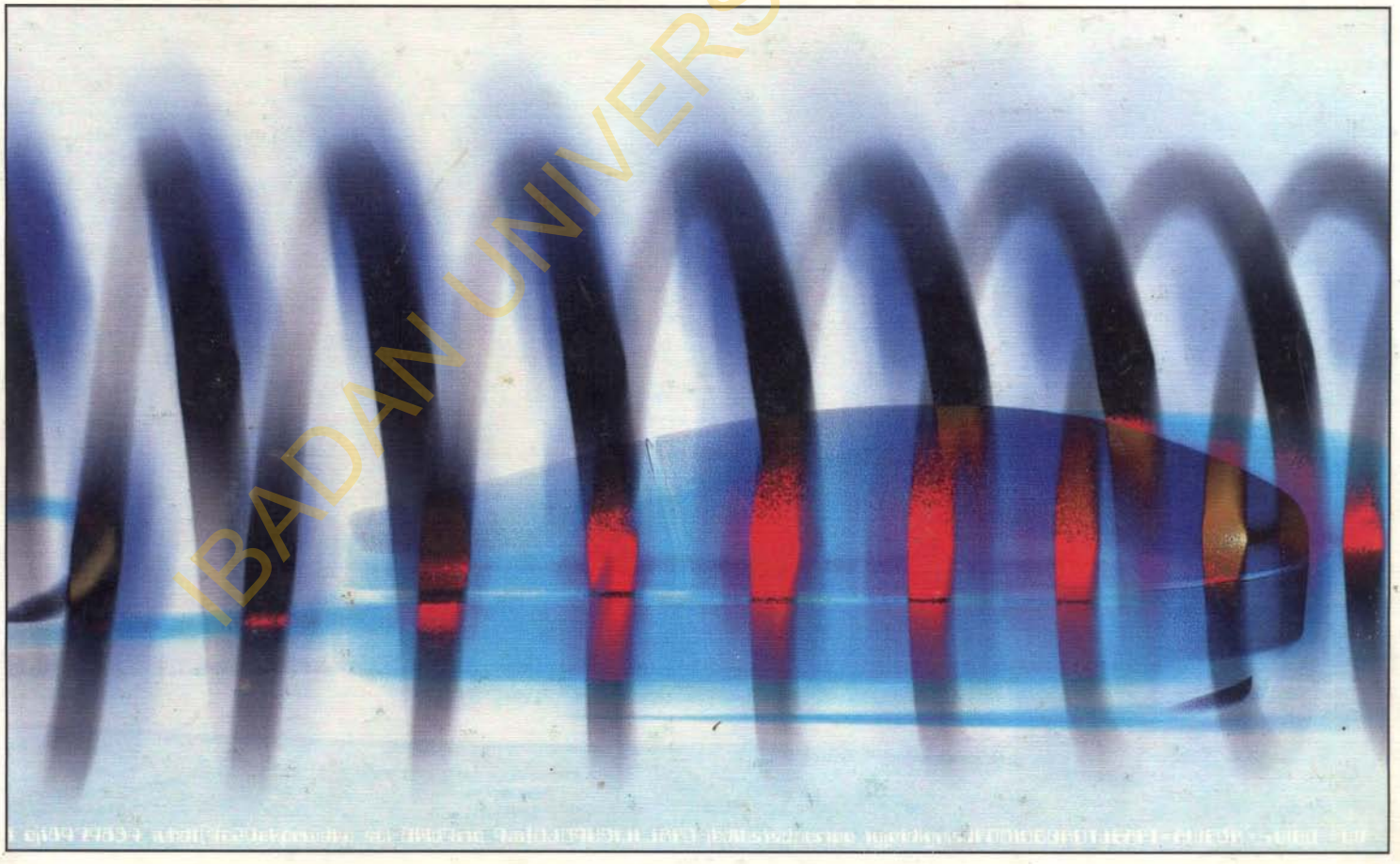
PREMIER REFERENCE SOURCE

SECURITY AND SOFTWARE FOR CYBERCAFÉS



ESHARENANA E. ADOMI

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Copy Editor: Joy Langel
Typesetter: Jeff Ash
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Security and software for cybercafes / Esharenana E. Adomi, editor.

p. cm.

