

## **Cyber Crimes in e-Registration**

**By**

**Prof. 'Dibu Ojerinde and Dr. Thomas N. Kolo  
Joint Admissions and Matriculation Board (JAMB), Abuja, Nigeria.**

*Being a paper presented at the 27<sup>th</sup> Annual conference of the Association for Education Assessment in Africa (AEAA), Yaoundé Cameroon from 24<sup>th</sup> – 28<sup>th</sup> August, 2009*

# Cyber Crimes in e-Registration

By

**Prof. 'Dibu Ojerinde and Dr. Thomas N. Kolo  
Joint Admissions and Matriculation Board (JAMB), Abuja, Nigeria.**

## Abstract

*Cyber Crimes during e-Registration of candidates have been on the increase despite control measures put in place in the system. These have been a source of concern to the examination bodies in Nigeria. Cyber crimes and other illegal activities by these cyber fraudsters have perverted the administration of some examinations. The criminal activities also, have caused untold hardships to candidates and parents who fall victims to their tricks. To reduce these hardships, some examination bodies spend a lot of money acquiring gadgets and devices aimed at thwarting their efforts. This paper therefore, attempts to discuss the various types of cyber crimes, their implications and some measures that could be adopted to reduce them.*

## 1.0 Introduction

The introduction of e-Registration in Nigeria is a welcome development. Prior to the introduction of the e-Registration, the Board's application forms were processed manually except for the Optical Mark Reader (OMR) forms, which were used for capturing the registration information of candidates. Application documents were physically brought from the various offices of the Board and some designated banks for processing. This processing method which involves collation, editing, scanning, storage, etc. was manual, cumbersome and time consuming.

In an attempt to log on to the Internet and make its operations easy, more effective and more accessible, the Joint Admissions and Matriculation Board (JAMB) introduced the e-Registration. This is an electronic method of registration of candidates online using the Internet facility. Since the introduction of online result checker by National Examination Council (NECO) in 2002, virtually all other examination bodies have adopted the use of online facility for registration of candidates. This online registration of candidates involves the use of scratch cards containing a PIN number and a serial number that enables a candidate carry out his/her registration interactively on a registered website.

It is a general observation that most schools in African countries do not have access to Internet facilities especially for those schools situated in rural areas. These schools, therefore, depend on accredited agencies or Internet Service Providers (ISPs) to carry out e-Registration for them. However, some of the schools make use of cyber cafés for the registration of their students. During this e-Registration, some cyber crimes are committed. This paper attempts to discuss various cyber crimes perpetrated by cyber fraudsters and suggests some measures that could be adopted to reduce them.

## **2.0 What is e- Registration?**

e-Registration can be defined as an electronic way of processing application forms using Internet technology. It is a service carried out interactively by the use of computers using the Internet facility. It is an operational and functional service on demand anytime and anywhere (Ojerinde, 2008). e-Registration can be seen as a service that is available for immediate correspondence. Online services provide an infrastructure in which subscribers can communicate with one another by participating in online conferences, e-mail messages or registration for examination, etc interactively on a dedicated site (Webopedia, 2008).

## **3.0 What is Cyber Crime?**

According to Pati (2008), cyber crime, e-crime, hi-tech crime or electronic crime generally refers to a criminal activity where a computer or network is the source, target or place of crime. Although, the term cyber crime is more or less used to describe criminal activities in which the computer or network is a necessary part of the crime, the term can also be used for traditional crimes such as fraud, theft, forgery and blackmail in which computers or network are involved. Therefore, a cyber-crime is said to be committed if the criminal activity involves an information technology infrastructure, including illegal access, illegal interception, data interference and electronic fraud. It is the latest and perhaps the most complicated problem in the cyber world.

Adamski (1998), Jaishankar (2007) and Jewkes (2006) defined cyber crime as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. This web page includes resources related to cyber stalking, electronic crime, high-tech crime, internet crime, etc.

