Journal of Positive School Psychology
2022, Vol. 6, No. 3, 3655–3664

Anticipatory assessment through Information Security Awareness: approaching of Local Government Units in a Province of Oriental Mindoro

Nicko A. Magnaye

Mindoro State University
nickoamagnaye.ccs.minsu.edue@gmail.com

Abstract

The studies give you the idea that local government unit employees today use the Internet exceedingly to find data and increase general knowledge. Therefore, the Internet has grown to be a data arterial highway wherever employee forces their thoughts and community experiences. on the other hand, utilize the Internet routinely opens up employees to a variety of dangers like cybercrime, identity theft, and malware infections. Consequently, it is necessary to know the Information Security practices and the level of awareness that Local government unit employees possess to assess and prevent them from harm's way. Methods: The research employed a Descriptive Correlation Method which involved the use of online questionnaires delivered through Google form, interviews and observations. The respondents of the study were four hundred eleven (411) employees during the year2019-2020. Simple Random Sampling was the method used for choosing the respondents. Findings: Outcomes indicate that there was a significant positive association between respondents Year level with the level of Information Security Awareness (ISA), ($r (411) =. 451$, $p < .001$). The result shows with the aim of the the Educational Attainment of the respondents, the higher the Comprehension and awareness in Information Security (IS). Employees improve their experience, knowledge, and awareness of the fortification and distribution of information when they developed to a Educational attainment in the study. This implies that the program successfully meets the knowledge requirements of the employees in the Local Government Unit. Application/Improvements: result of this study can serve as a basis for policy measures the use of Computer Networks in the Local Government Unit. It may also serve as a guide for developing inclusive and beneficial Information Security Awareness (ISA) training programs for the LGU Employees

Keywords— Information Security Awareness, Local Government Unit, Descriptive Correlation, Information, Social Computer Networking, Sciences

I.INTRODUCTION

Local government is an umbrella term that covers a spread of entities. These entities include jails, courts, police departments, local hearth offices, social services, public transportation offices, fire and police departments, native utilities/services and additional. Local government agencies square measure what keeps states, cities, towns, and municipalities running depending on the agency, it's terribly likely they'll have tons of in-person identifiable data (pii) to keep on their electronic systems. If is going in the incorrect hands, it will produce the terribly real potential for fraud. In order to shield government assets and native voters, agencies must always be up their security. The Internet has become a data superhighway where employees propel their ideas and social experiences. The new direction requires administrations to allow their community members particularly the Department Heads and staff to utilize their mobile devices in addition to computer systems to perform tasks. Such activities have led to an

increased number of attacks and information security breaches.

1.1 Research Objectives

This study aimed to determine the Information Security Awareness of Local Government Unit employee in Province of Oriental Mindoro. Specifically, it seeks to:

1. Describe the demographic profiles of the LGU employee regarding Age, Sex and Highest Degree Earned.
2. Identify the level of proficiency of the LGU employees regarding Computer Networking and Information System usage according to their perception.
3. Identify the Information Security awareness level of the LGU Employees.
4. Identify the extent of use of the LGU employment on the Computer Systems of the Province.
5. Find the significant relationship between the profile of the respondents and the following:
   a) Level of Proficiency in Computer Networking
   b) Level of Awareness to Information Security
   c) The extent of use on the Computer Systems of the Province.

II. LITERATURE

Electronic data, mobile devices, knowledge, behaviors and unintentional mistakes caused by users seemed to have contributed to this predicament [1] Literature reviews about information security support the importance of research in measuring information security where possible [2]. Thus, instead of opposing prohibitive approaches, it is better to cultivate a culture of appropriate use and raise awareness about information security among employees[3] The DPA is an act protecting individual personal data in ICT systems in both government and private sector. The law is crucial to help prevent cybercrimes by ensuring information are protected to prevent fraud. To the provisions of R.A 10173 and NPC's five pillars, Data Privacy Accountability also presented the same results. Moreover, the study revealed factors such as lack of awareness, budget, and time constraints as barriers to the DPA.[4] This only proves that although the government is trying its best to implement Information Security Awareness among Local Government Units still there are several factors that hinder its abilities to abide. Thus, it is now the responsibility of institutions to implement the ISA program to their own clients. The most recent study concerning ISA in the Philippines is that of Internet Subscribers in Iriga City Camarines Sur where findings show that despite existing cyber security laws (RA 8792 Electronic Commerce Act) and (RA 10173 the Data Privacy Act), users still are most vulnerable to phishing and malware attacks.

