Volume 4/Issue 11/ November 2026
ISSN :2584-2706
International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.67317/IJMSRT26NOV029

Cyber Hygiene Practices: An Analytical Study among Catholic Higher Education Institution Employees

Mark Anthony Duque Madalipay, MIT; Dr. Joey M. Suba
University of the Assumption

Abstract
This study examined the cyber hygiene practices of employees at the University of the Assumption (UA), a Catholic higher education institution in the Philippines, focusing on cybersecurity awareness, security behaviors, training needs, and institutional support. Guided by Protection Motivation Theory, the study employed a mixed descriptive research design involving 120 teaching and non-teaching employees selected through purposive sampling. Data were gathered using a structured questionnaire assessing awareness of common cyber threats, cyber hygiene practices, and perceptions of cybersecurity training and institutional support. Descriptive statistics and cross-tabulation were used to analyze the quantitative data, while thematic analysis was applied to employee feedback. Results showed moderate awareness of ransomware, malware, secure websites, and emerging cyber threats, while phishing recognition was relatively stronger (M = 3.69, SD = 1.26). Employees demonstrated stronger cyber hygiene practices in password management, software updates, multifactor authentication, and avoidance of suspicious links. However, antivirus use, file backups, social media verification, and technical website-security checks were less consistently practiced. Employees reported moderate confidence in their cybersecurity knowledge (M = 2.67, SD = 1.19) but strongly supported cybersecurity training (M = 4.41, SD = 0.92) and short, interactive workshops (M = 4.42, SD = 0.83). Qualitative findings further identified the need for continuous training, clearer policies, improved IT support, practical cybersecurity guidance, and proactive behavioral change. The study concludes that strengthening cyber resilience requires an institution-wide approach integrating employee education, policy communication, incident-response mechanisms, and continuous evaluation. The findings provide a basis for developing targeted cybersecurity interventions and strengthening the institutional cybersecurity culture of UA.

Keywords: *Cyber Hygiene, Cybersecurity Awareness, Higher Education, Information Security, Protection Motivation Theory, Cybersecurity Training, Institutional Cybersecurity, Catholic Higher Education.*

I. INTRODUCTION

In today's digitally interconnected world, safeguarding institutional information systems hinges not only on technological defenses but equally on human behavior and awareness (Hadlington, 2017). As organizations increasingly depend on digital platforms for communication, administration, and record-keeping, employee cyber hygiene—routine practices such as using strong passwords, recognizing phishing, applying software updates, and avoiding unsecured networks—has become critical (Alowais et al., 2023).

Studies show that these behaviors are often overlooked areas of vulnerability. For example, Concepcion and Palaoag (2024) conducted an assessment at Quirino State University and found that while many academic employees displayed basic cybersecurity awareness, significant gaps remained regarding device threats and procedural adherence. They recommended regular training, clear policy frameworks, and technological solutions to foster a robust culture of cyber hygiene.

Similarly, Garba, Siraj, and Othman (2022) reported low cybersecurity awareness among university staff in Nigeria, which correlated with increased susceptibility to cyber threats like phishing . Ifinedo, Mengesha, and Longe (2019) also highlighted how inconsistent cybersecurity practices among Nigerian workers led to organizational vulnerabilities . Furthermore, Alowais et al. (2023) demonstrated that cyber hygiene practices differ significantly across cultures (U.S. vs. Saudi Arabia), illustrating the crucial role of context and institutional support.

Despite this global evidence, cyber hygiene behaviors within the context of Catholic higher education institutions—particularly in the Philippines—remain under-researched. At the University of the Assumption (UA), employees across academic and administrative units regularly access sensitive data but may lack standardized practices to prevent human-error-driven security breaches.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV029

Accordingly, this study investigates the current state of cyber hygiene among UA personnel. It explores their awareness of cyber threats, frequency of security behaviors, and perceptions of existing policies and training support. Insights from this research aim to guide the design of tailored interventions—such as training, guidelines, and policy frameworks—to bolster cyber awareness and institutional resilience in similar educational settings.

This study seeks to explore and assess the cyber hygiene practices among UA employees. By identifying common behaviors, gaps in knowledge, and attitudes toward cybersecurity, the study aims to inform potential training initiatives and institutional policies that enhance information security. Through a structured and data-driven approach, this research contributes to building a culture of cyber awareness within the university.

This study specifically aims to answer the following;

1. To determine the level of awareness of UA employees regarding common cyber threats such as phishing, malware, and ransomware.