Summary: "This Book provides relevant theoretical frameworks and current empirical research findings on the security measures and software necessary for cybercafes, offering information technology professionals, scholars, researchers, and educators detailed knowledge and understanding of this innovative and leading-edge issue, both in industrialized and developing countries"--Provided by publisher.

ISBN 978-1-59904-903-8 (hbk.) -- ISBN 978-1-59904-905-2 (e-book)

1. Cybercafes--Security measures. 2. Computer security. I. Adomi, Esharenana E.

HE7581.5.S43 2008

647.95--dc22

2008001873

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Table of Contents

Section III
Cybercafés, Cyber Laws, and Control of Cyber Crime

Chapter VI
Cybercafé Physical and Electronic Security Issues

Adetoun A. Oyelude
University of Ibadan, Nigeria

Cecilia O. Bolajoko Adewumi
University of Ibadan, Nigeria

ABSTRACT

An overview of physical and electronic security issues in cybercafés in Ibadan city, Nigeria is presented in this chapter. The security measures taken by cybercafé managers for physical and electronic facilities and clients also, were observed in an in-depth study of sixty cybercafés purposively selected for location, popularity, and wide range of services offered, over a period of 2 months. Participatory observation, in-depth interview, and questionnaire methods were adopted, using trained research assistants. Results of the findings showed that cybercafé operators are having a hard time, some folding up due to activities of criminals, and the war against cyber crime can be better tackled if the operators have skilled staff to man the cafés; security measures like passwords that are hard to break, and especially monitor customers who do overnight browsing. Hackers and spammers caught should be handed over to law enforcement agents who will stick to the rule of law.

INTRODUCTION

The cybercafé is a café or shop open to the public, where a computer can be hired for a period of half an hour or more to access the Internet, write curriculum vitae, or play a game (Stewart, 1999). It serves as a rallying point for all sorts of information seekers and givers. Cybercafés have become so important that it is necessary to give a background to how they came into being.

Cybercafés are established in the public places of modern cities and towns and villages around the world. In December 1999 an online cybercafé guide listed 4397 cafés around the world. With the explosion in the use and profile of the Internet and personal use of new information and communications technology-'multimedia', cybercafés have become part of contemporary culture. In January 2000, there were about 72.4 million hosts on the Internet, and of these the third world is participating with a mere 3%. About 85% of worldwide Internet hosts are in the G7 countries, which make up only about 10% of world population. On the other hand, the most populated countries of the third world—China, India, Brazil, and Nigeria all together make up less than 1% of all hosts with more than 40% of world population. In developing countries there are only full Internet connections with all services in the capital cities and since there are three basic requirements for Internet access, that is, telephone connection, computer, and electricity, they are invaluable.

The reality however, is that one in three people lack electricity globally and 80% of the world population does not have a telephone line. The percentage of those who have is very low as shown.

Computers also suffer the same fate, as in year 2000, 28.32% of all computers were in the United States of America (USA), and Europe had 26.73% while countries like India and Mexico shared 1.08%. For countries without direct access to the Internet, costs of being connected are usually very high. Monthly fees for an Internet connection are often unreachable for common people in developing countries (Afemann, 2000). The costs of maintaining the facilities also posed problem. To overcome the big hurdles in financing individual Internet access, many civil organizations in developing nations found a more suitable way of using the Internet and decided to establish facilities called cybercafés, where several users at a fee could access the Internet.

In managing the cybercafés, security measures have to be taken to protect the equipment and the persons working as well as the clients. The equipment has to be physically protected by for example, labeling them through inscribing, and using iron bars on windows and doors to prevent theft. This helps protect staff and users.

Electronic security involves making the computers and the information on them, and received through them, safe for general use, and restricting usage of information that could be tampered with, or that could be used for criminal purposes, for example, keeping financial records away from open access.