The study anchor on the Information Security theory [6] which posits that Information security is aware or unconscious procedure in which people and organization challenge to create sustainable viable resources for information. The method works by using controls that protect data from threats, based on goals for the use of that information. Those goals, then result in sustainable resources. Therefore, the focal point of Information security is to make out the level of protection given to data, and what use that protected data can offer organizations. The theory supports the learning by as long as a concept which can classify the dissimilar motivations behind an organization or an individual to secure information against threats. These motivations include goals, purpose, wants and needs. Information security thus appeals to an human being understanding of how necessary and vital is the protection of valuable data from threats. This perception determines the steps that individuals take or apply to meet their desired outcomes. Furthermore, the theory explains the need to create information security resources that can later improve organizational performance.

These information security resources may be training, works, and policy development. Likewise, it formulates risk identification and data quality assurance through the application of security technology and management processes [7]in conclusion, the hypothesis of information security originate from the area of

information systems, constructed entirely from ideas that identify with data and the expansiveness of the frameworks that it can dwell on. It applies to different levels, together with strategy to protect information used by individuals, groups, organizations, and laws that defend information communal between organizations.

III. METHODOLOGY

3.1 Design

This study utilized a Descriptive Correlational research design. By means of this method, the researcher described the current put into practice and behaviors of the respondents relevant to Information Security. The Descriptive method was used to identify the demographic profile, Level of proficiency, Level of Awareness and the extent of use of the respondents to the subject Information security. The Correlational method was utilized to identify the relationship between two or more relevant variables.

3.2 Respondents of the Study

Four hundred eleven (411) randomly selected Local Government Unit (LGU) employees from where the respondents of the study. The employees were officially work in the LGU year 20192020.

3.3 Research Instrument

This study aimed to describe the Information Security Awareness of LGU Employees at selected Municipality of Second District an online survey questionnaire developed using Google forms was the main instrument used in the study. The instrument was first face validated by experts in the field. After which it was classified into four areas. The first part, the demographic profiles of the LGU employees to determine Age, Gender, Educational attainment and the Level of Proficiency was relative to Computer Networking. The second part, the level of Information Security Awareness and the Extent of use of Computer Systems at the Local Government unit to determine Computer network usage and identification of risks and threats. A 5-point Likert scale was utilized to gather responses.

3.3 Research Procedure

Within obtaining the desired results, the researcher sought first the approval of the respondents. Then the planning and designing of the procedure for data gathering followed. The researcher conducted interviews and observations of the respondents in the network setting. The researcher asked the employee employees about security practices, procedures and the extent of their compliance with the LGU security policies. The answers to the interview were classified and examined then revised for the drafting of the questionnaire. The survey questionnaire was finalized and then distributed for fielding after which the collection and tabulation of data followed.

3.4 The Statistical Analysis of Data

The researcher basically retrieved the responses of the electronic questionnaires through Google form then converted it to the prescribed excel format using Google Sheets. The Excel data was after that feed into the Statistical Package for Social Sciences (SPSS) software and descriptive statistics was applied. In obtaining the Demographic profile, the researcher made use of frequency counts and percentages. Then, in the identification of Information Security awareness level of the employees and the extent of use of the employees the weighted mean of each item in the form was determined using simple descriptive statistics. Pearson, R Correlation using SPSS determined and analyzed the relationships between the Demographic profile and the variables; Level of Security Awareness and Extent of Use of Network Computer Systems in the LGU.