2. To assess the frequency and consistency of cyber hygiene practices performed by UA employees.

3. To identify the need for training and institutional support mechanisms that promote better cybersecurity practices among university staff.

II. RESEARCH METHODOLGY

Conceptual Framework

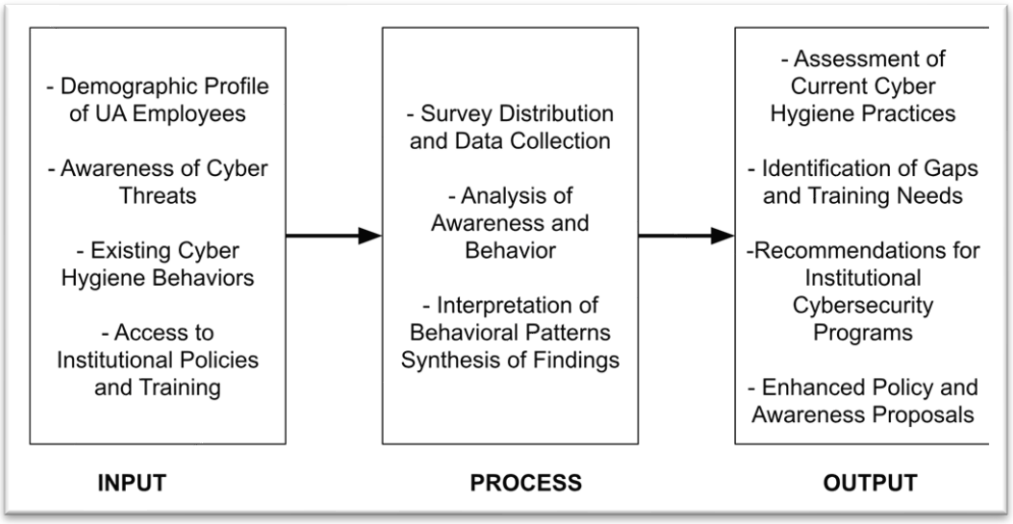


Figure 1. Conceptual framework

The conceptual framework, presented in Figure 1, is guided by Protection Motivation Theory (PMT) and posits that employees' cyber hygiene practices are influenced by their cybersecurity awareness, behavioral tendencies, and institutional support. The framework considers employees' demographic characteristics, knowledge of cyber threats, cybersecurity habits, and access to institutional training and policies as inputs.

Survey data are quantitatively analyzed to examine patterns between awareness and cyber hygiene practices. The resulting findings provide a basis for identifying gaps and developing data-driven recommendations for cybersecurity training, policies, and interventions to strengthen UA's cyber resilience.

Research Design

The study employed a mixed descriptive research design to assess employees' cyber hygiene awareness, practices, and behavioral tendencies. Quantitative survey data were used to identify patterns and gaps, while qualitative responses provided insights into training needs and institutional support.

Participants and Setting

The study was conducted at the University of the Assumption (UA) among teaching and non-teaching employees who regularly use digital devices and institutional online systems. Purposive sampling was used to select participants who met the inclusion criteria.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV029

From a population of 410 employees, the Raosoft Sample Size Calculator indicated a minimum of 120 respondents, based on a 93% confidence level and 7% margin of error. Participants were selected based on their regular engagement with institutional digital platforms and tools.

Research Instrument
Data were collected using a self-administered structured questionnaire consisting of four parts:

1. Demographic Profile: Age, gender, department/unit, and years of service.

2. Cyber Threat Awareness: Awareness of phishing, malware, ransomware, and password-related threats.

3. Cyber Hygiene Practices: Frequency of practices such as password updates, antivirus use, two-factor authentication, and safe internet and email use, measured using a 5-point Likert scale (Never to Always).

4. Institutional Support and Training Needs: Perceptions of cybersecurity policies, institutional support, and training requirements.

The questionnaire was adapted and refined from established cybersecurity assessment tools and studies, particularly the Ford Foundation Cyber Security Assessment Tool, Garba et al. (2022), Concepcion and Palaoag (2024), and Alowais et al. (2023). Items were contextualized to reflect cybersecurity practices within a higher education setting and aligned with the study objectives.

Data Collection Procedure
Prior to data collection, approval was secured from the University of the Assumption Research and Extension Office and Research Ethics Board. The validated questionnaire was distributed through Google Forms and printed copies over a 5–7 working-day period, with reminders sent through institutional communication channels to encourage participation.

