Internet Abuses as Hindrance to Development in Nigeria: A Christian Ethical Appraisal

Emeka C. Ekeke (Department of Religious/Cultural Studies, University of Calabar, PMB 1115 Calabar 540004, Cross River State, Nigeria)

Internet Abuses as Hindrance to Development in Nigeria: A Christian Ethical Appraisal

Abstract

The Internet is one of the fastest means of information technology now available to man. It has actually made the world to become one global village. Millions of people worldwide are now using the Internet. On the other hand, there are heinous abuses which hinder development, which are not readily noticed by the novice user. This paper therefore seeks to examine some of these abuses and ethically appraise their danger on the Internet users worldwide and Nigeria in particular. These abuses include: scams and pyramids, hackers and crackers, viruses and worms, cyber-stalking, adoption fraud, credit card theft and online pornography. It was recommended among others that the government of Nigeria should re-equip the Economic and Financial Crime Commission and Nigeria Police Force and other relevant agencies with high-tech knowledge to fight Internet abuse. Furthermore, the government should encourage self-regulatory body being set up by the Internet Service Providers (ISPs) to tackle these crimes and abuses.

Keywords: Internet Abuses; ethics; cyber fraud; computer crimes

Introduction

It has been observed by Asodike and Jaja (2012) that the advent of the 21st century to a large extent ushered in a renewed vigor, quest and zest for the use of Information Communication Technology (ICT) in the world. They argued that the use and impact of ICT facilities can be seen in almost every major city of Nigeria. This can be seen in the fact that “businesses, organizations, governmental agencies, educational institutions and so on all use digital technology to help utilize information in a more effective and faster way” (918-919). ICT is playing this wonderful role using Internet in this era commonly known as “Information age”.

In this Information technology age, the positive uses of computers and Internet have become so vast and its popularity has reached every nook and cranny of the world such that it has large variety of benefits for scientists, researchers, commercial activities etc. With this growing impact are its abuses, which fraudsters utilize for evil uses. Rusch (2001), in his work “The Rising Tide of Internet Fraud” argues that there are growing indication that along with the expansion of legitimate Internet use, the world is experiencing a rising tide of fraud that exploits the Internet and its users (6).

In some cases, the Internet is regarded as a world of its own where things are not always what they appear, especially to the novice user. National Computer Ethics and Responsibilities Campaign (NCERC) (2006) say, “Today, ethical collapse is no longer confined to the trauma ward. It is epidemic among information technology users. And you may be among them” (1). It is this ethical collapse among Internet users and providers that has given birth to various forms of abuses and crimes being committed via the Internet hence the need for Internet ethical appraisal. Today, the level of insult meted on political leaders through the social media- face book, twitter and the rest either because of misrule or perceived wrong policy is unprecedented. No one would have thought of this few years back but it has been
enhanced by the disembodied nature of the internet which gives room for free speech whether it is right or wrong. The abuse perpetrated in and through the internet is the clear demonstration of the level of ethical collapse in our society.

Internet is a network of networks of millions of computers from all over the world. The Internet allows computers to trade information using telephone lines, fiber-optic cables, and satellite links. It is also referred to as the “Net”.

In presenting an etymological definition of ethics Ozumba (2001) says the term comes from the Greek word “ethos”, which means “customary” (4). This makes ethics equivalent to morals or morality. Ethics as observed by Omoregbe (1993: 3) has no univocal definition. Various scholars from various backgrounds have attempted to define it based on their convictions. Iwe (1987) defines it as “a systematic study of the principles governing human conduct by human reason from the point of view of the right and wrong, the ought and the ought not” (18). He further sees ethics as “the orderly and logical applications of acknowledged moral principles to a given way of life” (20).

From the Christian point of view, ethics is needed in the society for harmony to exist. This is why Wikipedia, the free Encyclopedia (2006) writing about “Ethics in Religion” says “Christian ethics in general has tended to stress grace, mercy and forgiveness” (2) while Norton (1975) argues that:

Christian ethics has its foundation in the same principle of living as that of the Lord Jesus Christ. The commandments of God through his prophets and apostles and his Son, combined with the perfect example of Christ, provide the believer an absolute ethic rather than ethical relativism... The content of the Christian ethic is the will of God that must be done in love ‘faith working through love’ (Galatians 5:6) (561).