The following scale used in the evaluation of Information Security Awareness of LGU Employees.

Table 1. Security Awareness of the LGU employees

Rating Scale	Limits of Scale	Qualitative Description
5	4.21 – 5.0	Strongly Agree
4	4.21 – 5.0	Agree

3	2.61 – 3.4	Moderately agree
2	1.81 – 2.6	Disagree
1	1.0 – 1.8	Strongly Disagree

Table 2. Extent of Use of Network Computer Systems in the LGU

Rating Scale	Limits of Scale	Qualitative Description
5	4.21 – 5.0	Strongly Agree
4	4.21 – 5.0	Agree
3	2.61 – 3.4	Moderately agree
2	1.81 – 2.6	Disagree
1	1.0 – 1.8	Strongly Disagree

IV. RESULTS AND DISCUSSION

Table 3. Demographic profile of Respondent

Profile	**Frequency**	**Percentage**
Age		
46-Above	42	10.21%
42-45years old	37	9.00%
38-41 years old	32	7.79%
34-37 years old	31	7.54%
30-33 years old	29	7.06%
26-29 years old	56	13.63%
22-25 years old	60	14.60%
18-21 years old	124	30%
Total	**411**	**100%**
Sex	**Frequency**	**Percentage**
Male	150	36.49%
Female	261	63.51%
Total	**411**	**100%**

Educational attainment	**Frequency**	**Percentage**
With Doctoral	6	1.45%
MA Degree	37	9.00%
With MAUnits	80	19.47%
Bachelor's Degree	258	62.78%
High School graduate	30	7.30%
Total	**411**	**100%**

Level of Proficiency	**Frequency**	**Percentage**
Advance User	49	12%
Internet User	341	83%
Basic User	21	5%
Total	**411**	**100%**

Table 3 illustrates the breakdown of respondents by age of the total number of

respondents, the majority (124 or 30%) of the respondents were 18 to 21 years of age, followed by the Employee aged 22-25 years old at (60 or 14.60%). This was followed by respondents aged 26-29 (56 or 13.63%), 46-above (42 or 10.21%), 42 to 45 (37or 9.00%), 38-41 (32 or 7.79%), and 34 to 37 (31 or 7.06%). The employee age that had the lowest number of respondents were 34, 37 and 30-33 at (29 or 7.06%) respectively. The results prove that the majority of the respondents were 18 years and older. The age of the respondents is the legal age. The employee understands the survey questions and can relate their user experiences with their ISA. Cognitive growth and the amount of work and life experience at their ages show helpful for the study. Table 3 presenting the gender profile of the respondents. Out of the total number of respondents (188 or 45.7%) were Male and (223 or 54.3%) were Female. The result shows that the majority of the employees in the LGU are female. The result has also roped previous studies which show that among those with government in the Philippines; there are more female employees than male employees in LGU. Male individuals previously dominate the majority of local; government unit in the Philippines (Statistics on Filipino women admen's works. Hence, the gender is not a significant factor in information security awareness. Being male or female is not an assurance that an individual is performing safe online practices. Instead the key to safe computing is to educate and sharpen employee security skills to keep up with the times [10] Also, Table 3, below, shows the distribution of respondents regarding their Educational Attainment. Out of the total population of 411 LGU, the majority came from the Bachelors with (258 or 62.78%) respondents, the With MA Units with (80 or 19.47%), the MA Degree with (37or 9.0%) respondents and the LHS with (30 or730%) respondents and with doctoral (6 or 1.45%). Table 3 Further illustrates the self-perceived proficiency of the respondents in Computer Networking and Information System usage which contributes significantly to information security awareness. In the data presented (341 or 83 %) of the respondents described themselves as Intermediate users, while (21 or 5%) considered themselves as Basic users. A minimal number of respondents (49 or 12%) identified themselves as advanced users. The data exemplifies the knowledge of the respondents in the subject Computer Networking and Information systems. The respondent's knowledge of computer systems and Networks is the product of blended learning Technology. In classifying the appropriate user-levels of the respondents, we look at their compute skill. According to skills are fundamental since it enables employee to learn more effectively in information security. The more extensive the knowledge, the more likely they will be able to secure information. Hence, the Proficiency level of the respondents is very important in determining the ISA that they have currently.