Data Analysis
Data were encoded and analyzed using Microsoft Excel and Google Sheets. Descriptive statistics, including frequency, percentage, and mean, were used to summarize respondents' profiles, cybersecurity awareness, and cyber hygiene practices. Cross-tabulation was employed to examine patterns across demographic groups. Findings were interpreted using Protection Motivation Theory (PMT) and compared with related studies. All collected data were treated confidentially and used solely for academic and institutional cybersecurity improvement purposes.

III. RESULTS AND DISCUSSION

Awareness of Employees Regarding Common Cyber Threats
The results presented in the table reflect the varying levels of awareness of University of the Assumption (UA) employees—both Academic Personnel and Non-Teaching Personnel—regarding prevalent cyber threats, specifically phishing, ransomware, malware, and general cybersecurity practices. The responses are disaggregated by gender and categorized across awareness indicators: phishing recognition, ransomware understanding, malware differentiation, email domain verification, secure website identification, and awareness of emerging cyber threats.

Statement	Mean	SD	Interpretation
I can identify phishing emails based on suspicious links or poor grammar.	**3.69**	**1.26**	**High awareness**
I can check an email's domain to verify its legitimacy.	**3.39**	**1.38**	**Moderate awareness**

Table 1. Phishing Awareness Among Academic and Non-Teaching Personnel

Table 1 shows that employees demonstrated higher awareness in identifying phishing emails based on suspicious links or poor grammar (M = 3.69, SD = 1.26). However, their ability to verify email domain legitimacy was only moderate (M = 3.39, SD = 1.38). This indicates that while employees can recognize common phishing indicators, some may have difficulty applying more specific verification techniques. Overall, employees were more aware of phishing recognition than email domain verification, indicating an important gap in email-related cybersecurity awareness.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV029

Statement	Mean	SD	Interpretation
I am aware that ransomware can encrypt files and demand payment.	**2.79**	**1.31**	**Moderate awareness**
I know the difference between malware and a regular software update prompt.	**2.84**	**1.34**	**Moderate awareness**

Table 2. Ransomware Awareness Among Academic and Non-Teaching Personnel

Table 2 indicates that employees demonstrated moderate awareness of ransomware and malware-related threats, with mean scores of 2.79 and 2.84, respectively. The results suggest that employees have a general understanding of these threats but may have difficulty distinguishing malicious software from legitimate updates. This highlights the need for practical and scenario-based cybersecurity training to strengthen employees' ability to recognize and respond to malware and ransomware threats.

Statement	Mean	SD	Interpretation
I am familiar with how to distinguish between secure and non-secure websites (HTTPS).	**3.06**	**1.31**	**Moderate awareness**
I stay updated on common cyber threats such as phishing, malware, and ransomware.	**2.79**	**1.29**	**Moderate awareness**

Table 3. General Cyber Threat Awareness Responses Among Academic and Non-Teaching Personnel

Employees demonstrated moderate awareness of general cybersecurity threats as shown in Table 3, with mean scores of 3.06 for identifying secure websites and 2.79 for staying updated on common cyber threats. The results indicate a need to strengthen employees' understanding of secure browsing practices and current cybersecurity threats through regular awareness activities and targeted training.

Frequency and consistency of cyber hygiene practices performed by UA employees

This section shows the analysis of responses regarding the frequency and consistency of cyber hygiene practices among UA employees reveals varying degrees of adherence to essential cybersecurity measures across both academic (teaching personnel) and non-academic (administrative/support staff) groups, further differentiated by gender. The data underscores the presence of commendable practices in certain areas, while also highlighting critical gaps that warrant attention.

Statement	Mean	SD	Interpretation
I use strong and unique passwords for different accounts.	**4.18**	**1.01**	**Frequently observed**
I use a password manager app to store and manage passwords.	**3.93**	**1.22**	**Frequently observed**
I avoid storing passwords in browsers (e.g., Chrome, Firefox).	**4.26**	**1.12**	**Consistent and habitually observed**
I regularly change my passwords.	**4.41**	**1.03**	**Consistent and habitually observed**

Table 4. Frequency of Cyber Hygiene Practices among Academic and Non-Teaching Personnel - Password Management and Security

Table 4 indicates that employees generally demonstrated strong password management practices. Regular password changes recorded the highest mean (M = 4.41, SD = 1.03), followed by avoiding password storage in browsers (M = 4.26, SD = 1.12) and using strong, unique passwords (M = 4.18, SD = 1.01). The use of password managers was also frequently observed (M = 3.93, SD = 1.22). Overall, the results reflect consistent adherence to basic password security practices among employees.

