Information Security Issues Facing Internet Café Users

Alfred Thaga Kgopa

***Abstract*--** Information security threats destroy the value of e-business. The owners of Internet cafés extend the freedom of use of Internet access to the community but they fail to tighten their computer security to safeguard the private information of their customers. The aim of this study is to provide information for improving information security in the Internet Cafe strategically to ensure data privacy, data integrity, risk management and security compliance. The study investigates the information security issues that are faced by users of Internet cafés and explores the effects of these issues. It shows how users can improve their physical security to reach higher standards of information privacy over the Internet.

Much research has been conducted on the subject of information security but this research presented here focuses mainly on the issues that face users of Internet cafés and the improvement of public computer securities to safeguard users' information from hackers and malware. The study focuses on Internet cafes and users located in Pretoria, South Africa.

The studies found that majority of users are affected by information security issues such as viruses, scam, online harassment, information privacy and many more. The study also found that the users were also responsible to those issues due to their behaviour towards information security technologies such as antivirus software, password and physical security. User where not using strong password, they were forgetting to logout from their accounts, some were working on computers that the antivirus software was turned off.

***Keywords*---** Information, Information Security, Internet, Internet Cafe, South Africa

I. Introduction

THIS research deals with information security issues that are faced by Internet café users. The study will identify those issues and challenges that Internet café owners face in terms of implementing security tools in order to cover all angles of data integrity.

Whether one is sending messages by email, uploading or downloading information, making online hotel and flight bookings, checking or updating online banking details, making online account payments or conducting research via the search engines, there is a need of privacy for one's information [10].

Alfred Kgopa was with telecommunication company Telkom SA, Centurion 61 Oak Avenue. He is now employed and study at Tshwane University of Technology, in South Africa (SA), Pretoria. Phone: +2782 094 6339; email: kgopaat@tut.ac.za. His study leader is Prof Ray Kekwaletswe who is currently with Witwatersrand University, in SA.

According to Reference [7], if one is using an Internet café, there is always the possibility that some malicious café owner will capture one's confidential information. Moreover, Reference [6] believes that one should never trust the person next to you when using sensitive information such as login details and entering or viewing private data on the Internet. This shows that users face a serious problem and need to be extra vigilant when using the Internet in public spaces.

The following statement from one of the Internet café study participants supports Reference [7] assertion that one has to be careful regarding malicious café owners:

"*There was someone who logged on the banking webpage to do online banking. After a few days when he tried to withdraw money he found that there is nothing on his account. When he went to the bank they said he transferred his money to two different accounts on the certain day, when he checked he knows only one transfer that he did in the Internet café, the other transfer he doesn't know it happened on the same day. When the guy goes to the Internet café that he used, to check what might have happened he found that there is a webcam that is installed on each and every computer of the Internet café and the webcam is hanging on the computer screen facing the computer keyboard, then he realized that this webcams are used to capture every key you are using on the keyboard.*"

So, this shows that is true that malicious café owner can capture one's confidential information.

II. Problem Statement

Users of Internet cafés face serious challenges when it comes to information security in Internet cafés. The Internet café owners usually fail to cover all angles of information security, and in this way they breach the trust of their customers. Although they increase the freedom of customers to use the Internet, they don't improve their computer security to protect customer information from hackers and malicious damage.

III. Research Goal And Objectives

The goal of this study is to provide information for addressing information security issues in Internet cafés

A. Research Objectives

Below are the objectives of this research:

- To identify issues facing Internet café users.

- To identify factors contributing to issues of information security in Internet cafés.
- To identify the challenges that Internet café owners face in implementing IT security.

IV. Research Methodology

Methodology that was used for this study has been chosen in order to acquire information and deduce conclusions about how information can be secured in the internet café and how user can secure their sensitive information while surfing in the internet. On this research it was deemed appropriate to use the interpretive research method. And the strategy is to collect data from users who accesses Internet in the Internet cafés around Pretoria central, in South Africa.