Table 4. Information Security Awareness

Information Security Awareness	**Mean**	**Verbal Interpretation**
Information Security is an integral part of my works.	4.74	SA
I am aware that there is an existing Information Security policy and regulations of the LGU.	2.81	MA
I have received Information Security awareness training at the LGU.	2.62	MA
My work involved the use of research information.	4.60	SA
My work involved the use of personal information	2.68	MA
My work involved the use of confidential information	2.40	D
My work involved the use of financial information	2.81	MA
I am aware that there are security risks in using	4.94	SA

computers.		
I am aware that there are threats in the LGU computer network.	4.44	SA
I know that there are security software's that protect information.	4.75	SA
TOTALMEAN	**3.68**	***Agree***

Table 4 illustrates the Information Security Awareness of the respondents in the university with a qualitative description of *Agree* having a total mean of 3.68. The findings described the level of Information security awareness of the respondents towards the information that they sent and received thru the Network Information System (NIS) of the Local Government Unit.

The outcomes show that the highest qualitative description was *Strongly Agree* based on the following indicators. (I am aware that there are security risks in using computers = 4.94, I know that there are security software's that protect information = 4.75, Information Security is an essential part of my education = 4.74). The results show that employee put more attention to risk, protection, and edification as primary indicators of information security awareness. These characteristics are both preventive and protective. [11] When individuals are knowledgeable as to what to watch for, what to protect, and how to respond, this alone could prevent potential problems that could affect the infrastructure as a whole. Also, one of the most central mechanisms of individual security behaviour is the identification of risks [12] Recognizing threats, as well as managing those threats by learning protective methods will lessen the possibility of a security problem. Therefore, employee's technical abilities should be at par with their level of awareness as it is equally important to know how to prevent and thwart attacks using hardware or software configurations. Table 4 also illustrates the average responses of the Employees.With a qualitative description of *Moderately Agree* (I am aware that there is an existing Information Security policy andregulations in the LGU = 2.81, my works involves the useof financial information = 2.81, my work includes the use of personal information = 2.68). The lowest rated item in the table is (My works involves the use of confidential information) with a qualitative description of *Disagree* and a mean of 2.40.These results illustrate that the respondents are aware of the type of data that they distribute in the network. Furthermore, it shows that the respondents are mindful that certain kind's ofinformation such as financial and personal are attractive targets for the online scam, identity theft, and hacking [13] Respondents also exercise caution in providing information, especially in the network of the LGU where hundreds of individuals communicate at any given time. Thus, results imply that respondents are familiar with the existing policies of the LGU in the use of the system .[14]As explained by financial and personal information are the most common motivation of attackers due to the prospect of financial gain. Hence, the Employees awareness of the value of user information and the importance of policies are beneficial in the operationand management of the network as it provides a certain level of protection such as confidentiality of data. Finally, user Behaviour is a significant factor in the domain of Information Security [15] Negligence, ignorance, lack of awareness, and resistance to policies are the main factors in security breaches so respondents must focus to maintain adequate information security behaviour for minimizing if not reducing it.