Statement	Mean	SD	Interpretation
I use two-factor or multifactor authentication when logging in to email or systems.	**3.86**	**1.14**	**Frequently observed**
I do not share my credentials (e.g., name, DOB, account numbers) in emails or texts.	**3.52**	**1.18**	**Frequently observed**
I assess the authenticity of social media friends or information requests.	**3.03**	**1.32**	**Occasionally observed**

Table 5. Frequency of Cyber Hygiene Practices among Academic and Non-Teaching Personnel - Account and Identity Protection

Employees frequently practiced account and identity protection, particularly the use of two-factor or multifactor authentication (M = 3.86, SD = 1.14) and avoiding the sharing of credentials through emails or texts (M = 3.52, SD = 1.18) as indicated in Tabl e 5. However, assessing the authenticity of social media requests was only occasionally observed (M = 3.03, SD = 1.32). This indicates a need to strengthen employees'.

Overall, employees showed stronger adherence to authentication and credential protection than social media verification, highlighting the need for continued cybersecurity training, awareness of social engineering, identity-related risks, and consistent institutional security measures.

International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.67317/IJMSRT26NOV029

Statement	Mean	SD	Interpretation
I check the SSL certificate of a website before making financial transactions.	**3.04**	**1.06**	**Occasionally observed**
I avoid clicking links in emails from unknown senders or unfamiliar websites.	**4.02**	**1.13**	**Frequently observed**

Table 6. Frequency of Cyber Hygiene Practices among Academic and Non-Teaching Personnel - Safe Browsing and Email Practices

Table 6 shows that employees frequently avoided clicking suspicious or unfamiliar links (M = 4.02, SD = 1.13) but only occasionally checked SSL certificates before financial transactions (M = 3.04, SD = 1.06). Overall, employees demonstrated stronger behavioral caution toward suspicious links than technical verification of website security, indicating a need to strengthen technical safe-browsing practices.

Statement	Mean	SD	Interpretation
I regularly update my device operating systems and software.	**3.95**	**1.05**	**Frequently observed**
I run antivirus scans or use security software.	**2.73**	**1.09**	**Occasionally observed**
I manually or automatically back up my work files.	**2.79**	**1.30**	**Occasionally observed**
I use VPN when connecting to public or unsecured networks.	**3.85**	**1.21**	**Frequently observed**
I scan USBs or external devices before using them.	**3.91**	**1.22**	**Occasionally observed**

Table 7. Frequency of Cyber Hygiene Practices among Academic and Non-Teaching Personnel - Device and Data Security

Data in table 7 shows that employees generally demonstrated positive device and data security practices, particularly in regularly updating software (M = 3.95, SD = 1.05) and scanning external devices (M = 3.91, SD = 1.22). However, antivirus use (M = 2.73, SD = 1.09) and file backups (M = 2.79, SD = 1.30) were only occasionally observed. VPN use was also reported at M = 3.85 (SD = 1.21). Overall, the findings indicate stronger adherence to basic protective practices, while data backup and security software use require greater attention.

