An assessment of Internet Abuse in Nigeria

M.E Ezema*, H.C. Inyama+

Computer Science Department, University Nigeria Nsukka
Email: ezemamodesta@yahoo.com
+Department of Computer and Electronics Engineering, Nnamdi Azikiwe University Awka
Anambra State Nigeria, Email : drhcinyiama@gmail.com Phone: 08034701121

Abstract

As Internet use has proliferated worldwide, there has been debate whether some users develop disturbed patterns of Internet use (i.e., Internet abuse). This article highlights relevant literature on Internet abuse in Nigeria. Is the addiction paradigm appropriate for Internet use? Is behavior that has been labeled Internet abuse symptomatic of other problems such as depression, sexual disorders, or loneliness in Nigeria? What are alternative explanations for this phenomenon? Is there adequate research to support Internet abuse as a distinct disorder?

Key words: *Internet, Packet Switching, World Wide Web,* Computer Crime, Cyber-bullying Malware

---

Introduction

The Internet was the result of some visionary thinking by people in the early 1960s that saw great potential value in allowing computers to share information on research and development in scientific and military fields. J.C.R. Licklider of MIT first proposed a global network of computers in 1962, and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections. Lawrence Roberts of MIT connected a Massachusetts computer with a California computer in 1965 over dial-up telephone lines. It showed the feasibility of wide area networking, but also showed that the telephone line's circuit switching was inadequate. Kleinrock's packet switching theory was confirmed. Roberts moved over to DARPA in 1966 and developed his plan for ARPANET. These visionaries and many more left unnamed here are the real founders of the Internet

What is Internet Abuse?

Defining Internet abuse is the first challenge, and creating an organization wide acceptable use policy (AUP) is the first step in the definition. **Internet abuse** refers to improper use of the internet and may include: computer crime, cyber bullying, spam and malwares. An acceptable use policy defines what constitutes Internet abuse in an organization. Acceptable Internet behaviour in one organization may be unacceptable in another, so the acceptable use policy is a highly customized policy, based on the organizational mission. The organization determines what lines will be drawn when it comes to Internet abuse. The amount of resources and information the Internet contains is astounding. With the help of information collected on the net, people gain vast knowledge. Parents and children together can work to make the Internet a positive experience. However, some people can misuse this wonderful knowledge bank and with no rules or regulations, can discover surreptitiously how to commit crimes, see things they ought not to see and chat with people of questionable character[1]. Thus parents ought to take precautions to see that their children do not abuse the internet access. On the other hand there are people who use the internet for nefarious activities and they strike to win converts among the unwary.

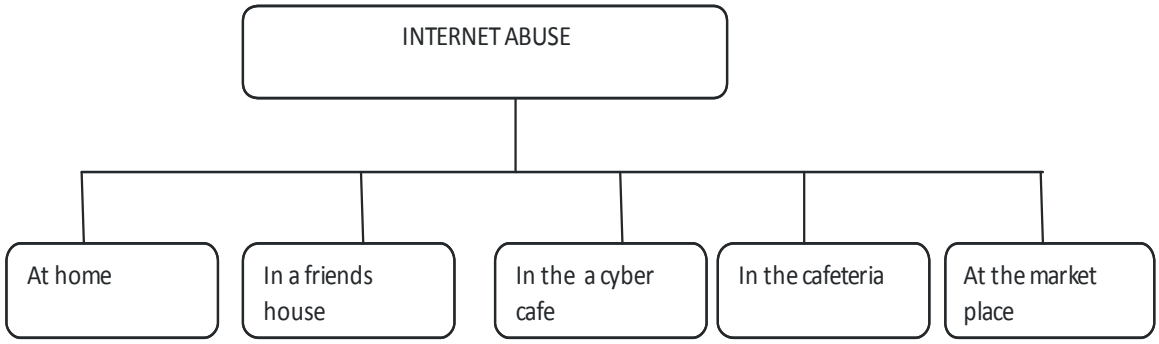

Fig 1: Review of the internet abuse in Nigeria

Close monitoring and forbidden access

The location of a computer may make a huge difference in the type of Web content one reads and surfs. If possible, computers should be in the office, living room, family room or some high traffic area so that one can always monitor the internet access. This will restrict abuse of the internet access at any given moment since someone may approach the computer while internet abuse is on going, hence people will be more cautious and careful of their online activities. On the other hand the cases of night browsing, parents should not allow their children to go to places they do not have adequate trust on what their child may be doing or likely to be doing there at night. The highest of all is disciplined parents have to tell their children the implications of certain actions like watching bad films, discussing online with people you do not know their family background very well so that even if their parents are not at home with them they will be limited with what they do with the internet.

Standard Internet Safety

Another important thing that one needs to know is standard internet safety [3]. The key to a successful acceptable use policy (AUP) implementation in most organizations is similar to other policy development issues in the workplace. There must be "buy-in" from the "top-down", in other words, the leaders of the organization must agree to the principles of the AUP and endeavour to push that policy down to the directors, managers and supervisors within the organization. The most critical stage of AUP development is dependent on upper management "buy-in" and their willingness to demonstrate the importance of this policy to the rest of the organization.

It is very essential for one to know about computers and be familiar with the World Wide Web. Nothing can be more intimidating than a child knowing more about computers and internet than their parents, and often this is what happens with today's parents who probably know very little about internet compared to their children. Thus consider this aspect no one can know if something is amiss with a child while being totally repugnant if you do not know or understand the child's online activities

The Internet has become an invaluable resource in the workplace, the world's biggest reference library, social media centre, and pornography outlet is now only a click away. This availability presents a significant risk factor for employer liability and costs employers thousands of hours in productivity each day. Monitoring employee Internet use is one way to reduce employer liability, and whether or not you agree with the principles behind Internet monitoring, many employers agree that it is a necessary evil [2]. Internet abusers range from upper management employees in private offices viewing hardcore pornography, to the department assistant in a cubicle that spends

3 hours a day using Facebook, doing online shopping, making travel arrangements, and paying bills through the company Internet. Internet abuse is endemic in the workplace and organizations are being forced to face the problem head on, or suffer the consequences.