Barnette (n. d) in his Crucial Problems in Christian Perspectives enumerates three important factors that should be considered as we look at Christian ethics and moral authority.

The first factor is the person of the Christian life (16). He explains that moral imperative is presented in the person of Jesus Christ and not in a code of dos and don’ts. Christ therefore is to be imitated as Lord of all life. The second factor is the principle of Christian action. He argues that Christ is the ultimate norm of Christian action while love should be “the ethical expression of personal faith in him” (16). The third and final factor is the power of the Christian life (17). He explains that Christ is the person for Christian ethics, love (agapeic), and the ethical principle upon which the Christian life should revolve, and then the Holy Spirit is the energizing power of the Christian’s existence. The Holy Spirit is the enabler of Christian character and conduct (20). In stressing the necessity of the Holy Spirit for a Christian to live a moral life and to make the right decisions in today’s world, Barnette (n. d) says “in seeking Christian decisions with reference to the moral ambiguities of our day, we measure right action by these criteria: the revelation of God in Christ, radical obedient love tempered with knowledge, and the guidance of the Holy Spirit” (21)

Christian ethics derives its source from the Bible especially, the Decalogue-the Ten Commandments, the New Testament especially Sermon on the Mount and Pauline Epistles. Having the definition of Internet, ethics and Christian ethics, in mind, this paper will therefore x-ray various abuses on the Internet today and ethically appraise its danger on the Internet users’ worldwide. The abuse that shall be dealt with in this paper includes: scams and pyramids, hackers and crackers, viruses and worms, cyber-stalking, adoption fraud, credit card theft and internet pornography. This work will help us to see the necessity for Internet ethics as a sin-qua-non in the world today.

Crimes Committed through the Internet

Bohlin (2006) in the work, “The value of the Internet for Christians” says, “The Internet provides a wealth of information, but not all the information is edifying or wise. Much of it is downright silly, but some of it is actually dangerous” (3). As has been expressed by Rusch, Crimes via the Net is growing at an alarming rate. Some of these that shall be discussed in this paper include scams and...
pyramids, hacking, cracking, viruses and worms, cyber-stalking, adoption fraud, credit card theft and identity theft and pornography.

**Scams and Pyramids**

The word Scam is not a conventional term rather it is a technical one which “Tour: Vocabulary” (2006) defines as “A ploy by a shyster—a mining promoter who mines the investor’s bank account and not the ground-to raise money” (3, 4). When interpreted in the conventional way it means fraud. Pollick (2006) defines fraud as “a deliberate misrepresentation which causes another person to suffer damages, usually monetary losses” (3).

Fraud can further be defined as “a scheme or knowing deception to obtain money by means of false pretenses, representations or promises” (Awake 2004: 4). Pyramid is another type of fraud where one is asked to buy four forms at N900 sells it to friends who in turn sell it to other friends. As the sale continues your name will continue to climb the pyramid until thousands of Naira or Dollar enters into your account. On the Internet it is regarded as a “make Money Fast Pyramid Scheme” (Covington 2006: 4). The system that is used is “Send 5 Dollars to the first person on the list, take that person’s name off, add yours at the bottom, and e-mail it to 100 of your friends”. Your mailbox will be filled with thousands of Dollars (Covington 2006: 4). The most deceitful thing in pyramids is that a few people make money at the beginning, this stimulates thousands to see it as a genuine business, but thousands more, farther down the line, get nothing. It is an evil and fraudulent scheme aimed at defrauding unsuspecting people. “Pyramid schemes always collapse because it is impossible to keep on recruiting new members” (Awake 2004: 6).