Perception of Employees on Training and Institution Needs and Support Mechanisms

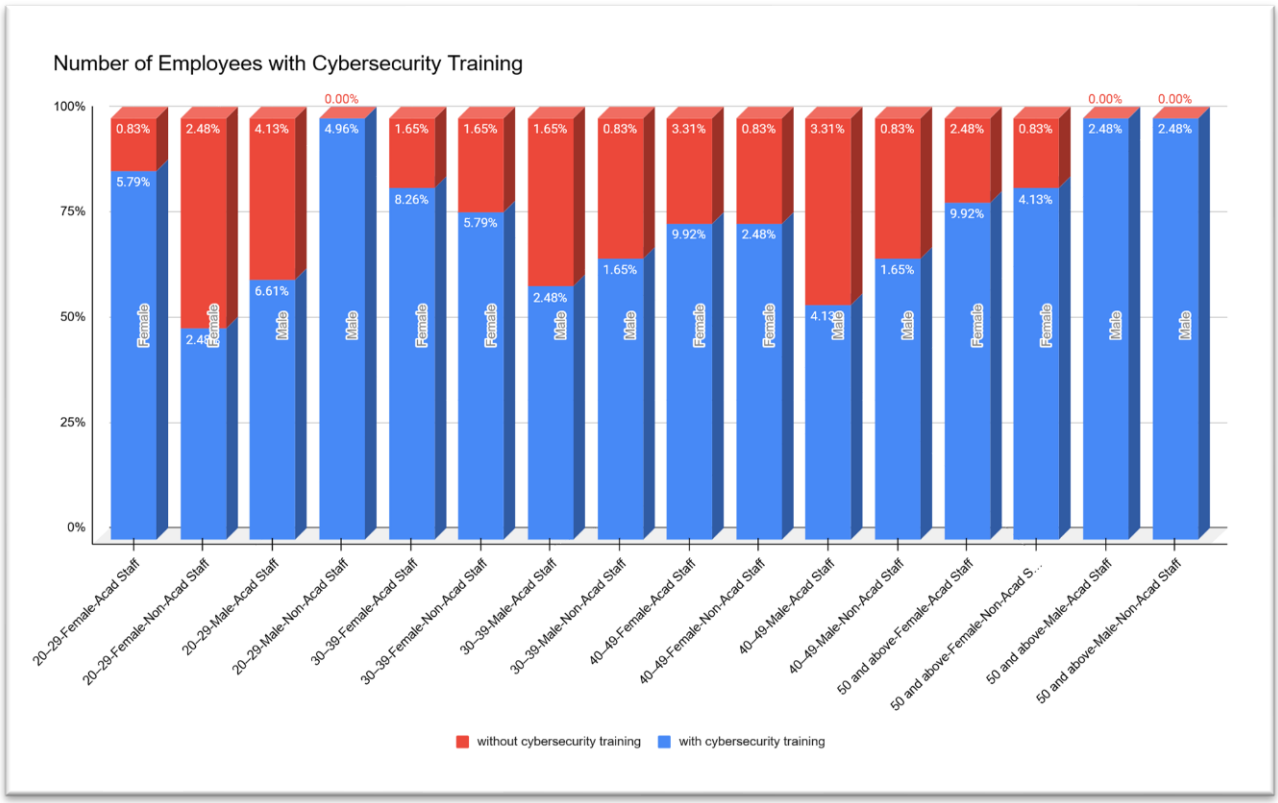


Figure 2. Demographic Distribution of University of the Assumption Employees Who Have Undergone Cybersecurity Training

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV029

While 75.21% of respondents reported prior cybersecurity training, coverage remains uneven across demographic groups. Academic personnel and employees aged 30–49 account for a larger share of those trained, whereas non-teaching staff, younger employees (20–29), and older staff (50+) show higher representation among the untrained. These disparities highlight the need for inclusive, institution-wide cybersecurity programs tailored to reach all employee classifications and age groups.

Statement	Mean	SD	Interpretation
I feel confident in my current level of cybersecurity knowledge.	**2.67**	**1.19**	**Moderately Needed**
I would benefit from attending cybersecurity training sessions.	**4.41**	**0.92**	**Highly Needed**
I would prefer short, interactive cybersecurity workshops to improve my digital practices.	**4.42**	**0.83**	**Highly Needed**

Table 8. Perceptions on Cybersecurity Knowledge and Training Needs among Academic and Non-Teaching Personnel

Table 8 shows that employees reported moderate confidence in their cybersecurity knowledge (M = 2.67, SD = 1.19), while strongly recognizing the value of cybersecurity training (M = 4.41, SD = 0.92). Employees also expressed a clear preference for short, interactive workshops (M = 4.42, SD = 0.83). Overall, the results indicate a gap between current cybersecurity confidence and training needs, with employees showing strong receptiveness to practical and accessible cybersecurity training programs.

Statement	Mean	SD	Interpretation
The university should conduct regular cybersecurity awareness campaigns.	**2.79**	**1.35**	**Moderately Needed**
There is a clear cybersecurity policy that employees are made aware of.	**2.74**	**1.28**	**Moderately Needed**
I believe cyber hygiene should be integrated into employee onboarding and offboarding.	**4.24**	**0.99**	**Highly Needed**

Table 9. Perceptions on Institutional Cybersecurity Support and Policy Awareness

Table 9 indicates that employees recognized the need for stronger institutional cybersecurity support and policy awareness. The moderate rating for regular awareness campaigns (M = 2.79, SD = 1.35) and awareness of existing cybersecurity policies (M = 2.74, SD = 1.28) suggests that cybersecurity communication may not be consistently reaching all employees. In contrast, the high rating for integrating cyber hygiene into onboarding and offboarding (M = 4.24, SD = 0.99) demonstrates strong support for making cybersecurity a formal part of the employee lifecycle. Overall, the findings suggest that UA can strengthen cybersecurity by improving the visibility and consistency of awareness initiatives and policies while embedding cyber hygiene into established institutional processes.