Among the many consequences of Internet abuse is a loss of productivity and scores of litigation issues such as sexual harassment, hostile work environment and discrimination. Monitoring Employee Internet access is one way that an organization can limit its liability.

Holding a series of Internet workshops with employees of an organization is one way to introduce new acceptable use policy. As an educational session, an Internet workshop can address the sensitive issues surrounding Internet abuse in an open forum where employees can ask questions and provide input in a non-confrontational setting.

During the Internet workshop, the organization can begin to educate the employees about Internet abuse and give them a chance to re-evaluate their Internet habits at work. It is important to be as open as possible with employees regarding chosen methodology for enforcing the AUP

For example, if the organization has decided to employ Internet blocking technologies, the AUP should define the specific types of websites that will be blocked, for example, many organizations block pornography, "gross depictions" and "hate" websites. Discussing the types of websites the organization has decided to block and answering questions regarding the reasons for blocking will reinforce the organizational mission, and demonstrate the types of websites that are inappropriate within an organization.

If an organization is going to monitor and report on employee Internet access, the workshop will give one a chance to show the employees what the Internet reports look like, and discuss the circumstances in which they will be used. Taking the mystery out of what the organization is planning in regards to Internet monitoring and blocking will reduce employee speculation and set new expectations throughout the organization

Problems with Internet Monitoring

The technical aspects of blocking website access and monitoring employee Internet access are not without problems. The software for blocking websites has advanced tremendously over the past 5 years; however, there are still problems with blocking "all" inappropriate websites and blocking websites that you did not intend to block. No system is perfect and one will need assistance from a selected software or hardware vendor in addition to information systems department. If possible, it is always better to meet, in person, with the vendor representatives prior to the purchase of any Internet monitoring software. Voice your concerns with the vendor and secure "after sale" support with the vendor help desk. If you have an information systems department, one should make sure they are involved from the start of the project to help address any technical problems that the new system could bring.

Monitoring Employee Internet Access - The People Side

Outside of the technical issues that will occur, the people side of Internet monitoring can be the most problematic of all. Even with the dissemination of information given at the Internet workshop and taking great care during policy development, some employees will, inevitably feel that Internet monitoring is unfair. Given this fact, it is of the utmost importance that the Internet reports are accurate, beyond question. Even if they are correct, there are still issues to consider. The scenarios listed below are examples of how employees could react if they are confronted with the accusation of Internet abuse.

Moreover, the excuses below may be completely accurate and good explanation by the accused.

"It wasn't me!"

It is always possible that some other person was on the accused employee's computer surfing the Internet. Once a user steps away from the computer, anything can happen. Another person sits down and starts using the computer logged in as the accused, everything they do on the Internet is recorded under somebody else's name. One suggestion is to have the user lock their computer before leaving for an extended period of time; this will reduce the chances of misidentification of the Internet abuser.

"They have my password"

This is a similar situation to the one mentioned above. If I have a user's password, I could log-in as the user and all of my Internet access would be attributed to them. How they got the password is another issue entirely, however the user makes a good point and has a potentially valid excuse for an Internet report that shows abuse.

"The Internet Report is Wrong"

This can occur if the monitoring software is setup incorrectly or if there are network issues causing identification problems. This is another reason why one will want information systems department involved from the start and technical support from the vendor who sold the Internet monitoring solution. Defending an Internet report that shows abuse is difficult when you do not understand how the technical aspects of **Internet monitoring work.**

Internet reporting is not an exact science, the reports could be wrong, and the person accused of Internet abuse may be completely innocent. The key is to research the potential offender and look into their history. People who abuse the Internet usually have a history of doing so, so look into their past Internet use first and then look at the Internet records on their computer. In short, do a "reality check". Too often we take technology for its word and fail to look on the human side for insight that may confirm or make us question our suspicions. This practice will help reduce the number of errors that could be made during the investigation of Internet abuse, and help the employer maintain their credibility.

Internet abuse is a fact of life in most large organizations today. Monitoring employee Internet use and employing blocking technologies can be helpful in reducing employer liability and improving employee productivity. Developing an acceptable use policy to outline acceptable Internet behaviour in an organization is the first step in the process. To implement this policy successfully, the policy must be supported by upper, mid, and line level managers. The organization should endeavour, with enthusiasm, to educate the employees of the organization about Internet abuse and share the organizations plans to monitoring use and block inappropriate websites.

Prior to purchasing a software or hardware solution for Internet monitoring and blocking, a vendor should be selected and invited into the organization to explain the technical problems that can occur with Internet monitoring and blocking technologies. During this vendor selection process, it is very important to include information systems department and other technical staff. Arranging after-sale support with the vendor of choice is highly recommended.

Finally, there is the people side of the problem. Internet monitoring and blocking are only as good as the software and hardware solutions that are developed. There are many ways that these solutions can fail, so doing a thorough investigation prior to accusing an employee of Internet abuse is also highly recommended.

References

[1] Acier, Didier and Laurence Kern. "Problematic Internet use: Perceptions of Addiction Counselors." ***Computers and Education***. *May 2011, Vol. 56: 983-989.*

[2] Block, Jerald. "Issues for DSM-V: Internet Addiction." **American *Journal of Psychiatry***. 2008, Vol. 165 No. 3: 306-307.

[3] Internet Abuse, www.buzzle.com/editorials/1-13-2005-64163.