Table 5. The Extent of use of employee in Network Computer

The Extent of use of employee in the Computer Systems of the LGU	**Mean**	**Verbal Interpretation**
I used the computer for two to three hours a day.	3.0	Moderately Agree

I used and exchanged information with Social Media sites.	3.29	Moderately Agree
I searched the Network for different kinds of Information.	3.18	Moderately Applicable
I shared my password and other login information with other people.	1.9	Strongly Disagree
I downloaded different material on the LGU Network.	4.5	Strongly Agree
I copied different file types to the computers in the Network.	4.67	Strongly Agree
I acquired data from other users in the network computers.	3.2	Moderately Agree
I accessed the network server remotely.	3.5	Agree
I visited untrusted and underground websites using the network.	3.7	Agree
TOTALMEAN	**3.43**	**Agree**

The table below (table 5) illustrates the Extent of use of the respondents in the Network Computers of the LGU with a qualitative result of Agree having a total mean of 3.43. The findings show the degree to which the respondents utilize the computers in the Network of the LGU. The majority of the items rated *Moderately Agree* (I used the computer two to three hours a day=3.0, I used and exchanged information with Social Media sites =3.29, I searched the Network for different kinds of Information=3.18, and I acquired data from other users in the network computers =3.2).The findings suggest that the respondent's extent of use of computers in the network have a more than average frequency involved. These findings also indicate that the regularity of using computers as well as the applications that were utilized such as social media poses a threat to its security. [16] Explains that the only safe system is the system that disconnects from a network. However, with the value placed on connectivity, it is almost impossible to abstain from using the Internet. Hence, there is no way of avoiding a potential attack from both internal and external threats. Thus, another indicators in Table 5 rated *strongly Agree (*I downloaded different material on the LGU Network=4.5, and I copied different file types to the computers in the Network=4.67).These findings indicate that the employee do not exercise caution when downloading or reproducing data to and from the Internet. The indicators used in Table 5 present a significant threat to the integrity of the Computer Network likewise employees responses exhibit complete disregard of LGU policies, controls, and restrictions [17] explains, wholesome of these actions may be harmless, a potential for a security breach possibly with devastating consequences always lurks in the background due to computers being susceptible to diverse forms of malicious IT infringements. Furthermore, in a study users who downloaded applications from various application repositories were found to have exhibited a blind trust in such deposits and did not necessarily exercise caution when selecting, downloading, and installing apps[18]. Finally, the lowest rated item in table 5, was (I shared my password and other log-in information with other people) with a qualitative result of *Strongly Disagree* and a mean of 1.9. The finding suggests that the respondents knowhow to secure their mail and online accounts from possible intrusions. They were aware of the risk of sharing their email and social media accounts and were cautious about divulging critical information to other people.

Table 6. Correlation Analysis

		Age	Sex	YrLvl	Prof	ISA	UCL
Age	Pearson Correlation	1	.177**	.001	.030	-.093	-.090
	Sig. (2-tailed)		.000	.978	.551	.060	.068
	N	411	411	411	411	411	411
Sex	Pearson Correlation	.177**	1	-.412**	.064	-.051	-.036
	Sig. (2-tailed)	.000		.000	.193	.303	.472
	N	411	411	411	411	411	411
YrLvl	Pearson Correlation	.001	-.412**	1	.028	.451**	.349**
	Sig. (2-tailed)	.978	.000		.570	.000	.000
	N	411	411	411	411	411	411
Prof	Pearson Correlation	.030	.064	.028	1	.000	-.003
	Sig. (2-tailed)	.551	.193	.570		.997	.954
	N	411	411	411	411	411	411
ISA	Pearson Correlation	-.093	-.051	.451**	.000	1	.454**
	Sig. (2-tailed)	.060	.303	.000	.997		.000
	N	411	411	411	411	411	411
ULC	Pearson Correlation	-.090	-.036	.349**	-.003	.454**	1
	Sig. (2-tailed)	.068	.472	.000	.954	.000	
	N	411	411	411	411	411	411