V. Data collection method

The data was collected from a variety of sources to ensure that the researcher had enough information to work from. For the purpose of this research and in order to achieve the objectives of this research, both primary and secondary data was collected. The secondary data provided a backdrop for the researcher in order to find the major issues facing Internet café users and for the reader to get a thorough understanding of the survey outcome, and also to understand the ultimate findings of the research. The following data collection method has been used.

A. Questionnaires

The questionnaire was typed out using Microsoft Word and printed to be distributed and collected physically by the researcher at three Internet cafés around Pretoria central. Most of the questions included multiple-choice questions, as well as yes or no, true or false questions. Some of the questions asked similarly-worded questions in order to cross-check answers, e.g. if the answer to a question such as "Have you ever been affected by any issues when using the Internet café?" is NO, and yet the user indicated some issues in the list of categorized issues related to the use of Internet cafés, this shows a discrepancy and may imply that the user was not always entirely accurate in their responses.

B. Observation

Participant observation was used, and the features such as visual observation were applied to observe things such as how the physical security in the Internet cafés is implemented and also how the physical network of computers was connected. Not only was there visual observation, but the researcher also visited two Internet cafés as a customer in order to verify some findings from the questionnaires.

VI. Sampling

The researcher delivered the questionnaires at three Internet cafés in Pretoria. The aim of the researcher was to get at least 20 users per Internet café to make up a total of 60 users. The table below provides a summary of the sampling results.

Table I
Sampling Of Participants

Sampling of Users of Internet Cafés in Pretoria			
Internet café	**Day 1**	**Day 2**	**Sample Size**
Pretoria Central 1	12	15	27
Pretoria Central 2	9	17	26
Pretoria Sunnyside	19	0	19
Total Size	40	32	72

The questionnaire was thus distributed randomly at the Internet cafés, and a total of 72 users participated in the survey.

VII. Data Analysis

During the data analysis some of the questionnaires had to be discarded because they had been completed incorrectly or the important questions had not been answered. For instance, the participant answered only relatively minor questions relating to the number of hours they spend in Internet cafés, their age, gender and so forth, which are of minor importance in this research study. The researcher thus decided not to include questionnaires that were not properly and fully completed. There were 9 questionnaires that were discarded, bringing down the sampling population to 63 participants. So the questionnaire findings of this research paper reflect the results of 63 users who participated in the survey.

VIII. Finding and Data Analysis

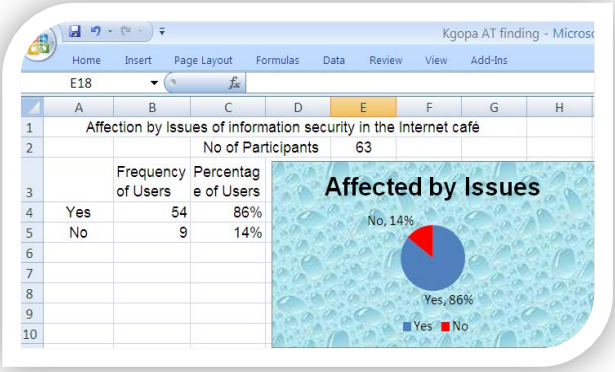

Fig. 1 Users affected by issues of Internet cafe

Fig. 1 results show that users of Internet cafés in Pretoria have been affected by issues of information security. Almost 86% of the participants agreed that they had experienced information security issues.

A follow-up question was used for users who replied "Yes" to "Are you comfortable using your confidential information in the computers of Internet cafe?" In their answers they had to specify what they have been doing with confidential

information they had ever used in the Internet cafe. Below are some of the answers:

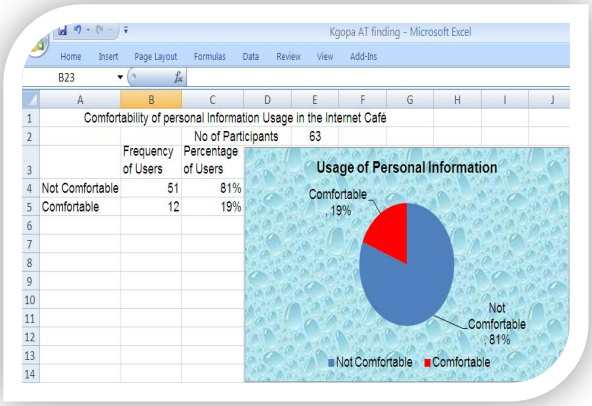

Fig. 2 Comfortable of using personal information

User: "*I connect to the SARS website for e-filling to apply for a tax return.*"

User: "*I was purchasing the car and the car dealer asked me to email my pay slip and bank statement to apply for finance, then I mailed them from the Internet café.*"

Some Users said: "*They used to attach their CV, qualifications and ID on career junction and other vacancies website, and email them from the Internet café.*"

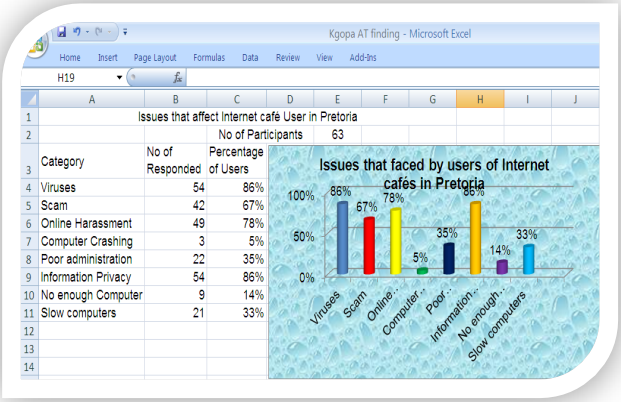

Fig. 3 Issues of Internet café

The results of fig. 3 the issues that affect the users of Internet cafés in Pretoria are important as it was the objective of this study to find out what issues regarding the use of Internet cafes affect users. It was found that most users have been affected by issues in terms of information security at Internet cafes and it was also found that most users did not feel comfortable transmitting any personal information when using the computers in Internet cafés.

One of the objectives of this study was to identify issues experienced by Internet café users. The findings of fig. 3 reflect some of these issues, and thus need to be addressed and tips or guidelines need to be given to users and Internet Café owners on how to avoid these issues.

A. Analysis of Issues and the Tips to Stay Safe

- Issue no 1: Viruses

According to the findings of this study, a large percentage of users (86%) complained about viruses. It is common knowledge that computer security is a major problem and that if not taken seriously, customers or important information stored on the computer or storage device can be lost. Moreover, lost data is not replaceable unless you have a backup.

For example, some users said that, "*when they open their USB in the Internet café they get some files that they never save and all the folders appear as short-cut and when they open them they don't open.*"

Another users said the following: "*When they use their USB in other computers after using them in the Internet café, files that are saved on the USB turn to white icons sort of setup file and when they scan the USB those file are deleted.*" In other words, they have lost their information.

- Issue no: 2 Information Privacy

The result about uncomfortable of information privacy from the questionnaire responded by Internet Café user in Pretoria is high by 86% and this almost 100% of users who said they were affected by this issue. So this shows that users need information privacy in the Internet Café

- Issue no: 3 Online Harassment

Users had different views about online harassment, for example:

User 1: "*I forget to logout my Facebook account and the next thing my friends phone me and ask why I type such stupid message on Facebook. I was surprised then I immediately go to the nearest Internet café. When I login I found that someone has typed embarrassing message and post it on my Facebook wall. When I check the time that the message was posted is just fewer minutes after I left from the Internet café I used earlier.*"

User 2: "*I don't know how this has happened but somebody if not him accepted this other boy as my Facebook friend and the next thing he proposed me on the Facebook and when I denied him, he started to send me insult message on the Facebook and imagine he was posting insulting messages on the wall messages so that everyone could see.*"

Online harassment is one of the highest ranking issues that affect the users of Internet cafés in Pretoria. About 78% of users complain about online harassment. They felt unsafe or even felt they were being bullied by other Internet users. Online harassment often takes place after users have made friends online. These type of online friendships are risky

because you are making friends with a stranger who might give you false information about themselves whereas you are giving this "friend" true information about yourself. Such online "friends" might send mail that contains embarrassing content or they can take your personal information that you shared with them and distribute it to other people thereby causing you huge embarrassment.