Statement	Mean	SD	Interpretation
I know who to contact in case of a cybersecurity incident.	**4.35**	**0.96**	**Highly Needed**

Table 10. Awareness of Cybersecurity Incident Response Protocols

Table 10 shows that employees reported a high level of awareness regarding whom to contact in case of a cybersecurity incident (M = 4.35, SD = 0.96). The result indicates that most employees are aware of the appropriate reporting channel, although the variation suggests that awareness is not uniform across all respondents. Maintaining clear and accessible incident-reporting procedures is therefore important to support timely and effective responses to cybersecurity incidents.

Overall, employees showed moderate confidence in their cybersecurity knowledge (M = 2.67, SD = 1.19) but expressed strong support for cybersecurity training (M = 4.41, SD = 0.92) and short, interactive workshops (M = 4.42, SD = 0.83). Moderate ratings for awareness campaigns (M = 2.79, SD = 1.35) and existing cybersecurity policies (M = 2.74, SD = 1.28) indicate area s where institutional communication can be strengthened. Employees also strongly supported integrating cyber hygiene into onboarding and offboarding processes (M = 4.24, SD = 0.99), while their high awareness of incident-reporting contacts (M = 4.35, SD = 0.96) provides a positive foundation for effective response. Overall, the findings support a comprehensive institutional approach that combines accessible training, consistent policy communication, and clearly communicated incident-response procedures.

International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.67317/IJMSRT26NOV029

Analysis of UA Employees' Cybersecurity Feedback

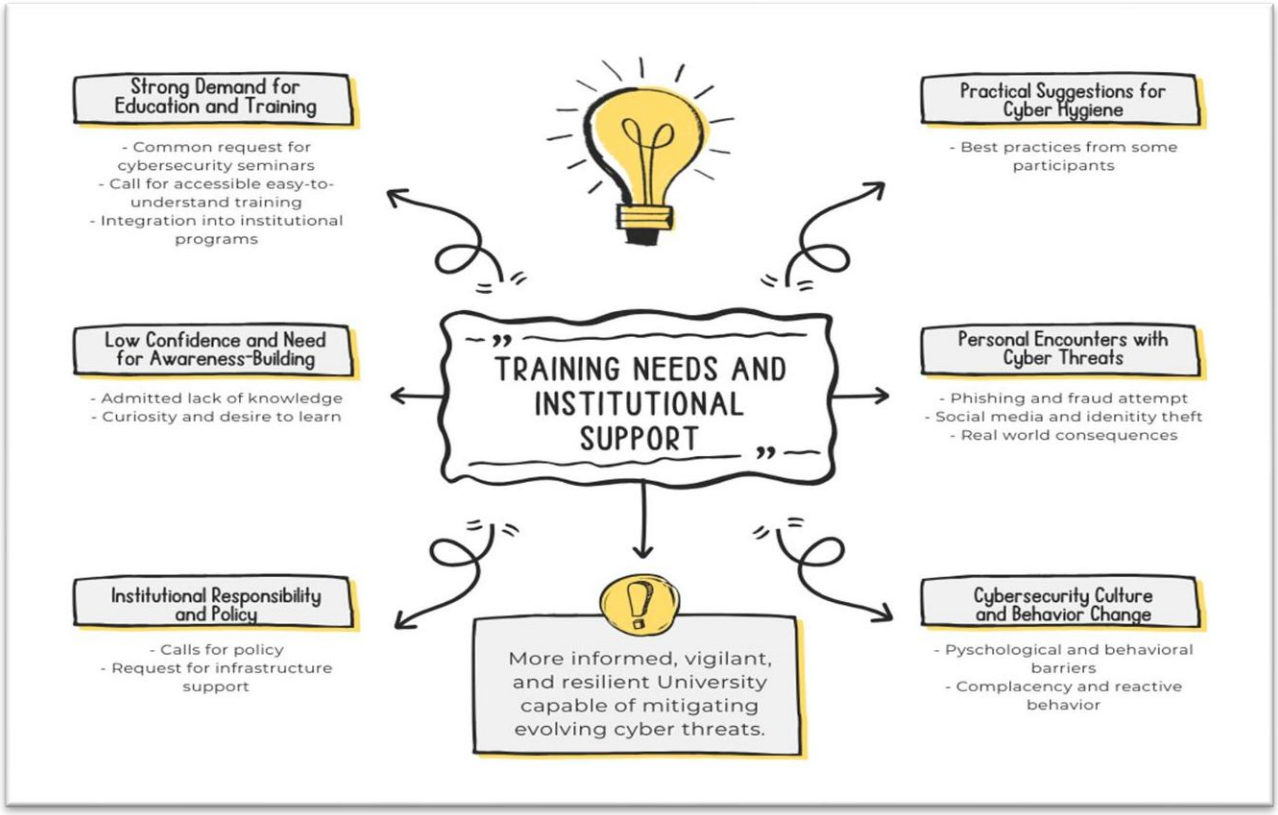


Figure 3. Emerging Framework for Training Needs and Institutional Support for UA Employees