This chapter discusses physical and security issues with respect to cybercafé management, as well as crimes committed using the Internet (now referred to as cyber crime). These issues would not be coming up if the incidence of cyber

Table 1. Telephone density in low & middle-income countries (Source: World Development Report 1998/99)

Region	No. of Tel.lines/100pers
East Asia & Pacific	4.1
Europe & Central Asia	18.5
Latin America & Caribbean	10.2
Middle East & N. Africa	6.5
South Asia	1.4
Sub-Saharan Africa	1.4

crime has not pervaded the Internet. As already presented in the background given, most people could not afford Internet access and as such patronize cybercafés to have access to the Internet and its abundant resources.

BACKGROUND

- **Cybercafé:** An Internet café or cybercafé is a place where one can use a computer with Internet access, most for a fee, usually per hour or minute; sometimes one can have unmetered access with a pass for a day or month, and so forth. It may or may not serve as a regular café as well, with food and drinks being served (Wikipedia, 2007).
- **Electronic security:** Electronic security, as used in this chapter, involves putting in place measures to protect electronic equipment, resources, programs, software, and databases used in cybercafés. These may involve use of passwords, cookies, and other electronic means of protection.
- **Physical security:** Physical security measures, as used in this chapter, involve protection from physical removal, damage or mutilation of the equipment, building, and persons in the cybercafé. These are inclusive of measures like labeling the equipment, fixing burglary proofs, alarms, smoke detectors, and such as can give physical protection.
- **Cyber crime:** A term used broadly to describe criminal activity in which computers or computer networks are used as a tool in perpetrating criminal activities via the Internet.

Crime is one phenomenon that takes on frightening dimensions to any peace-loving society. It brings about underdevelopment. Crime rate in Africa and the developed world is taking on a new face as this connotes theft, muggings, killing, suicide- bombing, fraud, and myriads of others. In the 21st century, with the advent of computer technology, and communication and trade through electronic media, crime is taking place by the day on the Internet, on desktops, laptops, and palmtops. Cyber crime, as it is now called (or Internet crime), has crept in. It is a term used broadly to describe criminal activity in which computers, or computer networks are used as a tool in perpetrating criminal activities via the Internet (e.g., spamming and criminal copyright crimes), a target (e.g., unauthorized access, malicious code, and denial of service attacks), or a place of criminal activity (e.g., theft of service and financial fraud). It also covers traditional crimes in which computers or networks are used to enable illicit activity (e.g., child pornography, online gambling, and advanced fee fraud known as 419 in Nigeria). Basically, cyber crime is criminal activity involving information technology infrastructure.

The Wikipedia (2007) names cyber crime types as:

- Unauthorized access (i.e., defeating access controls)
- Hacking
- Cyberterrorism
- Cyberstalking and online harassment
- Fraud and identity theft, including phishing
- Information warfare
- Fenial of service attack
- Malicious code (including use of a virus or Trojan horse) and virtual crime, such as the theft of virtual property (http:en.wikipedia.org/wiki/cybercrime).

Aghatise (2006) identified some cyber crimes in Nigeria as those of spamming, crimes perpetrated through hucksters and fraudsters; and piracy of software. He described a few cyber crimes concentrating on the victims of these crimes and also suggested ways of preventing

the crimes. It is reported that there are syndicates in South Africa mostly using cybercafés as their operating hubs for scams like the 419 (Magele, 2005). A scam is usually initiated by a proposal from someone claiming to have some money in foreign currency usually American dollars to transfer to a bank account. The writer of the e-mail actually, basically appeals to the intended victim's greed, promising a sizable percentage of the money (about 30-40%) to be transferred as commission for use of the victim's bank account. One of the researchers received several of such in the year 2006, and some more in the year 2007 (see Appendix).

Phishing, the practice of tricking consumers into revealing their online passwords and other information by luring them to fraudulent sites that appear to be those of banks or other legitimate businesses, has gained some ground in developing nations. The numbers of phishing attacks are increasing especially since phishing kits can be bought for $270 and there are sites that even present tutorials on how to phish (ITWEB, 2005). Phishing lures victims through spam e-mails carrying subject lines such as "account update needed."

