HACKING AND CYBER SECURITY IN NIGERIA TELECOMMUNICATION INDUSTRY: IMPLICATION FOR TEACHING AND LEARNING

Bartholomew Uchenna Arum*

Abstract

Over the years, the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Therefore, this paper focuses on the prominent cybercrimes carried out in the various sectors in Nigeria and presents a brief analysis of cybercrimes in the country. In conclusion, detection and prevention techniques are highlighted in order to combat hacking and cybercrimes in Nigeria. Cyber security is the guard of cyberspace and other associated technologies, from records and electronic data to the physical structures and security systems. Cyber security in Nigeria is a vital aspect of protecting/guarding the organizations and businesses in the country. It is imperative for every small, medium and large scale businesses organization in the country to strengthen their cyber security. Cyber security is of rising significance. The importance of cyber security is as a result of the increasing dependence on computer systems and the Internet, wireless networks like Bluetooth and Wi-Fi, and the development of "smart" devices, as part of the Internet of Things. In summary this paper, however, looks at the cyber security, its challenges in the country and it also made several recommendations on the way forward such as the need for the ethical hackers, education on the ethics of using the internet and enacting laws to guard against various types of cyber and internet-related crimes.

Keywords: Cyber Security, Harking, Nigeria, Teaching, Learning, Ethics

Introduction

Cyber security through ethical hacking plays an important role in the ongoing development of telecommunication industry, as well as Internet services (Odinma, 2010). Enhancing cyber security and protecting critical information infrastructures are essential to each nation’s security and economic well-being (Odinma, 2010). Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit (Okonigene & Adekanle, 2009).

Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security (Laura, 1995). The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems (Laura, 1995). It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures (Adebusuyi, 2008). At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.

The exceptional outbreak of cyber-crime in Nigeria telecommunication industry in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing. Over the past fifteen years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security (Oliver, 2010). This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users.

The first recorded cyber murder was committed in the United States of America seven years ago. According to the Indian Express in January 2002, when an underworld guru in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the

hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient. Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006. Prior to the year 2001 of the emergence of MTN in Nigeria, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet since that time. Right from then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Telecommunication facilities. Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks (Adebusuyi, 2008). The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters. This paper seeks to give an overview of ethical hacking and cyber-security in Nigerian telecommunication industry, outline some challenges and proffer solutions.

In 2014, the National Assembly of Nigeria made a bold move in the war against cybercrime when the Senate passed the Cybercrime Bill. This feat in addition to the cyber security strategy and policy documents introduced by the Office of the National Security Adviser (NSA) of the Nigeria government are attributes that will strengthen cyber security.

The "Internet"

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad set of computer memory units, arranged in lines across electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

Most traditional communications media including telephone, music, film, and television are reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP). Newspaper, book and other print publishing are adapting to Web site technology, or are reshaped into blogging and web feeds. The Internet has enabled or accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial services on the Internet affect supply chains across entire industries.

To Hack
This is to use a computer or other technological device or system in order to gain unauthorized access to data held by another person or organization.

Who is a Hacker?
This is someone who secretly uses or changes the information in other people's computer systems. *Hacker* also means someone who, beyond mere programming, likes to take apart operating systems and programs to see what makes them tick.

Hacker in computer science is originally, a person totally engrossed in computer programming and computer technology. In the 1980s, with the advent of personal computers and dial-up computer networks, *hacker* acquired a pejorative connotation, often referring to someone who secretively invades others' computers, inspecting or tampering with the programs or data stored on them.

Hacking
Hacking is the unauthorized access into a computer or network resources. The number of really gifted hackers in the world is very small, but there are lots of persons who tries to look or behave like someone famous or like a particular type of successful person, because they want to be like them etc. When we do an ethical hack, we could be holding the keys to that company once we gain access. It's too great a risk for our customers to be put in a compromising position. With access to so many systems and so much information, the temptation for a former hacker could be too great - like a kid in an unattended candy store.

Hacking - Early History
During the 1960s, the word "hacker" grew to prominence describing a person with strong computer skills, an extensive understanding of how computer programs worked, and a driving curiosity about computer systems. Hacking, however, soon became nearly synonymous with illegal activity. While the first incidents of hacking dealt with breaking into phone systems, hackers also began diving into computer systems as technology advanced.