Scams come in different ways; therefore Internet Users should be careful. “Fraud and Scams” online says that more than 9 million U.S. adults were victims of scams in 2004 with a cost of 52.6 billion Dollars. Scammers are increasingly using the Internet to defraud victims (Fraud and Scams 2006: 1). Today there are various forms of scams such as the pyramid schemes we have just mentioned, work-at home schemes, health and diet scams, investment opportunities, credit repair, and vacation prize promotions. Let us briefly look at some of these scams:

**Work-at-home**

You may be asked to “assemble such things as jewelry, toys or craft kits” (Awake 2004: 8). When you invest money and time in assembling the products, you discover later that the promoters will not be interested and your money is gone. Another form is where you are given an opportunity to fill a form online to be paid 100 dollars or 1000 dollars for every form you fill. You send them your account number and they use it to withdraw your money.

**Health and diet scams**

There are series of adverts on Internet showing drugs that help you reduce weight or “cures impotence and creams to counter hair loss”. Be careful most of these drugs or products do not work; they are fake drugs (Awake 2004: 8).

**Investment opportunities**

This is another kind of scam where “investors are hired by assurances that those handling their money have high-level financial connections” (Awake 2004: 8) if they will invest in one kind of business or the other most likely offshore bank. Be careful not all that glitters is gold.

**Vacation prize promotions**

In this kind of scam you may receive e-mail or a phone call congratulating you for winning a fat sum of money in a promotion. You will then be asked to send an amount of money regarded as a “processing fee” before you receive what you have won. At the end, you will not see the money you are said to have won and the processing fee gone.

One most terrible thing about scam is that it is not very easy to investigate and prosecute. This is because the legal system finds it “difficult to prove that deliberate deception has actually taken place” (Awake 2004: 4). This has made it possible for swindlers, having known the loopholes in the legal system; exploit it to defraud unsuspecting people. The following tips can help you protect yourself against scam: Use common sense in all your
dealings. Do not be greedy for money you never worked for. And if the seller is trying to rush you into making a decision leave it, it is a scam and do not respond to an e-mail by sending money to buy a product from any spammer (Internet advertisement). Do not do business over the phone with people you do not know and avoid taking any spammer seriously irrespective of how appealing the advert may be. Finally do not join or register in any pyramid scheme, it is fraudulent. With the above precautions you will be able to escape from the clutches of scammers.

**Virus and Worms**

Worms and viruses are the infections or sickness of the computer world. In defining “Worm” Dasgupta (2006) says “it is a self-contained, replicating program, [designed or written by somebody], that burrows its way from computer to computer, causing harm” (2). Dasgupta (2006) further gives a clear picture of the activity of worms in the Internet:

The Code Red Worm started its attack around July 13th, burrowing into a known “hole” or “vulnerability” in the web-server software from Microsoft (called 115). The worm compromised the servers and defaced web sites by replacing the contents with a page that proclaimed “Hacked by Chinese”. Code Red not only defaced web sites, but also injected programs into the compromised servers that started attacking the U.S. President’s web site, using a “Distributed Denial of Service (or DDOS) attack (1).

In this way worms are terrible programs and those who program them are called hackers while the process is hacking. On the other hand “a virus is a program fragment that needs to attach itself to a host program in order to live” (Dasgupta 2006:1). A virus is a computer program that can destroy files or make your computer crash. Viruses can be sent via e-mail or through other file-sharing programs or through a diskette. It should be noted, “Once a virus attaches itself, then it can replicate and travel and cause harm” (Dasgupta 2006: 1). Computer operating systems are designed in such a way that external programs cannot be injected into them but today it is no longer true for programs can now be injected into any computer that is connected to the Internet without any anti-virus.

**Hackers and Crackers**

A hacker is “someone who accesses computer information either legally or illegally” while crackers are criminal hackers. Dasgupta (2006) tells us that the word “hacker” was originally coined to mean “extreme programmer.” Normal programmers write programs that do normal things. Hackers are very sharp people with a deeper understanding of how computers work and can write programs that do things programs are not supposed to do. Programmers can make computers compute; hackers can make a computer sing, dance and fly or crash (2).