Combating cyber crime is not as easy, as rampant as it is. This is because it is reported much less than it occurs due to lack of tangible evidence or detection, or both. One third of companies that had reported fraud were unable to put value on the crime reported (Price Waterhouse Coopers, 2005). The major challenge facing many nations, both in developed and developing world now is the enactment of appropriate laws to combat cyber crime (or Internet crime). Since cyber crime keeps evolving by the day, perpetrators keep finding ways of circumventing the laws of the land. Laws against this crime need to be reviewed from time to time. For example in Nigeria, the National Assembly passed the bill on cyber crime, but you find that already individuals involved in it are more advanced in practice than the law. The Economic and Financial Crimes Commission (EFCC) has succeeded in raiding cybercafés and even sealing up some but that is really not enough.

The World Wide Web (WWW) opened up many new opportunities for business but also exposed them to new risks. Therefore, electronic security continues to be a challenge to using the electronic medium.

Some solutions or e-security measures that have been proffered for business organizations are:

- Ensure that all computer equipment and systems are sufficiently protected
- Ensure that e- security complies fully with any government legislation
- Ensure the nature and value of the organization's data
- Make security an integral part of running the business
- Ensure that employees understand the importance of security and own responsibility
- Ensure physical security, for example, who can access the server room and password list
- Provide means for identifying attempted unauthorized access to data and what the appropriate action will be to block or monitor intrusion
- Identify who has access what, where and when?
- Ensure development of a security policy that is continually monitored, managed, and updated (Vicomsoft Inc., 2002).

Cyber crimes have thus become a major cause for concern all over the world.

SECURITY ISSUES STUDY

Inspiration for this study came from a discussion between two embassy employees overheard in their office in Victoria Island, Lagos. The discussion focused on a businessman from Mali who

almost got killed after being lured to Nigeria, abducted and held for ransom in a remote village somewhere in Eastern Nigeria; this Malian had responded to an online pen pal's proposal of business opportunities. The pen pal, a female, purportedly invited him to Nigeria, but on getting to the airport in Lagos, was met by someone whose appearance was different from the picture he was sent via e-mail. The lady then took him to her village where a set of hefty fierce-looking men took him blindfolded to a mansion in the bush.

He was dispossessed of all his money and forced to phone his parents in Mali to send money to ransom him. They bluntly asked him to instruct them to sell his car, house, and other property, which they described to him, to his amazement. They knew where his office and home were in Mali! He only could escape after being severely matcheted, beaten, and tortured. This they did when he resolutely told his parents not to send anything, but consider him dead, as he preferred that to them being poor. He ran for dear life and through difficulties made it back to Mali, swearing never to use cybercafés anymore for business transactions.

The culprits had got information on him, as he was a good patron of a popular cybercafé in Mali. They had a dossier on him and could easily manipulate an unsuspecting victim such as him. This is a case of cyber crime mixed with other crimes. This narration set the writers thinking and the study was thus conducted to investigate the types of crime committed using cyberspace and how management of cybercafés dealt with or tried to curb or prevent such crimes.

In this bid to find out how cyber crimes are being dealt with, some cybercafés in Ibadan metropolis were visited and the operators/managers/staff of the cybercafés were interviewed on what their experiences were and how they have fared in the war against cyber crime.

There are about 220 cybercafés in Ibadan, that is, that have over 16 computers and offer Internet facilities. Sixty were used in the study. They were spread over five local government areas in Ibadan. Only the urban portions had cybercafés as the villages in the suburbs have no electricity.

Sixty-two (62) persons were owners or managers of the cafés while 47 were workers or staffing the cafés. The interviews lasted between 15 and 25 minutes depending on how busy or not the interviewee was at the time. Participatory observation methods were employed first, before either the interview was conducted, or the questionnaire administered.