#### **4.0 Problems Associated with Manual Services**

In the past, the Board adopted the use of OMR forms for registration of candidates which was partly manual and partly electronic. In addition, many staff were employed to process other application documents as well as to transcribe the substitute answer sheets into scannable OMR answer sheets. The following problems were encountered as listed by Ojerinde (2008).

- i. Theft and re-sale of completed OMR forms.
- ii. Mutilation of OMR forms.
- iii. Wrong coding of OMR registration forms by candidates.
- iv. Loss of completed OMR forms.
- v. Late submission/retrieval of completed application documents.
- vi. Long period of processing application documents.
- vii. No registration details or incomplete information.
- viii. Loss of candidates' examination notices (i.e. photocard, JAMB receipts, etc.).
- ix. Creation of special/stand-by/checking centers to accommodate late registration.
- x. Large space for storage of registration documents.
- xi. Difficulty in storage and retrieval of application documents.
- xii. Undue pressure on data entry operators with attendant human errors.
- xiii. Errors committed during the transcription of mutilated OMR forms and substitute answer sheets to new OMR forms.
- xiv. Late receipt of result slips and admission letters through postal agency.

#### **5.0 Advantages of e-Registration**

The following advantages have been achieved by the Board through e-Registration and other online services.

- (i) There is equity in treatment and access for all candidates irrespective of ethnicity, physical or mental disability, religion, culture, gender, social or economic background, etc.
- (ii) It enables candidates to register easily within and outside their home environment. This reduces unnecessary expenses and risks of travelling long distances.
- (iii) It allows candidates the freedom to edit or modify any registration information.

- (iv) It enables candidates to print-out registration slips, examination notices, result slips and admission letters by themselves without recourse to the Board for any assistance.
- (v) Brochures containing information for the completion of e-Registration can easily be downloaded from the net.
- (vi) The problem of “no registration details” or incomplete registration information is eliminated.

## **6.0 Problems of e-Registration**

Despite the advantages of e-Registration, it also has its problems. Some of the problems are enumerated below.

- (i) Dependence on cyber café operators by some candidates for e-Registration and result checking.
- (ii) Insufficient and/or lack of knowledge of some candidates on web-surfing.
- (iii) Unavailability of Internet facilities at the rural areas.
- (iv) Erratic power supply.
- (v) Narrow bandwidth provided by the Internet Service Providers (ISPs) on their communication channels.
- (vi) Denial of service and time theft as a result of network problem from the Internet.
- (vii) Provision of fake e-slips by cyber cafés.

## **7.0 Other Online Services Provided By the Board**

The introduction of online services by the Board commenced with the Monotechnics, Polytechnics and Colleges of Education Matriculation Examination (MPCEME) online checking of candidates’ examination centres in 2002. Thereafter, the online registration of candidates commenced in 2006 with the MPCEME. The other online services rendered by the Board include the following.

- (i) Online result checker.
- (ii) Change of courses and institutions.
- (iii) Printing of Result slips.
- (iv) Printing of Admission letters.
- (v) JAMB website for enquiries, etc.

## **8.0 Types of Cyber Crimes**

Generally, computer crimes may be classified into two categories. The crimes that target computer networks or devices directly and crimes facilitated by computer networks or devices. Some of the crimes committed by cyber café fraudsters include the following.

### **8.1 Fake e-Registration slips**

Some ignorant candidates are shortchanged by being issued with fake e-registration slips instead of using valid JAMB scratch cards to register them. The perpetrators of this crime usually modify the details of an existing candidates' information and allocate examination numbers to the affected applicants. Most often, two or more candidates come to the examination centre with e-registration slips having the same examination number and registration number with different names. The implication of this is that the candidate with fake e-registration slip will not be allowed to sit for the examination since he/she was not a registered candidate.

### **8.2 Phony result slips**

Some cyber cheats indulge in the act of issuing candidates with manipulated result slips similar to the one produced by the Board. Some have even perfected the slips by including the JAMB logo which is used as the water marks on the background of the result slips. They are so neatly done that it is difficult to distinguish the real from the phony one. However, these forged results do not have any registration details or scores/data information in the Board's website and computer.