Hacking became increasingly problematic during the 1980s. As a result, the Computer Fraud and Abuse Act were created, imposing more severe punishments for those caught abusing computer systems. In the early 1980s, the Federal Bureau of Investigation (FBI) made one of its first arrests related to hacking. A group known as the 414s was accused of breaking into 60 different computer systems. Later that decade, the infamous Kevin Mitnick was arrested and sentenced to one year in jail for damaging computers and stealing software. He was arrested again in 1995 for computer fraud and put in jail for hacking Motorola Inc., Sun Microsystems Inc., NEC Corp., and Novell Inc. to steal software, product plans, and data.

As negative publicity surrounding hackers continued to grow, those who considered themselves true hackers-computer programming enthusiasts who

pushed computer systems to their limits without malicious intent and followed a hacker code of ethics-grew weary of the media's depiction of hackers. As a result, several hacker groups coined the term 'cracker' in 1985 to define a person who broke into computer systems and ignored hacker ethics; however, the media continued to use the word hacker despite the fact that although most early hackers believed technical information should be freely available to any person, they abided by a code of ethics that looked down upon destroying, moving, or altering information in a way could cause injury or expense.

Types of Hacking

1. Inside Jobs - Most security breeches originate inside the network that is under attack. Inside jobs include stealing passwords (which hackers then use or sell), performing industrial espionage, causing harm, or committing simple misuse. Sound policy enforcement and observant employees who guard their passwords and PCs can thwart many of these security breeches.

2. Rogue Access Points - Rogue access points (APs) are unsecured wireless access points that outsiders can easily breech. (Local hackers often advertise rogue Access Points to each other.) Rogue Access Points are most often connected by well-meaning but ignorant employees.

3. Back Doors - Hackers can gain access to a network by exploiting back doors' administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups. With the aid of computerized searchers, hackers can probably find any weakness in your network.

4. Viruses and Worms - Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms attempt to shut down networks by flooding them with massive amounts of bogus traffic, usually through e-mail.

5. Trojan Horses - Trojan horses, which are attached to other programs, are the leading cause of all break-ins. When a user downloads and activates a Trojan horse, the hacked software kicks off a virus, password gobbler, or remote-control that gives the hacker control of the PC.

6. Denial of Service – Denial of Service attacks give hackers a way to bring down a network without gaining internal access. Denial of Service attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).

Distributed Denial of Services (DDoS) are coordinated Denial of Service attacks from multiple sources. A Distributed Denial of Services is more difficult to block because it uses multiple, changing, source IP addresses.

7. Anarchists, Crackers, and Kiddies - Who are these people, and why are they attacking your network?

Anarchists are people who just like to break stuff. They usually exploit any target of opportunity.

Crackers are hobbyists or professionals who break passwords and develop Trojan horses or other hacker software. They either use the hacker software themselves

(for bragging rights) or sell it for profit. Other attackers include disgruntled employees, terrorists, political operatives, or anyone else who feels slighted, exploited, ripped off, or unloved.

8. Sniffing and Spoofing - Sniffing refers to the act of intercepting Transmission/Transfer control protocol packets. This interception can happen through simple eavesdropping or something more sinister.

9. Phishing - This is another type of key logging, here you have to bring the user to a webpage created by you resembling the legitimate one and get him to enter his password, to get the same in your mail box.

10. Fake Messengers - it's a form of phishing in the application format. Getting user, to enter the login info in the software and check your mail!

Telecommunication: The Understanding Towards Crime.

Telecommunications are devices and systems that transmit electronic or optical signals across long distances. Telecommunications enables people around the world to contact one another, to access information instantly, and to communicate from remote areas. Telecommunications usually involves a sender of information and one or more recipients linked by a technology, such as a telephone system, that transmits information from one place to another. Telecommunications enables people to send and receive personal messages across town, between countries, and to and from outer space. It also provides the key medium for delivering news, data, information, and entertainment.

Telecommunications devices convert different types of information, such as sound and video, into electronic or optical signals. Electronic signals typically travel along a medium such as copper wire or are carried over the air as radio waves. Optical signals usually travel along a medium such as strands of glass fibers. When a signal reaches its destination, the device on the receiving end converts the signal back into an understandable message, such as sound over a telephone, moving images on a television, or words and pictures on a computer screen.

Telecommunications messages can be sent in a variety of ways and by a wide range of devices. The messages can be sent from one sender to a single receiver (point-to-point) or from one sender to many receivers (point-to-multipoint). Personal communications, such as a telephone conversation between two people or a facsimile (fax) message, usually involve point-to-point transmission. Point-to-multipoint telecommunications, often called broadcasts, provide the basis for commercial radio and television programming.