- Issue no 4: Scam

With regard to online scamming, one participant said the following: *"I played online competition to predict the score for Bafana Bafana vs. France in world cup 2010, the webpage required me to put my bank details. I thought is for incase I win the competition they will deposit the money. At the end of the month the amount of R210.00 (±$21 USD) was deducted from my account, when I go to bank and ask them, the bank teller told me that I have joined the life cover. When I ask the day that I have joined I found that it is that day when I play online competition in the Internet café."*

Scamming is a fraudulent attempt to get a user to part with their money. Most Internet scams take place without being noticed by the victim. The user will only know that they have been scammed when money is deducted from their bank account or credit card [8]. Scamming is another issue that affects users of Internet cafés, and if they are not careful the users can even be scammed by other users in the same Internet café or by the Internet café owner or administrators. The findings in this regard showed that 67% of the Internet café users complained about scams.

Is common that you can be scammed these days not only on the Internet Cafés, they have many ways to approach the victims. The scammers can send you email to inform you about an offer, or they can send you an SMS, or sometime may even call you in your personal cell number.

- Issue no 5: Poor Administration

Poor administration is one of the issues that need to be address by Internet café owners. Customers can only complain if they are not satisfied with the maintenance of the Internet café. Poor maintenance can ruin the business. Internet café owners thus need to ensure that their equipment is in good condition in order to keep their customers happy. Also if the person who is working as an administrator does not know how to run an Internet café, the business is at risk in terms of IT security.

- Issue no 6 & 7: Slow Computers and Computer Crushes

Only 33% of the users were not satisfied with the speed of the computers. Another problem that will result in the loss of customers is if the computers keep crashing. When a computer is very slow, one cannot install the latest software and play certain games. The computers will crash often if the latest windows version is installed or users play online games. Although an owner may not be able to afford the fastest computers for the Internet cafe, slow computers should not be purchased. When the computers were checked by the researcher, it appeared that most of them were in good condition, however, the researcher noticed that most of them were not branded computers and it thus appears that Internet café owners build their own computers. Most of Internet cafés that were visited also sold computer hardware and the employees in the Internet cafés also fixed computers which points to the fact that they would be able to build their own computers. The owners of Internet cafés need to buy branded computers because these are usually quality computers.

The problem of computers crashing is also caused by poor quality computers. When building your own computer, different branded parts might be used and some parts might not even be branded, and thus they might also not be compatible with each other. As a result, computers will crash or perform very slowly.

B. Observation Results and Suggested Solutions

- Viruses and Anti Virus Software

The researcher visited two Internet cafés as a customer. The researcher's aim was to verify the results from the questionnaire with regard to the presence of viruses that affect users making use of Internet cafés and also to check how information security is implemented in these cafés. A new, empty USB was used to copy information from the Internet at the Internet café and another USB was used in another Internet café. This USB was not new, but it was scanned first for viruses and no viruses were detected. So it was used to copy information but not from the Internet but just pictures such as a sample picture from the local drive at the Internet café.

The researcher used his computer to scan the two USBs after having used them at the Internet cafes and his findings supported the findings of the survey. There was a popup message immediately when the USBs were connected to the laptop. The message appeared in the notification area and read "potentially harmful software detected". The researcher then clicked on the message, which suggested scanning the USB, which was done. While the antivirus software was busy scanning, more messages about the harmful software detection kept appearing.

Fig. 4 is the print screen that was made from the USB that was used in the first Internet Café. The print screen shows the files affected by the viruses and also indicates the virus names.