It is these hackers and crackers that write programs called worms or viruses, which burrow into peoples computers connected to the Internet either to steal their files or destroy them. In some cases they do it to take control of the computer and its programs, to attack another computer or website. There are also good hackers whose duty is to deflect attacks on computer systems connected to the Internet. One of such groups is a team of dedicated computer engineers from Carnegie Mellon University known as the “Computer Emergency Response Team” popularly known now as CERT Coordination Center. Their work is to “delve into the inner mechanisms of worms and viruses, figuring out how each one works and how to stop the spread” (Dasgupta 2006: 4).

They also try to detect different types of worms or viruses and issue a bulletin to millions of subscribers warning them and advising on what to do. There are other good hackers who also “hack into systems, [purposely to] dissect software and uncover vulnerabilities. They publish their findings, urging software manufacturers to plug the holes” (4).

Today “Adobe” has manufactured a security program known as “Public-Key Encryption” (Covington 2006: 5) to secure files so that no one can break into a computer without authorization. Irrespective of how reasonable and powerful this is, a 26-year-old Russian Ph.D student Dmitry Sklyarov who studies Cryptography and works for Elmcomsoft has
developed a software system called the “Advanced e Book Processor” (Dasgupta 2006: 1). This “software breaks the so-called secure encryption built into electronic books” by Adobe showing that hacking and cracking and the release of viruses and worms have not yet been defeated. The first man who developed an Internet worm was Robert Morris and used it though by accident on November 2, 1988. It clogged all the computers connected on the Internet on that day and shut them off then rebooted to kill the worm. Morris was jailed for that his experiment.

Some of the measures that should be introduced to check viruses, worms, hackers and crackers include the installation of Public-key encryption, anti-virus software and not downloading information from people you don’t know can help keep virus from damaging your computer.

Cyber Stalking
This is one of the dark-sides of the web and is criminal in nature. It “violates the moral standard of majority of the population, and clearly goes against the principles of Christianity” (Vlach 2006: 7, 8). Internet Definitions (2006) see Cyber stalking as “the online enticement of children; rude or threatening messages; slanderous information; or repeated, unwanted messages” (3). Vlach (2006) defines it as “the terrorizing and harassing of people through the Internet” (8). It is sometimes through this means (cyber stalking) that terrorists recruit persons to carryout their nefarious activities. Some murderers also use this medium to recruit unsuspecting persons with a great threat to carryout a murderous operation. In most cases children who play with the Internet without parental guide are their victims. This is why Vlach (2006) advises, “Parents, in particular, should take steps to shield their children from Internet perversion and child solicitation” (8). In other cases children who try everything and browse into every site available for them may become instrument of passing on worms from a hacker who directs them under threat on what to do, and they do it not knowing the implication.

Dasgupta (2006) says, “Today…any kid with a computer can find a “phreaking” site, that is, a web site run by senior hackers who want to tell everyone how to cause trouble” (3). These cyber stalkers can hire children into sexual abuse using every amount of threat. Therefore, parents, especially Christian parents should monitor their children and their use of the Internet.

Adoption Fraud
This is another type of Internet abuse, which has caused men and women all over the world, pain and sorrow. Ashe (2006) therefore urges everyone who wants to adopt a child to “beware, be smart, do the research” (1) properly so that you will not be hooked into adoption fraud. If any proposal sounds too good to be true, it probably is. Adoption fraud includes (but is not limited to) the following: Adoption agency or facilitator that changes exorbitant fees, and is not properly staffed. An agency or facilitator that accepts money for services never rendered and misrepresent child emotional and physical history or background. This is generally referred to as “wrongful adoption” An expectant or biological parent accepting money for expenses from more than one prospective adoptive parent, with or without any intention of completing the adoption process (Ashe 2006: 1).