Telecommunication Sector in Nigeria

The Nigerian telecommunication sector is the largest segment of the Information and Communication sector. Nigeria has one of the largest telecom markets in Africa. The Nigerian Telecommunication sector has evolved over the years to an oligopolistic market structure (a small number of firms have the majority of market share). The sector includes a strong multinational presence. The leading players are MTN, a South African based multinational company with a market share of

37.21%, Airtel (an Indian based multinational telecommunication), Glo (a Nigerian multinational company) and 9mobile (formerly Etisalat).

The sector over the years has contributed immensely to Nigeria's economy and the lives of Nigerians. The advancement of mobile phone usage from basic phone telephony to new enhanced services and the introduction of new technology within diverse sectors of the country have seen the sector grow massively. The sector has experienced rapid growth and helps in e.g. easier banking services (bank mobile apps) and access to e-learning platforms to Nigerians.

The Challenges of Cyber Security in Nigeria

According to the United Nations Economic Commission for Africa (2014), Africa is going through numerous Internet-related challenges with concerning security risk, intellectual property breach and security of personal data. Nigeria as a country is not an exception. Cybercriminals aim at people within and outside their national borders, and various African governments do not have the technical and the financial capability to mark and supervise electronic communications believed to be sensitive for national security.

Challenges of Cyber Security include:

- Lesser security availability adequate to avert and manage technological and informational threat.

- Deficiency of technical know-how regarding cyber security and failure to watch or monitor and secure national networks, making Nigeria and several African countries susceptible to cyber espionage, and incidences of cyber terrorism.

- Failure to develop and improve the required cyber security legal structure to battle cybercrime.

- Cyber security issues are extensive in scope than national security concerns. However, little major significant cyber security measures in Nigeria and even in Africa have its implementation done. Cyber security is a serious concern that needs absolute tackling.

- There is also a necessity to develop an information society that respects values, rights, and freedoms and assures same access to information, even as stirring up the establishment of genuine knowledge that can put up assurance and confidence in the use of ICTs in Nigeria.

- Limited levels of consciousness of ICT-related security concerns by stakeholders, like ICT regulators, law enforcement agencies, the judiciary,

information technology professionals and users. (United Nations Economic Commission for Africa, 2014)

As it Concerns Teaching and Learning

The practice of hacking has become a widespread issue in the world today. Hackers can be anyone from a curious middle school student to a malicious criminal. They hack for a variety of reasons from testing their computer skills to committing fraudulent and harmful acts. It is important for individuals and corporations to protect themselves, their personal information, and their computers from hackers. In recent years, the practice of "ethical" hacking has received much attention. Many corporations are proponents of teaching employees how hackers think and work in an effort to determine whether a network has been hacked as well as to determine potential weakness and prevent future hacking. Consulting firms exist whose purpose is to instruct information technology professionals in the practices of ethical hacking, however these services tend to be rather costly. Proponents of ethical hacking have also introduced the concept of teaching university level future information technology professionals how to hack as well as the legal and ethical implications of such practices.

Teaching-Learning Implication

Teaching is systematic presentation of facts, ideas, skills, and techniques to students. Although human beings have survived and evolved as a species partly because of a capacity to share knowledge, teaching as a profession did not emerge until relatively recently. The societies of the ancient world that made substantial advances in knowledge and government, however, were those in which specially designated people assumed responsibility for educating the young.

Learning is acquiring knowledge or developing the ability to perform new behaviors. It is common to think of learning as something that takes place in school, but much of human learning occurs outside the classroom, and people continue to learn throughout their lives.

At the cause of teaching and learning process the work of ethical hackers must have in one way or the other evolved round the education arena to devour some aspects.

When a student giraffe during examination, it is an introduction to devouring the effort of someone nearby. He does this in other to create confusion during the marking activities, to merit more scores as against that he should have gotten. He can target someone textbooks or notebook and disappeared to tin air thereby putting confusion and anxiety in the owner while his tension increases and sometimes get heart failure.

In the university arena for instance, plagiarism has crippled some person's effort in the field of research and academics.

Plagiarism

Plagiarism is the Process of Copying another Person's Idea or Written Work and Claiming It As original. This is hacking in the education sector where someone's effort is coined to use without his consent thereby silencing ones effort, ideas and articulations. Piracy and plagiarism is synonymous to hacking and cybercrime all together.