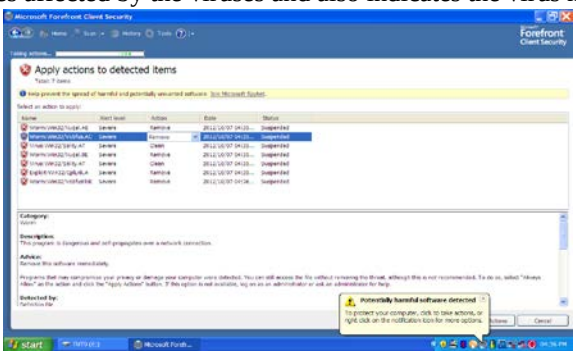

Fig. 4 Virus detection results

The following is a snapshot of the virus detection results from the second USB that was used in the second Internet café.

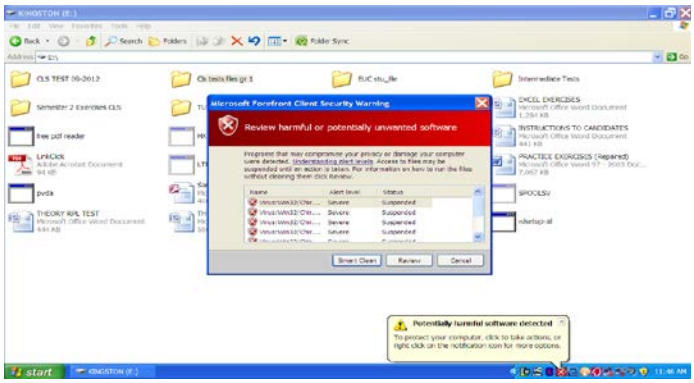

Fig. 5 Virus scan results

One of the USB showed information that was never stored on the USB and the original information was only showed as a white icons. This is an interesting finding because this kind of virus was first detected in 2010 but it still exists on some computers. The virus hides the original information that is stored in a folder on the storage device and it shows the shortcut, and anyone not familiar with this virus will think that the data has been lost.

For those who are still confronted with this virus, below are some tips to remove it. Once the USB is connected and only the shortcut of the stored data is visible or there is nothing on the USB, the following steps should be followed because even if the scan disk with antivirus is run, the data will still be hidden.

Click tools on the tool bar,

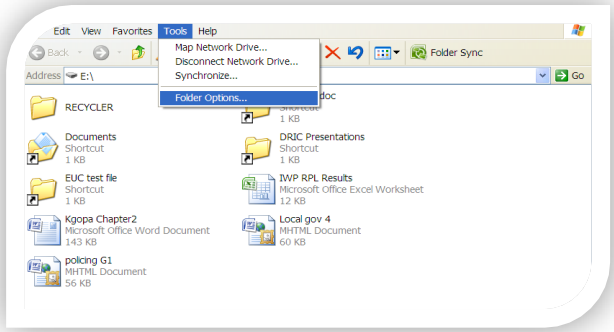

Fig. 6 Virus formatting step 1

then select folder options.