### **8.3 Result slips with enhanced scores**

What cyber fraudsters do is to reproduce result slips which are similar to that of the Board but with enhanced scores. These are issued to desperate candidates who want to gain admission into tertiary institutions by all means. These illegal result slips are so

neatly done, that it is difficult to distinguish them from the original. Despite the similarity, the Board still identifies the fake ones. The implication of this is that those with these illegal result slips would not be admitted into any tertiary institution. Even if admitted, when discovered, they are rusticated from the institution.

#### **8.4 Computer intrusion or “hacking”**

Computer Intrusion or “hacking” is like opening the door of a computer without ‘knocking’ i.e. accessing information without authorization. The aim of intrusion could be for money, fun or curiosity. These cases of computer intrusions result in the spread of malicious code or viruses. When some particular candidates discover that they did not perform well in the examination or have attempted the examination without success, they could connive to harm the system. The implication is that if the examination body does not have a good firewall to prevent intrusion, unimaginable danger could be done to their systems and the affected examination body could be in serious predicament.

#### **8.5 Remote access to systems**

Wireless short-range communication devices exist which facilitate data transmission over short distances from fixed and/or mobile devices. They provide ways to connect and exchange information between devices such as mobile phones, laptops, personal computers, printers, etc. When operational, the devices establish communication and control between the host computers and the remote ones on which file exchange is desired. The facilities enable a remote user have access to information from another computer system or hardware. The effect of this is that any device within the communication range could break into the established signals if the link is not adequately secured.

#### **8.6 E-mail bombing/spoofing**

This act is committed when large numbers of e-mail messages are sent to the victims’ e-mail boxes. A spoofed e-mail is one which misrepresents its origin. This causes crashing of the system.

#### **8.7 Virus/worm attack**

These are programs that tend to attach themselves to a computer file, replicate to other files and to other computers in a network. It works by altering the data in a file or deleting it. Worms do not need a host to get attached to. They merely replicate themselves and continue until they eat up all the available spaces on a computer memory. The world’s most famous worm was the Internet worm let loose on the

Internet by Robert Morris in 1988, which almost brought the development of the Internet to a halt.

### **8.8 Logic bomb**

Some computer programs are made to be dependent on certain events. Example is the Jerusalem 13, which compels computer systems affected by it to be activated on 13<sup>th</sup> December only. Some programs contain viruses termed logic bombs that lie dormant all through the year and becomes active only on a particular date such as *Chernobyl Virus*.

### **8.9 Internet time theft**

When the Internet surfing hours of a victim is used up by another person, we call that Internet time theft. This action is facilitated by logging in using a person's User Identification Code and password. There was a reported case of Internet time theft in India which made the police infamous due to lack of understanding of the nature of cyber crime.

### **8.10 Web jacking**

This term was derived from the word 'hijack'. This involves the hacker gaining access and control over the website of another. Information on the site is either mutilated or changed. In recent event, the Ministry of Information in Bombay, India was hijacked by a Pakistani hacker with some obscene matter placed inside the site. In some cases, a ransom of money is demanded to release control of the site. In Nigeria, websites of some banks and telecommunication companies have been recently jacked by some unidentified swindlers.

### **8.11 Cyber terrorism**

Cyber terrorism may be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker, 1983). A cyber terrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objective by launching computer-based attack against computers, network and information stored on them. Propaganda placed on the Internet that there will be bomb attack during a certain period can be considered as cyber terrorism. A cyber terrorist may use the internet or computer facility to carry out an actual attack. Cyber crime is different from cyber terrorism in the sense that while cyber crime is a domestic problem, cyber terrorism is a global one.

## **9.0 Reducing Cyber Crimes**

In order to reduce the activities of cyber fraudsters on e-Registration, the following measures are suggested.

### **9.1 Registration of cyber café operators**

All cyber café operators in the country should be registered under a regulatory body. This is to ensure that they comply with the acceptable standards in the process of providing services to the candidates. Unregistered cyber cafés and the erring registered ones should be sanctioned and blacklisted appropriately.