The thematic analysis of employee feedback reveals six core dimensions shaping cybersecurity readiness at the University of the Assumption (UA).

1. **Demand for Education and Training:** Employees strongly expressed the need for continuous, accessible, and non-technical-friendly cybersecurity seminars integrated into institutional programs.

2. **Low Confidence and Awareness Gaps:** Many participants acknowledged a lack of familiarity with cyber concepts, coupled with a strong underlying curiosity and willingness to learn.

3. **Personal Threat Experiences:** Numerous responses highlighted direct encounters with phishing scams, social media hacks, and fraud, illustrating the real-world impact of cyber threats.

4. **Practical Cyber Hygiene:** Some staff members independently practice good security habits, such as using two-factor authentication, backing up files, avoiding password sharing, and watching out for suspicious links.

5. **Institutional Responsibility:** Respondents stressed the importance of formalizing security guidelines through robust university policies and enhanced technical support infrastructure.

6. **Culture and Behavioral Change**: Acknowledging psychological barriers like complacency, participants noted the necessity of shifting away from reactive habits toward team-based, proactive security behaviors.

Overall, these findings highlight a community that recognizes the value of cybersecurity but requires a multifaceted approach—combining inclusive training, policy development, and behavioral reinforcement—to cultivate institutional resilience.

ISSN :2584-2706 DOI: https://doi.org/10.67317/IJMSRT26NOV029

IV. CONCLUSION

4.1 Conclusion

The findings indicate that UA employees possess moderate awareness of common cybersecurity threats, with stronger practices in areas such as password management, software updates, and cautious email use. However, gaps remain in the consistency of cyber hygiene practices, understanding of specific threats, and awareness of institutional cybersecurity policies and procedures.

Employees also demonstrated a clear need for practical and accessible cybersecurity training, particularly through short, interactive, skills-based workshops. The findings further highlight the importance of clear institutional guidelines, consistent policy communication, and accessible IT support to strengthen employees' ability to prevent and respond to cybersecurity incidents.

Overall, the study concludes that strengthening cybersecurity at UA requires a sustained, institution-wide approach that integrates employee training, clear policies, incident-response procedures, and individual accountability. While a foundation of cybersecurity awareness and responsible practices exists, continuous capacity-building and institutional support are necessary to develop a more consistent and resilient cybersecurity culture.

4.2 Recommendations

Based on the findings, the following recommendations are proposed:

1. **Strengthen Cybersecurity Education and Training.** Conduct regular, inclusive, and practical training for academic and non-teaching personnel, incorporating simulations, real-life scenarios, and short interactive workshops. Integrate basic cybersecurity orientation into employee onboarding.

2. **Institutionalize Cyber Hygiene Policies.** Establish clear and accessible guidelines on password management, software updates, secure device use, and incident reporting. Policies should be regularly communicated and reviewed to ensure continued relevance.

3. **Enhance IT Support and Communication.** Establish clear incident-reporting and IT support channels, while using institutional communication platforms to disseminate cybersecurity alerts, reminders, and practical security tips.

4. **Promote Positive Cybersecurity Behaviors.** Encourage employee participation through recognition programs and engaging activities, including gamified cybersecurity awareness campaigns where appropriate.

5. **Monitor and Evaluate Cybersecurity Practices.** Conduct periodic assessments of employees' cybersecurity awareness and practices and use feedback to continuously improve training, policies, and support mechanisms.

6. Collectively, these measures can help the University of the Assumption strengthen its cybersecurity culture by combining employee capability-building, institutional support, clear policies, and continuous evaluation.