After selecting the folder options, fig. 7 folder options window will appear,

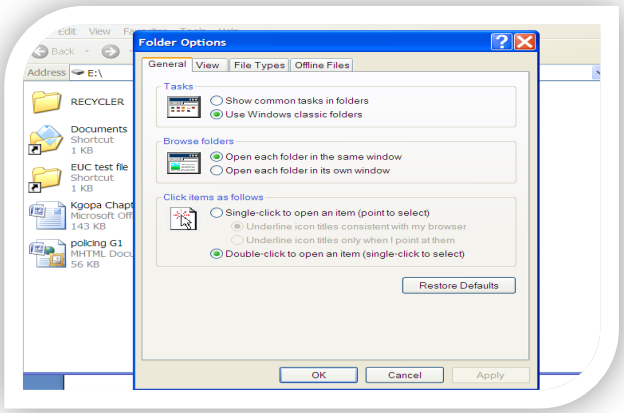

Fig. 7 Virus formatting step 2

Click view tap button of folder options window,

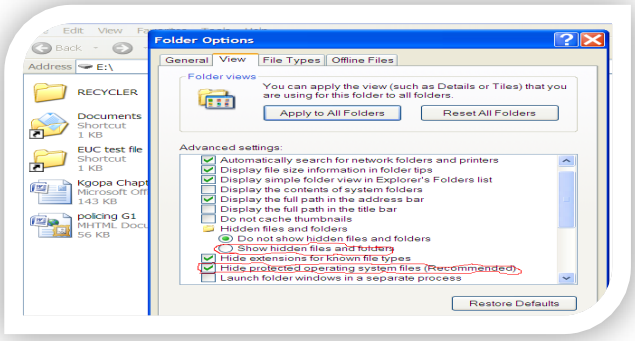

Fig. 8 Virus formatting step 3

Under view check “Hidden files and Folder” then select show hidden files and folders, also uncheck “hide protected operating system files (recommended)”. Once you uncheck the checked box the message will pop up and will ask you whether you are sure that you want to display the files.

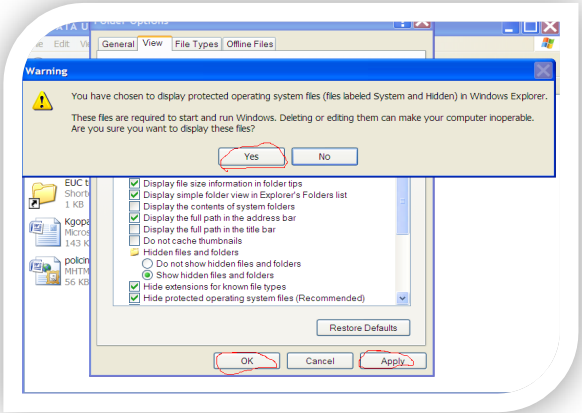

Fig. 9 Virus formatting step 4

Click “Yes” and the four buttons at the bottom of the message click “Apply” then click “OK”.

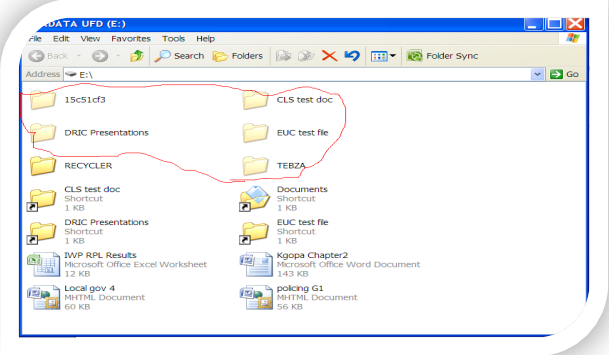

Fig. 10 Virus formatting step 5

After the above steps have been completed, all the hidden files and protected files will be displayed but if the computer does not have good and effective antivirus software, these steps will have to be repeated every time you want to use the information on the affected USB. The information keeps hiding until your antivirus software manages to clean or remove the virus, and the only way to clean it is to make sure that your computer security is up to date.

C. Physical Security

In one of the Internet cafés there was some other network hardware that could easily be accessed by the public. It should be remembered that it is not safe to store network equipment in easily accessible places.

During the observation process, the researcher noticed one user who went outside to answer cell a phone. During this time, the user left the Facebook page open without logging out. The user was opening himself up to problems had he returned from his phone call only to find his session had ended, he had thus been logged out and the next user who worked on that computer would find his Facebook account still active. In this case, a malicious user could have easily posted a negative message with regard to the account owner. This is just an example of the issues that face people using the Internet on public computers and which they should be aware of.

D. Network Layout

As mentioned in section C about physical security, during one observation session, the researcher noted some network hardware that was exposed to the public and also that the door to the server room was not closed. The users were able to see some of the hardware such as the Asymmetric Digital Subscriber line (ADSL) modem and hubs that should be locked away from the public area.