### **9.2 Periodic inspection**

The regulatory body should carry out periodic inspection of cyber café sites. This is to ensure proper supervision and monitoring of their activities. The monitoring report should be made public to guide parents and candidates in their choice of cafés to use during e-Registration.

### **9.3 Training of staff on e-Registration**

There is need for formal training of staff of examination bodies and secondary school examination officers on e-Registration processes. This would equip them with the functionality of the system and thereby be placed in a position to sensitize the public and candidates on proper utilization of the electronic devices and the Internet for e-Registration.

### **9.4 Enacting of cyber laws**

Cyber laws aimed at e-Examination should be enacted to regulate cyber crimes and to prosecute cyber criminals. Recent incidents have shown that cases of cyber stalking, cyber harassment, cyber nuisance and cyber defamation which are offences or crimes against individuals, organizations and humanity now exist.

### **9.5 Installing and updating computers with up-to-date Internet security**

In order to guide against intrusion or hacking of computers and network systems, constant updates of the virus guards and other security measures packages such as anti-phishing and anti-spyware must be put in place to forestall any form of intrusion by hackers. Installation of security cameras at strategic places can further check the activities of fraudsters.

## **9.6 Discouraging the use of pirated software**

Pirated software is one that is not licensed by the user. It is usually a fake product and most of these pirated products are embedded with viruses. The use of these products should be discouraged because cyber criminals take advantage of these lacunas to penetrate into their victims' computers.

## **9.7 Internet subscribers' databank**

Information about every prospective Internet subscriber should be obtained (in addition to passport photograph) by Internet Service Providers (ISPs). This could form a readymade source of information for the law enforcement agents.

## **9.8 Data back-up**

Data back-up is necessary to prevent hacking. This is done by sending both hard copy and soft copy to Universities, Polytechnics and Colleges of Education.

## **10.0 Conclusion**

It is observed that cyber crimes are mostly committed in the nights. As part of measures to check cyber crimes, night surfing should be discouraged as much as possible. It is advised that internet facilities should be extended to every school so as to equip the students with the knowledge on how to use Internet facilities. This would reduce the over dependence on cyber cafés during e-Registration.

One of the ways of curbing cyber crimes by all intent and purpose is through counseling. As advised by Omoluabi (2008), parents need to monitor their children especially when they spend time out of the home. In addition, there is need for law enforcement agencies to have a tighter control of cyber café operators because they aid and abet criminals. When such cases of cyber crimes are detected, the owners of cyber cafes should be prosecuted.

The school counselors should be mandated to sensitize their students on the dangers of cyber crimes and their attendant consequences.

On the part of government, it should expedite action on the training of more cyber crime busters so as to detect the sources, the modes and the ways through which these fraudsters perpetrate cyber crimes.

## References

1. **Adamski, A. (1998):** "Crimes Related to the Computer Network, Threats and opportunities: A Criminological Perspective," European Institute for Crime Prevention and Control, Website Search, 1998.
2. **Jaishankar, K. (2007):** "Cyber Criminology: Evolving a Novel Discipline with a New Journal," International Journal of Cyber Criminology, Vol.1, Issue I, January, 2007, website Search, 2007.
3. **Jewkes, Y. (2006):** comment on the Book "Cyber crime and society by Yar, M. Sage Publications, Website Search, 2006.
4. **Ojerinde, 'Dibu (2008):** "Online Services On Assessment: To Be Or Not To Be?," A Paper Presented for Academy Yearbook on Educational Measurement and Evaluation, 2008.
5. **Omoluabi, P. (2008):** "Tighter control of Cyber Café Operation Necessary," Newspaper Interview by Omolara Akintoye, The Nigeria Nation Newspaper, p.16, 19<sup>th</sup> October, 2008.
6. **Webopedia Computer Dictionary (2008),** website Search, 2008.
7. **Parker, D (1983):** "Fighting Computer Crime," Charles Scribner's Sons, United States,
8. **Parthasarathi Pati (2008):** 'Cyber Crime,'  
[www.naavi.org/pati/pati\\_cybercrimes\\_dec03.htm](http://www.naavi.org/pati/pati_cybercrimes_dec03.htm) - Cached