REFERENCES

[1]. Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering (IJECE), 12(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584

[2]. Concepcion, J. D., & Palaoag, T. D. (2024). An assessment of cybersecurity awareness among academic employees at Quirino State University: Promoting cyber hygiene. Journal of Electrical Systems. https://doi.org/10.52783/jes.3445

[3]. [Alowais, S., Armeen, I., Sharma, P., & Johnston, A. C. (2023). Cyber hygiene practices across cultures: A cross-cultural study of the US and Saudi Arabia based information systems users. Procedia Computer Science, 217, 2793–2802. https://doi.org/10.1016/j.procs.2023.01.347

[4]. Fikry, A., Hamzah, M. I., Hussein, Z., & Saputra, D. H. (2022). Cyber hygiene practices from the lens of professional youth in Malaysia. Environment-Behaviour Proceedings Journal, 7(21), 203–210. https://doi.org/10.21834/e-bpj.v8i25.4827

[5]. [Khader, M.,Karam, M., Fares,H. Cybersecurity awareness framework for academia. Information, 11(10), 515. https://doi.org/10.3390/info12100417

[6]. [6]. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology: Interdisciplinary and Applied91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

[7]. Ugwu, C., Ezema, M., Ome, U., Ofusori, L., Olebera, C., & Ukwandu, E. (2023). Impact of gender, employment status, and academic discipline on cyber hygiene: A case study of University of Nigeria, Nsukka. http://dx.doi.org/10.1007/978-981-19-6414-5_22

[8]. Yusuf, A. A. (2024). Employees' cybersecurity awareness and behaviour in South African higher education institutions (Master's thesis, University of Pretoria). University of Pretoria Institutional Repository. https://doi.org/10.25403/UPresearchdata.26311141.v1

[9]. Ifinedo, P., Mengesha, N., & Longe, O. (2019). Factors that influence workers' participation in unhygienic cyber practices: A pilot study from Nigeria. In L. T. A. G. Djeflat, A. A. Tonta, M. A. Mahfoudh (Eds.), IFIP Advances in Information and Communication Technology: Vol. 551. Information Technology for Peace and Security (pp. 321–332). Springer. https://doi.org/10.1007/978-3-030-19115-3_25
[10]. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
[11]. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699
[12]. Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. arXiv. https://doi.org/10.48550/arXiv.2302.02274
Ford Foundation Cyber Security Assessment Tool. https://www.fordfoundation.org/work/our-grants/building-institutions-
[13]. and-networks/cybersecurity-assessment-tool/
[14]. Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering (IJECE), 12(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584
[15]. Concepcion, J. D., & Palaoag, T. D. (2024). An assessment of cybersecurity awareness among academic employees at Quirino State University: Promoting cyber hygiene. Journal of Electrical Systems. https://doi.org/10.52783/jes.3445
[16]. Alowais, S., Armeen, I., Sharma, P., & Johnston, A. C. (2023). Cyber hygiene practices across cultures: A cross-cultural study of the US and Saudi Arabia based information systems users. Procedia Computer Science, 217, 2793–2802. https://doi.org/10.1016/j.procs.2023.01.347
[17]. Fikry, A., Hamzah, M. I., Hussein, Z., & Saputra, D. H. (2022). Cyber hygiene practices from the lens of professional youth in Malaysia. Environment-Behaviour Proceedings Journal, 7(21), 203–210. https://doi.org/10.21834/e-bpj.v8i25.4827
[18]. Khader, M.,Karam, M., Fares,H. Cybersecurity awareness framework for academia. Information, 11(10), 515. https://doi.org/10.3390/info12100417
[19]. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology:Interdisciplinary and Applied, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
[20]. Ugwu, C., Ezema, M., Ome, U., Ofusori, L., Olebera, C., & Ukwandu, E. (2023). Impact of gender, employment status, and academic discipline on cyber hygiene: A case study of University of Nigeria, Nsukka. http://dx.doi.org/10.1007/978-981-19-6414-5_22
[21]. Yusuf, A. A. (2024). Employees' cybersecurity awareness and behaviour in South African higher education institutions (Master's thesis, University of Pretoria). University of Pretoria Institutional Repository. https://doi.org/10.25403/UPresearchdata.26311141.v1
[22]. Ifinedo, P., Mengesha, N., & Longe, O. (2019). Factors that influence workers' participation in unhygienic cyber practices: A pilot study from Nigeria. In L. T. A. G. Djeflat, A. A. Tonta, M. A. Mahfoudh (Eds.), IFIP Advances in Information and Communication Technology: Vol. 551. Information Technology for Peace and Security (pp. 321–332). Springer. https://doi.org/10.1007/978-3-030-19115-3_25
[23]. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
[24]. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699
[25]. Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. arXiv. https://doi.org/10.48550/arXiv.2302.02274
[26]. Ford Foundation Cyber Security Assessment Tool. https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/