Mannix et al (2000: 1) described adoption fraud on Internet as one of the “bad stuff” on Internet. But because the Internet is so vast and uncharted, the full scope of its dark side has never been fully explored. The amount of bad stuff out there is truly staggering, rigged auctions, viruses, Adoption Scams and others. In June, police arrested the first Internet serial killer: John Edward Robinson, aka “Slave master” who was charged with murdering five women in two states in United States and stuffing their bodies into metal drums. John Edward Robinson did this evil through the Internet with the pretence that these women should come for adoption of children. When each of them came to a specified place for the adoption John killed her and stuffed her body into metal drum. These four precautionary steps should therefore be taken when going for adoption. First, trust your instincts: You are the best judge of when something doesn’t sound
“quite right”. Don’t rely mostly on Internet information in this regard. Meeting face-to-face can be the source of your best information because here you can see and hear how your questions are being answered. Second, ask the hard questions: Be careful to ask every necessary and hard question. “And if you don’t like the answers, find someone else” (Ashe 2006: 1). Thirdly, know the law: You must be aware of all the laws that relate to adoption so that your ignorance will not lead someone to defraud you. Finally, listen to experience: It is true that “experience is the best teacher” but a wise man learns from other people’s experiences. So you should look for support groups around and on the Internet where many have shared their experiences in stories and learn from them. It should be noted, “despite your best efforts, you may find yourself on the wrong end of [an Internet] scam or caught up in someone else’s fraudulent activity” (Ashe 2), be careful.

**Credit Card Theft**

This is the most committed Internet crime in the world of cyber-space today. Rusch (2001) in his article “The Rising Tide of Internet Fraud” states:

In a February 2001 report, the European Commission (EC) stated that credit card fraud in the European Union had risen by 50 percent in 2000 to $553 million in illegal transactions, and that the increase was greatest for “card-not-present” transactions (i.e., mail order, telephone, and Internet Sales), especially on the Internet (7).

Credit card theft or fraud is the fastest growing Internet fraud. Meridian Research in Rusch (2001), “Predicted in January 2001 that online payment-card fraud world-wide will increase from $1.6 billion in 2000 to $15.5 billion by 2005” (10). Credit card fraud is causing great problem for online merchants. It is criminal acts whereby the swindlers access valid payment card numbers through their unlawful access of e-commerce websites. He further adumbrates that:

Within the past year, several computer intrusions that made possible the downloading of tens of thousands, if not millions of credit card numbers- such as the exposure of more than 3 million credit cards at Egghead.com has received worldwide attention in the media (Rusch 2001: 10)

It should be seen here that the most known way of accessing these numbers is through Internet hacking- unauthorized breaking into of another’s computer to steal or destroy documents. Another means of acquiring these numbers is by “sorting through trash to find credit card bills or receipts” (Rusch 2001: 10). There is yet another method where by the criminals: Go to websites where others have posted credit card numbers, and even use credit card generator programs such as credit master, credit wizard, and generate batches of potentially valid credit card numbers.

When they confirm the validity of the numbers, they then meet any online merchant and buy what ever they want to buy. They will either give a foreign address or that of an accomplice who is living in the country of the merchant, so that the goods will be shipped. Many of these criminals can be found in America, Europe, Asia and Africa.

In January 2004, Life Way Christian stores provided some tips that every credit card carrier should follow to ensure the security of his/her card, according to Fraud and Scams: Keep an eye on your card during transaction and get it back as quickly as possible. Draw a line through any blank spaces above the total when you sign and never discard transaction slips that display the card number. Ask for the carbon copy when it passes through machine, do not lend your card to any body and make sure you destroy any out-of-date cards. Never leave your card where the details can be copied and avoid leaving your cards or the receipts in your car. Credit card theft is evil. It is for this reason that these researchers are calling for ethics on the Internet and proper monitoring and surveillance by law enforcement agents. To Internet users, it can be reduced by regularly updating firewall, anti-spy ware and anti-virus software.

**Internet Pornography**

“Online pornography appears to be one of the greatest threats to the spirituality of Christian
men” and Christian men must also take protective measures (Vlach 2006: 8). Christian online Magazine in Vlach (2006) argues “online pornography poses a greater threat to Christian men and leaders than ANY other type of pornography in the market” (9) Covington (2006) has seen decency and pornography as a serious “issue if the Internet is to be usable by school children” (5). This is why many organizations in U.S.

Are stepping in to do what government can’t (and shouldn’t): promoting voluntary standards of decency and rating the suitability of Web pages and news groups for children. At least two companies, Cyber Patrol and Surfwatch, presently do this. Teachers and parents can set up their Internet software so that students can only access approved materials (Covington 2006: 5).