Putting network hardware such as a modem into a public space is very dangerous because malicious users could copy the product serial number and use it to connect to your network wirelessly. Most of the Internet service providers (ISP) such as Telkom and MWeb release their internet modems with the same default password and to connect wirelessly you need to know the product serial number and the password. Thus if the default password that comes with the modem is not changed and an unauthorized person obtains the product serial number, that person can use the data bundle wirelessly without you noticing.

In one of the Internet cafés the computers were connected to the ADSL modem through the hub. For instance, an ADSL had four ports and each port was split into four port hubs and 16 computers where directly connected to the hubs, i.e. there were four computers per port. This kind of connection appeared to have no server because all the 16 computers were labeled User 1 to User 16. Moreover, the administrator of the Internet café gave the researcher a piece of paper indicating the start time and the end time for the Internet session, the start time being 11:21 and the end time 12:21. The fact that four hubs were connected to a four-port ADSL with 16 user computers implies that there was no server to serve as a firewall in order to monitor security. Moreover, the fact that the researcher was given a piece of paper with the start and end times, points to the fact that there was no Internet café software to take control of the administration computer.

IX. Recommendations

A. Recommendations to prevent unauthorized user account access

- Accounts should never be shared.
- Password should be at least the minimum of 8 characters long [5].
- Password should be formulated of mixed characters such as letters (both lower and upper case), special character and numbers [3].
- Avoid using name of account, your names or family member names, date of birth, social security number, your business name or any other information that can be easily discovered as your password [5].
- Avoid writing down the password
- Password should be regularly change in an interval of at least 1 to 3 months, and should also be changed immediately there is suspicions of been compromised [5].
- Use different password for files and for loggings on the Internet [5].

B. Recommendations to Owners of Internet Cafés for Physical Security

- Try to employ reliable people who will be responsible for data security and system administration in your Internet café.
- You can use computer lock systems like special cabinet or durable cables to tie your computers to the desk. Keep the server room close at all the time only

the Internet café administrator or technicians can have the keys to access it [3].

- Devices such as security video cameras can be also installed in the premises.
- Never leave the Internet café with the stranger or without any one who is not an employee and assume that they will check out for you will you are going out to buy something or to do whatever [1].
- Backup your file, Internet café software and other important data regularly and store the copies in another location, because if anything can happen as data loss it might be expensive to get that again and go back to track and service your customers. Some windows include backup programs and also there are some third party vendors who sell and support this type of service [3].
- Use uninterrupted power supply and avoid overloading [1].

C. Recommendations for Virus Issues.

- Always purchase a copy of latest version or use a trial version of antivirus software and install it on your computer. Most antivirus software offer 3 month trial, once you purchase the software then you get the full vision and other features such as additional firewall protection, feature to scan any web sites you visit, and others [9].
- After installing the antivirus software in all computers of the Internet café, scan all of them for any possible viruses that could be hiding or spread in the computers [4].
- Make sure you get the subscription of antivirus update to get notices of virus, spyware definitions and the patches for the program.
- Setup the virus scan time to occur every time when you switch-on your computer [9].
- Make sure your antivirus software will scan all the external storage devices such as USB and external hard drive when the user of your Internet café attached them in your computers [4].

D. Recommendations for Information Privacy Issues.

- Remove key loggers- this is a device capable of tracing all the keystrokes and transferring the information to a distant computer. So you need to physically check around the computer you are using in the Internet café otherwise you may lose your confidential data [1].
- Don't save your confidential information in the computers of Internet [6].
- Don't complete any forms on the Internet unless you really want something from that website.
- While you are checking emails or using any other service where you need to enter your username and password, remember to "sign out" or "log out" when you have finished [1].
- Delete cookies and history of the website you have visited from the computer you are using [4].
- Consider creating a separate email address for information that is not personal and use an alias instead of your name [4].
- Never leave your device driver such as USB or external hard drive that contains your personal information displayed in a public area especially in the Internet café [7].
- Don't give out your banking or credit card details indiscriminately.

