Personal Computer Usage and Security Threats in the New Juaben Municipality, Ghana

Sarah Dsane-Nsor[1,*], Akyene Tetteh[2], Joseph A.K. Nsor[3]

[1]Computer Science Department, Koforidua Polytechnic,
P.O. Box KF 981, Koforidua, Ghana

[2]Department of Management Studies, University of Mines and Technology
P.O. Box 237, Tarkwa, Ghana

[3]Ghana Atomic Energy Commission
P.O. Box LG 80, Accra, Ghana

[*]*Corresponding author's email: saransor [AT] outlook.com*

ABSTRACT--- ***Personal computer (PC) usage in Ghana is on the rise but its security threat lacks behind because most PC owners do not know how to guard themselves and unaware of it danger. This paper studies the current state of PC security threat in the New Juaben Municipality, Eastern Region Ghana. SPSS was used to analyze the questionnaires gathered. The results suggest that (i) good authentic password does not guarantee PC owners safety, (ii) lapse in anti-virus routine update empowers malicious attackers to attack personal computers and (iii) PC's owners are not free from privacy threat so far as they subscribe to free email accounts.***

Keywords---- Personal Computer, Ghana, Security Threats

---

1. INTRODUCTION

There is no doubt that the use of information technology has increased in recent years. The daily major technological advancement breakthrough in the computer world raises new security threats. Ironically, it has also presented major security challenges and serious ethical questions, as more and more people move towards personal computing for privacy. Whiteman [1] defines computer security as "the quality and the state of a computer being secured." The meaning of computer security varies among computer literates: for software developers' security interferes with features and time to market while administrators and users security interferes with getting work done conveniently [2] In Ghana today, personal computer security to a large extent has been viewed with very low precedence, probably because of the unawareness of the eminent danger it possess. The general perception is that most third world countries are not able to keep up with the pace of the ever increasing threats on the Internet and other networks. Most of them are unaware of the threats or do not know how to protect themselves. This paper seeks to determine the current state of personal computer security, and to identify the prevalent threats against personal computer users in the New Juaben Municipality, in the Eastern Region of Ghana.

According to Chen et al. [3] in "Exploring internet security perceptions and practices in urban Ghana" suggests that personal computer users rely heavily on password as security in the usage of their social media. Even though passwords are deemed as security features to protect personal information on computers, most passwords according to Proctar et al. [4] are notoriously weak, hence easy to crack or guess. Their study concluded that increasing the minimum character length reduces crackability and increases security. Hence personal computer users are advised by Bleha et al. [5] to consider using phrases as passwords. Bonneau et al. [6] suggested that password threats are more prevalent. In minimizing these threats further authentication needs to be looked at.

The issue of software security is one that is very critical to individual computer users in Ghana. A significant number of the Ghanaian populace are below the minimum wage level, hence only a few are able to actually buy original software. In such an environment filled with pirated software what threats are personal computers owners facing? Personal computer owners are exposed to a wide range of vulnerabilities that attackers can exploit [7]. This paper seeks to re-emphasis that there are security flaws in both the hardware and software of the computer system. The software flaws based on some taxonomy created by some researchers: Landwehr et al [8] categorized software flaws into three namely operating system, support and application. The flaws in the operating system may come from the system initialization,

memory management, process scheduling, device management, file- management and authentication among others. Furthermore most emails subscribed by respondents where free emails hence susceptible to attacks and privacy issues over the Internet. The Internet is the most vulnerable electronic communication media, owing to its public nature and virtually without centralized control [9]. This paper provides an insight to security threats that external users, viruses, Internet and email software are likely to pose to individual PC owners, and what security actions they are likely to take in their everyday usage of the computer system. Some of these approaches may include authentication and identification [10], passwords and pass phrases [11, 12], Additional approaches include the use of policies, procedures, and computer monitoring [13].

