Table 4. Difference in the Level of Cyber Hygiene Practices being Implemented by Government Employees Between the Two Groups of Respondents

Indicators	Coefficient	p-value	Decision	Remarks
Email Safety	255	<0.001	Reject H_0	Significant
Password Security	2429	0.062	Accept H_0	Not Significant
Software and System Updates	422	<0.001	Reject H_0	Significant
Data Backup	306	<0.001	Reject H_0	Significant
Safe Internet Usage	282	<0.001	Reject H_0	Significant
Device Security	2319	0.023	Reject H_0	Significant
Reporting of Suspicious Activities	316	<0.001	Reject H_0	Significant

Challenges that Influence the Practice of Cyber Hygiene

The study identified key challenges faced by government employees in maintaining consistent cyber hygiene. These challenges include low risk perception and complacency, forgetfulness and inconsistent cybersecurity hygiene habits, and technical limitations and usability barriers.

Government employees face several challenges in maintaining effective cyber hygiene. A major issue is low risk perception and complacency, where many employees believe they are unlikely targets of cyberattacks, leading to negligence in preventive measures such as updating passwords, avoiding phishing links, or installing security software. This attitude increases vulnerability, particularly within government networks, emphasizing the need for awareness strategies that make cyber threats personally relevant.

Another significant challenge is forgetfulness and inconsistent cybersecurity hygiene habits. Even when employees are aware of proper practices, failure to integrate them into daily routines results in lapses such as neglected password updates or unmonitored suspicious activities. Behavioral interventions, including automated reminders, cue-based prompts, and habit-forming training, are necessary to reinforce consistent cyber hygiene practices.

Lastly, technical limitations and usability barriers further hinder secure behavior. Complex devices, confusing interfaces, and performance-related frustrations often discourage adherence to security measures. Addressing these issues requires user-friendly systems, accessible training, default security settings, and automated tools that make cybersecurity practical, effective, and easily incorporated into daily workflows.

Support or Resources that Help Maintain Consistent Cyber Hygiene Practices

The respondents' answers show their reliance on colleagues, family members, and peers for cybersecurity support highlights the powerful role of informal social networks in shaping digital behavior. In the absence of structured institutional support or formal training, many government employees turn to those within their immediate social environment for assistance in carrying out even the most basic cyber hygiene practices. This includes tasks such as installing or updating antivirus software, setting up security features like fingerprint locks or two-factor authentication, and addressing device issues related to malware or suspicious activity. Respondents shared sentiments like: "My

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

friends at work help me", "My daughter helps me with my phone", and "My cousins help me clean viruses on my desktop". This form of knowledge transfer is reflective of Bandura's (1986) Social Learning Theory, which suggests that learning occurs within a social context and is facilitated through observation, imitation, and modeling. Overall, peer and family assistance plays a role in support to maintaining the respondents' consistent cyber hygiene practices.

Cyber Hygiene Training and Awareness Framework

Based on the results, the study revealed significant gaps in both cyber hygiene knowledge and practices among local government employees compared to their counterparts in national agencies. To address these challenges, the study proposes a Cyber Hygiene Training and Awareness Framework designed to enhance understanding in areas such as email safety, password management, software updates, data backup, safe internet use, device security, and incident reporting. The framework also emphasizes translating knowledge into consistent practices through hands-on training, habit-forming interventions, simulations, and automated reminders, while institutionalizing cyber hygiene within organizational culture by providing formal training, dedicated IT support, and designated "Cyber Hygiene Champions." Collectively, these measures aim to strengthen individual behavior and organizational capacity, fostering a more secure and resilient digital environment at the local government level.

CONCLUSION AND RECOMMENDATIONS

This presents the conclusions and recommendations drawn from the study.