Where the questionnaire proved cumbersome, due to time and convenience constraint on the part of the interviewee, an unstructured interview was carried out. The researcher would buy airtime, do some browsing, and eventually ask questions pertaining to the research. A few users of the cafés, especially those who offer night browsing, were interviewed and they gave an insight into their experiences.

FINDINGS OF THE STUDY

One major finding is that many cybercafés in Ibadan are closing down. Some had to close down because they had been recognized as a haven for spammers, and had therefore been raided by law enforcement agents a number of times. Another category of cybercafés that had closed down did so because spam mails were traced to them and they had to pay heavily for the crimes committed by their patrons, therefore they were grounded financially. Another factor is that of dwindling patronage, which is as a result of the recent influx of fixed wireless lines, which enable individuals to have Internet access at home at a cost. Because they are not making profit, many have had to close down.

Findings also revealed that a majority of the cybercafé patrons are students of higher institutions, like polytechnics and universities. Another category of users is unemployed graduates. They use the cybercafés mainly at night for what is

called 'night browsing' and cybercafé personnel have established that a high percentage of them are engaged in cyber crimes, especially spamming, which is now tagged '*Yahoo-Yahoo*', and the perpetrators are known as '*Yahoo boys*'. This corroborates Aghatise (2006), when he stated, "The Internet has enabled young Nigerians to become active cyber criminals. They queue up in cyber cafés to send '419 mails' (Nigerian word for fraudulent businesses online)".

From the interview with staff in the cybercafés, it was gathered that they try as much as they know and as much as is within their means to protect physically and electronically both their electronic systems and their users. In terms of knowledge about IT (information technology), most of them (both cybercafé staff and their managers) are unskilled, but in a few you find one person who is very good, and this is quite inadequate to monitor the activities of the patrons.

Some of the measures employed by cybercafés to ensure security of their systems and patrons are still much unsophisticated. These include:

PHYSICAL SECURITY

Quite a number of the cybercafés (45 i.e., 90%) have space problems as the equipment and users literally fight for the little space there is. Many users bring friends along with them; so more than one user is often at a system. This makes it easy for password theft to occur. It was also noticed that users not information-technology-literate bring more competent hands along, or give their passwords to the café attendant to assist, thus security is breached. Many do not manage the time paid for very well and so end up being shut off, before they can close their mailboxes. Some do not close their mail before logging off; therefore, the next user of the system can have a field day!

Only about 20 (40%) of the cafés studied offer night browsing. Some revealed that they do not have the staff to man at such hours, while others felt it was too risky as it was likely that shady characters would be on the prowl at such hours.

The cybercafés are very busy during the day, in commercial and academic environments in Ibadan. In the less busy areas, (mostly residential), night browsing is more common, and clients who have no internet facilities at work, patronize cybercafés after office hours.

Physical security at night does not go beyond locking the doors leading into the café and checking the ticket of the users. Some of the cafés require that you book 12 to 24 hours ahead. This is so they can get staff to work at those hours. In some, if a certain number of clients are not attained, they do not accept to open for night browsing as it may not be profitable.

Power supply is a problem for cybercafés, and having to use generators as alternative power supply is sometimes a security problem at night. The noise of the generator attracts thieves! The generator itself can also be a source of danger if not well managed. Generator fumes getting into the cybercafé has been known to kill staff and client of a cybercafé in Lagos. The cybercafés also have to get extra security night guards to keep watch on their cafés if night browsing is the practice.

They also try to make patrons conscious of security by putting up banners on the wall warning them against spamming, pornography, gambling, and other vices.

Building their tables in forms of carrels to ensure the privacy and security of patrons is also found to help. Many of the cafés also try to employ more hands to monitor the sites being visited by their patrons.

ELECTRONIC SECURITY MEASURES

The electronic security measures start from installing passwords as tickets on the computers. Without a ticket and password, the client cannot

have access to the computer. The system would require authorized users to dial in a pre-assigned personal identification number (PIN). A unique and/or frequently changing password or using a password that cannot be easily connected to the obvious circumstances surrounding the owner may enhance this strategy of electronic security.