E. Recommendation for Network setup

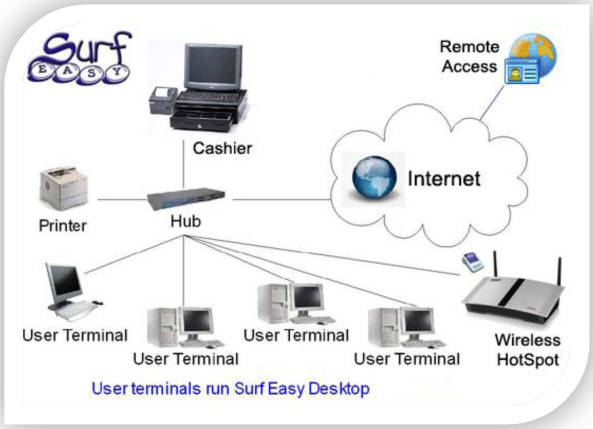

Fig. 11 Network setup layout. Source [11]

For better Administration in the Internet café, this network setup layout is recommended for Internet cafés around Pretoria because most of them they run their business in the traditional way. An administrator will accept payment from users and logs on for users on available computers through the administrative computer that is installed Internet café administration software. Once the user has made the payment then they can go to the user terminal and use the computer to access the Internet. It is also recommended that the server room must always be locked and only authorized people should access it.

REFERENCES

[1] D. Debajyoti, Security *Tips to Follow at a Cyber Cafe – Browse Safe & Protect Privacy.* Henderabad, 2009 [Online]. Available from: http://www.snaphow.com/1109/security-tips-to-follow-at-a-cyber-cafe-browse-safe-protect-privacy [Accessed: 05 October 2012].

[2] D. Defranza, 5 tips every traveler should know about internet security. Published: Matador Network, 2008 [Online]. Available from: http://matadornetwork.com/bnt/5-tips-every-traveler-should-know-about-internet-security/ [Accessed: 16 October 2012].

[3] S. Hernan, M. McDowell, & J. Rafail, *Choosing and Protecting Passwords.* United State: Published by United State Computer Emergency Readiness Team, *2004* [Online]. Available from: http://www.us-cert.gov/cas/tips/ST04-002.html. [Accessed: 16 October 2012].

[4] M. Mcdowell, *How can you protect both your personal and work-related data?* United Sated: Published by United State Computer Emergency Readiness Team 2006 [Online]. Available from: http://www.us-cert.gov/cas/tips/ST06-008.html [Accessed on: 14 October 2012].

[5] Microsoft, *Tips for creating strong password*. Published by Microsoft, 2013 [Online]. Available from: http://www.microsoft.com/security/online-privacy/passwords-create.aspx [Accessed: 14 October 2012].

[6] L. Notenboom, Keeping Your Computer Save on the Internet: *The Electronic Journal of Internet Safety, 2008,* Vol. 1, no 2, pp. 1-40.

[7] C Roseberry, Top 8 Tips for Using Internet Cafés. United kingdom: Published by BSI Global, 2009 [Online]. Available from: http://mobileoffice.about.com/od/overseasinternetaccess/tp/internetcafe.htm [Accessed: 05 September 2012].

[8] ScamWatch, *Online scam*. Australia: published by Australian Competition and Consumer Commission (ACCC) 2012 [Online]. Available from: http://www.scamwatch.gov.au/ content /index. phtml/tag/onlinescams [Accessed on: 11 September 2012].

[9] M Stamp, Information security principles and practice. Hoboken, New Jersey. JohnWiley& Sons 2006, Inc.ISBN-10 0-471-73848-4.

[10] A. Tilley, Securing Internet Cafés while maximizing customer freedom. Brisbane, Australia: Published by SANS Institute, 2005, pp. 1-21.

[11] ARINDA. A guide to start an Internet café business. Published by Surf Easy. 2012. Available from: http://www.arinda.com [Accessed: 22 November 2012].