Conclusion

Based on the findings of the study, it is revealed that there are significant differences in cyber hygiene knowledge and practices between National Agency (R-NA) and Local Government Unit (R-LGU) employees in Ifugao. R-NA employees demonstrated higher knowledge and more consistent implementation across key domains such as Email Safety, Password Security, Software and System Updates, Data Backup, Safe Internet Usage, Device Security, and Reporting of Suspicious Activities, while R-LGU employees were generally only slightly knowledgeable and practiced cyber hygiene inconsistently. Key challenges affecting compliance included low risk perception and complacency, forgetfulness and lack of habitual routines, and technical limitations or usability barriers. To cope with these gaps, employees often relied on peer and family assistance for guidance which highlights the role of informal social support in maintaining cyber hygiene. The proposed Cyber Hygiene Training and Awareness Framework can address these gaps through awareness, behavioral reinforcement, technical training, organizational support, and peer mentorship, strengthening overall cyber resilience.

Recommendations

Based on the findings, it is recommended that the Provincial Government of Ifugao institutionalize a Cyber Hygiene Knowledge Enhancement Program for LGU personnel, covering all seven domains with localized language, visuals, and relatable examples. Joint training initiatives with national agencies should be organized to bridge gaps in knowledge and skills, while behavior-focused interventions such as checklists, reminders, and scenario-based exercises should reinforce consistent cyber hygiene practices. LGUs should also provide institutional technical support, strengthen authentication policies, and implement monitoring and evaluation mechanisms to ensure accountability. Finally, the proposed Cyber Hygiene Training and Awareness Framework should be piloted, evaluated, and adjusted before full implementation to ensure effectiveness, sustainability, and long-term impact.

ACKNOWLEDGMENT

The researcher expresses sincere gratitude to all who contributed to the completion of this study. Special thanks to Dr. Marlyn P. Wacnag, advisor, for her guidance and insightful feedback; Atty. Joaquin R. Alva, Dean, and the esteemed panel members—Dr. Paolo Lumanlan, Dr. Ambrosio P. Detran, Dr. Imelda C. Runas, Dr. Ramil M. Las-Igan, and Atty. Theodore M. Timpac—for their support and valuable insights. The researcher is also grateful to the participants for their time and contributions, and to family members, especially Ermelinda Z. Bongayon, for their unwavering support. Finally, appreciation is extended to everyone who assisted directly in this research, whose support was essential to its success.

REFERENCES

1987 Constitution of the Republic of the Philippines. (1987).

1. *Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. Computer Science & IT Research Journal, 5(1), 100–119.*
2. *Alkhaledi, R., & Hawamdeh, S. (2023). Electronic Health Records and Cyber Hygiene: A Qualitative Study of the Awareness, Knowledge, and Experience of Physicians in Kuwait. Proceedings of the Association for Information Science and Technology, 60. https://doi.org/10.1002/pra2.765*
3. *Amante, J. A., & Cacho, R. M. (2020). Cybersecurity awareness and practices among university students in Metro Manila: A cross-sectional study. Philippine Journal of Information Technology, 15(2), 45–62.*
4. *Atisa, G., Zemrani, A., & Weiss, M. (2021). Decentralized governments: local empowerment and sustainable development challenges in Africa. Environment, Development and Sustainability, 23(3), 3349–3367.*
5. *Averia, A., Santos, M., & Delos Reyes, P. (2022). Cybersecurity posture in the Philippine public sector: Issues and challenges. Philippine Journal of Information Technology, 18(1), 55–70.*
6. *Bautista, D. (2023, December 2). Cybercrime Cases 400 Percent 2023 – PNP. Philstar. https://www.philstar.com/headlines/2023/12/02/2315819/cybercrime-cases-400-percent-2023-pnp*
7. *Castillo, C. (2023). Philippine Cybersecurity in Retrospect 2016-2021. NDCP. https://ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