2. PROBLEM DEFINITION

There is a huge gap between the way PC owners know, appreciate and protect their computers from the way corporate organizations handle their security. Why is this so? Are there security threats associated with the use of personal computers? Does the internet pose a threat to PC owners? If the answer is yes to any of the above questions then what actions are they taking to protect themselves? As more people tend to depend on technology how does a PC owner perceive computer security? What precautions are PC owners likely to take against possible computer threats? How important is computer security to the individual? Refer to figure 1.

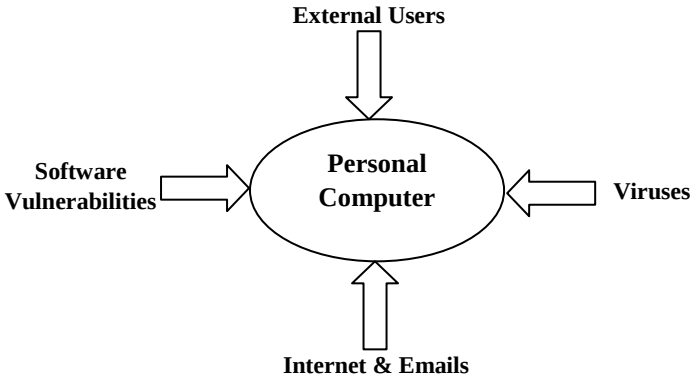

Figure 1; Prevalent Personal Computer Threats

3. METHODOLOGY

Structured interview, questionnaires were used to obtained the necessary information for this study. Respondents were selected based on convenience random sampling. In setting up the questionnaire certain prevalent areas were identified and categorized into Internet and emails, software securities, external users and passwords. Structured interviews were conducted face to face whiles the questionnaires were also administered randomly to a cross sectional respondent who owned Personal computers. In all 20 people were interviewed out of the total sample size of 230. 210 questionnaires were also randomly distributed, out of which only 180 (78%) were returned. Hence the analysis was based on 200 respondents. All the statistical procedures were performed using SPSS version 19.0.0 with p-value less than or equal to 0.10 considered statistically significant.

3.1 Results

Out of the entire respondents 166 participant representing 83% said they were using a good password, but further investigations revealed that 123 participant representing 61.5% where really using good password which were either strong or medium password. 38.5% representing 77 participant passwords were weak. This is shown in Table 1 below. Only 3% of users interviewed did not use password at all, this is also the default setting in Windows.

An external party (user) is anyone who uses (has access) to the content of the PC besides the owner. Most (73% of respondents representing 146 participants) PC owners agreed that external users are a threat to their computers refers to Table 2 below. Whereas 52 participants representing 26% of respondents do not perceive external users as threat and 1% do not know whether external users pose a threat to their PC security. Out of the entire 200 participants 110 participants representing 55% allowed their PC's to be accessed by external users and the remaining 90 participants did not allow their PC's to be used external parties. The participants who allowed their PC's to used, were further categorized into two, those who monitor the use of their PC's by external users and those who did not monitor. A total of 87 participants representing 43.5% said they monitored the use of their PC's by external users. Only 22.5% of respondents were not exposed to the threats of external user.

Table 1: Nature of Password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Weak	77	38.5	38.5	38.5
	Medium	85	42.5	42.5	81.0
	Strong	38	19.0	19.0	100.0
	Total	200	100.0	100.0	

Table 2: External Users

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	146	73.0	73.0	73.0
	No	52	26.0	26.0	99.0
	I dont know	2	1.0	1.0	100.0
	Total	200	100.0	100.0	

About 96.5% of respondents who took part in the user survey described computer virus or worm as "a malicious software / code that can infect and harm the computer in various ways causing a malfunction". 182 users had an anti-virus program installed, but some of the anti-virus programs were not set to update automatically. Table 3 below shows the frequency distribution of the various types of anti-virus programs participants had installed on their PC's.