Paper/Document Forgery in Institutions

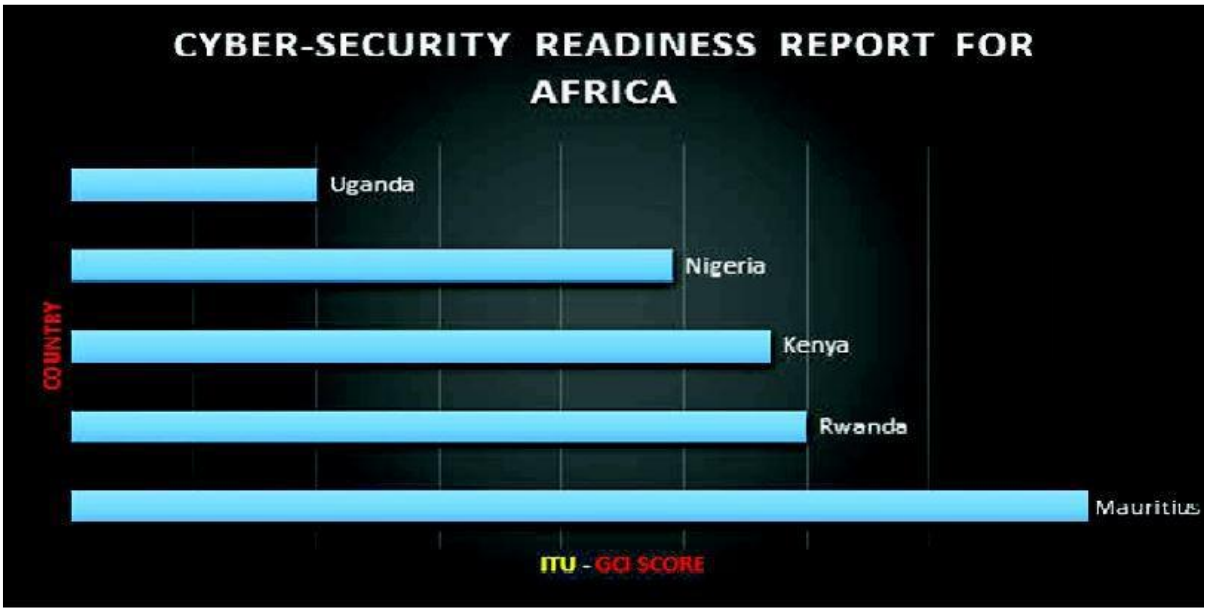
Some of our students nowadays, have many crimes they commit in the institution that can be likened to the system of ethical hackers and cybercrime. The system of replicating the schools receipt, result sheets, question paper and others are solely not left on the line up of the hacking process in the education system.

Tackling Cyber Security Challenges in Nigeria

According to Ibikunle (2013), Cyber security has grown to become a national issue as risk about it now requires to be taken more seriously. The big question is "How ready is Nigeria to tackle the challenges of cyber securities and fight cybercrime. The diagram below shows cyber security readiness report for Africa. One of the most critical ways of tackling the challenges of cyber security and ensuring adequate cyber security is through ethical hacking. Cyber security via ethical hacking plays a significant part in the development of telecommunication industry, and Internet services (Odinma, 2010).

Improving cyber security and guarding vital information infrastructures are essential to national security and economic well-being (Odinma, 2010). An ethical hacker is a networking expert who systematically tries to break in a computer system or telecommunication network on behalf of its owners to find security vulnerabilities that a malicious hacker could exploit (Okonigene & Adekanle, 2009). Hackers use the same techniques to analyze and evade a system's defenses as their less-principled counterparts, but instead of taking advantage of any vulnerability discovered, they take note of them and present a recommendation on how to fix them so the organization can improve its security (Laura, 1995). Therefore, raising and training ethical hackers will provide a level of safety measures in the cyberspace.

Tackling the challenges of cyber security in Nigeria requires education to train IT and internet specialists, the creation of forums and program for the youths to acquaint them with the ethics of using the internet and also others measures of ensuring cyber security and tackling its challenges in Nigeria include; the use of Address Verification System (AVS), Interactive Voice Response (IVR), IP Address tracking, the use of antivirus, anti-spyware software, use of firewall and intrusion detection systems and cryptography. (Ibikunle, 2013)



Effects of Cyber Crime

- Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
- Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
- Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
- Vulnerability of their Information and Communication Technology (ICT) systems and networks.