The results show, depicted in the Table below (Table 6), there is a significant positive association between respondents Educational Attainment with the level of Information Security Awareness (ISA),(r (411) =. 451, p < .001). The result shows that the higher the Educational Attainment of the respondents, the higher the comprehension and awareness in IS of the respondents. When employees progressed to a higher Educational Attainment in the employee and their experience, knowledge, and awareness on the protection and dissemination of Computer Information grew. The results infer that knowledge thru higher learning contributes to a widened and holistic view of employees understanding of IS consciousness. Therefore, this implies that education plays an imperative role in acquiring a conscious and constructive knowledge of IS. The below (Table 6) also showed there was a significant relationship between Educational Attainment and the Extent of Use of the Computer Systems by the respondents (r (411) =.349, p < .001).These means that the higher the Educational Attainment of the respondents, the higher the extent of use of Computer Systems that they observe relative to IS. The result indicates that the respondents require more hours as they progress in their levels to master, secure, and protect their information. Further, it proves that even in an ideal workplace, ISA requires more time, focus and expertise for employees. Likewise, the respondents needed vast amounts of practice and study to further improve their skills in securing information and protecting valuable data. Table 6. Also disclosed a significant positive relationship between the employees Level of ISA and the Extent of Use of the Computer Systems by the respondents (r (411) =.454, p < .001).It means that the higher the employees Level of ISA the higher the Extent of Use of the Computer Systems by the respondents. The findings state that employees increase and grow their ISA through constant and frequent use of computer and internet based systems. Furthermore, Human knowledge directly affects our attitudes; this effect comes from our direct personal experience or the result of our observations [18]. Hence, the result implies that employee learns ISA not only through instruction and lessons but moreover from hours and days spent using computer systems. Individuals have different personalities and attitudes and may develop positive or negative effects based on

what they experienced. The result of the correlation process also showed a negative correlation between Educational Attainment and Gender on the level ofInformation Security Awareness ($r (411) = -.412$, $p < .001$). The finding suggests merely that there is no significant relationship between the gender and the Educational Attainment of the employees relative to ISA. The gender does not determine the level of ISA.

V. CONCLUSION

Based on the outcome, the researcher concludes that the employee of the LGU has an adequate level of Information Security Awareness. Their self-perceived proficiency in Computer Networking and Information systems, computing knowledge and practices suggest that they have an Average understanding of the subject Information Security. The respondents are also somewhat knowledgeable of the risks, Threats and the types of data they utilize for online processing of transactions.

However, a need for regular orientation and Enforcing effective methods for information and security awareness because of the employee's unsafe practice of Downloading data from different sources. The employee is careless in their behaviour of not being selective about the type of information that they share and obtain from online sites and other network sources. These actions indicate that the awareness level about the rules and knowledge-required issues is still low. Furthermore, the development of an efficient and well-planned Information Security Awareness Training program must be conducted for the employees to maintain and protect their valuable information.

REFERENCES

1. Khan, H. U., &Gadhoum, Y. (2018). MEASURING INTERNET ADDICTION IN ARAB BASED KNOWLEDGE SOCIETIES: A CASE STUDY OF SAUDI ARABIA. *Journal of Theoretical & Applied Information Technology*, *96*(6).
2. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers& security*, *32*, 90-101.
3. Vicks, M. E. (2013). An examination of internet filtering and safety policy trends and issues in south carolina's.
4. Ching, M. R. D., Fabito, B. S., &Celis, N. J. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. *Advanced Science Letters*, *24*(10), 7042-7046.
5. Omorog, C. D., & Medina, R. P. (2018). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research*, *1*(4), 14-26.
6. Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A Theory on Information Security.
7. Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345361.
8. Justice, E. M., & Dornan, T. M. (2001). Metacognitive differences between traditional-age and nontraditional-age college employees. *Adult works quarterly*, *51*(3), 236-249.
9. Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330.
10. Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.
11. Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.
12. Omorog, C. D., & Medina, R. P. (2018). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research*, *1*(4), 14-26.
13. Newman, G. R., & McNally, M. M. (2005). Identity theft literature review.

14. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 6578.
15. Darmawan, N., Ooi, K. B., Chong, A. Y. L., & Venggadasallam, V. (2009). Security mechanism in computer network environment: a study of adoption status in Malaysian company. *Journal of Applied Sciences*, *9*(15), 2735-2743.
16. Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235.
17. Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.
18. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445.