Again, there is restriction on the use of diskettes and flash drives (memory sticks) in nearly all of the cafés studied. This is to prevent introduction of viruses to the systems, as this can be quite devastating.

Disabling or uninstalling certain packages such as anti-spy ware on their systems is also adopted as a security measure. Firewalls provide the most cost-effective solution to the problem of hacking for the cybercafés studied. They most commonly use Mozilla Firewall.

Antivirus software is also routinely installed to protect the computer system against viruses. This screens all downloaded programs and documents before use, runs virus scan frequently on a daily basis, and also ensures comprehensive backup to restore data, perform audit trials, scan files before upload or after download, and makes frequent back ups to avoid loss of data.

These measures are grossly inadequate compared to the sophistication of the techniques used by cyber criminals and armed robbers as well. The literature confirms some of the findings of this study. For example, that robbers steal money, handsets, and sometimes cars from cybercafé patrons (Stohs, 2004). The cafés need police protection or well trained and well equipped night guards. In addition, the electronic security issues need expertise and technical know-how as hackers are now focusing on new targets and looking beyond the operating system to gain access to computers (Czernowalow, 2005 quoting Gary Middleton of Dimension Data).

Some female patrons interviewed report that they have been sexually harassed when on night browsing when some male patrons open pornographic sites and try to assault them. They do not make formal complaints because the general belief of many people is "W*hat are the women doing overnight in the cybercafés anyway?*"

FUTURE TRENDS

The advent and the continued development of the CDMA (code division multiple access) technology in telephony has posed a threat to the establishment of cybercafés. This however does not put cyber crimes in check because of the 'anonymous' nature of acquiring fixed wireless lines in Nigeria; anonymous, because fixed wireless operators do not take records (bio-data information) of their various customers/subscribers. Therefore, it is quite difficult to trace or investigate perpetrated crimes. With increasing awareness of the Federal Government of Nigeria about the situation, something is being done and this will lead to added scrutiny of how to curb the menace.

University units are providing cybercafé facilities as opposed to the former trend of such services being got from commercial enterprises. The University of Ibadan has an ICT unit that provides cybercafé facilities. The security measures are as obtains in any café outside the university, but with restrictions to only bonafide students with university identity cards and staff of the university.

CONCLUSION

From this work, we conclude that cyber crime in Nigeria has developed into a full-blown menace, which has hitherto been tackled with kid gloves. There is a lack of technical know-how and adequate legislation to serve as deterrent to offenders. This is however not peculiar to Nigeria alone. According to Magele (2005), South African legislation on e-crime is still very new and is only beginning to have an impact.

Cybercafés operating in Nigeria do not seem to be guided by firm laws that will ensure registration and proper monitoring. The following are recommended in the light of what has been presented so far:

- Cybercafé operators should closely monitor their customers especially night browsers. They should maintain carrel-like tables to aid privacy of clients.
- Clients should be encouraged to report any suspicious moves by other users.
- Internet users should be proactive. They should fight spammers if they can. For example, reports of the case of Bob who lures fraudsters to meet him face to face and disgraces them. This may be extreme and dangerous but it is a fight against cyber crime.
- Electronic security is a bit more difficult to ensure, but being "alert" is the watchword.
- People who need to use IT facilities should get themselves well trained so they do not need too much assistance from others to do their Internet transactions.
- People should adopt the method of never giving out their passwords to unauthorized persons.
- Passwords in cybercafés should be changed periodically.
- Training of law enforcement agents to effectively combat cyber crime at any level. This means they need high level IT training to keep them abreast and even more advanced than cyber criminals in the computer world.
- Establishment of cybercafés should be guided by laws, which should be enforced by the appropriate bodies.
- Government should encourage operators of cybercafés who should form advocacy groups that will ensure their interests are protected.

FURTHER RESEARCH DIRECTIONS

It is suggested that research on cybercafé management and cyber crime be replicated across the country to give a complete picture on a national level.