The majority of participants making up 74.5% knew, or thought they knew what a firewall is (149/200), but not all of them actually had a firewall installed and enabled. 121 participant representing 60.5% of the people were familiar with the term spyware but only 69 participants representing 34.5% did have antispyware programs installed. Most of the users in the survey said they knew how to use email attachments in a secure way, about 150 participants representing 75.0%. This statistics is confirmed in the Table 4 below with mode value of 1. Only 50 participants did not know how to use email attachments securely. 130 users did not respond or ignored to spam, and didn't unsubscribe to them. This means that 130 respondents "no" to spam and did not subscribe to them representing a mode value of 2 in Table 4. Most users also ignored ads telling them that their computer has been hacked (107 out of 200). Almost an equal number responded to these malicious ads (93 participants representing 46.5%).

Table 3: Anti-Virus Programs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Avast / Avira	82	41.0	41.0	41.0
	McAfee	38	19.0	19.0	60.0
	Norton	77	38.5	38.5	98.5
	Others	3	1.5	1.5	100.0
	Total	200	100.0	100.0	

Table 4: Internet and Email

		Do you ignore ads that tell you that your computer has been hacked?	Do you respond to spam, even to "unsubscribe"?	Do you know how to use email attachments securely?
N	Valid	200	200	200
	Missing	0	0	0
Median		1.00	2.00	1.00
Mode		1	2	1

3.2 Discussions

On the whole this paper has pointed out that personal computer owners are conscious of their security. The weak password has between 2 to 8 characters and easily predictable. The medium password for the purposes of this paper is defined as a string of 8 or more characters, but that may be easy to predict. Such as name of children, spouse, close friend or telephone number among others. The strong password on the other is defined as a string of more than 8 characters with a combination of special symbols and numbers, easy to recollect but difficult to predict. Over 80% of respondents said "YES", to having good password because their systems had log in password, but as it turned out only about 60% were actually using a good password. 60% of respondents' is a very significant number that goes to prove that individual PC owners appreciates and prioritizes their security in terms of protecting their data from external users. There is no empirical evidence to proof however that having a good (i.e. medium or strong) password will actually reduce harm to the PC. This implies that having a good password is not a guarantee that your computer is free from harm.

PC owners use passwords as authentication to protect their user accounts and sensitive data from intrusion by external user. Even though majority of respondents agreed that external users are a threat to their PC's, they did very little to monitor their use of the computer system because owners of PC feel external users are uncomfortable with their monitoring approach. Besides respondents also believes external users are reckless in their usage of their computers (This is parallels with [6]).

Updating the operating system, firewall, antivirus and anti-spyware regularly from trusted sources, will decrease the possibility of being infected by worms or viruses. Most viruses and worms propagate and infect PC's over the internet mostly through emails attachments and secondary storage devices. In this study it was evident that most users allowed external parties to use their systems with minimal or no monitoring mechanisms. This in itself is a threat to security, as these users easily access untrusted sources and easily attached secondary storage devices (which may be infected) to PC's without scanning. Malicious attackers are working around the clock to infect PC's owners with viruses. This implies PC's owners should not take their routine update for granted since any lapses may cause harm. Routine updates are also crucial especially because of software vulnerabilities.

This paper points out that security holes in some software are to blame for many of the problems the ordinary computer owner faces. There is not much the user can do about these security holes, except by updating the software regularly. Many programs today offers auto-updating functionality, fortunately as shown in the user survey most users are at ease with the auto-updating feature of their software. That way they don't have to worry about when they did the last update and so on.

Another very sensitive issue that raises eyebrow is that of privacy over the Internet. All PC owners in the survey had subscribed to free email accounts. These emails as marketing strategies make their clients (PC owners) feel they are anonymous when in fact; their personal details are being sold to third party organizations and institutions for market research, data mining and the like. These can lead to even more serious privacy threats such as phishing, customer profiling and spamming. PC owners today have serious concerns about their privacy and security while using the Internet for studies, business and other activities. They are apprehensive about the protection and confidentiality of their data.