The only way of keeping our children from online pornography is “parental vigilance” (Bohlin 2006: 5). Parents should always “know what their children are doing at the computer.” Computers in the home should not be placed at the corner or hidden part of the room but in an open place where everybody will see what every other person sitting on the computer is doing.

In a developing country like Nigeria, where computers are not yet rampant, every parent should be careful of allowing the child to go to the cyber cafe either for day or night browsing without giving him/her a guide who will monitor what the child is browsing, especially, now that almost all examination registrations are online. Children may, in the pretence of looking for materials for their assignments, plunge themselves into pornographic sites. Every Christian parent should therefore endeavor to become computer literate so as not be deceived by their children over Internet porn and other crimes on the net.

The Nigerian government should enforce their laws on Internet crimes and also persuade all Internet Service providers (ISPs) to post a filtering program, which will reside on a remote computer. This is the safest and most effective system, much harder for technically savvy kids and teens to circumvent (Bohlin 2006: 5).

The law on pornography whether offline or online should be enforced. Law enforcement agencies should be visiting the cyber cafes from time to time to catch offenders whether kids or adults and to close down such cafes that allowed their equipments to be used in committing crime.

**Conclusion and Recommendations**

In conclusion therefore we can say that the Internet is a veritable tool for good and for bad uses. This is why ethics should be introduced among Internet Service Providers and users. We therefore recommend as follows:

The Christian churches in Nigeria should rise to the challenge of fighting this great monster that is about to leak up world economy. This they will do by maintaining a site online where gospel messages and teachings shall be posted that tackles crimes and other vices. The churches should also train their members on how to use computers and how to pluck vulnerabilities in programs on which hackers and crackers capitalize to commit wickedness against our economy. Furthermore, the church should speak vocally and persistently on the need to introduce ethics to the Internet as a measure to stem the tide of crime.

At the International level, the fight against Internet crime is global in nature; therefore let us join the Church of Scientology International, The Computer Ethics Institute (CEI), and the National Computer Ethics & Responsibilities Campaigns (NCERC) to raise awareness on standards for conduct among Internet Service Providers (ISPs) and users. There should be an international cooperation among nations of the world on how to develop a collaborative best practice and a common approach to combating computer-related crime. Self-regulatory bodies among Internet Service Providers (ISPs) should be established with the aim of improving the detection and prosecution of computer related crimes (Ascroft 2006: 1).

1. That the government of Nigeria should re-equip EFCC, Nigerian Police and other
related agencies with high-tech knowledge to fight Internet abuses.

2. The cyber space is such a disembodied system that can lure anybody into evil if one is not careful. These rules should therefore be applied to anyone online at anytime:
   - Guard your online relationship
   - Be careful to visit websites that do not compromise your ethical and moral life.
   - Take care that every written communication on the Internet reflect your moral and ethical principle of life; and
   - Guard your time to be sure your online is kept in proper balance with the rest of your life.

3. Furthermore, the government should encourage Internet Service Providers (ISPs) to establish a pledge of self-regulatory body to tackle these abuses and crimes online. These Internet Providers and cyber cafes should post a filtering technology in their servers in order to monitor what users are doing indirectly. Again cyber cafes should report fraudsters who use their systems for scam so that stiff penalties could be meted on them.

4. The government, the public-spirited people and the religious bodies should pursue public awareness and education through media vigorously.

5. There are new ways to committing crimes, which the Internet has brought; therefore, there should be legislation to cover those areas. Every state government in Nigeria should establish a legislation to tackle Internet crimes and various abuses online.

The household is the veritable microcosm of the city. It is the primary school of morality and all forms of exchange that constitute friendships and all the relationships of power, protection, submission, honor and duty that must be properly turned if a city is to flourish, exist in the household. Therefore, the parents should supervise and monitor their children in their use of the Internet. The time to see Internet as part of the society, which must be ethically regulated either directly or indirectly, is now. If these recommendations are adhered to Internet abuses shall be minimized.

References