Solutions to Cybercrime using Cyber security

- **Education:** Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

- **Establishment of IT Programs Forums for Nigerian Youths:** Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could

come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

- **Address Verification System:** Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed.

- **Interactive Voice Response (IVR) Terminals:** This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.

- **Internet Protocol Address Tracking:** Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.

- **Use of Video Surveillance Systems:** The problem with this method is that attention has to be paid to human rights issues and legal privileges.

- **Antivirus and Anti spyware Software:** Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.

- **Firewalls**: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.

- **Cryptography**: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient.

Recommendations

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities.

1. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. A combination of sound technical measures tailored to the origin of Spam (i.e. the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is need to create a security-aware culture involving the public, the Internet Service Providers (ISPs), cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. However, Mishandling of enforcement can backfire.

2. To ensure sustainable growth, the sector is in need of reform. Previous changes (e.g. the Nigerian Communications Act 2003) are outdated as they focus on how voice calls are regulated and not on matters that relate to the new technological era. The focus today should cover competition in the sector, the market and other services the telecom sector is linked closely to such as finance, technology and media services. The current government has shown its commitments in creating an enabling environment for the private sector to contribute innovative solutions to allow consumers to benefit from Information Communication Technology (ICT) advancements. This will in turn bring about efficiency and productivity in the telecom sector and eventually enhance economic growth.

3. Although the telecommunication industry has gone through turmoil, it can bounce back from its recent challenges and boost economic growth. With the sixth consecutive decline in year on year inflation and the simultaneous appreciation of the naira, the sector will see a steady growth in its activities. To drive economic growth, it needs to establish new reforms and review existing policies and regulatory actions to monitor the health of the sector. To ensure longterm growth and sustainability there is a need to improve on general business processes/practices to create new revenue streams, recreate existing products, diversify into new areas for which the resources and capabilities are available and establish a minimum market price.

Securing your Password, Two Step Verification and Using Free Antivirus
Guideline for setting secure Password

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be

a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basics

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting **e** to **3**, **L** or **i** to **1**, **o** to **0**. as in "z3r0-10v3"

Hints

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birth date, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birth date.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".

- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell **anyone** your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- Use a secure password manager.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

How would a Potential Hacker get hold of my Password Anyway?

There are four main techniques hackers can use to get hold of your password:

1. **Steal it.** That means looking over your should when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.

2. **Guess it.** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.

3. **A brute force attack.** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.

4. **A dictionary attack.** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Conclusion

In an organization, to accomplish an effective Cyber Security approach, the peoples, processes, computers, networks and technology of an organization either big or small should be equally responsible. If all components will complement each other then, it is very much possible to stand against the tough cyber threat and attacks.

Bartholomew Uchenna Arum, MSc, PDE, HND
Spiritan International School of Theology,
Attakwu, Enugu State, Nigeria
Email: uchenna.bartholomew84@gmail.com

References

Adebusuyi, A. (2008): The Internet and emergence of Yahooboys sub-culture in Nigeria, *International Journal of Cyber-Criminology*, 0794-2891, December

Cyberpedia (2017). What Is Cyber security? Downloaded on 20 September 2017, from https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security.

Ibikunle, F. (2013). *Approach to cyber security issues in Nigeria: Challenges and solution*. International Journal of Cognitive Research in Science, Engineering, and Education.

Laura, A. (1995). *Cyber Crime and National Security: The Role of the Penal and Procedural Law. Downloaded on 21 October 2017, from* http://nials-nigeria.org/pub/lauraani.pdf.

Laura, A. (1995): Cyber Crime and National Security: The Role of the Penal and Procedural Law", Research fellow, Nigeria Institute of Advanced legal Studies, Retrieved from http://nials-nigeria.org/pub/lauraani.pdf

Okonigene, R. E., Adekunle, B. (2009): Cybercrime in Nigeria, Business intelligence Journal, Retrieved from http://www.saycocorporativeo.com/saycoUk/BIJ/journal/Vol3No1/Article7.pdf

Odimma, Augustine C. MIEEE (2010): Cybercrime & Cert: issues & Probable policies for Nigeria, DBI Presentation, Nov. 1-2.

Oliver, E.O.(2010): Being Lecture Delivered at DBI/George Mason Univeristy conference on Cyber security holding, Department of Information Management Technology, Federal Univerity of Technology, Owerri, Nov. 1-2