8. *Department of Information and Communications Technology. (2022). National Cybersecurity Plan 2022–2028. Republic of the Philippines.*
9. *Dimitrov, K. (2024). Improving compliance and transparency in financial reporting: strategies for promoting accountability and integrity in corporate practices. In Сборник доклади от научна конференция „Знание, наука, иновации, технологии" (Vol. 1, No. 4, pp. 364–376).*
10. *Friday, S. C., Lawal, C. I., Ayodeji, D. C., & Sobowale, A. (2022). Strategic model for building institutional capacity in financial compliance and internal controls across fragile economies. International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), 944–954.*
11. *Frischmann, B. M., & Johnson, A. (2023). Common nonsense about password security and the expert-layperson knowledge gap. SSRN 4345028.*
12. *Gaurav, D., Ronak, G., & Kumbharana, C. K. (2022). The Reviewed Study of Various Techniques to Control and Defeat Cybercrime. International Journal of Scientific and Research Publications, 12(3). https://doi.org/10.29322/ijsrp.12.03.2022.p12305*
13. *Howell, C. J., Maimon, D., Muniz, C. N., Kamar, E., & Berenblum, T. (2024). Engaging in cyber hygiene: the role of thoughtful decision-making and informational interventions. CrimRxiv. https://doi.org/10.21428/cb6ab371.e828a968*
14. *Karayel, T., & Akbıyık, A. (2024). Managing Cyber Security Risks and Cyber Hygiene in Organizations. Advances in Electronic Commerce Series. https://doi.org/10.4018/979-8-3373-0086-3.ch010*
15. *Malatji, M. (2022). Industrial control systems cybersecurity: Back to basic cyber hygiene practices. 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–7. https://doi.org/10.1109/ICECET55527.2022.9872810*
16. *Marcelo, T., Diaz, F., & Almazan, L. (2022). Cybersecurity knowledge and training gap among academic staff (Unpublished master's thesis).*
17. *Mendoza, L., Reyes, F., & Torres, S. (2022). Compliance with the Data Privacy Act among Philippine businesses: A comparative study of large corporations and SMEs (Technical Report).*
18. *Mersinas, K., & Bada, M. (2023, July). Behavior change approaches for cyber security and the need for ethics. In The International Conference on Cybersecurity, Situational Awareness and Social Media (pp. 107–129). Singapore: Springer Nature Singapore.*
19. *Mtukushe, N., Onaolapo, A. K., Aluko, A., & Dorrell, D. G. (2023). Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems. Energies, 16(13), 5206.*
20. *Nyachiro, A., Hadullo, K., & Tole, K. (2024). Cybersecurity: A Case of Company and Organization Security. International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1307.1006*
21. *Oliveira, L., Chmielewski, A., Rutecka, P., Cicha, K., Rizun, M., Torres, N., & Pinto, P. (2023). Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus: A Case Study of Higher Education Institutions in Portugal and Poland. 2023 International Conference on Cyber Security Review (CSR), 168–173. https://doi.org/10.1109/csr57506.2023.10224910*
22. *Pfleeger, S. L., Caputo, D. D., & Rathi, N. (2015). Reporting is security: A framework for breach escalation (Conference paper).*
23. *Philippine National Security Policy 2023–2028. (2023). National Security Council, Republic of the Philippines.*
24. *Reittinger, T., Glas, M., Aminzada, S., & Pernul, G. (2025). Motivational factors in cybersecurity: linking theory to organizational practice. Information & Computer Security.*
25. *Republic Act No. 10173. (2012). Data Privacy Act of 2012. Republic of the Philippines.*
26. *Republic Act No. 10175. (2012). Cybercrime Prevention Act of 2012. Republic of the Philippines.*
27. *Reyes, V., & Garcia, H. (2021). Mobile device security practices and user behavior in the Philippines (Journal article).*
28. *Schneider, G. B. C. (2025). The Importance of Cybersecurity in Digital Government Implementations. COGNITIONIS Scientific Journal, 8(1), e585–e585.*
29. *Sulaiman, N. S., Fauzi, M. A., Hussain, S. T., & Harun, S. A. (2022). Cybersecurity behavior among government employees: The role of Protection Motivation Theory and responsibility in mitigating cyberattacks. Social Sciences, 11(9), 386. https://doi.org/10.3390/socsci11090386*
30. *Tan, R., & Lopez, J. (2022). Implementation challenges of the National Cybersecurity Plan 2022 in Philippine Local Government Units (Research Report).*
31. *Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. Journal of Asia Business Studies. https://doi.org/10.1108/jabs-01-2024-0058*
32. *Varma, Y. (2020). Governance-Driven ML Infrastructure: Ensuring Compliance in AI Model Training. International Journal of Emerging Research in Engineering and Technology, 1(1), 20–30.*