There is need to conduct research on the effect of the fixed wireless operators on the phenomenon of cyber crime in Nigeria. This can also be studied as regards the GSM operators too.

This study was carried out in Ibadan, which is an urban city in Nigeria. A similar study in a rural setting will reveal what the situation is regarding Internet connection, cybercafés, and cyber crime and security issues in those areas.

REFERENCES

Afemann, U. (2000, March 22-25). *Internet and developing countries—Pros and cons.* Paper presented at the International Workshop on Social Usage of Internet in Malaysia (p. 14). Universiti Kebangsaan Malaysia Bangi.

Aghatise, E. J. (2006). Cybercrime definition. *Computer Crime Research Center.* Retrieved from http://www.crime-research.org/articles/joseph06/

Aginam, E. (2005, December 14). Cybercrime on the increase? *Vanguard*, p. 31.

Amaefule, E., & Akintunde, (2005, March 3). Global businesses fight cybercrimes with $14bn. *Punch*, p. 19.

Google makes hacking easier. (2005, May 4). *Sun*, p. 33.

How internet scammers work. (2005, August 8). *Punch*, p. 51.

IT Web. (2005). *South Africa flags on security spending.* http://www.itweb.co.za

Jefersson, G. (2002). *Cybercafes serve an explosive brew.* Retrieved from http://www.almericoni.com.new/feb02/022502.html

Jonah, I. (2005, April 5). How to ruin cybercafe's profitability. *Punch*, p.16.

Magele, T. (2005). *E- Security in South Africa.* Prepared as a delegate brief for the Forge Ahead E-Security event held Feb. 16-17, 2006 (p. 32).

PriceWaterhouse Coopers. (2005). *How to use identity management to reduce the cost and complexity of Sarbanes-Oxley compliance.* http://www.pwc.com.servlet/pwcPrintPreview

Sani, A., & Tiamiyu, M. (2005). Evaluation of automated services in Nigerian Universities. *The Electronic Journal*, *23*(3), 274-288.

Shuman, B. A. (2002). Case Studies in library security. *Connecticut, Libraries Unlimited*, p. 252.

Stewart, J. (1999). *Cafematics? The cybercafe and the community.* Retrieved from http://www.homepages.ed.ac.uk/jkstew

Stohs, B. (2004). Privacy, free speech and the Garden Grove cybercafe experiment. *Duke Law and Technical Review, 0012.*

Vicomsoft. (2002). *Mac guide to e-security.* Retrieved from http://www.zdnet.com.au/whitepaper/0,20000063328,22093796p-16003339,00.htm

ADDITIONAL READING

Akore, A. (2005, March 5). Laws against cybercrime underway. *The Guardian*, p. 55.

Alcatel, (2001). *Network security: Issues, processes and technologies.* Retrieved on January 20, from http://quistnet.net.au/questnet2001/ppt/Lawlence_Wong-v2.ppt

Chachage, B. L. (2001). Internet cafés in Tanzania: a study of the knowledge and skills of end-users. *Information Development*, *17*(4), 226-233.

Government plans laws to check cybercrime. (2005, March 15). *The Guardian*, p. 1.

How to avert cybercrime in banks by NCWG. (2005, March 1). *The Guardian*, p. 55.

Ikhuemeumhe, G. (2005, March 16). Nigerian cybercrime law and human rights concerns. *The Vanguard*, p. 29.

Mutula, S. (2003) Cyber café industry in Africa. *Journal of Information Science*, *9*(6), 489-497. Report of International Software Consortium ISC. http://www.isc.org/ds/www-20001.report

Obadina, T. (2005, August 8). Financial crimes ruin Nigeria. *Punch*, p. 17.

Udy, O. (2005, February 26). Internet fraud: The new youth menace. *The Sun*, p. 49.

World Development Report. (1998/1999). Retrieved from http://www.worldbank.org/wdr/wdr98/contents/htm

Why cyber crimes are on the rise—VGCC boss. (2005, October 2). *Punch*, p. 33.