4. CONCLUSION AND RECOMMENDATIONS

PC owners use passwords for authentication and protection of their data, but there is no relations between having a good password and preventing harm to the computer. This study has confirmed that PC owners are particularly concerned about their privacy over the internet. However, subscribing to free email accounts and downloading pirated software from untrusted sources can be detrimental to their security concerns. Significantly PC owners can do very little about software vulnerabilities hence to ensure the safety and confidentiality of data, PC owners are advised to only visit trusted sources over the internet, buy and use original software, update their systems periodically and put in place monitoring schemes for external users. Since the issue of software security is quite sensitive, PC owners can do very little about it owing to their economic strength. A potential limitation that exists when surveying individuals about sensitive topic such as security is response distortion caused by the desire of the respondent to provide socially desirable answers and sample size.

5. REFERENCES

[1] Whitman M.E, Mattord H.J., Principle of Information Security, Thomson Course Technology, USA, 2003.
[2] Lampson B.W., "Computer security in the real world", IEEE Computer, vol. 37, pp. 37-46, 2004.
[3] Chen J., Paik M., McCabe K., "Exploring Internet Security Perceptions and Practices in Urban Ghana", In Symposium on Usable Privacy and Security (SOUPS), 2014.
[4] Proctor R.W., Lien M.C., Vu K.P.L. Schultz E.E., Salvendy G., "Improving computer security for authentication of users: Influence of proactive password restrictions", Behavior Research Methods, Instruments & Computers, vol. 34, no. 2, pp. 163-169, 2002.
[5] Bleha, S., Slivinsky, C., Hussien, B., "Computer-access security systems using keystroke dynamics", Pattern Analysis and Machine Intelligence, IEEE Transactions, vol. 12, no. 12, pp. 1217-1222, 1990.

[6] Bonneau, J., Herley, C., van Oorschot, P. C., Stajano, F., "Passwords and the evolution of imperfect authentication", Communications of the ACM, vol. 58, no. 7, pp. 78-87, 2015.
[7] McGraw, G., Software security: Building Security In (Vol. 1), Addison-Wesley Professional, USA, 2006.
[8] Landwehr, Carl E., Alan R. Bull, John P. McDermott, and William S. Choi., "A taxonomy of computer program security flaws", ACM Computing Surveys (CSUR) vol. 26, no. 3, pp. 211-254, 1994.
[9] Banday, M. T., Qadri, J. A., & Shah, N. A., "Study of Botnets and their threats to Internet Security", Working Papers on Information Security, 2009.
[10] Zviran, M., & Erlich, Z., "Identification and authentication: technology and implementation issues", Communications of the Association for Information Systems, vol. 17, no. 1, pp. 1- 4, 2006.
[11] Keith, M., Shao, B., & Steinbart, P., "A behavioral analysis of passphrase design and effectiveness", Journal of the Association for Information Systems, vol. 10, no. 2, pp. 63-89, 2009.
[12] Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J., "Improving multiple-password recall: An empirical study", European Journal of Information Systems, vol. 18, no. 2, pp. 165-176, 2009.
[13] Ariss, S. S. "Computer monitoring: benefits and pitfalls facing management", Information & Management, vol. 39, no. 7, pp. 553-558, 2002.

Sarah Dsane-Nsor is a Computer Science lecturer of Koforidua Polytechnic. She received her Masters Degree in Business Information Technology from Kwame Nkrumah University of Science and Technology, Kumasi. She pursued Computer Science at All Nations University College, Koforidua. Her fields of research interests include Computer security, E- commerces, Wireless and Mobile Computing.

Akyene Tetteh is a Lecturer in the field of Supply Chain Management, in the Department of Management Studies, University of Mines and Technology. He received his PhD in Economic Management Decision Making and Analysis, from the school of Management Science & Engineering, Donghua University, China, MSC in Economics International Finance, from Shanghai University of Finance and Economics, China and BSC in Mineral Engineering from University of Mines and Technology, Ghana. His fields of research interests include Supply Chain Management, E-commerce and Decision Science.

Joseph A.K Nsor is a Master student of Telecommunications Engineering at Kwame Nkrumah University of Science and Technology, Kumasi. He received his bachelor's degree in Electronics Communication Engineering from All Nations University College, Koforidua. His fields of research interests include Radio Frequency Interference, System Performance Modeling and Computer Network Security.